



**Mason County PUD No. 1
Regular Board Meeting
September 28, 2021
1:00 p.m.**

Join Zoom Meeting

<https://us02web.zoom.us/j/85869053743>

Meeting ID: 858 6905 3743

1 (253) 215-8782

1:00 p.m. Call to Order & Flag Salute

1) Consent Agenda

Minutes: September 14, 2021 Regular Meeting

Disbursements:	Accounts Payable Wire	\$ 49,922.18
	Check Nos. 120697-120761	\$157,271.86
	A/P Sub-Total	\$ 207,194.04
	Payroll Wire	\$ 61,981.01
	Grand Total	\$ 269,175.05

2) Public Comment- *Members of the public wishing to comment may request permission to do so during the Public Comment portion of the agenda. Comments shall be limited to no more than 5 minutes per speaker. There will be no action or discussion of public comment items, although the board may defer to PUD management for any necessary response.*

3) Business Agenda

- a. Set Public Hearing for Updating Fee Schedule
- b. Claim for damages- Karjo
- c. August Financials
- d. Approval of 2021 PCI Policies
- e. Approval of Policy 609 – Employee Recognition
- f. Approval of Employee Handbook
- g. Award Generator Project to Legacy Power Systems

4) Staff Reports

- a. General Manager
- b. Treasurer
- c. Water Resource Manager
- d. Legal Counsel

5) Correspondence

6) Board Comments

7) Other Business/Public Comment

8) Executive Session - Threatened or pending litigation RCW 42.30.110(i)

9) Adjournment

2021 Calendar

September 30	WPAG - 9:00 a.m.
October 6	PPC
October 8	Customer Appreciation Event, PUD 1 Campus, 11-2
October 12	PUD 1 Budget Workshop- 10:00 a.m. via Zoom
October 14	WPUDA-Virtual Budget Committee
October 21	WPAG- 9:00 a.m.
November 3	PPC (Town Hall with Marty Kanner 4-5:30 p.m.)
November 17	WPAG -1:00 pm
November 17-19	WPUDA-Olympia
December 1-3	WPUDA Annual Meeting



Mason County Public Utility District No. 1

Board of Commissioners Board Meeting
September 14, 2021 Potlatch, Washington

Present:

Mike Sheetz, President (Online)
Jack Janda, Vice President (Online)
Ron Gold, Board Secretary (Online)
Kristin Masteller, General Manager (Online)
Katie Arnold, District Treasurer (Online)
Brandy Milroy, Water Resource Manager (Excused)
Julie Gray, Executive Assistant (Online)
Rob Johnson, Legal Counsel (Excused)

Visitors:

Marcus Perry, BPA

CALL TO ORDER: Mike Sheetz called the meeting to order at 1:00 p.m.

APPROVAL OF CONSENT AGENDA:

Minutes: August 24, 2021 Regular Board Meeting
August 31, 2021 Special Board Meeting

Disbursements:	<u>Accounts Payable Check Register</u>	
	Accounts Payable Wire	\$ 295,420.75
	Check Nos. 120567-120696	\$ 442,593.99
	A/P Sub Total	\$ 738,014.74
	<u>Payroll Expense</u>	
	Payroll Wire	\$ 73,297.85
	Grand Total	\$ 811,312.59

Jack made a motion to approve the consent agenda as presented, Ron seconded the motion. Motion carried.

PUBLIC COMMENT: None.

BUSINESS AGENDA:

Marcus Perry, Bonneville Power Administration – Marcus reported on BPA updates.

Resolution No. 2051 – Adoption of a Life Insurance Plan w/Long Term Care Rider – Jack made a motion to approve Resolution No. 2051 – Adoption of a Life Insurance Plan w/Long Term Care Rider, Ron seconded the motion. Motion carried.

Resolution No. 2052 – Declaration of Surplus Property – Jack made a motion to approve Resolution 2052 – Declaration of Surplus Property, Ron seconded the motion. Motion carried.



Mason County Public Utility District No. 1

Board of Commissioners Board Meeting
September 14, 2021 Potlatch, Washington

Authorize the GM to sign agreement with GDS Associates for Engineering Services – Jack made a motion to authorize the general manager to sign the agreement with GDS Associates for engineering services, pending language change for location of venue and interest rate; Ron seconded the motion. Motion carried.

Authorize the GM to sign agreements with Mason County for ARPA Funds - Jack made a motion to authorize the general manager to sign the agreements with Mason County for ARPA Funds; Ron seconded the motion. Motion carried.

General Manager – Kristin reported that the Vuecrest project has been started. The Agate Beach mainline replacement will be finished by the end of next month. The water crew has been busy finishing up with strategic plan items for 2021. She also reported that on Thursday, September 16th, she, Katie and Mike Oblizalo from Hood Canal Communications will present at the CERB board meeting. Kristin reported that the electric crew was currently working on the WaWa Point rebuild and then will do an underground project in Alderbrook on Vine Maple Court.

Director of Business Services – Katie reported that she is currently working on the 2022 budget. She reported she is also working on FEMA Hazard Mitigation and DOH construction grants for the 2022 year. The first step is identifying projects that would qualify for funding, and then submit the pre-application by the end of November to see if we'll get invited to complete a full application. She stated that the CSR position closes on September 14. She and Kristin will be going through those applications and setting up interviews. She also reported that the water tech position is posted and open until October 8th. The disconnect moratorium ends at the end of September, and Katie stated that she & Kristin are working with staff to develop a plan for how the disconnection process will work.

Correspondence – None

Board Reports –

Mike – None

Jack – Jack reported that he had virtually attended the Energy Northwest meeting last week.

Ron – Ron reported that he had attended the NWPPA Conference last week.

PUBLIC COMMENT - None

EXECUTIVE SESSION – None

Adjournment: 2:07 p.m.

Mike Sheetz, President

Jack Janda, Vice President

Ron Gold, Secretary

09/23/2021 9:44:19 AM

GENERAL LEDGER
TRANSACTION DETAIL

Page: 1

SEP 2021 To SEP 2021

Date	Journal Description	Actv BU Project	Mod	Jrnl Reference Code	
Account: 0 131.2 CASH-GENERAL FUND (DISTRICT)			Department:	0	
09/16/21	61398 Check Print	0	PL	2 PAYROLL	61,981.01

PARAMETERS ENTERED:

Division: All

Accounts: 0 131.2

Department: All

Activity: All

Sort By: Div/Acct

Date Selection: Period

Period: SEP 2021 To SEP 2021

Module: PL

Journal Activity: All

Accounts With No Transactions: Yes

Extended Reference: No

Interface Detail: No

Group by Department: Yes

51217

/pro/rpttemplate/acct/2.51.1/gl/GL_TRANS_DETAIL.xml.rpt

Karnold

09/24/2021 10:30:01 AM

Accounts Payable Check Register

Page 1

09/13/2021 To 09/24/2021

Bank Account: 4 - COLUMBIA BANK - DISTRICT

Check / Tran Date	Pmt Type	Vendor	Vendor Name	Reference	Amount
536 09/16/2021	WIRE	IRS	WEST COAST BANK	FEDERAL TAX LIABILITY	24,387.72
537 09/16/2021	WIRE	WASH 1	WA DEPT OF RETIREMENT SYS	STATE RETIREMENT - PLAN 2	15,598.55
538 09/16/2021	WIRE	WASH 7	WA STATE TREAS-MS: PO-11	DEFERRED COMPENSATION	7,280.75
539 09/16/2021	WIRE	HRA	HRA VEBA TRUST CONTRIBUTI	VEBA MEDICAL SAVINGS	2,655.16
2019 09/23/2021	DD	RWC GROUP	RWC GROUP	TRUCK #46-CREDIT BRAKE SHOES	0.00
120697 09/13/2021	CHK	REEVE SHERWO	REEVE SHERWOOD CONSULTING LLC	JORSTAD CREEK PROJECT	1,215.00
120698 09/13/2021	CHK	2	JULIE DAUM	INACTIVE REFUND	38.15
120699 09/13/2021	CHK	2	LUSNILA ENCISO GOMEZ	INACTIVE REFUND	512.25
120700 09/13/2021	CHK	2	ALBERT FREY	INACTIVE REFUND	4.39
120701 09/13/2021	CHK	2	LONNIE HOLBROOK	INACTIVE REFUND	4.48
120702 09/13/2021	CHK	2	KHOSROW KASHANI SR	INACTIVE REFUND	123.03
120703 09/13/2021	CHK	2	SHIRLEY A PHILLIPS	INACTIVE REFUND	173.72
120704 09/13/2021	CHK	2	JOHANNES M PRINS	INACTIVE REFUND	4.66
120705 09/13/2021	CHK	2	ROGER RICKER	INACTIVE REFUND	4.31
120706 09/13/2021	CHK	2	MARCIA TINAZA	INACTIVE REFUND	549.88
120707 09/14/2021	CHK	WRIGHT	WRIGHT EXPRESS FINANCIAL	MO.MASTERCARD 5569 6200 0003 6811	3,683.51
120708 09/16/2021	CHK	IBEW	IBEW LOCAL UNION #77	UNION DUES	805.96
120709 09/16/2021	CHK	PUDEMP	PUD #1 EMPLOYEE FUND	EMPLOYEE FUND	190.00
120710 09/16/2021	CHK	US TREASURY	US TREASURY	LEVY PROCEEDS #91-1197062	100.00
120711 09/16/2021	CHK	AMERICOOOL	AMERICOOOL HEATING & AIR CONDITI	DUCTLESS HEATPUMP REBATE-DAN/KAREN RAGAN	1,300.00
120712 09/16/2021	CHK	ASPECT CONSU	ASPECT CONSULTING LLC	VIEWCREST WATER WELL ASSESSMENT	3,770.00
120713 09/16/2021	CHK	DAMON CONSU	DAMON CONSULTING SERVICE	HOODSPORT WTAER TANK-UPGRADE POWER SUPPL	597.43
120714 09/16/2021	CHK	DOH	DEPT. OF HEALTH	LAKE ARROWHEAD WATER PROJECT MAIN	382.00
120715 09/16/2021	CHK	GCR TIRES	GCR TIRES & SERVICE	TRUCK#71-NEW TIRES	2,321.11
120716 09/16/2021	CHK	GOLDSTREET	GOLDSTREET DESIGN AGENCY, INC.	WEBSITE FOOTER DESIGN-CUSTOM	5,171.25
120717 09/16/2021	CHK	HDFOWL	HD FOWLER COMPANY	WATER NON INVENTORY	5,279.29

09/24/2021 10:30:01 AM

Accounts Payable Check Register

Page 2

09/13/2021 To 09/24/2021

Bank Account: 4 - COLUMBIA BANK - DISTRICT

Check / Tran Date	Pmt Type	Vendor	Vendor Name	Reference	Amount
120718 09/16/2021	CHK	MAS 10	MASON COUNTY PUBLIC WORKS	HIGHLAND ESTATES MITIGATION PERMIT	128.50
120719 09/16/2021	CHK	MILES	MILES SAND & GRAVEL COMPANY	ORRE NOBLES WATER BUCKSHOT	38.71
120720 09/16/2021	CHK	MOTORS	MOTORS & CONTROLS CORP.	BAY EAST WATER 3 PHASE VOLTAGE MONITOR	129.61
120721 09/16/2021	CHK	NISC	NISC	POSTAGE, ACH E-CHECK, & SONICWALL RENEWA	1,774.58
120722 09/16/2021	CHK	PETTYJOHN ENT	PETTYJOHN ENTERPRISES, LLC	VUECREST WATER PROJECT	4,100.00
120723 09/16/2021	CHK	SPEER	SPEER TAPS, INC.	HOOD CANAL WATER PROJECT	3,450.30
120724 09/16/2021	CHK	SHOP	THE SHOPPER'S WEEKLY	WATER CONSERVATION POSTCARDS & POSTAGE	984.98
120725 09/16/2021	CHK	US BANK	US BANK	2018 ELECTRIC SYSTEM REVENUE ANNUAL FEE	770.00
120726 09/16/2021	CHK	WPUDA	WASHINGTON PUD ASSOC.	FULL CONFERENCE REGISTRATION-KRISTIN	2,119.00
120727 09/16/2021	CHK	2	LARRY CODIGA	DUCTLESS HEAT PUMP REBATE & BPA INCENTIV	1,300.00
120728 09/16/2021	CHK	2	ERIN WILSON	DUCTLESS HEATPUMP REBATE & BPA INCENTIVE	1,300.00
120729 09/23/2021	CHK	ASPECT CONSU	ASPECT CONSULTING LLC	POLE YARD CLEAN-UP	51,209.89
120730 09/23/2021	CHK	BUILDERS	BUILDERS FIRSTSOURCE, INC	VUECREST WATER PROJECT SUPPLIES	21.16
120731 09/23/2021	CHK	CASCA1	CASCADE COLUMBIA DIST.CO.	SODIUM HYPOCHLORITE	520.38
120732 09/23/2021	CHK	CENTURYLINK	CENTURYLINK	LONG DISTANCE & OUTBOAND CHARGES(21)LINE	184.13
120733 09/23/2021	CHK	CNA	CNA SURETY DIRECT BILL	WA HIGHWAY PERMIT	250.00
120734 09/23/2021	CHK	DON SMALL & S	DON SMALL & SONS OIL DIST	DIESEL	3,638.71
120735 09/23/2021	CHK	EVER	EVERGREEN RURAL	QUEST 2.0 PROGRAM-TJ GOOS	1,100.00
120736 09/23/2021	CHK	GCR TIRES	GCR TIRES & SERVICE	TRUCK #71-BALANCE OWING ON INVOICE	6.00
120737 09/23/2021	CHK	GRAY1	GRAY, JOYCE	REIMBURSE FOR WIFI AT HOME (JUNE)	100.34
120738 09/23/2021	CHK	HACH	HACH COMPANY	HOLIDAY BEACH WATER	2,040.00
120739 09/23/2021	CHK	HDFOWL	HD FOWLER COMPANY	VUECREST WATER PROJECT SUPPLIES	758.63
120740 09/23/2021	CHK	ITRON	ITRON, INC.	BALANCE OWING ON INVOICE-SALES TAX	3.40
120741 09/23/2021	CHK	J&I	J & I POWER EQUIPMENT INC	REPAIR TO CHAINSAW	439.30
120742 09/23/2021	CHK	NORTH SAFE	NORTHERN SAFETY CO., INC.	HARD HATS	113.60
120743 09/23/2021	CHK	30	NORTHWEST ROCK, INC	ROCK	611.55

09/24/2021 10:30:01 AM

Accounts Payable Check Register

Page 3

09/13/2021 To 09/24/2021

Bank Account: 4 - COLUMBIA BANK - DISTRICT

Check / Tran Date	Pmt Type	Vendor	Vendor Name	Reference	Amount
120744 09/23/2021	CHK	NWPPA	NWPPA	NORTHWEST INNOVATIONS CONF-KRITIN & KATI	170.00
120745 09/23/2021	CHK	PLATT ELECTRI	PLATT	ELECTRIC NON INVENTORY PARTS	138.07
120746 09/23/2021	CHK	PMI	PMI TRUCK BODIES INC	TRUCK-#77-BOLT ON REMOVABLE VISE STAND	434.50
120747 09/23/2021	CHK	ROHLIN	ROHLINGER ENTERPRISES INC	HYDROLIC CUTTER REPAIR	630.74
120748 09/23/2021	CHK	SHELTON FLOO	SHELTON FLOOR COVERING	CARPET MCREAVY RENTAL HOUSE	4,609.13
120749 09/23/2021	CHK	TECHNIART INC	TECHNIART INC	600 ENERGY EFFICIENCY KITS	16,855.30
120750 09/23/2021	CHK	WPUDA	WASHINGTON PUD ASSOC.	2021 VIRTUAL WATER WORKSHOP-BRANDY	875.00
120751 09/23/2021	CHK	WESCO	WESCO RECEIVABLES CORP.	CT METERS	6,292.99
120752 09/24/2021	CHK	15	MARY BECHTOLT	REIMBURSE FOR WIFI AT HOME (SEPTEMBER)	29.45
120753 09/24/2021	CHK	BKI ENGINEERI	BKI ENGINEERING SERVICES	MINERVA TERRACE WATER SYSTEM PLAN	9,116.84
120754 09/24/2021	CHK	CENTUR	CENTURYLINK	TELEPHONE CHARGES-ACCT#206-Z05-0016 020B	2,135.24
120755 09/24/2021	CHK	DAY	DAY WIRELESS SYSTEMS	RECURRING CHARGES-TWO WAY RADIO 26 UNITS	525.18
120756 09/24/2021	CHK	GRAY	GRAY & OSBORNE, INC	HOOD CANAL CONNECTION ANALYSIS	4,340.66
120757 09/24/2021	CHK	ITRON	ITRON, INC.	ANNUAL HARDWARE & SOFTWARE MAINTENANCE	5,760.94
120758 09/24/2021	CHK	18	TRISH MARTIN	REIMBURSE FOR WIFI AT HOME (SEPTEMBER)	36.95
120759 09/24/2021	CHK	PARSON	PARSONS DIESEL & STEAM	SERVICE VARIOUS VEHICLES	1,717.01
120760 09/24/2021	CHK	VERIZO	VERIZON WIRELESS	ISLAND LAKE MANOR,BEL AIRE, & SHADOWOOD	234.14
120761 09/24/2021	CHK	NAPA AUTO PA	WESTBAY NAPA AUTO PARTS	TRUCK #46-FAN BELT	46.53
Total Payments for Bank Account - 4 :					(70) 207,194.04
Total Voids for Bank Account - 4 :					(0) 0.00
Total for Bank Account - 4 :					(70) 207,194.04
Grand Total for Payments :					(70) 207,194.04
Grand Total for Voids :					(0) 0.00
Grand Total :					(70) 207,194.04

09/24/2021 10:30:01 AM

Accounts Payable Check Register

Page 4

PARAMETERS ENTERED:**Check Date:** 09/13/2021 To 09/24/2021**Bank:** All**Vendor:** All**Check:****Journal:** All**Format:** Summary**Extended Reference:** No**Sort By:** Check/Transaction**Voids:** Current**Payment Type:** All**Group By Payment Type:** No**Minimum Amount:** 0.00**Authorization Listing:** No**Credit Card Charges:** No



PUBLIC UTILITY DISTRICT NO. 1

OF MASON COUNTY

N. 21971 Hwy. 101
Shelton, Washington 98584

BOARD OF COMMISSIONERS

MIKE SHEETZ, Commissioner
JACK JANDA, Commissioner
RON GOLD, Commissioner

STANDARD CLAIM FORM PLEASE TYPE OR PRINT IN INK

Please return to:

General Manager
21971 N. Hwy 101 Shelton, WA 98584

Business Hours: 8:00am - 5:00pm

PERSONAL INFORMATION

1. CLAIMANT'S NAME:

Karjo Aaron
Last Name First Middle

2. RESIDENCE ADDRESS CURRENT ADDRESS:

26947 N. 88th Lane, Peoria, AZ 85383

3. MAILING ADDRESS (IF DIFFERENT):

4. RESIDENTIAL ADDRESS AT TIME OF INCIDENT:

26947 N. 88th Lane, Peoria, AZ 85383

5. CLAIMANT'S DAYTIME TELEPHONE: (623) 523-4140 ()
Home Business

6. CLAIMANT'S E-MAIL ADDRESS dbtransllc@gmail.com

INCIDENT INFORMATION

7. DATE OF INCIDENT: 08 / 04 / 2021
month day year

8. TIME: 1158 A.M. ☒ P.M. (CIRCLE ONE)

9. IF THE INCIDENT OCCURRED OVER A PERIOD OF TIME PLEASE PROVIDED:

BEGINNING TIME: 08 / 04 / 2021
month day year

ENDING TIME: 08 / 04 / 2021
month day year

10. LOCATION OF INCIDENT:

SR NB 101, 30 miles N of Bee Mill RD Mason
Address/Street/Mile Post City County



PUBLIC UTILITY DISTRICT NO. 1
OF MASON COUNTY
N. 21971 Hwy. 101
Shelton, Washington 98584

BOARD OF COMMISSIONERS

MIKE SHEETZ, Commissioner
JACK JANDA, Commissioner
RON GOLD, Commissioner

11. NAMES, ADDRESSES, AND TELEPHONE NUMBERS OF ALL PERSONS INVOLVED, OR WITNESS, TO THIS INCIDENT:

Aaron Karjo 26947 N. 88TH LANE, PEORIA, AZ 85383 623-523-4140

Rocky Bloomfield, 120 DARK RD, BRINNON, WA 98320

Hunter Smith, 1233 MIDDLE FORK RD, ONALASKA, WA 98570

12. NAMES, ADDRESSES, AND TELEPHONE NUMBERS OF ALL DISTRICT EMPLOYEES HAVING KNOWLEDGE ABOUT THIS INCIDENT (ATTACH ADDITIONAL SHEETS, IF NECESSARY):

OFFICER: KATHERINE WEATHERWAX, BADGE#648 WASHINGTON STATE PATROL

PUD EMPLOYEE: MIKE ROSE, 2621 E. JOHNS PRAIRIE RD, SHELTON, WA 98584

13. DISTRICT EMPLOYEE ALLEGEDLY RESPONSIBLE FOR DAMAGES/INJURY: PUD Power Pole

14. DESCRIBE CONDUCT AND CIRCUMSTANCES CAUSING INJURY OR DAMAGES, EXPLAINING EXTENT OF MEDICAL, PHYSICAL, OR MENTAL INJURIES (ATTACH ADDITIONAL SHEETS, IF NECESSARY):

Aaron Karjo was driving northbound on SR 101 near MP302. A utility pole fell onto the northbound lane and onto the Volvo tractor and trailer as Aaron. The power lines also fell over the tractor and trailer. There was no way for Aaron to avoid the pole. The utility pole damaged the right side mirror and hood. Aaron did not sustain any physical injury, however, he does have post traumatic stress from incident.

15. LAW ENFORCEMENT/SECURITY/FIRE/EMERGENCY AGENCIES WHO RESPONDED TO THE INCIDENT (PLEASE INCLUDE REPORT OR CASE NUMBER IF AVAILABLE)

OFFICER: KATHERINE WEATHERWAX, BADGE#648 WASHINGTON STATE PATROL. Police report# EB55613

PUD EMPLOYEE: MIKE ROSE, 2621 E. JOHNS PRAIRIE RD, SHELTON, WA 98584

Fire Department was also on the scene, but Aaron does not recall which unit.

16. NAME, ADDRESS, AND TELEPHONE NUMBER OF TREATING PHYSICIAN(S) AND ATTACH COPIES OF MEDICAL REPORTS AND BILLINGS:

17. PLEASE PROVIDE COPIES OF ANY DOCUMENTS, PICTURES, OR OTHER RECORDS THAT SUPPORT OR RELATE TO YOUR CLAIM. We will need you to provide the year, make and model for each item you claim was damaged such as appliances or vehicles.

2020 VOLVO VNL860 TRACTOR, LICENSE PLATE AL13159, VIN# 4V4NC9EJ6LN228874



PUBLIC UTILITY DISTRICT NO. 1
OF MASON COUNTY
N. 21971 Hwy. 101
Shelton, Washington 98584

BOARD OF COMMISSIONERS

MIKE SHEETZ, Commissioner
JACK JANDA, Commissioner
RON GOLD, Commissioner

18. I / WE DO HEREBY CLAIM DAMAGES FROM 08/04/2021 IN THE SUM OF \$ 6900.89.

This claim form must be signed either:

- (i) By the claimant, verifying the claim;
- (ii) Pursuant to a written power of attorney, by the attorney in fact for the claimant;
- (iii) By an attorney admitted to practice in Washington state on the claimant's behalf; or
- (iv) By a court-approved guardian or guardian ad litem on behalf of the claimant.

I certify or declare under penalty of perjury under the laws of the State of Washington that the foregoing is true and correct.

A handwritten signature in cursive script, appearing to read 'Aaron Karpis', written over a horizontal line.

Signature of Claimant

9/9/2021

Date

How your claim will be processed:

1. Claimant submits claim and supporting material to the General Manager.
2. GM conducts an internal investigation to gather facts and review claim with senior staff team.
3. PUD attorney reviews claim and makes recommendation to either approve or deny the claim, or to send it to the PUD's insurance carrier for independent investigation and review.
4. After the investigation is completed, the claim is presented at following Board of Commissioners meeting for approval/denial if it does not need to be sent to the insurance carrier.
5. If the claim is denied, a letter is sent to the claimant explaining why it was denied.
6. If the claim is not initially denied by the Board of Commissioners, it will be sent to the PUD's insurance carrier for processing.
7. If the claim is approved, payment unless the amount is minimal, in which case it may be processed in the PUD's next accounting cycle.

No claims shall be considered without completion of the standard tort claim form and supporting documentation. No claims shall be presented to the Board of Commissioners without going through the investigation process, internal review and review by the PUD's attorney.



STATE OF WASHINGTON
POLICE TRAFFIC
COLLISION REPORT



1591071

REPORT NO. **EB55613**

1 1 8 27
2
3
1 5 6 28
2
3

INTERSTATE <input type="checkbox"/>	CITY STREET <input type="checkbox"/>	FIRE RESULTED <input type="checkbox"/>
STATE ROUTE <input checked="" type="checkbox"/>	OTHER <input type="checkbox"/>	STOLEN VEHICLE <input type="checkbox"/>
COUNTY RD <input type="checkbox"/>	PRIVATE WAY <input type="checkbox"/>	HIT & RUN INVOLVED <input type="checkbox"/>

CASE #			
LOCAL AGENCY CODING			
TOTAL # OF UNITS	4	OBJECT STRUCK	Utility Pole

DATE OF COLLISION	M 8	D 4	Y 2021	TIME (2400)	1158	COUNTY #	16	MILES	32	00	N <input type="checkbox"/> S <input checked="" type="checkbox"/>	E <input type="checkbox"/> W <input checked="" type="checkbox"/>	IN <input type="checkbox"/> OF <input checked="" type="checkbox"/>	CITY #	1005
-------------------	-----	-----	--------	-------------	------	----------	----	-------	----	----	--	--	--	--------	------

ON (PRIMARY TRAFFIC WAY)	INTERSECTION <input type="checkbox"/>	NON-INTERSECTION <input checked="" type="checkbox"/>			
SR NB 101	BLOCK NO.		MILE POST	<input checked="" type="checkbox"/>	302.00

DISTANCE	0	30	MILES <input checked="" type="checkbox"/>	N <input checked="" type="checkbox"/> S <input type="checkbox"/> E <input type="checkbox"/> W <input type="checkbox"/>	FEET	CF (REFERENCE OR CROSS STREET)	BEE MILL RD
----------	---	----	---	--	------	--------------------------------	-------------

UNIT 01	MOTOR VEHICLE <input checked="" type="checkbox"/>	PEDAL CYCLE <input type="checkbox"/>	DAMAGE THRESHOLD MET YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	PHONE	
---------	---	--------------------------------------	--	-------	--

LAST NAME	KARJO	FIRST NAME	AARON	MIDDLE INITIAL	M
-----------	-------	------------	-------	----------------	---

STREET NEW ADDRESS	26947 N 88TH LN	CITY	PEORIA	ST	AZ	ZIP	8538337
--------------------	-----------------	------	--------	----	----	-----	---------

CDL	A	IGNITION INTERLOCK YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	REQUIRED YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	IGNITION INTERLOCK YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	PRESENT YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	MEDICAL TRANSPORTED YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
-----	---	--	--	--	---	---

DRIVER'S LICENSE #		STATE	AZ	SEX	F	D.O.B. MMDDYYYY	3	12	1980
--------------------	--	-------	----	-----	---	-----------------	---	----	------

ON DUTY <input type="checkbox"/>	STATUS	AIRBAG	2	RESTR.	4	EJECT	1	HELMET USE		INJURY CLASS	1	NATURE OF INJURIES	
----------------------------------	--------	--------	---	--------	---	-------	---	------------	--	--------------	---	--------------------	--

LICENSE PLATE #	AL13159	STATE	AZ	VIN#	4V4NC9EJ6LN228874
-----------------	---------	-------	----	------	-------------------

TRAILER PLATE #	Y1A3DC	STATE	AZ	TRAILER PLATE #		STATE	
-----------------	--------	-------	----	-----------------	--	-------	--

TRLR VIN#	1UYVS2533N3448206	TRLR VIN#	
-----------	-------------------	-----------	--

VEH YEAR	2020	MAKE	VOLV	MODEL	TT	STYLE	SE	VEHICLE TOWED DUE TO DISABLING DAMAGE YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	TOWED BY		GOVT VEHICLE YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
----------	------	------	------	-------	----	-------	----	---	----------	--	--

REGISTERED OWNER INFO.	LLC, DIAMONDBACK
------------------------	------------------

LIABILITY INSURANCE IN EFFECT <input checked="" type="checkbox"/>	INSURANCE CO & POLICY #	GREAT WEST CASUALTY COMPANY 11371
---	-------------------------	-----------------------------------

VEHICLE LEGALLY STANDING YES <input type="checkbox"/> NO <input type="checkbox"/>	CITATION #	CHARGE
---	------------	--------



UNIT 02	MOTOR VEHICLE <input checked="" type="checkbox"/>	PEDAL CYCLE <input type="checkbox"/>	PEDESTRIAN <input type="checkbox"/>	PROPERTY OWNER <input type="checkbox"/>	DAMAGE THRESHOLD MET YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	PHONE	
---------	---	--------------------------------------	-------------------------------------	---	--	-------	--

LAST NAME	BLOOMFIELD	FIRST NAME	ROCKY	MIDDLE INITIAL	L
-----------	------------	------------	-------	----------------	---

STREET NEW ADDRESS	120 DARK RD	CITY	BRINNON	ST	WA	ZIP	9832095
--------------------	-------------	------	---------	----	----	-----	---------

CDL		IGNITION INTERLOCK YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	REQUIRED YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	IGNITION INTERLOCK YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	PRESENT YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	MEDICAL TRANSPORTED YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
-----	--	--	--	--	---	---

DRIVER'S LICENSE #		STATE	WA	SEX	M	D.O.B. MMDDYYYY	6	3	1960
--------------------	--	-------	----	-----	---	-----------------	---	---	------

ON DUTY <input type="checkbox"/>	STATUS	AIRBAG	2	RESTR.	4	EJECT	1	HELMET USE		INJURY CLASS	1	NATURE OF INJURIES	
----------------------------------	--------	--------	---	--------	---	-------	---	------------	--	--------------	---	--------------------	--

LICENSE PLATE #	B59323V	STATE	WA	VIN#	1FTHX26F8TEB21131
-----------------	---------	-------	----	------	-------------------

TRAILER PLATE #	9776UF	STATE	WA	TRAILER PLATE #		STATE	
-----------------	--------	-------	----	-----------------	--	-------	--

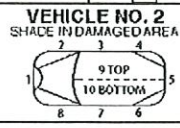
TRLR VIN#		TRLR VIN#	
-----------	--	-----------	--

VEH YEAR	1996	MAKE	FORD	MODEL	F250	STYLE	PK	VEHICLE TOWED DUE TO DISABLING DAMAGE YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	TOWED BY		GOVT VEHICLE YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>
----------	------	------	------	-------	------	-------	----	---	----------	--	--

REGISTERED OWNER INFO.	BLOOMFIELD, WENDY
------------------------	-------------------

LIABILITY INSURANCE IN EFFECT <input checked="" type="checkbox"/>	INSURANCE CO & POLICY #	MUTUAL ENUMCLAW INSURANCE COMPANY AB10045023
---	-------------------------	--

VEHICLE LEGALLY STANDING YES <input type="checkbox"/> NO <input type="checkbox"/>	CITATION #	CHARGE
---	------------	--------



OFFICER'S NAME (PRINT)	WEATHERWAX, KATHERINE	OFFICER PHONE		BADGE CRID #	648	AGENCY	WASHINGTON STATE PATROL
------------------------	-----------------------	---------------	--	--------------	-----	--------	-------------------------

0 1 29
0 1 30
1 1 2 31
1 1 2 32
5 1 33
1 5 34
5 35
4 37
4 38
3 39
3 40
1 41
1 42
43
44



STATE OF WASHINGTON
POLICE TRAFFIC
COLLISION REPORT



1591972

REPORT NO. **EB55613**

CASE #

ADDITIONAL PERSONS INVOLVED (PASSENGERS AND/OR WITNESSES ONLY)

NAME
(LAST, FIRST, MIDDLE INITIAL)

UNDERWOOD II, JAMES R

ADDRESS & PHONE #

3513 40TH AVE SE Olympia, WA 985014303

SEX

M

D.O.B.
MM/DD/YYYY

2

2

1995

PASSENGER ☒

WITNESS ☐

UNIT #

3

SEAT
POS.

3

AIRBAG

2

RESTR.

4

EJECT

1

HELMET
USE

2

INJURY
CLASS

1

NATURE OF INJURIES

NAME
(LAST, FIRST, MIDDLE INITIAL)

ADDRESS & PHONE #

SEX

D.O.B.
MM/DD/YYYY

PASSENGER ☐

WITNESS ☐

UNIT #

SEAT
POS.

AIRBAG

RESTR.

EJECT

HELMET
USE

INJURY
CLASS

NATURE OF INJURIES

NAME
(LAST, FIRST, MIDDLE INITIAL)

ADDRESS & PHONE #

SEX

D.O.B.
MM/DD/YYYY

PASSENGER ☐

WITNESS ☐

UNIT #

SEAT
POS.

AIRBAG

RESTR.

EJECT

HELMET
USE

INJURY
CLASS

NATURE OF INJURIES

DIAGRAM

Please see subsequent diagram page

INDICATE NORTH
BY ARROW



NARRATIVE

Please see subsequent narrative page(s)

I CERTIFY (DECLARE) UNDER PENALTY OF PERJURY UNDER THE LAWS OF THE STATE OF WASHINGTON THAT THE FOREGOING IS TRUE AND CORRECT. (RCW 9A.72.085)

KATHERINE WEATHERWAX

INVESTIGATING OFFICER'S SIGNATURE

8/6/2021

DATED

PLACE SIGNED

APPROVED BY

Fallon, Jason 361

DATE

BADGE OR ID #

648

ORI #

WAWSP0812

TIME POLICED/SPATCHED

11:58 AM

TIME POLICE ARRIVED

12:20 PM



SUPPLEMENTAL
POLICE TRAFFIC
COLLISION REPORT



013197

REPORT NO. **EB55613**

CASE #

1 1 8 27
2
3
1 28
2
3

COMMERCIAL MOTOR CARRIER

INTERSTATE ☒ INTRASTATE ☐

UNIT # 1 USDOT 2118344 ICC # VEHICLE TYPE 6 CARGO BODY TYPE 2

CARRIER NAME DIAMONDBACK TRANSPORTATIO

CARRIER ADDRESS 26947 N 88TH LN

CITY PEORIA ST AZ ZIP 853833733

NAME SOURCE 4 # AXLES 3 GVWR 80000 PLACARD + NAME IF NO NUMBER

ADDITIONAL UNITS

UNIT # 3 MOTOR VEHICLE ☒ PEDAL-CYCLE ☐ PEDESTRIAN ☐ PROPERTY OWNER ☐ DAMAGE THRESHOLD MET YES ☒ NO ☐ PHONE

LAST NAME SMITH FIRST NAME HUNTER MIDDLE INITIAL L

STREET NEW ADDRESS 1233 MIDDLE FORK RD CITY ONALASKA ST WA ZIP 9857097

CDL IGNITION INTERLOCK YES ☐ NO ☒ REQUIRED INTERLOCK YES ☐ NO ☒ PRESENT INTERLOCK YES ☐ NO ☐ MEDICAL TRANSPORTED YES ☐ NO ☒

DRIVER'S LICENSE # STATE WA SEX M D.O.B. MDDDDYYY 2 - 7 - 2001

ON DUTY ☐ STATUS AIRBAG 2 RESTR. 4 EJECT 1 HELMET USE INJURY CLASS 1 NATURE OF INJURIES

LICENSE PLATE # 34362K STATE 3 VIN# 1FT7W2BT6FEC38284

TRAILER PLATE # STATE TRAILER PLATE # STATE

TRLR VIN#

VEH YEAR 2015 MAKE FORD MODEL F250 STYLE PK VEHICLE TOWED DUE TO DISABLING TOWED BY GOVT. VEHICLE YES ☒ NO ☐

REGISTERED OWNER INFO SMITH, HUNTER PHONE #: (360) 742-8872

LIABILITY INSURANCE IN EFFECT ☒ INSURANCE CO & POLICY # SELF INSURED

VEHICLE LEGALLY STANDING YES ☐ NO ☐ CITATION # CHARGE



UNIT # 4 MOTOR VEHICLE ☐ PEDAL-CYCLE ☐ PEDESTRIAN ☐ PROPERTY OWNER ☒ DAMAGE THRESHOLD MET YES ☒ NO ☐ PHONE

LAST NAME PUD FIRST NAME MIDDLE INITIAL

STREET NEW ADDRESS 2621 E JOHNS PRAIRIE RD CITY SHELTON ST WA ZIP 98584

CDL IGNITION INTERLOCK YES ☐ NO ☐ REQUIRED INTERLOCK YES ☐ NO ☐ PRESENT INTERLOCK YES ☐ NO ☐ MEDICAL TRANSPORTED YES ☐ NO ☐

DRIVER'S LICENSE # STATE SEX D.O.B. MDDDDYYY - -

ON DUTY ☐ STATUS AIRBAG RESTR. EJECT HELMET USE INJURY CLASS NATURE OF INJURIES

LICENSE PLATE # STATE VIN#

TRAILER PLATE # STATE TRAILER PLATE # STATE

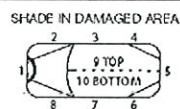
TRLR VIN#

VEH YEAR MAKE MODEL STYLE VEHICLE TOWED DUE TO DISABLING TOWED BY GOVT. VEHICLE YES ☐ NO ☐

REGISTERED OWNER INFO

LIABILITY INSURANCE IN EFFECT ☐ INSURANCE CO & POLICY #

VEHICLE LEGALLY STANDING YES ☐ NO ☐ CITATION # CHARGE



0 6 29
30
1 1 2 31
2
3
1 32
2
3

FROM TO 1 5 33
FROM TO
5 35
36

4 37
38
3 39
40
1 41
42
43
44

I CERTIFY (DECLARE) UNDER PENALTY OF PERJURY UNDER THE LAWS OF THE STATE OF WASHINGTON THAT THE FOREGOING IS TRUE AND CORRECT. (RCW 9A.72.065)

KATHERINE

8/6/2021

INVESTIGATING OFFICER'S SIGNATURE OFFICER'S PHONE UNIT OR DIST DET DATED PLACE SIGNED

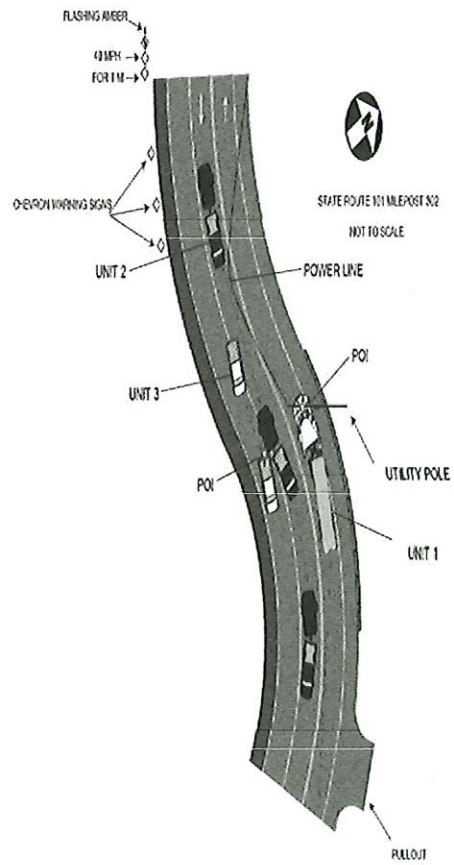
BADGE OR ID # 648 ORI # WAWSP0812 APPROVED BY Fallon DATE PAGE 3 OF 5

Narrative

UNIT 1 WAS TRAVELLING NB ON SR 101 NEAR MP 302 IN LANE 1 OF 1. A UTILITY POLE FELL INTO THE NB LANE AND THE POWER LINES WERE HANGING LOW IN THE NB AND SB LANE. UNIT 1 STRUCK THE POLE WITH ITS RIGHT MIRROR AND HOOD. UNITS 2 AND 3 WERE TRAVELLING SB ON SR 101 IN LANE 1 OF 1. UNIT 3 TRAVELLED ONTO THE SB SHOULDER TO AVOID THE POWER LINES AND STOPPED. UNIT 2 SLAMMED ON ITS BRAKES AND SKID TO AVOID THE POWER LINES. UNIT 2 WAS HAULING A TRAILER WITH GRAVEL. THE FRONT RIGHT CORNER OF THE TRAILER STRUCK THE REAR BUMPER OF UNIT 3.

PUD STATED THAT THEY THINK THE POLE WAS PREVIOUSLY DAMAGED AND FINALLY GAVE OUT. THE SUPPORT BEAM TO THE POLE WAS DAMAGED. THERE WAS NO DAMAGE TO THE POWER POLE OR TO THE GUARD RAIL. DUE TO THE CURVE THERE WAS NO WAY UNIT 1 COULD AVOID THE POLE.

Report Number: EB55613



COMMERCIAL COLLISION & PAINT INC.

2095 Corey Rd.
 Central Point, Or, 97502
 Tel: 541-826-4210 Fax: 541-826-4229
 commercialcandp5@gmail.com
 Tax ID: 93-1182121

Estimate - Preliminary**Estimate Prepared by:**

Accident Date:

Date of Loss:

Arrival Date:

Type of Loss:

Policy Number:

Claim Number:

Appraised for:

Date: 8/9/2021

Estimate#: DIAMONDBACK

Insured:

Company: DIAMONDBACK

TRANSPORTATION LLC

Contact: OWNER AARON M KARJO

Address: 26947 NORTH 88TH LANE

City, State, Zip Code: PEORIA, ARIZONA 85383

Telephone, Fax: 623-523-4140

Notes: dbtransllc@gmail.com

Year	Make	Model	Color	Trim
2020	VOLVO	VNL/VNM	GREY METALLIC	CHROME
Unit Number	License Plate #	Mileage	Serial#/VIN#	
#8874	AL13159	133,038	4V4NC9EJ6LN228874	

Sup	Seq	Labor Type	Labor Op	Description	Part Type	Part Number	Dollar Amount	Labor Units
	1	Body	Rem/Rep	Hood Shell Assy. (See Photos, Broken R Front Fender, Hood Top Panel & Multiple Inner Structures)	New	N.A.	\$3,150.89	T 8.5*
	2	Body	Rem/Ins	Measure & Drill Hood For R&L Fender Mounted Spot Mirrors, As Before	Exist			T .6*
	3	Body	Rem/Rep	R Front OEM Fender Mounted Spot Mirror (See Photos, Broken In Half)	New		\$277.92	T .3*
	4	Body	Rem/Ins	R&I L Front Fender Mounted Spot Mirror	Exist			T .3*
	5	Body	Rem/Rep	Hood Insulation Kit	New		\$191.88	T 1.0*
	6	Ref	Ref	Refinish Hood Exterior, Complete	Exist			8.5*
	7	Ref	Ref	Clearcoat, As Before	Exist			T 2.0*
	8			Paint Materials			\$504.00	*

Sup	Seq	Labor Type	Labor Op	Description	Part Type	Part Number	Dollar Amount	Labor Units
	9			**** Paint Is Axalta Imron Elite BC/CC ****				*
	10	Body	Rem/Rep	Custom Two Color Vinyl Truck Numbers (To Be Supplied By the Customer From The Original Vendor)	New		\$40.23	T *
	11			Shipping			\$50.00	*

* - Judgement Item

- Labor Note Applies

Labor

Body	10.7	Hrs @	\$125.00	\$1,337.50
Refinish	10.5	Hrs @	\$125.00	\$1,312.50
Labor Total				\$2,650.00

Parts

Parts Subtotal	\$3,660.91
Less Adjustments	
Parts Total	\$3,660.91

Additional Costs and Operations

Addl. Costs/Ops Total	\$554.00
-----------------------	----------

Tax

Labor Tax	@	0.57%	\$15.11
Parts Tax	@	0.57%	\$20.87
Tax Total			\$35.98

Totals

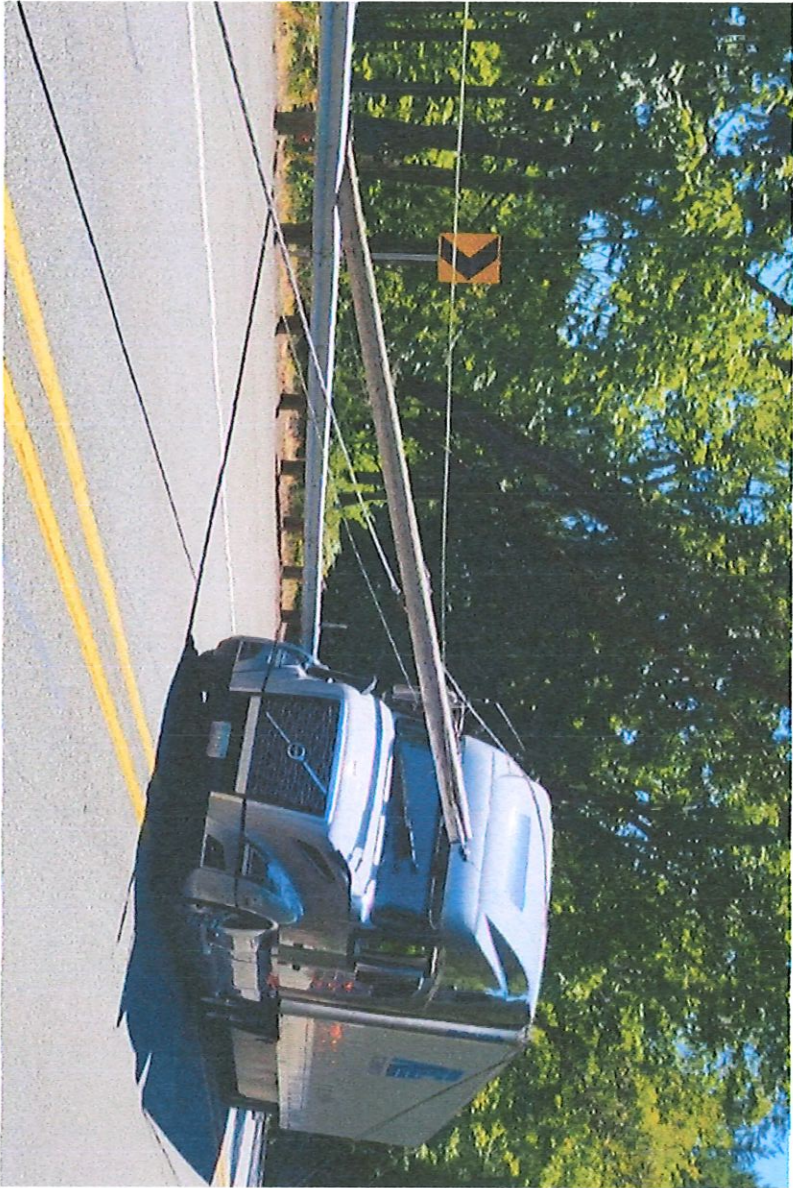
Sub Total:	\$6,900.89
Customer Resp.	\$0.00
Net Total	\$6,900.89

The above is an estimate based on our inspection and does not cover any additional parts or labor which may be required after the work has started. Occasionally, worn or damaged parts are discovered which may not be evident on the first inspection. Because of this, the above prices are not guaranteed. Quotations on parts and labor are current and subject to change.

This is a preliminary estimate. Additional changes to the estimate may be required for the actual repair.

TruckEst does not automatically include items required by many business repair partners. This application allows the author to manually enter line items such as overlap deductions.

2020 VOLVO VNL/VNM







PUD1 – Executive Summary – August 2021

This report summarizes information on the current financial status of Mason County PUD No. 1 for the month of August 2021:

- **Work in Progress:**
 - FEMA Funding
 - Cash Flow Monitoring from COVID-19 Effects
 - 2022 Budget Development
 - Hazard Mitigation Grants – 2021 / 2022
 - DOH Construction Loans / Grants for 2022 Projects
- **Completed Projects:**
 - 2020 Annual Report – State Auditor
 - 2020 Privilege Tax Return (Due February 28, 2021)
 - 2020 RUS Form 7 (Due March 31, 2021)
- **Planned Key Milestones, Activities and / or Events:**
 - Long range financial and budgetary planning – ongoing.

Financial Highlights:

- Revenue – Gross Revenue was \$1,079,488 for the month of August 2021.
- Expenditures – Gross expenditures were \$968,410 for the month of August 2021.
- COVID Metrics – Cash on Hand is down overall, \$146,863 due to delayed account payments, late fees etc. We have applied \$117,607 to customer's accounts to assist with past due balances. As of August, there were 164 electric accounts and 101 water accounts that were 90 days or more past due for a total of \$94,179.

Financial Metrics as Compared with Prior Year:	August 2021	August 2020
Total General Cash and Investments	\$1,134,936	\$959,350
Current Ratio (Current Assets/Current Liabilities)	2.67 to 1	3.88 to 1
Debt Service Coverage (O&M/ Debt Service)	2.76	2.66
Long-Term Debt to Net Plant	38%	42%
Total Debt to Equity Ratio (Total Liabilities/Total Equity)	52%	57%
Long Term Debt to Equity Ratio (Long Term Debt / Total Equity)	47%	53%
Times Interest Earned Ratio (Earnings before Interest & Taxes/Total Interest)	4.65	4.23
Cash on Hand (Total Available Cash/Average Daily Costs)	52 Days (General) 175 Days (All Funds)	42 Days (General) 190 Days (All Funds)



Mason County PUD No 1

Budget Summary by Division For the Month Ended August 31, 2021

	<u>Electric</u>	<u>Water</u>	<u>Sewer</u>	<u>Totals</u>
Total Revenue	\$ 800,038.64	\$ 278,546.91	\$ 902.05	\$ 1,079,487.60
Budgeted	\$ 612,033.59	\$ 237,577.78	\$ 745.00	\$ 850,356.37
Difference (-/+)	\$ 188,005.05	\$ 40,969.13	\$ 157.05	\$ 229,131.23
% of Budget	131%	117%	121%	127%
Total Expenditures	\$ 788,051.36	\$ 179,896.92	\$ 461.80	\$ 968,410.08
Budgeted	\$ 657,453.19	\$ 194,614.50	\$ 747.97	\$ 852,815.66
Difference (-/+)	\$ 130,598.17	\$ (14,717.58)	\$ (286.17)	\$ 115,594.42
% of Budget	120%	92%	62%	114%
Net Operating Margins	\$ 11,987.28	\$ 98,649.99	\$ 440.25	\$ 111,077.52
Budgeted	\$ (45,419.60)	\$ 42,963.28	\$ (2.97)	\$ (2,459.29)
Difference (-/+)	\$ 57,406.88	\$ 55,686.71	\$ 443.22	\$ 113,536.81
% of Budget	-26%	230%	-14823%	-4517%



Mason County PUD No 1

Budget Summary by Division for the Eight Months Ended August 31, 2021

	<u>Electric</u>	<u>Water</u>	<u>Sewer</u>	<u>Totals</u>
Total Revenue	\$ 6,887,823.05	\$ 1,874,104.10	\$ 5,878.05	\$ 8,767,805.20
2021 Budget	\$ 9,167,191.56	\$ 2,286,636.00	\$ 8,940.00	\$ 11,462,767.56
Difference (-/+)	\$ (2,279,368.51)	\$ (412,531.90)	\$ (3,061.95)	\$ (2,694,962.36)
% of Budget	75%	82%	66%	76%
Total Expenditures	\$ 6,003,518.02	\$ 1,454,232.33	\$ 5,220.71	\$ 7,462,971.06
2021 Budget	\$ 8,913,965.00	\$ 2,132,621.00	\$ 7,194.24	\$ 11,053,780.24
Difference (-/+)	\$ (2,910,446.98)	\$ (678,388.67)	\$ (1,973.53)	\$ (3,590,809.18)
% of Budget	67%	68%	73%	68%
Net Operating Margins	\$ 884,305.03	\$ 419,871.77	\$ 657.34	\$ 1,304,834.14
2021 Budget	\$ 253,226.56	\$ 154,015.00	\$ 1,745.76	\$ 408,987.32
Difference (-/+)	\$ 631,078.47	\$ 265,856.77	\$ (1,088.42)	\$ 895,846.82
% of Budget	349%	273%	38%	319%

Cash Flow

Beginning Cash (General Fund)	49,753.30	97,382.51	4,195.20	151,331.01
Net Operating Margin (Excluding Depreciation)	1,231,713.41	764,522.30	408.16	1,996,643.87
Cash Transferred to / from Special Funds	(743,265.28)	(40,929.43)	(22.65)	(784,217.36)
Change in Accounts Receivable	(65,566.26)	238,134.51	2,210.16	174,778.41
Change in Accounts Payable	2,384.88	6,697.03	249.18	9,331.09
Cash Expended on Utility Plant	(504,864.67)	(633,957.51)	0.00	(1,138,822.18)
Change in CWIP	231,305.06	(335,565.53)	(2,844.85)	(107,105.32)
Ending Cash (General Fund)	201,460.44	96,283.88	4,195.20	301,939.52



Mason County PUD No. 1

Cash & Investment Balances

As of August 31, 2021

Cash Balances

Cash - General Funds

\$ 302,140.03

Cash - Restricted

\$ 49,596.78

Total Cash

\$ 351,736.81

Investment Balances (LGIP)

Investments - Electric

\$ 488,184.38

Investments - Sewer

\$ 30,540.50

Investments - Water

\$ 264,473.96

Total Investments

\$ 783,198.84

Total Cash & Investments

\$ 1,134,935.65

***Does Not Include Designated Funds*

MASON COUNTY PUD #1

Credit Card Security Policies

PCI DSS 3.2.1

Version 2.1 - 2021-6-8

CONFIDENTIAL INFORMATION

This document is the property of MASON COUNTY PUD #1; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of MASON COUNTY PUD #1.

Revision History

[illegible]

INTRODUCTION AND SCOPE

Introduction

This document explains MASON COUNTY PUD #1's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. MASON COUNTY PUD #1 management is committed to these security policies to protect information utilized by MASON COUNTY PUD #1 in attaining its business goals. All employees are required to adhere to the policies described within this document.

Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, MASON COUNTY PUD #1's cardholder environment consists only of limited payment applications (typically point-of-sale systems) connected to the internet, but does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in **Self-Assessment Questionnaire (SAQ) C, ver. 3.2.1, released June, 2018**. Should MASON COUNTY PUD #1 implement additional acceptance channels, add additional connected systems, begin storing cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C, it will be the responsibility of MASON COUNTY PUD #1 to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Requirement 1: Build and Maintain a Secure Network

Firewall Configuration

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. Access to the internet must be through a firewall, as must any direct connection to a vendor, processor, or service provider. (PCI Requirement 1.2)

Inbound and outbound traffic must be restricted by the firewalls to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied. (PCI Requirement 1.2.1(a))

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)

Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment. (PCI Requirement 1.3.3)
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized by management and controlled by the firewall. (PCI Requirement 1.3.5)
- Firewalls used to protect the cardholder data environment must implement stateful inspection, also known as dynamic packet filtering. (PCI Requirement 1.3.6)

Any mobile and/or employee-owned computers with direct connectivity the Internet (for example, laptops used by employees), which also have the ability to access the organization's cardholder data environment must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or employee-owned computer users. (PCI Requirement 1.4)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Vendor Defaults

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to: (PCI Requirement 2.1.1)

- Default encryption keys
- Passwords
- SNMP community strings
- Default passwords/passphrases on access points
- Other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption (such as WPA or WPA2) for authentication and transmission of data over wireless networks.

Configuration Standards for Systems

Configuration standards for all system components must be developed and enforced. MASON COUNTY PUD #1 must insure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. (PCI Requirement 2.2)

Configuration standards must be updated as new vulnerability issues are identified, and they must be enforced on any new systems before they are added to the cardholder data environment. The standards must cover the following:

- Changing of all vendor-supplied defaults and elimination of unnecessary default accounts.
- Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (PCI Requirement 2.2.1)
- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system. (PCI Requirement 2.2.2)
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure. (PCI Requirement 2.2.3)
- Configuring system security parameters to prevent misuse
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (PCI Requirement 2.2.5)

System administrators and any other personnel that configure system components must be knowledgeable about common security parameter settings for those system components. They must also be responsible to insure that security parameter settings set appropriately on all system components before they enter production. (PCI Requirement 2.2.4)

System administrators are responsible to insure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (PCI Requirement 2.5)

Non-Console Administrative Access

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. Encryption technologies must include the following: (PCI Requirement 2.3)

- Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested.
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.

- Must include administrator access to web-based management interfaces.
- Use vendor documentation and knowledge of personnel to verify that strong cryptography is in use for all non-console access and that for the technology in use it is implemented according to industry best practices and vendor recommendations.

Requirement 3: Protect Stored Cardholder Data

Prohibited Data

Processes must be in place to securely delete sensitive authentication data (defined below) post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)

Payment systems must not store of sensitive authentication data in any form after authorization (even if encrypted). Sensitive authentication data is defined as the following:

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. (PCI Requirement 3.2.3)

Displaying PAN

MASON COUNTY PUD #1 will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show at most only the first six and the last four digits of the PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. Policies and procedures for masking the display of PANs must mandate the following: (PCI requirement 3.3)

- A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access.
- PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN.
- All other roles not specifically authorized to see the full PAN must only see masked PANs.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

In order to safeguard sensitive cardholder data during transmission over open, public networks, MASON COUNTY PUD #1 will use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.). These controls will be implemented as follows: (PCI Requirement 4.1)

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use.

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder

data environment. Weak encryption (for example, WEP, SSL version 2.0 or older) is not to be used as a security control for authentication or transmission. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Requirement 5: use and Regularly Update Anti-Virus Software or Programs

Anti-Virus Protection

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software. (PCI Requirement 5.1, 5.1.1)

For systems considered to be not commonly affected by malicious software, MASON COUNTY PUD #1 will perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. (PCI Requirement 5.1.2)

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and be capable of as well as configured to generate audit logs. Anti-virus logs must also be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2)

Steps must be taken to insure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. (PCI Requirement 5.3)

Requirement 6: Develop and Maintain Secure Systems and Applications

Risk and Vulnerability

MASON COUNTY PUD #1 will establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

Risk rankings are to be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. (PCI Requirement 6.1)

All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. All applicable non-critical vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). (PCI Requirement 6.2)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to MASON COUNTY PUD #1's cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.2)

Privileges must be assigned to individuals based on job classification and function (also called "role-based access control"). (PCI Requirement 7.1.3)

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Remote Access

Two-factor authentication must be incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (PCI Requirement 8.3)

Vendor Accounts

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. (PCI Requirement 8.1.5)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically Secure All Areas and Media Containing Cardholder Data

All publicly accessible network jacks must have physical and/or logical controls to restrict access to the secure network by unauthorized personnel. (PCI requirement 9.1.2)

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI requirement 9.5)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include: (PCI Requirement 9.6)

- Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.6.1)
- Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.6.2)
- Management approval must be obtained prior to moving the media from the secured area. (PCI Requirement 9.6.3)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.7)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.8)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI requirement 9.8.1.a)

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. (PCI requirement 9.8.1.b)

Protection of Payment Devices

Devices that capture payment card data via direct physical interaction with the card (such as swipe readers and any other payment terminals) must be protected. This protection must include preventing the devices from being tampered with or substituted. (PCI requirement 9.9)

MASON COUNTY PUD #1 must maintain an up-to-date list of devices. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following: (PCI requirement 9.9.1(a))

- Make and model of all devices.
- Location of each device (for example, the address of the site or facility where the device is located).
- Device serial number or other method of unique identification.

The payment devices must be periodically inspected. Check surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). (PCI requirement 9.9.2(a))

Employees and contractors who interact with the payment devices must be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI requirement 9.9.3)

- Employees must verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices.
- Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added.
- Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).

Requirement 10: Regularly Monitor and Test Networks

Audit Log Collection

MASON COUNTY PUD #1 will implement technical controls that create audit trails in order to link all access to system components to an individual user. The automated audit trails created will capture sufficient detail to reconstruct the following events:

- All actions taken by any individual with root or administrative privileges. (PCI Requirement 10.2.2)
- All invalid logical access attempts (failed logins). (PCI Requirement 10.2.4)
- Any use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. (PCI Requirement 10.2.5)

MASON COUNTY PUD #1's log generating and collecting solution will capture the following data elements for the above events:

- User identification. (PCI Requirement 10.3.1)
- Type of event. (PCI Requirement 10.3.2)
- Date and time. (PCI Requirement 10.3.3)
- Success or failure indication. (PCI Requirement 10.3.4)
- Origination of event. (PCI Requirement 10.3.5)
- Identity or name of affected data, system component, or resource. (PCI Requirement 10.3.6)

Audit Log Review

MASON COUNTY PUD #1's systems administrators will perform daily review of the audit logs. This review may be manual or automated but must monitor for and evaluate: (PCI Requirement 10.6.1)

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

The audit review must also check the logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. (PCI Requirement 10.6.2)

Subsequent to log review, systems administrators or other responsible personnel will follow up exceptions and anomalies identified during the review process. (PCI Requirement 10.6.3)

MASON COUNTY PUD #1 must retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). (PCI Requirement 10.7)

Requirement 11: Regularly Test Security Systems and Processes

Testing for Unauthorized Wireless Access Points

At least quarterly, MASON COUNTY PUD #1 will perform testing to ensure there are no unauthorized wireless access points (802.11) present in the cardholder environment. (PCI Requirement 11.1)

The methodology must be adequate to detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components.
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.).
- Wireless devices attached to a network port or network device.

To facilitate the detection process, MASON COUNTY PUD #1 will maintain an inventory of authorized wireless access points including a documented business justification. (PCI Requirement 11.1.1)

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), the configuration must be capable of generating alerts to notify personnel. Detection of unauthorized wireless devices must be included in the Incident Response Plan (see PCI Requirement 12.10). (PCI Requirement 11.1.2)

Vulnerability Scanning

At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), MASON COUNTY PUD #1 will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Internal vulnerability scans must be performed at a minimum quarterly and repeated until passing results are obtained, or until all “high” vulnerabilities as defined in PCI Requirement 6.1 are resolved. Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.1)

Quarterly external vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures). External vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.2)

For both internal and external vulnerability scans, MASON COUNTY PUD #1 shall perform rescans as needed to validate remediation of failures detected during previous scans, as well as after any significant change to the network. Scans must be performed and reviewed by qualified personnel. (PCI Requirement 11.2.3)

If segmentation is used to isolate the CDE from other networks, perform tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. These tests need to be done from multiple locations on the internal network, checking both for improper accessibility from the out-of-scope zones to the in-scope zone as well as the reverse. (PCI Requirement 11.3.4)

For all in-scope systems for which it is technically possible, MASON COUNTY PUD #1 must deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. The change detection software must be integrated with the logging solution described above, and it must be capable of raising alerts to responsible personnel. (PCI Requirement 11.5.1)

For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider). (PCI Requirement 11.5)

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

Security Policy

MASON COUNTY PUD #1 shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data. (PCI Requirement 12.1)

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.1)

Critical Technologies

MASON COUNTY PUD #1 shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

These policies must include the following:

- Explicit approval by authorized parties to use the technologies. (PCI Requirement 12.3.1)
- Authentication for use of the technology. (PCI Requirement 12.3.2)
- A list of all such devices and personnel with access. (PCI Requirement 12.3.3)
- Acceptable uses of the technologies. (PCI Requirement 12.3.5)
- Acceptable network locations for the technologies. (PCI Requirement 12.3.6)

- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. (PCI Requirement 12.3.8)
- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. (PCI Requirement 12.3.9)

Security Responsibilities

MASON COUNTY PUD #1's policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

Incident Response Policy

Katie Arnold shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Inaccurate information within databases, logs, files or paper records.

Reporting an Incident

The Katie Arnold should be notified immediately of any suspected or real security incidents involving cardholder data:

Contact the Katie Arnold to report any suspected or actual incidents. The Internal Audit's phone number should be well known to all employees and should page someone during non-business hours.

No one should communicate with anyone outside of their supervisor(s) or the Katie Arnold about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Katie Arnold.

Document any information you know while waiting for the Katie Arnold to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response Policy (PCI requirement 12.10.1)

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.

Visa

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at

<http://usa.visa.com/download/business/accepting Visa/ops risk management/cisp what to do if compromised.pdf>

MasterCard

Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

Discover Card

Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

American Express

Contact your relationship manager or call the support line at 1-(800)-528-5200 for further guidance.

2.Alert all necessary parties. Be sure to notify:

- a. Merchant bank
- b. Local FBI Office
- c. U.S. Secret Service (if Visa payment data is compromised)
- d. Local authorities (if appropriate)

3.Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used:

<http://www.ncsl.org/programs/lis/cip/priv/breach.htm>

4.Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Katie Arnold will work with legal and management to identify appropriate forensic specialists.

5.Eliminate the intruder's means of access and any related vulnerabilities.

6.Research potential risks related to or damage caused by intrusion method used.

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Katie Arnold and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Security Awareness

MASON COUNTY PUD #1 shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

Service Providers

MASON COUNTY PUD #1 shall implement and maintain policies and procedures to manage service providers. (PCI requirement 12.8)

This process must include the following:

- Maintain a list of service providers. (PCI requirement 12.8.1)
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess. (PCI requirement 12.8.2)

- Implement a process to perform proper due diligence prior to engaging a service provider. (PCI requirement 12.8.3)
- Monitor service providers' PCI DSS compliance status. (PCI requirement 12.8.4)
- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. (PCI requirement 12.8.5)



PCI Maintenance Program

Introduction

The Payment Card Industry's Data Security Standard, or PCI, is not just an annual obligation like doing your taxes: it requires you to perform a number of security maintenance tasks at regular intervals throughout the year, like checking that documents are up to date, or that computers in your network are still healthy.

This document is a guide to help you perform, these regular tasks. It has been provided to you as part the PCI Rapid ComplySM solution.

Area of Responsibility

The following labels are used later in the document to assign responsibilities for specific tasks.

Label	Description
Computers	The person or people in the company responsible for the security of the company's computers
Network	The person or people in the company responsible for the security of the company's computer networks
Cardholder Data	The person or people in the company responsible for the security of the cardholder data used or kept by the company or its 3rd party service providers
Access Control	The person or people in the company responsible for managing the company's access control systems such as user accounts and passwords
Management	The person or people in the company responsible for the general management of security issues across the company

Step One: Take Care of Your PCI Compliance and Validation Obligations

The first step is to make sure that you are compliant with PCI and have taken care of your PCI paperwork by completing your PCI Self-Assessment Questionnaire. You should have already completed this step using the PCI Rapid Comply solution, but if not, please do so before proceeding.



Step Two: Maintaining Your PCI Program

On this page is a form to be maintained, rather than just a document to read. When each of the tasks below has been completed by the appropriate person, the item should be signed and dated. Additional comments should be recorded in the box below so that the same task is simpler when it needs to be performed again.

Month One _____ (Write full name of month)

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Review firewall and router rule sets.	Network			Every 6 months
3	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly
4	Review network diagram to see if update required.	Network			Quarterly
5	Conduct Risk Assessment.	Management			Annual

Comments



Month Two _____ **(Write full name of month)**

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Conduct a review to verify that no cardholder data is stored unnecessarily, and that any stored cardholder data is not kept for longer than necessary.	Cardholder Data			Quarterly
3	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly
4	Review information security policy and update as needed to reflect changes to business objectives or the risk environment.	Management			Annual

Comments



Month Three _____ **(Write full name of month)**

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Conduct a search in order to detect and identify wireless access points.	Network			Quarterly
3	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly
4	Review Incident Response Plan and update as needed to reflect changes to business objectives or the risk environment.	Management			Annual
5	Test your Incident Response Plan.	Management			Annual
6	Give all staff security training.	Management			Annual

Comments



Month Four _____ **(Write full name of month)**

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly
3	Review network diagram to see if update required.	Network			Quarterly
4	Ensure that all partners and service providers who store, transmit, or process cardholder data on your behalf are also PCI DSS compliant.	Management			Annual

Comments



Month Five_____ (Write full name of month)

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Conduct a review to verify that no cardholder data is stored unnecessarily, and that any stored cardholder data is not kept for longer than necessary.	Cardholder Data			Quarterly
3	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly

Comments



Month Six _____ **(Write full name of month)**

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Conduct a search in order to detect and identify wireless access points.	Network			Quarterly
3	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly

Comments



Month Seven _____ **(Write full name of month)**

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Review firewall and router rule sets.	Network			Every 6 months
3	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly
4	Review network diagram to see if update required.	Network			Quarterly

Comments



Month Eight _____ **(Write full name of month)**

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Conduct a review to verify that no cardholder data is stored unnecessarily, and that any stored cardholder data is not kept for longer than necessary.	Cardholder Data			Quarterly
3	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly

Comments



Month Nine _____ **(Write full name of month)**

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Conduct a search in order to detect and identify wireless access points.	Network			Quarterly
3	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly

Comments



Month Ten _____ (Write full name of month)

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly
3	Review network diagram to see if update required.	Network			Quarterly

Comments



Month Eleven _____ **(Write full name of month)**

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Conduct a review to verify that no cardholder data is stored unnecessarily, and that any stored cardholder data is not kept for longer than necessary.	Cardholder Data			Quarterly
3	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly

Comments



Month Twelve _____ (Write full name of month)

#	Task	Area of Responsibility	Notes	Tracking: Sign and Date	Frequency
1	Check for critical security patches/updates for computers and software, install all that apply.	Computers			Monthly
2	Conduct a search in order to detect and identify wireless access points.	Network			Quarterly
3	Check for user accounts that have been inactive for more than 90 days, and disable those that are not needed.	Access Control			Monthly

Comments

Notes

To check for critical security patches / updates for computers and software, sign up for automatic updates where possible (such as Windows Update), and subscribe to any alert services provided by vendors or resellers.

It is strongly recommended that you do not store any sensitive cardholder data unless strictly necessary, and that you avoid using systems that do so unless strictly necessary. The review should involve a search of all computers to ensure that you know where all cardholder data is located and identify why the data is being stored, and for how long it has been stored.

Any cardholder data that is not necessary should be deleted, and the system, process, or behavior that led to its being stored should be changed. Any cardholder data that has been kept for longer than necessary should be deleted, and the system, process, or behavior that led to its being stored for too long should be changed.

See the **Access Control Guide** provided by First Data for more detailed advice on this issue.

To search for wireless access points you may use one or more of the following, as appropriate:

- Wireless network scans (these are scans for the radio signals used by wireless devices)
- Physical / logical inspections of system components and infrastructure, network access control (NAC)
- Wireless intrusion detection or intrusion prevention system

The objective is to make sure that you can detect, and remove, any unauthorized access points that have been added to your network.

All staff are to be given yearly security training, to ensure that they understand their responsibilities for information security, and to remind them of what to do, and what not to do, in order to protect the company and its customers.

See Also:

- Firewall and Router Configuration and Management Guide
- Risk Management Guide
- Information Security Policy
- Incident Response Plan
- Incident Response Plan

As part of your own PCI obligations you are required to ensure that that all partners and service providers who store, transmit, or process cardholder data on your behalf are also PCI compliant. If they cannot provide formal assurance that they are compliant, you should strongly consider changing partners to one who is PCI compliant and who can provide suitable proof.





Access Control Policy

Introduction

This document is a guide on how to control and manage user access to specific information and systems within your company: your **Access Control Policy**. It has been provided to you by First Data, and while it gives you useful guidance and information, it does not replace the product-specific guides and information that came with the computer systems that you use.

Definitions

Authentication: The process of checking that a person, device, or entity is who they claim to be. Authentication typically occurs through the use of one or more authentication methods:

- a password or passphrase
- a token device or smart card
- a biometric

Authorization: The granting of access privileges to a user, device, or program, based on who they are and the company's rules on who should be allowed to do what.

Example: Jill is authorized to look at the general ledger, because she is the company accountant. Bob is not authorized, because he is a salesman.

Access Control: A mechanism that actively limits what users can access or which functions they can perform, based on:

- who they are
- what they are authorized to do.

Example: The enforced use of passwords before being able to use a computer is a form of access control: Only people who have been given an account on the computer are given access, and they first have to prove who they are (using their password) before they are given access.

Privilege: Permission to perform some action that is not automatically available to everyone.

Example: Being able to open a sensitive website or document and read its contents is a privilege, as is being able to log on to a particular computer.



PCI Requirements

PCI requires that you protect sensitive systems and data in your company by controlling and monitoring who has access to them. Failure to do this properly means that you are not compliant with PCI and means that your business and your customers are at increased risk. To comply with PCI, and protect your customers and your business, you must complete and follow this document:

Network Management

Formal responsibility for the management of the following policies and procedures has been assigned to these individuals within the company:

Name of Person	Role and Responsibility for Access Control Management
Katie Arnold	Supervisor, Director of Business Services
Spencer Jones	IT Mgr. Hood Canal Communications- Contractor

General Rules about Access Control

- Access to system components and cardholder data must be limited to only those individuals whose jobs require such access.
- Privileges are to be assigned to individuals based on their job classification and function.
- All individuals granted access to system components and cardholder data must be given the smallest set of privileges possible (while still allowing them to do their job).
- Privileges granted are subject to a formal approval process and such approval must be formally documented. For example, sensitive systems should have a formal list kept of which people have been granted access.

Access Control Mechanisms

- All users are to be assigned a unique ID before allowing them to access system components or cardholder data. No use is permitted of group, shared, or generic accounts or passwords, and all such accounts must be disabled or removed where possible, and their use prohibited where disabling or removal is not possible.
- All users are to be authenticated before access to system components and cardholder data is granted.
- Authentication must be based on the use of passwords or a stronger alternative.
- The password system must enforce the following:

- Passwords must be at least 7 characters long.
- Passwords must contain both numeric and alphabetic characters.
- Passwords must be changed every 90 days.
- All passwords must be rendered unreadable during transmission and storage on all system components by the use of strong cryptography.

Management of Access Control Systems

- All additions, deletions, and modifications of user IDs, passwords, other credentials, and other identifier objects must be controlled, to make sure that privileges are only assigned via the correct formal process described above.
- The identity of users must be confirmed before password resets are performed.
- When passwords are first created or reset, they must be set to a unique value for each user, and users must be required to change that password immediately after the first use.
- When a user is terminated, all their accounts are to be immediately deactivated.
- All accounts which have been inactive for more than 90 days are to be either removed or disabled.
- Accounts are to be locked out or disabled after 6 unsuccessful login attempts. Accounts which have been locked out are to remain locked out for a minimum of 30 minutes or until an administrator overrides the lockout.
- Computer usage sessions which have been idle for more than 15 minutes are to be locked.

Access Control for Devices and Critical Technologies

- For devices and technologies identified as critical (such as remote access technologies, wireless, removable electronic media, laptops, smart-phones, and tablets) the following requirements apply:
 - Use of the technology is subject to explicit approval by management.
 - All use is subject to authentication of users.
 - A list of all such devices and technologies must be maintained, along with the list of approved users.
 - All such devices must be labeled for asset tracking, and usage management.
 - All such devices must have a formal acceptable usage policy created, including any appropriate restrictions on how, where, when, why, and by whom such usage takes place.



Staff Training Regarding Access Control Systems

Staff members are to be educated on the following requirements at their time of hiring and in subsequent years using annual re-training sessions:

- All staff members are responsible for protecting sensitive systems and cardholder data from misuse, loss, and damage. This includes, but is not limited to, an obligation to:
 - Never access any information or system to which they are not authorized
 - Never share account information or passwords
 - Never write down account or password information
 - Never use passwords that could be easily guessed
 - Never re-use passwords from other systems or accounts outside the company
 - Never bypass any company security system
 - Never assist anyone else in bypassing any company security system

Staff may only access systems and information if required to do so as part of their formal job duties, and if management approval has already been given. Where approval has not been provided, it must be obtained before attempting access.

Note: Violation of these requirements is grounds for immediate termination.

Disclaimer

Organizations must ensure for themselves that they meet all the compliance and validation requirements of the Payment Card Industry Security Standards Council. First Data is not responsible for errors or damages of any kind resulting from the use of the information or guidance contained herein, and makes no warranty, guarantee, or representation as to the accuracy or sufficiency of the information provided herein, and assumes no responsibility or liability regarding the use or misuse of such information. For more information, go to https://www.firstdata.com/en_us/products/merchants/security-and-compliance.html.

Security Policy Package for MASON COUNTY PUD #1

Instructions:

- This Security Policy package was designed specifically for MASON COUNTY PUD #1, based on information you provided to us as you completed the Security Assessment. Because this policy is specific to MASON COUNTY PUD #1, it should not be used by any other entity as a basis for its own security policy.
- There are two parts to this package:
 - A. The first half describes the MASON COUNTY PUD #1 Security Policy as it relates to managers and anyone responsible for keeping your business and computer systems safe and in operation. It should not be given out to general staff (or anyone else) to read.
 - B. The second half is the MASON COUNTY PUD #1 Security Policy for ALL staff with access to credit card processing or data, and should be printed out and displayed on a notice board where all staff can read it, (but where members of the public cannot). ALL staff members with access to credit card processing or data need to read it, and then sign the back page to show that they have read it, and understood it.
- This Security Policy package is intended to relate only to your systems and processes that are involved in processing, transmitting or storing credit or debit card information (your "Card Transaction System"). While the principles, steps and statements outlined and made in this policy may apply generally to other of your systems and processes that are not involved in card transactions, you should not assume this policy is sufficient to cover your entire business.
- Because this Security Policy package is specific to the Card Transaction System you described to us as you completed the Security Assessment, modifications to that system may require changes to this policy. If you modify your Card Transaction System, please update your responses to the Security Assessment and, for a period of one year, we will make the necessary changes to this Security Policy for free. An out-of-date security policy may give you advice that is no longer suitable, and put your security and compliance status at risk.

Having a formal security policy, and even following it perfectly, does NOT guarantee that MASON COUNTY PUD #1 will not be damaged by hackers, an accident, or some other event. It DOES help you reduce your risk. If you feel that you need more detailed advice on security policies, or on how to implement them, please visit <http://www.pcirapidcomply.com>, or contact an information security specialist in your area.

Security Policy for MASON COUNTY PUD #1

Instructions For Managers and System Administrators ONLY

This section of the document is for all staff with managerial responsibilities within MASON COUNTY PUD #1 and all staff tasked with any security or technology responsibilities. It should not be distributed to other staff, or to anyone outside the company that does not have authorization and a clear need to know.

Controlling the Scope of PCI

These policies should be applied everywhere (to all computers, to all people, etc.) but they **MUST** in particular apply to any computers, devices, or records that are subject to PCI. Computers and other network devices are subject to PCI if they process, store, or transmit cardholder information (such as account numbers, names, etc.) **OR IF THEY ARE CONNECTED TO ANY SUCH DEVICE**. So, for example, **ANY** device connected to a Point of Sale (POS) terminal is definitely subject to PCI.

Complying with the PCI Data Security Standard

In addition to the specific policy elements described below, the company and all staff are required to make sure that at all times they act in accordance with all requirements of the latest version of the Payment Card Industry Data Security Standard.

Computers and Software

- No computers are to be used to store cardholder data (such credit card numbers or information read off a card's magnetic stripe).
- No computers are to be connected to any Point of Sale terminal (via cables, wireless, or anything else).
- No computers other than virtual terminals are to be used to process cardholder data (such credit card numbers).
- No computers other than virtual terminals are to be used to transmit or share cardholder data over any sort of network.

Information and Records Stored On Computers and Devices

- **DO NOT** record, copy, or store cardholder information (such as account numbers) on any computer, thumb-drive, CD, DVD, etc. This includes magnetic stripe information, and other information like the three-digit numbers printed on the signature panel of cards.
- It **IS** allowed to record the last 4 digits **ONLY** of an account number.
- **NEVER, UNDER ANY CIRCUMSTANCES**, record, copy, or store cardholder PINs **ANYWHERE**.

Physical copies of Records (Paper Records, Thumbdrives, CD, DVDs, etc.)

- Cardholder data shall be stored only if strictly necessary, and only for as long as necessary. Data that is prohibited by other parts of this security policy must not be

stored at all.

- NEVER, UNDER ANY CIRCUMSTANCES, write down, record, copy, or store cardholder PINs ANYWHERE.
- DO NOT record, copy, or store the three-digit number printed on the signature panel of any card.
- All paper records of cardholder data, and all thumbdrives, CDs, DVDs, etc, holding cardholder data are to be treated like cash. They must be kept in a locked area and access to them must be tightly restricted.
- Staff access to cardholder data records must be on a 'need to know' basis.
- Never share cardholder records with anyone outside the company, or with anyone inside the company who does not have management approval to use those records.
- Paper records of cardholder data, and thumbdrives, CD, DVDs, etc, holding cardholder data must not be thrown out or re-used for other purposes. When you are finished with them, they must be destroyed via shredding, using a company or machine approved of by management.
- Paper records of cardholder data are to be destroyed via cross-cut shredding, incineration, or pulping after five years (or at a time determined by management), using a company or machine approved of by management.
- Electronic media such as thumbdrives, CDs, DVDs, etc, ever used to hold cardholder data are to be physically destroyed after five years (or at a time determined by management), using a company or machine approved of by management.

Transmitting Information and Records

- Cardholder information must never be sent outside the work network unless it is protected by encryption. That encryption can either be on the communications channel (like SSL version3 for the web), or on the data itself (such as PGP). It is NOT enough to use winzip.

Physical Security

- Physical access to all Point of Sale terminals is restricted to those who have formal management approval.
- All visits to company premises by non-staff must be managed to make sure that cardholder data is not threatened. This includes, but is not limited to, making sure that visitors do not interfere with sensitive systems, or have unsupervised access to sensitive data or systems.
- If it is ever possible for visitors to be mistaken for staff by other staff members, visitors shall be required to wear visitor's badges, with badges assigned, tracked, and collected at the end of a visit by a staff member who has been explicitly assigned responsibility for this process.
- If any visitors are ever given any access to sensitive data or systems, they shall be required to first enter their information in a visitor's log, with the information gathered to include their name, the company they represent, and the name of the staff member who is authorizing their access.

- Paper records or electronic records of cardholder information must be kept in a locked drawer or box inside a separate room (like a back office), and the door must be locked unless someone with formal management approval is in the room at the time.
- Paper records or electronic records of cardholder information must not be removed from the secure area without formal management approval and a formal record made.
- Paper records and media holding cardholder information must be inventoried.
- Physical access to paper records with cardholder information on them is restricted to those who have formal management approval.
- Physical access to each computer or network device must be restricted to those with a need to have such access.

Policies and Procedures

- Responsibility for updating and distributing this Security Policy shall be formally assigned to one or more specific individuals.
- The company shall each year conduct a security review to identify threats and vulnerabilities, and to produce a risk assessment based on that review.
- In the event of suspicious behavior, or a security problem, all staff are required to contact management immediately.
- The company security policy must be reviewed on at least an annual basis.
- The company security policy must be reviewed whenever a change is made to the company's handling of cardholder data. These changes can be to either the company technology environment, or business processes.
- Management shall create a formal Incident Response Plan, ready to be executed in case of a security incident. Responsibility for creating, documenting, updating and distributing this plan shall be formally assigned to one or more specific individuals.
- The above formal Incident Response Plan must be updated as appropriate whenever a staff-member that is responsible for carrying out any part of your Incident Response Plan changes employment status in a way which affects the Incident Response Plan.
- The above formal Incident Response Plan must be tested at least annually, and updated as appropriate.
- The company must have a process in place to educate staff on security issues. This must include training at the time of hiring and at least annually.
- All staff with access to cardholder account numbers must either be known to management and known to be of good character, or must be subject to a background check.
- A list of third-party service providers given access to cardholder data will be maintained, and it will be kept complete and up-to-date.
- A written agreement will be created and enforced to bind third-party service providers given access to cardholder data to be responsible for the security of all cardholder data they deal with. It will include an acknowledgement by the service providers of their responsibility for securing the cardholder data.
- Proper due diligence will be exercised to ensure that service providers under consideration are PCI DSS compliant prior to engaging any service provider.



- A program to monitor service providers' PCI DSS compliance status will be maintained to ensure that cardholder data is shared only with service providers that are (and continue to be) PCI DSS compliant.

SECURITY POLICY FOR MASON COUNTY PUD #1

ALL STAFF with access to credit card processing or data MUST READ THIS DOCUMENT, AND SIGN THE BACK PAGE TO INDICATE THAT THEY UNDERSTAND IT AND WILL FOLLOW IT.



It is absolutely critical that all staff actively protect customer cardholder information from thieves and hackers. This is a legal requirement, and a business requirement, and must not be ignored.

This document is the company security policy. It describes what staff should do, and what they should not do. All staff with access to credit card processing or data are required to have read this document, and follow its directions at all times. **Failure to do so will result in disciplinary action, up to and including immediate termination.**

General Notes

- These policies apply everywhere (to all computers, to all people, etc.) but apply particularly to any computers, devices or records involved with cardholder information such as account numbers, names, and so on.

Computers and Software

- No computers are to be used to store cardholder data (such credit card numbers or information read off a card's magnetic stripe).
- No other computers are to be connected to any Point of Sale terminal (via cables, wireless, or anything else).
- No computers other than virtual terminals are to be used to transmit or share cardholder data over any sort of network.

Information and Records Stored On Computers and Devices

- DO NOT record, copy, or store cardholder information (such as account numbers) on any computer, thumb-drive, CD, DVD, etc. This includes magnetic stripe information, and other information like the three-digit numbers printed on the signature panel of cards.
- It IS allowed to record the last 4 digits ONLY of an account number.
- NEVER, UNDER ANY CIRCUMSTANCES, record, copy, or store cardholder PINs ANYWHERE.

Physical copies of Records (Paper Records, Thumbdrives, CD, DVDs, etc.)

- Cardholder data shall be stored only if strictly necessary, and only for as long as necessary. Data that is prohibited by other parts of this security policy must not be stored at all.
- NEVER, UNDER ANY CIRCUMSTANCES, write down, record, copy, or store cardholder PINs ANYWHERE.
- DO NOT record, copy, or store the three-digit number printed on the signature panel of any card.
- All paper records of cardholder data, and all thumbdrives, CDs, DVDs, etc, holding cardholder data are to be treated like cash. They must be kept in a locked area and access to them must be tightly restricted.
- Paper records or electronic records of cardholder information must not be removed from the secure area without formal management approval and an formal record made.

- Never share cardholder records with anyone outside the company, or with anyone inside the company who does not have management approval to use those records.
- Paper records of cardholder data, and thumbdrives, CD, DVDs, etc, holding cardholder data must not be thrown out or re-used for other purposes. When you are finished with them, they must be destroyed via shredding, using a company or machine approved of by management.
- Paper records or thumbdrives, CD, DVDs, etc, of cardholder data are to be destroyed via shredding after five years, using a company or machine approved of by management.

Transmitting Information and Records

- Cardholder information must never be sent outside the work network unless it is protected by encryption. That encryption can either be on the communications channel (like SSL version3 for the web), or on the data itself (such as PGP). It is NOT enough to use winzip.

Physical Security

- Physical access to all Point of Sale terminals is restricted to those who have formal management approval.
- If you see anyone (staff-member or not) near a Point of Sale terminal who does not have approval, you are required to report it to management immediately.
- All visitors must either be in the presence of a staff member who is responsible for supervising them, or be wearing a visible visitor's badge. All unsupervised visitors who are not wearing a visible visitor's badge must be escorted away from sensitive systems such as computers or paper records, and reported to management immediately.
- Paper records or electronic records of cardholder information must be kept in a locked drawer or box inside a separate room (like a back office), and the door must be locked unless someone with formal management approval is in the room at the time.
- Physical access to paper records with cardholder information on them is restricted to those who have formal management approval.
- If you see anyone (staff-member or not) near such paper records who does not have approval, you are required to report it to management immediately.

Policies and Procedures

- In the event of suspicious behavior, or a security problem, contact management immediately.
- Management is required to have in place a formal incident management plan, ready to be executed in case of a security incident.

Final Comments

This document, and the requirements described in it, helps the company in several important ways:

1. it reduces the chance that the company will be damaged by hackers or thieves.



2. it reduces the chance that customer information will be stolen, and so reduces the chance that the company will be sued.
3. it helps the company comply with an industry standard called the Payment Card Industry Data Security Standard (PCI DSS). Failure to do so can result in large fines, and the termination of the company's credit card processing services.
4. it reduces the chance that customer information will be stolen, and so reduces the chance that the company will be sued.

If you have any questions or comments about this policy, or about security issues, ask your manager.

5). First Data

I have read and understood this policy document, and agree to follow it.

[illegible]

This Document only valid until Mar 6, 2015. It can be revised or updated at <http://www.pcirapidcomply.com>



Firewall and Router Management and Configuration Guide

Introduction

This document is a guide on how to configure and manage your firewalls and routers in order to comply with the Payment Card Industry Data Security Standard PCI-DSS. It has been provided to you by First Data, and while it gives you useful guidance and information, it does not replace the product-specific guides and operations manuals that came with your firewall or router.

Definitions

Firewall: A device and/or software that help protect network resources from unauthorized access through computer networks. It does this by residing in the traffic flow of network communications and blocking bad or unauthorized traffic. This helps separate your systems into different levels of security. Firewalls use a set of rules to identify good versus bad traffic.

Firewalls can either be stand-alone devices or software that operates inside a normal computer or device. Most modern DSL modems or routers come with a built-in firewall.

Router: Hardware or software that connects two or more computer networks (for example, a router might connect your internal network to the outside network. Routers work as a traffic sorter, receiving multiple packets of information intended for multiple destinations, and sending each packet off in the right direction so that it reaches its destination.

DMZ: An acronym for Demilitarized Zone. It is a separate part of your network that provides a middle ground between the external network (which cannot be trusted at all), and your internal private network (which you should be able to trust a great deal). The DMZ is where you should place your network devices like Web Servers, which need to be accessible to the outside world, but which do not need to be directly connected to the highly-trusted internal private network. The DMZ is separated from and protected from, the outside world by a firewall, and the internal private network is also separated from, and protected from, the DMZ by a firewall. External parties and the internet should only be allowed to have direct connections into the DMZ, not the rest of the network.

PCI Requirements

PCI requires that you configure and manage your firewalls and routers in a way that protects your customers and their cardholder data. Failure to do this properly means that you are not compliant with PCI and means that your business and your customers are at increased risk. To comply with PCI, and protect your customers and your business, you must complete and follow the network management plan in the next section.

Network Management

Formal responsibility for the logical management of network devices (computers, routers, switches, modem) has been assigned to the following individuals within the company:

Name of Person	Role and Responsibility in Management of Network
Spencer Jones	IT Manager, Hood Canal Communications
Katie Arnold	Supervisor- Director of Business Services

Network Layout

1. Create a network diagram, showing:
 - what computers and devices you have in your network or connected to your network
 - how these devices are interconnected
 - how cardholder data flows over this network, and in and out of this network
 - where, if applicable, cardholder data is processed inside this network
 - where, if applicable, cardholder data is stored inside this network.

Responsible party within company for this
action/procedure: Katie Arnold & Hood Canal Communications

2. Keep this network diagram current, by updating it whenever anyone changes how computers or devices are interconnected, or adds/removes a computer or device, or changes what these computers or devices do. Perform a formal review annually.

Responsible party within company for this
action/procedure: Katie Arnold & Hood Canal Communications

3. Make sure that before you add or change any external network connections, you formally review the proposed change from a security and compliance perspective, and only proceed once the changes have been shown to be safe and reasonable. Formal approval must be given for the change and the change must be recorded.

Responsible party within company for this
action/procedure: Hood Canal Communications & Katie Arnold.



4. Make sure that before you make any significant changes to how your internal network is laid out, you formally review the proposed change from a security and compliance perspective, and only proceed once the changes have been shown to be safe and reasonable. Formal approval must be given for the change and the change must be recorded.

Responsible party within company for this
action/procedure: Katie Arnold & Hood Canal Communications

5. Make sure that every external or Internet connection into your DMZ has a firewall between the internet and the DMZ, controlling what traffic is allowed to pass in or out.

Responsible party within company for this
action/procedure: NISC

6. Make sure that every network connection between your DMZ and your internal private network has a firewall between the two, controlling what traffic is allowed to pass in or out.

Responsible party within company for this
action/procedure: NISC

Incident Response Plan for MASON COUNTY PUD #1

Instructions:

- This Incident Response Plan was designed specifically for MASON COUNTY PUD #1, based on information you provided to us as you completed the Security Assessment. Because this plan is specific to MASON COUNTY PUD #1, it should not be used by any other entity as a basis for its own Incident Response Plan.
- This Incident Response Plan is intended to relate only to your systems and processes that are involved in processing, transmitting or storing credit or debit card information (your "Card Transaction System"). While the principles, steps and statements outlined and made in this plan may apply generally to other of your systems and processes that are not involved in card transactions, you should not assume this plan is sufficient to cover your entire business.
- Because this Incident Response Plan is specific to the Card Transaction System you described to us as you completed the Security Assessment, modifications to that system may require changes to this plan. If you modify your Card Transaction System, please update your responses to the Security Assessment and, for a period of one year, we will make the necessary changes to this Incident Response Plan for free. An out-of-date Incident Response Plan may give you directions that are no longer suitable, and put your business at risk.
- Please note that the PCI Data Security Standard requires that you test this plan annually. Regular testing of this plan will help ensure that individuals with responsibility under this plan know what they need to do if an actual incident occurs.
- Some elements of this plan could not be generated in advance, because they require input from a responsible party at MASON COUNTY PUD #1. We have provided space for the appropriate information to be added to the document. This Incident Response Plan is NOT complete until that information is provided. If that information has not already been added to the document, we strongly recommend that it be done immediately.
- We recommend that you make copies of this plan available to all relevant staff members, and take steps to ensure that they understand it and what is expected of them.

Having a formal Incident Response Plan, and even following it perfectly, does NOT guarantee that MASON COUNTY PUD #1 will not be damaged by hackers, an accident, or some other event. It DOES help you reduce your risk. If you feel that you need more detailed advice on Incident Response Plans, or on how to implement them, please visit <http://www.pcirapidcomply.com>, or



contact an information security specialist in your area.



Introduction

This document describes a plan for how you should respond in the event of a security incident. It is important to know this in advance, because in the middle of a crisis it is hard to put together a careful plan, especially when key staff members may be unavailable and computers, phones, etc., may not be working.

By 'security incident' we mean any deliberate attacks on your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage your company. Either way, having a plan in place will allow you to react more quickly and intelligently, and help you control the consequences to you and your company.

In broad terms, you should react to a security incident by:

- Immediately investigate the incident to determine what has happened, what harm has been done, and if the incident is still in progress.
- Take action as soon as possible to limit the scope of the damage. This typically includes preventing further unauthorized access to customer or company information. (Keep in mind, though, that in many cases it is impossible to undo the damage already done.)
- Notify those who need to be notified of what has happened, and what you are doing about it.
- Complete your investigation as to what happened and why. Use this opportunity to identify how your security processes and systems could be improved
- Notify all those necessary of your investigation findings.
- Start to make any appropriate changes identified in your findings for improving your security processes and systems.

The rest of this document is spent expanding on the above points, giving useful specific details, and laying out a specific set of actions and responsibilities.



Immediate Investigation

It should already be part of your corporate security policy that all staff are required to report any suspicious behavior or signs of a security problem. If this is not the case, you need to have your security policy revised by a security professional (we can do this for you at very low cost because of the technology we use.)

There needs to be at least one designated person in the organization who will be responsible for dealing with any security problems or questions. If you have computers in your organization, this person needs to either be "computer smart" or have assistance from someone who is. In the table below, put in the CURRENT contact details for anyone you might need in a security emergency:

Name	Phone/Cell 1	Phone/Cell 2	Pager #
Hood Canal Communications		360-898-2481	
Kristin Masteller	360-790-1552		
Katie Arnold	360-490-9914		

When a security incident occurs, or is suspected, this person (or people) should investigate to see if there really is a problem. If there is, then:

- If there is any threat whatsoever of physical harm to staff or others (for example, from a burglar) withdraw immediately and call the police.
- If there is no immediate threat, start a written event log by noting date and time of all actions.
- Your first priority is to limit the damage to your customers and your company (as described in the next section), but your next highest priority should be to try and preserve information about the attack.
- If the attack involved physical evidence (such as from a break-in), do not disturb the area, but call the police.
- If the attack affected computers, make every effort to NOT use the computers: DO NOT log on to them, DO NOT turn them off (this is because doing so destroys forensic evidence of what the attackers did and how they did it.). DO disconnect them from all networks and connections.
- If it is absolutely critical that the computers be used, make copies of any relevant files on a thumbdrive, DVD, or similar, before using them again.
- Try to identify at a high level what damage has been done. Has sensitive information about the company or its customers possibly be stolen, or changed without permission, or destroyed/deleted? Make an estimate of how sensitive this information is, and how many people have possibly been affected.



Limit The Damage

- If there is any chance that damage is still being done (for example, if hackers are still looking at your computer files, or if a computer is still infected with a virus), your first priority must be to limit the damage. Where possible, DO NOT turn computers off, but instead disconnect them from all network connections so that hackers cannot get in (or stay in) and viruses, etc, cannot spread to other devices.
- If there is any physical damage (for example, broken locks on doors) try to secure the area to prevent anyone else from getting in after the fact.
- When you contact the police, ask them to try to recover any stolen property, etc.

Notify Those Who Need To Be Notified

There are some people you should notify because they can help you, and others you need to notify because you are legally obliged to. Contact the first set of people as soon as you know there is a real problem, and contact the second set of people as soon as is reasonable or required.

People to contact as soon as possible (management, police, insurers, etc.):

Name	Contact Info	Why Contacting
Katie Arnold	(360) 490-9914	Office Supervisor
Kristin Masteller	(360) 790-1552	General Manager
Mary Adair- NISC First Data	(866) 999-6472 (800) 365-1998	Billing System Support Billing System Support
Steve Foitle Mason Co. Sheriff	(913) 541-2911 (360) 427-9670 x. 313	Federated Insurance Report theft/crime

People to contact as soon as reasonable (Credit card providers affected, etc.):

Name	Contact Info	Why Contacting
Rob Johnson First Data	(360) 426-9728 (800) 365-1998	District's Attorney (First Data will contact all affected customers)



Depending on your location, where you do business, and what sort of damage was done, you may be required by law to notify any potentially-affected customers directly. You will need to consult a lawyer to clarify this point.

Complete The Investigation (within 3 days if possible)

Investigating the problem may be expensive if over-done, so you need to look at how serious the problem might be (use the worst-case scenario to estimate this) and decide how much time and effort you should put into the investigation. (After all, it does not make sense to spend a thousand dollars trying to figure out who broke your hundred-dollar ancient computer.)

At a minimum, you should try to figure out: When the attack happened, over what time period, what the damage was (for example, what data was affected, what happened to it, which people were affected), and how the attack succeeded (if it did).

Try to figure out what could have been done to prevent the attack from causing damage.

Report Your Findings

As a result of notifying people above, you probably have been asked for reports on what happened and why. Decide who needs this information, and/or has a legal right to it, and give them a copy of your investigation report. Remember that some of this information might be very sensitive, and where appropriate, you can give people a partial version with some information removed.

Implement The Recommendations

Based on what your investigation found, try to improve your security solutions so that the same thing cannot happen again. Remember that security solutions includes things like training and processes, not just software and "computer stuff".

609 Employee Recognition

Effective Date: 08/13/2021

609.1 Purpose

609.2 Definition

609.3 Policy

609.1 **Purpose**

To establish procedures and guidelines under which Mason County Public Utility District (PUD) No. 1 funds can be utilized for the purpose of employee recognition.

609.2 **Definition**

Employee Recognition: For the purpose of this policy, employee recognition means any award, time in service, prize, meal, entertainment or event that is intended specifically to promote good will, foster a sense of pride in affiliation with the District, promote safety, productivity, reliability, efficiency, dedication, and longevity commitment to the community and/or cost savings for the District among the PUD employees.

609.3 **Policy**

609.3.a The PUD or its individual departments or work units may, subject to budgetary authority, expend funds for the purpose of employee recognition. This amount will be budgeted on an annual basis and may be adjusted annually on the recommendation of the General Manager. The General Manager must authorize the expenditure of funds for the purpose of employee recognition.

609.3.b

Service Award Table

Effective January 1, 2012, all employees will receive service awards only for the specific anniversary date that they have reached.

Years of Service	Examples of Recognition Items with District Logo	Maximum Value
1	Logo Item	\$30
5	Items to be determined	\$50
10	Items to be determined	\$75
15	Items to be determined	\$100
20	Items to be determined	\$130
25	Items to be determined	\$160
30	Items to be determined	\$190
35	Items to be determined	\$220
40	Items to be determined	\$250

609.3.c Employee recognition events, contests or awards programs are subject to the following requirements:

- a. The award program or contest must be preceded by written criteria which clearly delineate 1) the rules, procedures or basis for eligibility for the program or contest: and 2) the procedure to be used in determining the winner of the award or prize;
- b. A written description of the type of award or prize which will be given must be available to all eligible employee in advance: and
- c. The award program or contest must, within reason and consistent with the purpose of the program, be designed to include as many employees as possible.

609.3.d Once yearly, the District may have a company picnic or party for employee appreciation and recognition of the above rewards. The maximum amount of this event is \$2,500.00. The District may also conduct other staff appreciation events as approved by the General Manager, such as twice-annual service award recognitions (when applicable) and a winter party or similar gathering, with a maximum of \$2,500.00 allowed for expenses.

This policy applies equally to all employees.

Adopted this day on September 28, 2021 at a regular meeting of the Board of Commissioners.

Mike Sheetz – President

Jack Janda - Vice President

Ron Gold –Secretary

A SUMMARY OF CHANGES TO THE HANDBOOK:

1. Replaced Kristin's name for Steve's
2. Added PUD's Core Values
3. Replaced "our Company" with "the District" and / or Mason County PUD No. 1
4. Updated the handbook with gender neutral pronouns instead of "he / she, her/ him"
5. Updated language to include all protected classes in the EEO and Harassment policies, as well as Company IT Resources.
6. Removed language regarding open source software policy since we do not use.
7. Added language in Personal Appearance for examples of acceptable business attire.
8. Added Workplace Searches policy as recommended by Employment Law Attorney
9. Updated language for Pregnancy Disability Leave policy to coincide with current law.
10. Removed reference to Washing Family Leave Act as it is no longer in effect and was replaced by Washington Paid Family Medical Leave Act.
11. Removed reference to Short Term Disability Coordination since PUD 1 does not have STD.
12. Added language in Domestic Violence Leave to include reasonable safety accommodations as per 2018 law.
13. Added language under "Safety" to include the proper use of cell phones when operating a vehicle.



Mason County Public Utility District No. 1

EMPLOYEE HANDBOOK

September 28, 2021

TABLE OF CONTENTS

WELCOME.....	4
PURPOSE OF THE HANDBOOK.....	5
POLICIES AND PRACTICES	6
EQUAL EMPLOYMENT OPPORTUNITY	6
PAY PERIODS AND PAY DAYS.....	6
EMPLOYEE CLASSIFICATIONS	7
OVERTIME	7
OPEN DOOR	7
USE OF CELL PHONES.....	8
TRAVEL POLICY	8
STANDARDS OF CONDUCT	11
STANDARDS OF CONDUCT	11
HARASSMENT	12
USE OF COMPANY IT RESOURCES AND COMMUNICATION SYSTEMS	13
CELLULAR PHONE, REIMBURSEMENT AND DISTRICT PAYMENTS.....	18
DRUG AND ALCOHOL FREE WORKPLACE.....	19
WORKPLACE VIOLENCE	19
PERSONAL APPEARANCE.....	20
RETURN OF PROPERTY.....	20
RESIGNATION	20
REPORTING (WHISTLEBLOWER ACT).....	21
CORRECTIVE DISCIPLINE	23
PROBLEM RESOLUTION	24
USE OF KEYS & SECURITY CODES	25
DATING/PERSONAL RELATIONSHIPS IN THE WORKPLACE	26
CONFLICTS OF INTEREST.....	26
OUTSIDE EMPLOYMENT	27
WORKPLACE SEARCHES	28
BENEFITS	28
BENEFITS	28
HEALTH INSURANCE	28
LIFE INSURANCE	29
LONG-TERM DISABILITY	29
EMPLOYEE ASSISTANCE PROGRAM	29
BENEFITS CONTINUATION (COBRA)	30
RETIRED EMPLOYEES MEDICAL INSURANCE	31
EDUCATIONAL ASSISTANCE.....	32
PAID TIME OFF (PTO)	35
WASHINGTON STATE PAID SICK LEAVE (CHAPTER 49.46 RCW).....	37
MILITARY LEAVE.....	41
UNPAID LEAVE	41

BEREAVEMENT	42
PREGNANCY DISABILITY LEAVE	43
SHARED LEAVE POLICY & PROCEDURES	44
FAMILY & MEDICAL LEAVE.....	46
JURY DUTY.....	59
WORKPLACE HEALTH AND INJURY	60
ACCIDENT REPORTING.....	60
SAFETY	60
SMOKING	61
USE OF EQUIPMENT & VEHICLES.....	62
EMERGENCY CLOSINGS	65
ACKNOWLEDGMENT	66

WELCOME

It is my pleasure to welcome you to Mason County PUD No. 1 ("PUD 1 or the District"). We take great pride in our excellent public service model and in our positive and safe work culture.

MASON COUNTY PUD NO. 1 hopes to provide a stimulating work environment, opportunities for personal growth, and job satisfaction. We recognize that our employees are our most valuable resource. We depend on you to help our District meet its mission to provide safe, reliable and valued utility services to the public.

At MASON COUNTY PUD NO. 1, we feel that it is important that we share common values. Our core values are:



We expect our team to take pride in their work and respond to our customers, fellow employees and other stakeholders with the highest integrity. We have a reputation for going the extra mile to serve our community.

On behalf of everyone here at MASON COUNTY PUD NO. 1, we welcome you to our team. We hope you will find your employment with us a rewarding and challenging experience.

Kristin Masteller, General Manager

PURPOSE OF THE HANDBOOK

The purpose of this handbook is to help you find answers to some of the basic questions regarding your employment with the District. The following policies are not intended to be, nor do they create, a contract for employment. They are only intended to be guidelines, which describe the District's general philosophy concerning policies and procedures. The District reserves the right to amend, modify, or discontinue any benefit or policy at its sole discretion, with or without prior notice. The provisions of this handbook take precedence over all other oral and written representations, which may have been made by District representatives. Employment at the District is "at-will", meaning that both you and the District have the right to terminate the employment relationship at any time with or without reason or notice. No representative of the District has any authority to enter into any agreement for employment for any specified period of time or to make other commitments or promises or assure any benefit or terms and conditions of employment unless such promises are made in writing and signed by the General Manager of the District.

This employee handbook does not negate any provisions in an applicable Collective Bargaining Agreement or Civil Service Rule. If there is a conflict with any provision in this handbook, the Collective Bargaining Agreement or Civil Service Rule will apply.

This Employee Handbook presents an overview of the policies, benefits and work environment of Mason PUD 1. Please read the handbook carefully. It is important that you familiarize yourself with both your rights and responsibilities as an employee of the District. If you wish more detailed information on any of these policies or have other questions, please feel free to direct them to your immediate supervisor or any District executive.

EQUAL EMPLOYMENT OPPORTUNITY

MASON COUNTY PUD NO. 1 is an equal opportunity employer. We believe that every employee has the right to work in surroundings which are free from all forms of discrimination. It is our policy that all decisions involving any aspect of the employment relationship will be made without regard to race, religion, color, national origin, age, sex, genetic information, the presence of a sensory, physical, or mental disability, marital status, honorably discharged veteran or military status, citizenship or immigration status, sexual orientation, gender identity, and status as a victim of domestic violence, sexual assault, or stalking or on any other basis protected by federal, state, or local law. Discrimination and/or harassment based on any of those factors contradicts our philosophy of doing business and will not be tolerated.

If you feel that you have been a victim of or witness to discrimination, you must notify your supervisor or the Human Resources Manager. If you have communicated your concerns to that individual without appropriate results, contact any member of the executive management team, including the General Manager. No employee will be retaliated against in any way for bringing a complaint under this policy to management. A timely, full, and complete investigation of any complaint will be undertaken. Confidentiality will be respected on a need-to-know basis.

Any employee found in violation of this policy shall be subject to appropriate discipline, up to and including discharge.

With regard to qualified applicants or employees with disabilities, the company offers "reasonable accommodation" to enable a person to perform the job.

Employees concerned about company conduct or who have questions in the area of non-discrimination or reasonable accommodation should direct any inquiry to their supervisor or a member of the executive management team.

PAY PERIODS AND PAY DAYS

All employees are paid on semimonthly on or before the 5th and 20th days of the month. Each paycheck will include earnings for all work performed through the end of the previous payroll period. Pay periods are from the 1st through the 15th, and the 16th through the end of the month.

In the event that the 5th of the 20th falls on a weekend or holiday, employees will be paid on the preceding working day.

All employees must maintain a personal record of hours worked, using the Company-provided time sheets and submitting these time sheets to their supervisor at the end of each pay period.

Any paycheck deductions, which are not specifically required by law, must be authorized by you in writing in order to take effect. The District does not permit draws against wages.

The District takes precautions to ensure that employees are paid correctly. In the event of an error, we will make every attempt to adjust the error no later than your next regular pay

period. Employees should notify the Payroll Department of any suspected error as soon as possible.

EMPLOYEE CLASSIFICATIONS

All employees are categorized as either Exempt or Non-exempt for overtime purposes.

Exempt: an employee who is exempt from the overtime provisions of federal and state law. Executive, professional, administrative, computer-related, or outside sales positions, as defined by federal wage and hour law, are classified as exempt.

Non-exempt: an employee who is not exempt from the overtime provisions of federal and state law. Non-exempt employees are entitled to receive overtime for all hours worked beyond 40 in a workweek.

All employees are also categorized as being a Regular Full-Time employee, Regular Part-Time employee, or a Temporary employee.

Regular Full-Time: an employee who is regularly scheduled to work 40 hours per week. Full-time employees are generally eligible for the complete company benefit package.

Regular Part-Time: An employee who is regularly scheduled to work less than 40 hours per week.

Temporary: an employee who is hired for a specific period of time (such as a fill-in for a vacationing employee) or for the duration of a specific project is considered temporary. Temporary employees are not eligible for benefits, unless otherwise provided by law.

OVERTIME

When operating requirements or other needs cannot be met during regular working hours, employees may be scheduled to work overtime. When appropriate, advance notification of these mandatory assignments will be provided. All overtime work must receive the supervisor's prior authorization. Overtime assignments will be distributed equitably as practical, subject to the organizational requirements as determined by the manager or their designee to all employees qualified to perform the required work.

Overtime compensation is paid to all nonexempt employees at double time. Overtime pay is based on actual hours worked. Vacation time or any leave of absence will not be considered hours worked for purposes of overtime.

OPEN DOOR

Employees are encouraged to share their concerns, seek information, provide input, and resolve problems/issues through their immediate supervisor and, as appropriate, consult with any other member of management or the human resources department. Managers, supervisors, and members of the human resources are expected to listen to employee concerns, to encourage their input, and to work towards solutions to the presented problems/issues.

USE OF CELL PHONES

Cell phones can be a valuable tool for servicing our customers. However, cell phones (whether company-provided or personal) may not be used to conduct company business while operating a vehicle. If you have a hands-free telephone device, you may use it while driving; otherwise, should you need to use your cell phone, you must pull off the road, park, and make or receive the call. Reading, typing or sending a text message, while driving, is strictly prohibited by law.

During work hours within the office, employees should keep cell phones on silent. While occasional, brief personal phone calls are acceptable, frequent or lengthy personal calls can affect productivity and disturb others. Personal calls should be made during non-work hours or breaks wherever possible.

Use of cell phones is strictly prohibited while performing traffic control and other safety-sensitive work in the field. As a general rule, cell phones should be put away until break periods.

TRAVEL POLICY

This policy sets forth conditions of allowable travel, travel expenses, authorization and reimbursement for persons on official District business. (Employee includes Commissioners) Mason County PUD No. 1 adheres to IRS Code Section 463, under "An Accountable Plan".

Administration of this policy is the responsibility of the General Manager. It is the responsibility of each employee to review this policy and understand its intent and requirements prior to departure.

Claimed travel expenses will be authorized only when essential to the transactions of official District business. Travelers are expected to exercise prudence in incurring expenses.

All travel plans require prior approval of respective Department Directors. Airline tickets, car rental, and hotel reservations may be arranged through Human Resources or Accounting.

Required Approval:

- Commissioners, Attorney, General Manager - Authorized by the Commission/GM
- Department Directors - Authorized by the General Manager
- All other employees - Authorized by the Department Director (supervisor)
- All travel outside the continental United States and British Columbia - Authorized by the Commission

Travel arrangements shall be made for the most direct routing, taking the shortest, reasonable amount of District time. Any other routing, except as required in order to obtain reasonable accommodations and schedules, is presumed to be for the personal benefit of the traveler with the excess cost payable by the traveler.

Employees shall make every reasonable effort to travel on the same day as the meeting's beginning or end. Exceptions to this must have prior approval from the Department Directors.

Because of varied costs associated with travel dates, distances and locations, three types of travel reimbursement are recognized by the District:

1. Company or Personal charge card
2. Per Diem in accordance with Federal GSA Per Diem Rates

3. Reimbursement for Actual Cost with Department Director and General Manager approval

Credit Cards:

The District will allow travel expense to be charged on District-sponsored charge cards or personal charge cards to be reimbursable to the employee. Itemized receipts will be required. The District may at the employee's request, provide a District credit card to each employee when traveling on company business and/or meets the qualifying criteria as determined by the Department Director or General Manager.

No personal expenses are allowed on company credit cards.

All non-exempt employees shall be required to return District credit cards to the finance department upon return from business travel. Upon separation from the District, all employees must return all District-issued credit cards to the finance department.

Per Diem:

Per Diem is available for meals and incidental expenses for overnight travel. If an employee is representing the PUD at a meeting or conference outside the local area (defined as District services areas, Mason County and South Jefferson County) Per Diem shall be paid at \$45 for the first and last full day of overnight travel and \$65 for any additional overnight days of travel.

When a meal is provided by an organization or included in a membership registration fee, the per diem rate will be reduced by Breakfast \$12, Lunch \$18 and Dinner \$35. In the event of a part day travel then meals will be covered in accordance to the set meal rate.

Incidental expenses are \$5.00 per day.

Excess reimbursement of travel advances must be reimbursed upon return.

Actual Expense within Mason County and South Jefferson County:

Expenses related to local business travel and meetings (within Mason County and South Jefferson County) are reimbursed according to actual cost. Receipts must be itemized when submitted for reimbursement or for purchases made with the District credit card.

Subsistence expense within Mason County and South Jefferson County is not considered a travel expense, but rather a business meeting or hosting expense. Subsistence expense incurred within Mason County and South Jefferson County shall be reimbursed at actual expense, and must be approved by the employee's Department Director or the General Manager.

Air Travel Policy:

The District pays for coach class air travel for the employee. The District does not pay for air travel for the employee's family members.

Travel arrangements should be made 15 days in advance if possible to take advantage of the most economical rate. Every effort should be made to take advantage of government rates and other reduced fares.

If there are penalties associated with changing reservations, the District will pay for these, provided the District required the change or the change was beyond the control of the employee. Penalties or cancellation charges incurred for personal reasons will be the responsibility of the employee.

Travel to and from Terminals:

Travel to and from airport terminals should be by a reasonable method available consistent with business requirements; e.g.; ride share, car rental, airport bus, limousine or taxi. On trips of more than one day's duration, long-term or economy parking should be used and receipts attached to the expense report.

District Owned Vehicles:

Every reasonable effort should be made to use District vehicles when official business requires automotive transportation, and pool travel in one vehicle when possible. District-owned vehicles are not to be used for personal purposes, except for incidental stops that are along the route to be traveled.

Non District Personnel may ride in the District-owned car as long as such use is handled with discretion and, approved by the General Manager. The fact that a spouse is going along on a business trip is not sufficient reason to request use of a personal car.

Driving District-owned vehicles requires thoughtful discipline, constant attention to safe driving practices, observation of traffic laws and regulations, and recognition that driving safety and courtesy.

An employee operating a District vehicle shall have a current and valid driver's license in his or her possession while driving. Parking of District vehicles at employees' homes for extended periods of time or on a regular basis is prohibited unless specifically permitted by the General Manager.

Rental Car:

When possible, District vehicles will be used for employee travel outside the District on District business. Rental vehicles may be used for District business if necessary and by approval of the Department Director or General Manager.

District insurance provides for collision coverage for a rental vehicle used for District business. Additional insurance coverage is at the employee discretion and expense. Fuel and associated costs, such as parking fees, are paid by the District when on official business; and, by the employee (at the current IRS rate) when the District or rental vehicle is used for personal business.

The rental car should be returned immediately following the completion of District business with a full tank of fuel. Rental charges must be supported by a receipt and should be charged to a credit card.

Use of Personal Automobile:

When a privately owned vehicle is used (such as when a car is needed but no District vehicle is available), reimbursement for official travel will be adjusted according to the current reimbursement schedule approved by the Commission, plus tolls and reasonable parking charges. When traveling, such reimbursement will not exceed the cost of commercial air fare, including mileage to and from the airport, airport parking fees, transportation to and from destination airport to motel and/or meeting place, and those motel and meal expenses that would have been incurred with air travel for the same trip. Employees traveling by personal automobile on company business are required to carry, at the employee's expense, liability and property damage insurance at the minimum required by law, and that policy shall be primary.

Lodging:

When making reservations, request the least expensive rate available, usually the government rate. When lodging is part of the official business "package" an employee may use or reserve the accommodations provided. That is, if meetings are held in hotel/motel-owned facilities, or if arrangements have been made to reserve a block of rooms for participants, it is sufficient reason to use such accommodations.

When lodging expense is increased because it includes family members traveling with the employee, the employee shall pay the difference in cost. Suite accommodations are not permitted; the District pays only for standard single rooms.

Receipts will be required for all charges and should be charged on a District or personal credit card. The charges, when shown on the expense report form, should be itemized to show meals, telephone charges, etc.

In-room movies and use of the mini-bars are considered personal expenses and not reimbursable. These expenses should not be reflected among the charges on the District-issued credit card.

STANDARDS OF CONDUCT

STANDARDS OF CONDUCT

Acts which are offensive or threatening to the safety of others will not be tolerated. The following are examples of conduct which may result in discipline, up to and including discharge. This list may be modified at any time and is for illustration purposes only and should not be considered exhaustive.

1. Insubordination, including deliberate failure or refusal to follow a supervisor's directions or to perform assigned work.
2. Theft from the company or other employee(s) and failure to report theft or concealment of theft.
3. Giving false or misleading information as a means of obtaining employment.
4. Falsifying company records, such as but not necessarily limited to payroll timesheets, production records, invoices, etc.

5. Conducting work under the influence of any alcohol, marijuana, controlled substance, or drug not medically authorized, or other substances which impair job performance or pose a hazard to the safety and welfare of the employee, other employees, or the general public.
6. Assault, altercations or fighting.
7. Immoral, indecent, illegal or other questionable conduct which occurs on or off company premises and reflects unfavorably upon the employee's ability to perform his/her job.
8. Possessing weapons on company premises.
9. Interfering with or obstructing production.
10. Sleeping on duty.
11. Unexcused failure to call in before the start of shift to report absence or tardiness.

HARASSMENT

It is the policy of the District to maintain a work environment free from all forms of harassment on the basis of any status or characteristic protected by law.

The District prohibits harassment by and toward employees, managers, and non-employees such as customers, vendors, or contractors. Unacceptable conduct includes offensive verbal comments, use of ethnic slurs or derogatory terms, stalking, intimidation, physical assault or battery relating to a person's race, religion, color, national origin, age, sex, genetic information, the presence of a sensory, physical, or mental disability, marital status, honorably discharged veteran or military status, citizenship or immigration status, sexual orientation, gender identity, and status as victim of domestic violence, sexual assault, or stalking or on any other basis protected by federal, state, or local law.

Examples of prohibited discriminatory harassment include, but are not limited to:

- use of ethnic slurs or derogatory terms relating to an individual's gender or sexual orientation;
- distribution of racially or sexually offensive e-mail or other electronic communications; and/or
- threatening, intimidating, or hostile acts directed at a sex or religious group or directed at an individual because of their sexual orientation, color or ethnicity.

Harassment does not require intent to offend. Thus, inappropriate conduct or language meant as a joke, a prank, or even a compliment can lead to or contribute to harassment. Sexual or other harassing conduct, even if not unlawful, will not be tolerated. For example, a stray comment that degrades an employee's gender may not be unlawful harassment, but it is an example of prohibited conduct under this policy.

Sexual harassment is a specific type of discriminatory harassment. This includes comments or conduct of a sexual nature and behavior that tends to threaten or offend an employee or third party. Any behavior by a manager, supervisor, employee, or non-employee which constitutes unwelcome sexual advances, requests for sexual favors, the display of sexual images, use of the Internet to display or distribute sexually explicit images or messages and verbal or physical conduct of a sexual nature violates this policy, including when:

1. Submission to such conduct is made a condition of an individual's employment;
2. Submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual; and/or
3. Such conduct has the purpose or effect of interfering with an individual's work performance or creating an unfriendly or offensive work environment.

This policy prohibits unacceptable harassment or conduct in the workplace and at company sponsored business and social events, or events with co-workers entirely unrelated to the workplace. Additionally, harassment via social media, email and text messages are within the scope of prohibited conduct; for example, a harassing post on an employee's private Facebook page violates this policy if it is about a co-worker or customer.

If you believe that you have been the object of harassment or conduct in violation of this policy, or if you witness harassment or inappropriate conduct, report the incident to the Human Resources Manager. If the individual from Human Resources is the cause of the problem, seems unwilling to resolve the issue, or appears unresponsive, please contact the General Manager. Any supervisor or manager who witnesses an act of harassment or who receives a complaint of harassment and fails to take appropriate action, which includes reporting the act or complaint to Human Resources, may be subject to disciplinary action.

All complaints about an employee or non-employee will be thoroughly and promptly investigated. Every complaint will be kept confidential to the maximum extent possible. All employees have an obligation to cooperate in an investigation of harassment complaints. The results of any investigation will be communicated to the complaining employee(s). Prompt and appropriate corrective action will be taken if the company concludes that an employee or non-employee has engaged in harassing conduct, even if the conduct is not unlawful. Corrective action may include discipline up to and including termination of employment or the relationship with the non-employee.

Complaining employee(s), witnesses to an investigation, and employees associated with a complaining employee or witness, such as a spouse, will be afforded protection from retaliation. Examples of prohibited retaliation include: discharge, material changes to terms and conditions of employment, and ostracism or disparagement of an individual. Retaliation is prohibited even in the case where an underlying complaint, made in good faith, has no merit. No employee may be subject to retaliation for bringing a complaint of harassment, filing a Charge of Discrimination or lawsuit, or for participating as a witness in an investigation, Charge or lawsuit.

Employees who believe they have been subject to retaliation must immediately bring it to the attention of Human Resources or the General Manager. Complaints of retaliation will be investigated and addressed according to this policy.

USE OF COMPANY IT RESOURCES AND COMMUNICATION SYSTEMS

The District wishes to establish its expectations of employees who use its IT Resources, computer, and communications systems for e-mail, text messaging, chat, video conferencing or to access the Internet.

District-owned computers, networks, communications systems, and other IT resources are intended for business purposes only (except for limited personal use as described below) during working time and at all other times. To protect Mason PUD 1 and its employees, it is the company's policy to restrict the use of all IT resources and communications systems as

described below. Each user is responsible for using these resources and systems in a productive, ethical, and lawful manner.

The company's policies prohibiting harassment and discrimination apply to the use of the company's IT resources and communications systems. No one may use any communications or computer system in a manner that may be construed by others as harassing or offensive based on to race, religion, color, national origin, age, sex, genetic information, the presence of a sensory, physical, or mental disability, marital status, honorably discharged veteran or military status, citizenship or immigration status, sexual orientation, gender identity, and status as a victim of domestic violence, sexual assault, or stalking or on any other basis protected by federal, state, or local law.

The use of the District's IT resources and communications systems by an employee shall signify their understanding of and acknowledgement of the terms and conditions of this policy, as a condition of employment.

Administration of this Policy. The Director of Business Services and Contracted IT department are responsible for the administration of this policy. If you have any questions regarding this policy, please contact the Human Resources Department.

Security, Access, and Passwords. Security of the District's IT resources and communications systems is the responsibility of the Information Technology (IT) Department, including approval and control of employees' and others' access to systems and suspension or termination of access in cases of misuse and when a user is no longer an employee or otherwise is ineligible to use the systems.

It is the responsibility of each employee to adhere to IT security guidelines including but not limited to the creation, format, and scheduled changes of passwords. All usernames, pass codes, passwords, and information used or stored on the company's computers, networks, and systems are the property of Mason PUD 1. No employee may use a username, pass code, password, or method of encryption that has not been issued to that employee or authorized in advance by the company.

No employee shall share usernames, pass codes, or passwords with any other person. An employee must immediately inform the IT Department if they know or suspect that any username, pass code, or password has been improperly shared or used, or that IT security has been violated in any way.

Resources and Systems Covered by This Policy. This policy governs all IT resources and communications systems owned by or available at the District, and all use of such resources and systems when accessed using an employee's own resources, including but not limited to:

- Email systems and accounts.
- Chat
- Video conferencing (such as Microsoft Teams)
- Internet and intranet access.
- Telephones and voicemail systems, including wired and mobile phones, smartphones, and pagers.
- Printers, photocopiers, and scanners.
- Fax machines, e-fax systems, and modems.

- All other associated computer, network, and communications systems, hardware, peripherals, and software, including network key fobs and other devices.
- Closed-circuit television (CCTV) and all other physical security systems and devices, including access key cards and fobs.

No Expectation of Privacy. All contents of the District's IT resources and communications systems are the property of the company. Therefore, employees should have no expectation of privacy whatsoever in any message, file, data, document, facsimile, telephone conversation, social media post, conversation, or any other kind or form of information or communication transmitted to, received, or printed from, or stored or recorded on the company's electronic information and communications systems.

The District reserves the right to monitor, intercept, and review, without further notice, every employee's activities using the company's IT resources and communications systems, including but not limited to email (both outgoing and incoming), telephone conversations and voice mail recordings, instant messages, and internet and social media postings and activities, and you consent to such monitoring by your acknowledgement of this policy and your use of such resources and systems. This might include, without limitation, the monitoring, intercepting, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages, communications, postings, log-ins, recordings, and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The company may also store copies of such data and communications for a period of time after they are created, and may delete such copies from time to time without notice.

Do not use the company's IT resources and communications systems for any matter that you desire to be kept private or confidential from the company.

Network Systems. Mason PUD 1 maintains integrated computer and data communications networks to facilitate all aspects of its business. No employees should access, attempt to access, alter, or delete any network document except in furtherance of authorized District business.

Downloading and Installing Software/Website Agreements. Email and downloading from the internet are prime sources of viruses and other malicious software. Therefore, no one may download or install any software or shareware to their hard drive that is not expressly authorized or approved by the IT Department. In addition, employees may not accept the terms or conditions of website agreements without first obtaining approval from the IT Department.

Confidentiality and Proprietary Rights. Mason PUD 1's confidential information and intellectual property (including trade secrets) are extremely valuable. Treat them accordingly and do not jeopardize them through your business or personal use of electronic communications systems, including email, text messaging, internet access, social media, and telephone conversations and voice mail. Disclosure of the company's confidential information to anyone outside the District and use of the company's intellectual property is subject to the company's Confidentiality Policy. Ask your manager if you are unsure whether to disclose confidential information to particular individuals or how to safeguard the company's proprietary rights.

Do not use the District's name, brand names, logos, taglines, slogans, or other trademarks without written permission from the District.

This policy also prohibits use of the company's IT resources and communications systems in any manner that would infringe on or violate the proprietary rights of third parties. Electronic communications systems provide easy access to vast amounts of information, including material that is protected by copyright, trademark, patent, and/or trade secret law. You should not knowingly use or distribute any such material downloaded from the internet or received by email without the prior written permission of the District's Legal Counsel.

Email and Text Messaging. Mason PUD 1 provides certain employees with access to email and/or text messaging systems for use in connection with performing their job duties. MASON COUNTY PUD NO. 1 seeks to provide stable and secure email and text messaging systems (including SMS and internet-based instant messaging) with rapid, consistent delivery times that promote communication for business purposes without incurring unnecessary costs or generating messages that are unproductive for the recipient. Many of the policies described below governing use of the company's email and text messaging systems are aimed at reducing the overall volume of messages flowing through and stored on the network, reducing the size of individual messages, and making the system more efficient and secure.

Spam. Unfortunately, users of email and text messaging will occasionally receive unsolicited commercial or bulk messages (spam) which, aside from being a nuisance and a drain on IT resources, might be a means to spread computer viruses and other malicious software. Avoid opening unsolicited messages and report any suspicious messages to the administrator. Delete all spam immediately. Do not reply to the message in any way, even if it states that you can request to be removed from its distribution list. If delivery persists, contact the email administrator who will block any incoming messages from that address.

Users should be aware that spammers have the ability to access email addresses that are listed as senders or recipients on email messages, on websites, user discussion groups, and other internet areas. Therefore, you should be cautious about using and disclosing your company email address.

Personal Use of Company-Provided Email. The email system is District property and is intended to be used during working time for business purposes only. However, personal use of company-provided email is permitted on non-working time, such as authorized breaks or meal periods, only so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity.

Internet and Social Media. Mason PUD 1 expressly reserves the right, without further notice, to monitor and review records of all websites visited by you, any postings or downloads you make while visiting websites, and during your other internet activities using the company's IT resources and communications systems, and you consent to such monitoring and review by your acknowledgment of this policy and your use of internet access provided by the company.

Using the internet (including social media) to access pornographic, sexually explicit, or "hate" sites, or any other website that might violate law or District policies against harassment and discrimination is never permitted.

Use of Social Media. Mason PUD 1 respects the right of any employee to use social media. However, to protect the company's interests and ensure employees focus on their job duties, employees must adhere to the general internet use guidelines and rules in this policy, and the following related specifically to social media use:

Like other uses of the internet, occasional personal use the company's computers, networks, and other IT resources for social media activities is authorized, so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity.

- Remember that anything you post or send using social media, even outside the workplace, could reflect on Mason PUD 1, in addition to yourself, and might create legal liabilities for the District or damage its business or reputation.
- To avoid the risk of the company incurring legal liability or business damage as a result of your use of social media, even outside of the workplace, remember that you are solely responsible for all content that you post or send. If you identify yourself as an employee of Mason PUD 1, you may not identify yourself as a representative of Mason PUD 1 and it is recommended that you include a disclaimer that your views do not represent those of your employer. For example, consider such language as "the views expressed by me do not represent the views of my employer". This is necessary to avoid damage to the District's business reputation and goodwill in the community
- If your job duties require you to speak on behalf of the company in a social media environment, you must be authorized by the General Manager to act as the District's representative or must otherwise seek approval for such communication from the General Manager. Likewise, if you are contacted for the District's comment for any publication, including any social media outlet, direct the inquiry to the General Manager and do not respond without written approval. Note that Mason PUD 1 owns all social media accounts used for business purposes on behalf of the District, including any and all content associated with each account, such as followers and contacts. The District owns all such information and content regardless of the employee that opens the account or uses it, and will retain all such information regardless of separation of any employee from employment with Mason PUD 1.
- Do not post or send anything through social media that your co-workers or customers, clients, business partners, suppliers, vendors, or other stakeholders of Mason PUD 1 or its affiliates could reasonably find offensive, including ethnic slurs, sexist comments, discriminatory comments, or obscenity.
- If you are unsure about the appropriateness of any posting or communication, discuss it with your manager and refrain from making the posting or communication until you have had it approved.
- If you see content in a social media environment that reflects poorly on Mason PUD 1 or its stakeholders, notify your manager immediately. Protecting the District's goodwill and business reputation is part of every employee's job.
- Finally, keep in mind the speed at which information can be relayed through social media, and the manner in which it can be misunderstood and distorted by readers and subsequent re-posters. Accordingly, the District urges all employees not to post information regarding the utility or their jobs that could lead to morale issues in the workplace or that might detrimentally affect Mason PUD 1's goodwill or business reputation.

Personal Use of Telephone and Voicemail. We recognize that employees might occasionally need to use company telephones and voicemail for personal activities. We authorize occasional personal use of the company's telephones and voicemail systems so long as it

does not comprise unprofessional or inappropriate conversations or messages, and does not interfere with your employment responsibilities or productivity. Company telephones may not be used for commercial, religious, or political solicitation, or to promote outside organizations.

Inappropriate Use of Company IT Resources and Communications Systems. You are never permitted to use the company's IT resources and communications systems, including email, text messaging, internet access, social media, telephones, and voicemail, for any inappropriate or unlawful purpose. This includes but is not limited to:

- Misrepresenting yourself as another individual or company.
- Sending, posting, recording, or encouraging receipt of messages or information that may be offensive because of their sexual, racist, or religious content.
- Revealing proprietary or confidential information, including official Mason PUD 1 information, or intellectual property without authorization.
- Conducting or soliciting illegal activities.
- Representing your personal opinion as that of Mason PUD 1.
- Interfering with the performance of your job or the jobs of other District employees.
- For any other purpose that violates District policies or practices.

Discipline. Employees who violate any provision of this policy are subject to discipline, up to and including termination of employment.

Conduct Not Prohibited by This Policy. This policy is not intended to restrict communications or actions protected or required by state or federal law.

CELLULAR PHONE, REIMBURSEMENT AND DISTRICT PAYMENTS

Mason PUD 1 recognizes the need to provide efficient, cost effective communication equipment and services to meet our business goals. This policy defines the conditions under which the District shall reimburse for technology expenses for the District business.

A District supplied cellular phone or stipend requires the approval of the employee's General Manager. Written request for a cell phone shall be submitted by the Department Director and will include justification supporting the need for cellular communication for District business.

COMMISSIONERS & KEY EMPLOYEES

- Commissioners and key employees authorized for a District issued phone or a payroll stipend for their personal cellular phones, in which case the employee or commissioner will be responsible for entering into a contract for cellular service with the provider of their choice. The District will not be responsible, in any way, for the commissioner/employee's personal cell phone and/or associate service, regardless of the type of use, including inappropriate charges, a lost/stolen phone or delinquent payments.
- For commissioners/employees who desire to carry the cell phone and respond to District business during and outside of normal business hours (e.g., WPUDA, ENW), the reimbursement will be \$30 per month.
- For commissioners/employees who frequently travel outside the District, or who have a demonstrated business need for enhanced communications options (such as email) while away from their home, the reimbursement will be \$65 per month.

- This amount shall be reviewed annually.

RESPONSIBILITY

The Commissioners shall be responsible for approval of any changes to this policy. The General Manager shall be responsible for the administration of this policy, and for recommending to the Board of Commissioners.

DRUG AND ALCOHOL FREE WORKPLACE

It is the goal of Mason PUD 1 to foster a safe and healthy work environment, free from the behavior altering effects of drugs and alcoholic beverages. Use of alcohol and drugs alter an employee's judgment resulting in increased safety risks, workplace injuries, and faulty decision making. Therefore, working after the apparent use of alcohol, a controlled substance, or abuse of any other substances is prohibited. Although State laws have legalized marijuana for medicinal or recreational purposes, the District is not required to allow the medicinal or recreational use of marijuana in the workplace. Marijuana use or being under the influence is strictly prohibited on District property, in District vehicles, and while conducting District business. This includes working after the apparent use of marijuana, regardless of marijuana's legal status. Furthermore, the possession, manufacture, purchase, consumption (use) or sale of a controlled substance or alcohol on District premises or while conducting District business is prohibited. Moderate alcoholic consumption in conjunction with an authorized District event is an exception to this prohibition.

If at any time we have reason to believe that you may be drug or alcohol impaired on the job or may be using illegal drugs on the job, you may be required to submit to immediate drug and/or alcohol testing.

If you are taking prescribed medication which may impair your job performance, you must report this fact to your supervisor, and obtain your supervisor's approval, before reporting to work. If you refuse to take a drug or alcohol test or if you test positive on a drug or alcohol test may result in corrective action up to and including termination.

WORKPLACE VIOLENCE

Mason PUD 1 has a "zero tolerance" policy for any actions that threaten its employees, customers or vendors. This includes verbal and physical harassment, verbal confrontations, and any actions that cause others to feel unsafe in the workplace. As part of this policy, employees are prohibited from bringing weapons to work or on District premises, including the District parking lot. The District reserves the right to inspect all District property with or without notice and reserves the right to ask employees to take PTO to remove weapons from District property or District-owned premises. Employees with complaints regarding these issues should submit them in accordance with this policy.

You are encouraged to raise workplace concerns with your immediate supervisor. If your supervisor is unavailable, if the complaint remains unresolved after talking with your supervisor, or if the nature of the complaint is such that you do not feel you can discuss the complaint with your supervisor, you may make a complaint to Human Resources or the General Manager.

Upon receiving a complaint, the District will promptly investigate the matter to determine relevant facts and circumstances. You may make an anonymous complaint; however, this may limit the District's ability to investigate it.

If you have obtained, or are protected by, an Order for Victim Protection that includes Mason PUD 1 as your workplace, immediately provide a copy of the order to Human Resources or your supervisor. Orders for Victim Protection include the following types of court orders – protection order, no contact order, restraining order and anti-harassment order.

PERSONAL APPEARANCE

Dress, grooming, and personal cleanliness standards contribute to the morale of all employees and affect the business image PUD No.1 presents to customers and visitors.

During business hours or when representing PUD No.1, you are expected to present a clean, neat, and tasteful appearance. You should dress and groom yourself according to the requirements of your position and accepted social standards. This is particularly true if your job involves dealing with customers or visitors in person. Business casual attire such as nice jeans or slacks with a professional top is an acceptable standard for office personnel. FR or Hi-Vis clothing (whichever is appropriate) with jeans or work pants that are in good condition is an acceptable standard for outside workers.

Clothing with slogans or logos, other than PUD-issued, should be avoided, as should excessive use of colognes or perfumes. All clothing must be clean, pressed and in good repair without holes or tears.

Your supervisor or department head is responsible for establishing a reasonable dress code appropriate to the job you perform. If your supervisor feels your personal appearance is inappropriate, you may be asked to leave the workplace until you are properly dressed or groomed. Under such circumstance, you may not be compensated for the time away from work. Consult your supervisor if you have questions as to what constitutes appropriate appearance. Where necessary, reasonable accommodation may be made to a person with a disability.

RETURN OF PROPERTY

Employees are responsible for all District property, materials, or written information issued to them or in their possession or control. Employees must return all District property immediately upon request or upon termination of employment.

RESIGNATION

Resignation is a voluntary act initiated by the employee to terminate employment with the District. Although advance notice is not required, PUD No.1 requests at least two weeks' written resignation notice from all employees.

Although advance notice is not required, the District requests that all senior staff/management team members give verbal notice of their intent to resign or retire from employment as soon as possible and (60) sixty calendar days written notice of their intent to resign or retire from employment with the district.

REPORTING (WHISTLEBLOWER ACT)

REPORTING IMPROPER GOVERNMENT ACTION AND PROTECTING EMPLOYEES AGAINST RETALIATION (RCW 42.41)

It is the policy of Public Utility District No. 1 of Mason County (Mason County PUD No. 1) to encourage its employees to report improper governmental action taken by Mason County PUD No. 1 officers or employees and to protect Mason County PUD No. 1 employees who have reported improper governmental actions in accordance with Mason County PUD No. 1's policies and procedures.

"Improper governmental action" means any action by a Mason County PUD No. 1 officer or employee:

1. That is undertaken in the performance of the officer's or employee's official duties, whether or not the action is within the scope of the employee's employment, and
2. That is in violation of any federal, state, or local law or rule; is an abuse of authority; is of substantial and specific danger to the public health or safety; or is a gross waste of public funds.

Transfers & Demotions

"Improper governmental action" does not include personnel actions, including employee grievances, complaints, appointments, promotions, assignments, reassignments, reinstatements, restorations, reemployments, performance evaluations, reductions in pay, dismissals, suspensions, violations or collective bargaining or civil service laws, alleged violations of labor agreements or reprimands.

"Retaliatory action" means any adverse change in the terms and conditions of a Mason County PUD No. 1 employee's employment.

"Emergency" means a circumstance that if not immediately changed may cause damage to persons or property.

Procedures for Reporting

Mason County PUD No. 1 employees who become aware of improper governmental actions should raise the issue first with their supervisor. If requested by the supervisor, the employee shall submit a written report to the supervisor, or to some person designated by the supervisor, stating in detail the basis for the employee's belief that an improper governmental action has occurred. Where the employee reasonably believes the improper governmental action involves his or her supervisor, the employee may raise the issue directly with the Mason County PUD No. 1 General Manager or such other person as may be designed by the Mason County PUD No. 1 General Manager to receive reports of improper governmental action.

In the case of an emergency, where the employee believes that immediate and irreparable damage to persons or property may result if action is not taken immediately, the employee may report the improper governmental action directly to the appropriate government agency with responsibility for investigating the improper action.

The supervisor, the Mason County PUD No. 1 General Manager or the Mason County PUD No. 1 General Manager's designee, as the case may be, shall take prompt action to assist Mason County PUD No. 1 in properly investigating the report of improper governmental action.

Mason County PUD No. 1 officers and employees involved in the investigation shall keep the identity of reporting employees confidential to the extent possible under law, unless the employee authorizes the disclosure of his or her identity in writing. After an investigation has been completed, the employee reporting the improper governmental action shall be advised of a summary of the results of the investigation, except that personnel actions taken as a result of the investigation may be kept confidential.

Mason County PUD No. 1 employees who fail to make a good-faith attempt to follow Mason County PUD No. 1's procedures in reporting improper governmental action shall not receive the protections provided by Mason County PUD No. 1 in these procedures.

Protection Against Retaliatory Actions

Mason County PUD No. 1 officials and employees are prohibited from taking retaliatory action against a Mason County PUD No. 1 employee because they have in good faith reported an improper governmental action in accordance with these policies and procedures.

Employees who believe that they have been retaliated against for reporting an improper governmental action should advise their supervisor, the Mason County PUD No. 1 General Manager or the Mason County PUD No. 1 General Manager's designee. Mason County PUD No. 1 officials and supervisors shall take appropriate action to investigate and address complaints of retaliation.

If the employee's supervisor, the Mason County PUD No. 1 General Manager or the Mason County PUD No. 1 General Manager's designee, as the case may be, does not satisfactorily resolve a Mason County PUD No. 1 employee's complaint that they have been retaliated against in violation of this policy, the Mason County PUD No. 1 employee may obtain protection under this policy and pursuant to state law by providing a written notice to the Mason County PUD No. 1 Board of Commissioners that:

- a) Specifies the alleged retaliatory action, and
- b) Specifies the relief requested.

Mason County PUD No. 1 employees shall provide a copy of their written charge to the Mason County PUD No. 1 General Manager no later than thirty (30) days after the occurrence of the alleged retaliatory action. Mason County PUD No. 1 shall respond within thirty (30) days to the charge of retaliatory action.

After receiving either the response of Mason County PUD No. 1 or thirty days after the delivery of the charge to Mason County PUD No. 1, the Mason County PUD No. 1 employee may request a hearing before a state administrative law judge to establish that a retaliatory action occurred and to obtain appropriate relief provided by law. An employee seeking a hearing should deliver the request for hearing to the Mason County PUD No. 1 General Manager within the earlier of either fifteen (15) days of delivery of Mason County PUD No. 1's response to the charge of retaliatory action, or forty-five (45) days of delivery of the charge of retaliation to Mason County PUD No. 1 for response.

Upon receipt of request for hearing, Mason County PUD No. 1 shall apply within five (5) working days to the Washington State Office of Administrative Hearings for an adjudicative proceeding before an administrative law judge:

Office of Administrative Hearings
P. O. Box 42488
Olympia, WA 98504-2488
(360) 407-2700

(Physical Address)
2420 Bristol Court SW
Olympia, WA 98502

Mason County PUD No. 1 will consider any recommendation provided by the administrative law judge that the retaliator be suspended with or without pay, or dismissed.

Responsibilities

The Mason County PUD No. 1 Board of Commissioners is responsible for implementing Mason County PUD No. 1 policies and procedures for reporting improper governmental action, and for protecting employees against retaliatory actions. This includes ensuring that this policy and these procedures are permanently posted where all employees will have reasonable access to them, are made available to any employee upon request and are provided to all newly-hired employees.

Officers, the manager and supervisors are responsible for ensuring the procedures are fully implemented within their areas of responsibility. Violations of this policy and these procedures may result in appropriate disciplinary action, up to and including dismissal.

List of Agencies

A list of agencies responsible for enforcing federal, state and local laws and investigating other issues involving improper governmental action is available from Human Resources. Employees having questions about these agencies or the procedures for reporting improper governmental action are encouraged to contact the Mason County PUD No. 1 General Manager.

CORRECTIVE DISCIPLINE

The purpose of this policy is to state the District's position on administering equitable and consistent discipline for unsatisfactory conduct in the workplace. The best disciplinary measure is the one that does not have to be enforced and comes from good leadership and fair supervision at all employment levels.

Mason PUD 1's own best interest lies in ensuring fair treatment of all employees and in making certain that disciplinary actions are prompt, uniform, and impartial. The major purpose of any disciplinary action is to correct the problem, prevent recurrence, and prepare the employee for satisfactory service in the future.

Although employment with the District is based on mutual consent and both the employee and the District have the right to terminate employment at will, with or without cause or advance notice, and the District may use appropriate discipline at its discretion.

Disciplinary action may call for any of four steps -- verbal warning, written warning, suspension with or without pay, or termination of employment -- depending on the severity of the problem and the number of occurrences. There may be circumstances when one or more steps are bypassed.

With respect to most disciplinary problems, these steps will normally be followed:

- a first offense may call for a verbal warning;
- a next offense may be followed by a written warning;
- another offense may lead to an unpaid suspension; and, still
- another offense may then lead to termination of employment.

PUD No. 1 recognizes that there are certain types of employee problems that are serious enough to justify either a suspension, or, in extreme situations, termination of employment, without going through the usual discipline steps.

While it is impossible to list every type of behavior that may be deemed a serious offense, the Standards of Conduct policy includes examples of problems that may result in immediate suspension or termination of employment. However, the problems listed are not all necessarily serious offenses, but may be examples of unsatisfactory conduct that will trigger appropriate discipline.

By using appropriate discipline, we hope that most employee problems can be corrected at an early stage, benefiting both the employee and the District.

PROBLEM RESOLUTION

Mason PUD 1 is committed to providing the best possible working conditions for its employees. Part of this commitment is encouraging an open and frank atmosphere in which any problem, complaint, suggestion, or question receives a timely response from supervisors and management.

Mason PUD 1 strives to ensure fair and honest treatment of all employees. Supervisors, managers, and employees are expected to treat each other with mutual respect. Employees are encouraged to offer positive and constructive criticism.

If employees disagree with established rules of conduct, policies, or practices, they can express their concern through the problem resolution procedure. No employee will be penalized, formally or informally, for voicing a complaint with the District in a reasonable, business-like manner, or for using the problem resolution procedure or the Open Door approach.

If a situation occurs when employees believe that a condition of employment or a decision affecting them is unjust or inequitable, they are encouraged to make use of the following steps. The employee may discontinue the procedure at any step.

1. Employee presents problem to immediate supervisor after incident occurs. If supervisor is unavailable or employee believes it would be inappropriate to contact that person, employee may present problem to Human Resources Department or any other member of management.

2. Supervisor responds to problem during discussion or after consulting with appropriate management, when necessary. Supervisor documents discussion.
3. Employee presents problem to General Manager if problem is unresolved, preferably in writing
6. General Manager reviews and considers problem, then informs employee of decision and forwards copy of written response to Human Resources Department for employee's file. The General Manager has full authority to make any adjustment deemed appropriate to resolve the problem.

Not every problem can be resolved to everyone's total satisfaction, but only through understanding and discussion of mutual problems can employees and management develop confidence in each other. This confidence is important to the operation of an efficient and harmonious work environment and helps to ensure everyone's job security.

USE OF KEYS & SECURITY CODES

The District strives to operate with as few keys as possible, and the number of keys issued should be limited and tightly controlled. This policy applies to all departments, and to keys to all District facilities and spaces, including but not limited to the main campus, water and electric facilities and structures.

Authorized use of keys and door/alarm codes for PUD facilities

Employees shall only use their keys and door/alarm codes to access their assigned work areas and should lock doors when leaving any secured area or at the end of their shift. Employees must also ensure that keys and door/alarm codes are safeguarded and properly used. The unauthorized possession, use or reproduction of a key may constitute theft or misappropriation. Employees must report any lost or misplaced keys to their department director immediately. The unauthorized posting of or sharing of District door/alarm codes with individuals not employed by the District, including contractors, may constitute misappropriation.

Authorize use of vehicle keys

Employees shall be responsible for the proper care of the keys for the vehicle to which they are assigned to drive to perform the District's work. Keys should not be left inside a PUD vehicle that is unoccupied and not in use. Employees should report any lost or misplaced keys to their department director immediately. If an employee needs to use a back-up set of keys from the PUD vault, they should return the set of keys to the vault at the end of their shift.

Any employee who violates this policy may be subject to disciplinary action up to and including termination.

DATING/PERSONAL RELATIONSHIPS IN THE WORKPLACE

The employment of relatives or individuals involved in a dating relationship in the same area of an organization may cause serious conflicts and problems with favoritism and employee morale. In addition to claims of partiality in treatment at work, personal conflicts from outside the work environment can be carried over into day-to-day working relationships.

For purposes of this policy, a relative is any person who is related to another by the third degree of kinship either by birth, marriage or adoption, or is a first cousin either by birth, marriage or adoption, or is in a dating relationship, or whose relationship with the employee is similar to that of persons who are related by marriage. A dating relationship is defined as a relationship that may be reasonably expected to lead to the formation of a consensual "romantic" or sexual relationship. This policy applies to all employees without regard to the gender or sexual orientation of the individuals involved.

It is the policy of Mason PUD 1 to not hire a relative. Relatives of current employees may not occupy a position that will be working directly for or supervising their relative. Individuals involved in a dating relationship with a current employee may also not occupy a position that will be working directly for or supervising the employee with whom they are involved in a dating relationship.

If a relative relationship or dating relationship is established after employment between employees who are in a reporting situation described above, it is the responsibility and obligation of the supervisor involved in the relationship to disclose the existence of the relationship to management. The individuals concerned will be given the opportunity to decide who is to be transferred to another available position. If that decision is not made within 30 calendar days, management will decide who is to be transferred or, if necessary, terminated from employment.

In other cases where a conflict or the potential for conflict arises because of the relationship between employees, even if there is no line of authority or reporting involved, the employees may be separated by reassignment or terminated from employment. Employees in a close personal relationship should refrain from public workplace displays of affection or excessive personal conversation.

CONFLICTS OF INTEREST

Employees have an obligation to conduct business within guidelines that prohibit actual or potential conflicts of interest. The purpose of these guidelines is to provide general direction so that employees can seek further clarification on issues related to the subject of acceptable standards of operation. Contact the General Manager for more information or questions about conflicts of interest.

An actual or potential conflict of interest occurs when an employee is in a position to influence a decision that may result in a personal gain for that employee or for a relative, as a result of the District's business dealings. For the purposes of this policy, a relative is any person who is a relative as defined in policy 105 (Dating/Personal Relationships in the Workplace).

No "presumption of guilt" is created by the mere existence of a relationship with outside firms. However, if employees have any influence on transactions involving purchases, contracts, or leases, it is imperative that they disclose to the General Manager as soon as

possible of the existence of any actual or potential conflict of interest so that safeguards can be established to protect all parties.

Personal gain may result not only in cases where an employee or relative has a significant ownership in a firm with which the District does business, but also when an employee or relative receives any kickback, bribe, gift of more than nominal value, or special consideration as a result of any transaction or business dealings involving Mason PUD 1. An appearance of conflict needs to be acknowledged and addressed to determine a possible solution or fix.

OUTSIDE EMPLOYMENT

The District recognizes that some employees may need or want to hold additional jobs outside their employment with the company. Employees of the District are permitted to engage in outside work or hold other jobs, subject to certain restrictions.

The District applies this policy consistently and non-discriminatorily to all employees, and in compliance with all applicable employment and labor laws and regulations. The following rules for outside employment apply to all employees notifying their supervisors or managers of their intent to engage in outside employment:

1. Work-related activities and conduct away from Mason PUD 1 must not compete with, conflict with or compromise the company's interests or adversely affect job performance and the ability to fulfill all responsibilities to the District. Employees are prohibited from performing any services for customers of Mason PUD 1 that are normally performed by the District. This prohibition also extends to the unauthorized use of any company tools or equipment and the unauthorized use or application of any company confidential information. In addition, employees may not solicit or conduct any outside business during work time for the District.
2. District employees must carefully consider the demands that additional work activity will create before accepting outside employment. Outside employment will not be considered an excuse for poor job performance, absenteeism, tardiness, leaving early, refusal to travel, or refusal to work overtime or different hours. If outside work activity causes or contributes to job-related problems at the PUD, the employee will be asked to discontinue the outside employment, and the employee may be subject to the normal disciplinary procedures for dealing with the resulting job-related problem(s).
3. In evaluating the effect that outside work may have on an employee's job performance and other job-related responsibilities, PUD department heads and the human resources department will consider whether the proposed employment:
 - a) May reduce the employee's efficiency in working for the company.
 - b) Involves working for an organization that does a significant amount of business with the company, such as major contractors, suppliers and customers.
 - c) May adversely affect the company's image.

4. An employee's refusal to discontinue outside employment after being requested to do so by his or her department head or the human resource department will result in disciplinary action up to and including termination of employment.

WORKPLACE SEARCHES

Mason County PUD No. 1 reserves the right to use any lawful method of investigation it deems necessary to determine whether any person has engaged in conduct that interferes with or adversely affects business. A search does not imply an accusation of theft or that an employee has broken a company rule.

Employees entering and leaving the facility are subject to questions and search at the employer's discretion. Lockers, vehicles, and personal possessions on Mason County PUD No. 1 premises will also be subject to search. This policy applies to all employees—management, clerical, union and non-union personnel. Failure to comply may result in the termination of your employment.

BENEFITS

BENEFITS

Mason PUD 1 provides full-time employees health and welfare benefits. Please see Human Resources for benefit booklets, enrollment applications, and for the cost of employee and/or dependent coverage.

HEALTH INSURANCE

The District's health insurance plan provides employees and their dependents access to medical, dental, and vision care insurance benefits. Employees in the following employment classifications are eligible to participate in the health insurance plan:

- * Regular full-time employees
- * Regular part-time employees (limited to insurance carrier qualifications and State of Washington Public Employees Benefits Board (PEBB) regulations)

Eligible employees may participate in the health insurance plan subject to all terms and conditions of the agreement between the District and the insurance carrier.

A change in employment classification that would result in loss of eligibility to participate in the health insurance plan may qualify an employee for benefits continuation under the Consolidated Omnibus Budget Reconciliation Act (COBRA). Refer to the Benefits Continuation (COBRA) policy for more information.

Details of the health insurance plan are described in the Certificate of Coverage. A Certificate of Coverage and information on cost of coverage will be provided in advance of

enrollment to eligible employees. Contact the Human Resources Department for more information about health insurance benefits.

LIFE INSURANCE

Life insurance offers you and your family important financial protection. The District provides a basic life insurance plan for eligible employees. Additional supplemental, dependent life and Accidental Death and Dismemberment insurance coverage may also be purchased.

Employees in the following employment classifications are eligible to participate in the life insurance plan:

- * Regular full-time employees
- * Regular part-time employees (limited to insurance carrier qualifications)

Eligible employees may participate in the life insurance plan subject to all terms and conditions of the agreement between the District and the insurance carrier.

Details of the basic life insurance plan, including benefit amounts, are described in the Certificate of Insurance provided to eligible employees. Contact the Human Resources Department for more information about life insurance benefits.

LONG-TERM DISABILITY

Mason PUD 1 provides a long-term disability (LTD) benefits plan to help eligible employees cope with an illness or injury that results in a long-term absence from employment. LTD is designed to ensure a continuing income for employees who are disabled and unable to work.

Employees in the following employment classifications are eligible to participate in the LTD plan:

- * Regular full-time employees
- * Regular Part-time employees (limited to insurance carrier qualifications)

Eligible employees may participate in the LTD plan subject to all terms and conditions of the agreement between the District and the insurance carrier.

Details of the LTD benefits plan including benefit amounts, and limitations and restrictions are described in the Certificate of Insurance provided to eligible employees. Contact the Human Resources Department for more information about LTD benefits.

EMPLOYEE ASSISTANCE PROGRAM

Mason PUD 1 cares about the health and well-being of its employees and recognizes that a variety of personal problems can disrupt their personal and work lives. While many employees solve their problems either on their own or with the help of family and friends, sometimes employees need professional assistance and advice.

Through the Employee Assistance Program (EAP), Mason PUD 1 provides confidential access to professional counseling services for help in confronting such personal problems as alcohol and other substance abuse, marital and family difficulties, financial or legal troubles, and emotional distress. The EAP is available to all employees and their immediate family members offering problem assessment, short-term counseling, and referral to appropriate community and private services.

The EAP is strictly confidential and is designed to safeguard your privacy and rights. Information given to the EAP counselor may be released only if requested by you in writing. All counselors are guided by a Professional Code of Ethics.

Personal information concerning employee participation in the EAP is maintained in a confidential manner. No information related to an employee's participation in the program is entered into the personnel file.

PUD No. 1 may request that the employee waive his or her right to confidentiality in those circumstances that involve disciplinary actions so that it can assist the District and the employee in bringing remediation of the conflict giving rise to the discipline.

There is no cost for employees to consult with an EAP counselor. If further counseling is necessary, the EAP counselor will outline community and private services available. The counselor will also let employees know whether any costs associated with private services may be covered by their health insurance plan. Costs that are not covered are the responsibility of the employee.

Minor concerns can become major problems if you ignore them. A professional counselor is available to help you when you need it. Please see the Human Resources Department for more information.

BENEFITS CONTINUATION (COBRA)

The federal Consolidated Omnibus Budget Reconciliation Act (COBRA) gives employees and their qualified beneficiaries the opportunity to continue health insurance coverage under Mason PUD 1's health plan when a "qualifying event" would normally result in the loss of eligibility. Some common qualifying events are resignation, termination of employment, or death of an employee; a reduction in an employee's hours or a leave of absence; an employee's divorce or legal separation; and a dependent child no longer meeting eligibility requirements.

Under COBRA, the employee or beneficiary pays the full cost of coverage at Mason PUD 1's group rates plus an administration fee. The District provides each eligible employee with a written notice describing rights granted under COBRA when the employee becomes eligible for coverage under its health insurance plan. The notice contains important information about the employee's rights and obligations.

RETIRED EMPLOYEES MEDICAL INSURANCE

Eligibility to Remain Insured: All employees and commissioners who are vested in the Public Employees Retirement System (PERS), (five years under PERS 1 and 2, or 10 years under PERS 3), and who leave the employ of PUD 1 by retiring and immediately receiving benefits under PERS are eligible to remain a part of the PUD 1 group medical and dental insurance plans available to retirees through the Public Employees Benefits Board.

Employees retiring with less than 15 years of service are not eligible for premium payment reimbursement credits from the PUD. Employees with less than 15 years' service shall be responsible for payment of all premiums through the Department of Retirement Systems.

Any PERS employee or commissioner who retires from the District and does not immediately begin receiving benefits under PERS will not be eligible for insurance plans available to retirees through the Public Employees Benefits Board. Said retirees and commissioners shall be eligible for continuing coverage under federal COBRA law.

Eligibility to Participate in Premium Payment Reimbursement Credits (also commonly referred to in the CBA as "Retiree Medical Stipends"): All employees who are vested in the Public Employees Retirement System (PERS), and have worked for PUD 1 a minimum of fifteen (15) consecutive years and less than thirty consecutive years at the time of retirement, and who voluntarily retire from the PUD and begin receiving PERS retirement benefits, shall also be eligible for premium payment reimbursement from the PUD.

Premium payment reimbursement will be based on a credit of 3% per year of service for a period of ten (10) years after retirement. The reimbursement shall only be eligible for the percentage the District pays for the retired employee on the date he/she leaves employment with the District, provided however that no payment on behalf of the retired employee shall exceed the premium amount paid on behalf of the active employees for insurance.

Said retired employee shall cease to receive the premium contributions if they become employed and have access to another group medical insurance plan and in which they have not waived the right to participate. Any premium payment reimbursements made while the retired employee was covered under another group medical insurance plan through their new place of employment shall be repaid to the PUD.

The maximum number of payments for each person is 120, regardless if an individual is reelected to the board or returns to work in a benefit-eligible position and retires again later.

The District will provide for employees leaving the District who have 30 consecutive years of employment with the District, 100% of the District's share of monthly medical and dental premium for a period of ten (10) years after leaving employment, provided however that no payment on behalf of such employee shall exceed the premium amount paid on behalf of the active employees for insurance. This benefit is extended to the employee's dependents that are covered on the employee's health care plan at the time of leaving employment.

Exclusions:

Any union-represented employee whose employment with the District is terminated due to fraud, theft or embezzlement, shall forfeit all claim to the retiree medical stipend.

Any non-represented employee that is terminated for cause or who resigns in lieu of termination for cause shall forfeit all claim to the medical stipend.

Surviving dependents:

The surviving spouse or dependent children (as defined by the PUD 1 employee health care plan) of a retiree who were covered at the time of the retiree's death may continue his/her coverage with the same premium payment credits as the deceased retiree for the remainder of the ten-year period following retirement. A new spouse to a surviving spouse is not eligible for premium credits.

EDUCATIONAL ASSISTANCE

Purpose

PUD No. 1 recognizes that the skills of its employees are critical to the success of the organization. The educational assistance program encourages personal development through formal education so employees can maintain and improve job-related skills.

Policy

General Eligibility Requirements:

This program is open to regular, full-time employees with 180 days of continuous, regular, full time service. The employee must be in active, paid status when applying for approval (employees on a Leave of Absence are not eligible). They must remain a regular, full-time employee while taking the course and when requesting reimbursements at its completion. Part-time, temporary, and seasonal employees are not eligible for this program.

Deadlines:

To ensure your reimbursement requests are included in the annual budget, employees must submit any assistance requests by September 30th in the year prior to when he or she plan to begin his or her studies. Exceptions are allowed for requests not leading to a degree if class availability has not yet been published for the term. Requests submitted after this date will be reviewed on an individual basis. Requests also may be rejected due to budget constraints.

Degree Program or Coursework Eligibility Requirements:

Degree programs or individual coursework must be related to District business. This means the degree program may, in part, prepare the employee for a job to which they could reasonably aspire during their foreseeable tenure with the District. This determination will be made by those persons responsible for approving the employee's application for assistance.

- Any approved courses must be taken on the employee's own time.
- Degree programs or coursework must be:
 - Approved prior to enrolling in classes each term
 - Conducted by an accredited academic institution
 - Result in a transcript of grades, or a certificate of satisfactory completion

Reimbursement for Approved coursework:

Payment by the District to the employee shall be on a reimbursement basis only. Employees must pay for covered expenses first, and then seek reimbursement from the District after the course has been completed. Reimbursement is subject to all provisions of this policy.

Grade Requirements:

- Official documentation showing a grade of "C" (2.0 GPA) or better is required for reimbursement.
- Please note that minimum grade requirements for reimbursement apply to individual courses and are not averaged over the degree.
- Approved courses offered only as Pass/Fail will be reimbursed if passed.

Other Financial Aid

- Reimbursement is not available to the extent an employee receives grants, scholarships, and other financial aid for the same course. Reimbursement by the District may be requested for amounts reimbursable under this policy in excess of grants, scholarships, and other financial aid received by the employee.
- Employees shall submit a FAFSA application and exhaust all tuition reduction options prior to asking the District for funding.

Limitations

- Reimbursement for approved courses is limited to tuition.
- Following is a partial list of fees and expenses which are excluded from reimbursement by the District. This is not intended to be an all-inclusive list.
 - Late fees and interest for delayed payment plans;
 - Transcript fees;
 - Application fees;
 - Parking fees;
 - Testing fees;
 - Institutions, institutional accreditation, or programs of study non-pre-qualified or annually approved by the District;
 - Audited courses;
 - Executive degree programs, unless approved by the General Manager;
 - A law degree, unless approved by the General Manager;
 - Ph.D. degree programs, unless approved by the General Manager; and
 - The cost of supplies, equipment, drawing instruments, calculators, electronic equipment, document copying fees, recording devices or other course materials, including textbooks.

Annual Reimbursement Maximum:

Tuition reimbursement maximums are determined by the date reimbursements are issued by the District, not the date of the courses. Employees must submit for reimbursement no later than one month following the close of the learning period (quarter, semester or other period). The annual reimbursement maximum shall be equivalent to the minimum tuition (excluding fees or other education related expenses) required for a full-time undergraduate at a four-year in-state college. Due to its proximity to the District, The Evergreen State College's in-state undergraduate tuition will be used as the basis for this maximum, regardless of the community college or university that the employee attends.

IRS regulations may require tuition reimbursement to be counted as imputed income and subject to taxation when in excess of certain limitations. Employees reaching this level will be notified prior to the issuance of the pay checks in which such limitations have been exceeded and taxation will take effect.

Employees withdrawing from a course prior to course completion for any reason, including medical leave, are not eligible for reimbursement.

Reimbursement to the District upon Separation of Employment:

Investing in an employee's college education represents a significant financial investment for the District. It is anticipated that investing in our workforce through college coursework or degree programs will provide future value to our ratepayers by bringing enhanced knowledge, skills and abilities into employee's work performance and by preparing us to meet future employment needs. Employees who depart prior to or soon after completing college courses or degree programs have not had the opportunity to provide such future benefits in return for the District's investment in the employee's development.

Therefore, participants who are approved for tuition reimbursement are required to fulfill a commitment period prior to separating employment from the District. (*See Separating Employment, below*).

The commitment period is designated as a three (3) year period from *either* the a) date reimbursement is made for tuition or b) the date the schooling session ended, whichever is later. If the employee separates employment prior to completing the three year commitment period, the employee agrees to repay the amount reimbursed for tuition by the District. The amount owed to the District is based on the date of each reimbursement received over the course of employment. For reimbursements received within the three calendar year period prior to separation of employment, the amount owed to the District will be prorated over 36 months (repayment obligation will be reduced by 1/36th per month worked after receipts of each reimbursement).

Repayment will be made by payroll deduction of earnings, personal leave cash out, or, if those are not sufficient to repay the debt, by personal repayment to the District. Employee participation in the tuition reimbursement program constitutes express authorization for the payroll deductions or, if insufficient payroll funds available to repay the District, it is also an agreement by the employee to direct-pay the District for any repayment required.

Separating Employment:

- **Course Completion:** Employees who separate employment voluntarily or involuntarily for disciplinary reasons prior to course completion are not eligible for reimbursement. Employees involuntarily separating employment for reason other than disciplinary reasons (i.e. laid off, disability, etc.) after course completion are eligible for reimbursement by the District if all other conditions of the directive are met, including achieving a passing grade, timely expense report filing, etc.
- **Commitment Period and Repayment:** Employees who separate employment voluntarily or involuntarily for disciplinary reasons prior to fulfilling the commitment

period are subject to the repayment obligation. Employees involuntarily separating employment for reasons other than disciplinary reasons (i.e. lay off, disability, etc.) prior to fulfilling the commitment period are not subject to the repayment obligation.

Ongoing Requests to Attend School:

Once it is determined attending school is an appropriate part of an employee's development plan, the employee completes a "Request for Tuition Reimbursement" form, estimating the tuition for each course and explaining the business purpose for his or her attendance. This form is routed for review and approval to the immediate supervisor/manager and General Manager. The employee will be notified of whether or not the request has been approved. Approval is contingent upon both the alignment with employee development and business need, as well as budgetary considerations. An employee who chooses to enroll in the course prior to receiving approval from Human Resources is responsible for their own expenses if the course is later not approved.

PAID TIME OFF (PTO)

PAID TIME OFF USE & ACCRUAL

Personal Leave, or Paid Time Off (PTO), is an all purpose time-off policy for eligible employees to use for vacation, illness or injury, and personal business. It combines traditional vacation and sick leave plans into one flexible, personal leave policy. For the purposes of the Washington State Paid Sick Leave requirements, designated "Paid Sick Leave" is the portion of the PTO bank which is accrued pursuant to Chapter 49.56 RCW which will be tracked and earmarked within the PTO bank. See "Washington State Paid Sick Leave" section below for details.

Employees in the following employment classification(s) are eligible to earn and use Paid Time Off as described below:

- * Regular full-time employees

Once employees enter an eligible employment classification, they begin to earn Paid Time Off according to the schedule below. They can request use of Paid Time Off after it is earned.

The amount of Paid Time Off employees receives each year increases with the length of their employment as shown in the following schedule:

After Completing:	Six Months of Service	10 days
	One-Four years of Service	20 days
	Five-Nine years of Service	25 days
	Ten-Fifteen years of Service	30 days
	Sixteen years of Service	31 days
	Seventeen years of Service	32 days
	Eighteen years of Service	33 days
	Nineteen years of Service	34 days
	Twenty years and above	35 days

A portion of the earned PTO will be designated as Paid Sick Leave and shall consist of one hour of the PTO bank for every forty hours worked by the employee. The length of eligible service is calculated on the basis of a "benefit year." This is the 12-month period that begins when the employee starts to earn PTO. An employee's benefit year may be extended for any significant leave of absence in excess of 12 weeks in a calendar year except military leave of absence. Military leave has no effect on this calculation. (See individual leave of absence policies for more information.)

PTO can be used in minimum increments of 15 minutes (quarter-hours). Employees who have an unexpected need to be absent from work should notify their department director before the scheduled start of their workday, if possible. The direct supervisor must also be contacted on each additional day of unexpected absence. For unexpected absences due to illness or injury, see "Washington State Paid Sick Leave" section below for reasonable notice requirements.

Each employee shall take a minimum of two weeks PTO per year. New hires shall use 80 hours of PTO within their first 24 months of employment. Following the 24 month period, they shall use 80 hours annually. An employee may accumulate any portion of his earned PTO (except Paid Sick Leave) in excess of two weeks to a maximum of one hundred fifty (150) days personal leave.

Full time active employees who have completed 6 months of continuous employment will be credited with 40 hours of PTO effective January 1st of the year. Inactive employees, except those employees on short term disability, workers' compensation leave, military leave of 15 days or less, or as prescribed by law, will not be eligible for the 40 hours of PTO. The additional PTO will be combined with each employee's PTO accruals.

Employees who receive these additional 40 hours of PTO annually will have the option to cash out these hours at their current wage rate, provided that the PTO bank is not reduced to less hours than the "Paid Sick Leave" accrual amount. In addition, employees may cash out an additional 40 hours of PTO per year provided that it does not reduce the employee's PTO bank to less than 300 hours. The 80 hours of PTO allowed for cash out may also be rolled over into the employee's 457 Deferred Compensation plan, provided that the rollover does not violate contribution limits set by the IRS.

To schedule planned PTO, employees should request advance approval from their supervisors. Requests will be reviewed based on a number of factors, including business needs and staffing requirements. PTO is paid at the employee's base pay rate at the time of absence. It does not include overtime. The employee shall designate if they are seeking to utilize Paid Sick Leave hours. Retaliation for using Paid Sick Leave for authorized sick leave purposes is prohibited.

As an additional condition of eligibility for PTO, an employee on an extended absence for illness or injury may be required to apply for any other available compensation and benefits, such as workers' compensation. PTO will be used to supplement any payments that an employee is eligible to receive from state disability insurance, workers' compensation, or PUD No. 1-provided disability insurance programs.

In the event that available PTO is not used by the end of the calendar year, employees may carry unused time forward to the next calendar year up to a maximum of 1,200 hours. Employees may not carry more than 1,200 hours, of which no more than 40 hours may

consist of designated Sick Leave, in their PTO banks. They must use the time in the following pay period or forfeit the excess hours.

Upon termination of employment, employees will be paid for unused PTO that has been earned through the last day of work. .

RETIREMENT TERMINATION LEAVE

A minimum of sixty (60) days official written notice of intent to retire shall be required of District employees. Accordingly, it is suggested that the employee allow adequate time to complete State and District requirements for retirement (up to one year's time is necessary).

PTO use for retirement termination leave will be allowed. Retirement termination leave will commence at the end of the sixty (60) day notice period required to be given prior to retirement. During retirement termination leave, the employee will receive medical, dental, life and LTD insurance benefits. There will be no further PTO accrued during this leave period.

SERVICE CREDIT FOR RECRUITMENT/RETENTION OF STAFF POSITIONS

An employee, who holds a senior staff position, may accrue PTO at the rate equal to their years of regular full-time service with the District, plus up to an additional 10 years of service credit for similar, recent work experience gained outside the District. The credit will continue to advance through the PTO accrual schedule annually, not to exceed the maximum of 35 days.

The additional accrual rate will become effective on the date the employee assumes the responsibilities of the senior staff position. Senior staff is defined as Director, Department Head, Assistant General Manager, General Manager and or equivalent responsibility.

WASHINGTON STATE PAID SICK LEAVE (Chapter 49.46 RCW)

A portion of the employees' earned PTO bank shall be subject to and regulated under the provisions of Chapter 49.46 RCW, Paid Sick Leave. The Paid Sick Leave portion of the PTO bank is available for employees to care for their health and the health of their family members. Employees accrue one designated sick leave hour for every 40 hours of actual time worked, including overtime hours. Vacation time, holidays and comp time used in lieu of regular paid time does not count toward Paid Sick Leave accrual.

Paid Sick Leave may be used for the following purposes:

- An employee's mental or physical illness, injury, or health condition; preventative care such as medical, dental or optical appointments and treatment.
- Care of a family member with an illness, injury, health condition and/or preventative care such as a medical, dental or optical appointment.
- Closure of the employee's place of business or child's school/place of care by order of a public official for any health-related reasons.
- If the employee or the employee's family member is a victim of domestic violence, sexual assault, or stalking.

Authorized use of Paid Sick Leave for domestic violence, sexual assault or stalking includes:

- Seeking legal or law enforcement assistance or remedies to ensure the health and safety of employees and their family members including, but not limited to, preparing for, or participating in, any civil or criminal legal proceedings related to or derived from domestic violence, sexual assault or stalking.
- Seeking treatment by a health care provider for physical or mental injuries caused by domestic violence, sexual assault or stalking.
- Attending health care treatment for a victim who is the employee's family member.
- Obtaining, or assisting the employee's family member(s) in obtaining, services from: a domestic violence shelter; a rape crisis center; or a social services program for relief from domestic violence, sexual assault or stalking.
- To obtain, or assist a family member in obtaining, mental health counseling related to an incident of domestic violence, sexual assault or stalking in which the employee or the employee's family member was a victim of domestic violence, sexual assault or stalking.
- Participating, for the employee or for the employee's family member(s), in: safety planning; or temporary or permanent relocation; or other actions to increase the safety from future incidents of domestic violence, sexual assault, or stalking.

Family members included in this policy:

- "Family member" is defined as the child or parent (including biological, adopted, foster, step or legal guardian), a spouse, registered domestic partner, spouse's parent, grandparent, grandchild, or sibling.

Accrual of Paid Sick Leave:

- Paid Sick Leave begins to accrue at the start of employment. Employees are provided with a "Paid Sick Leave" notification posted in breakrooms in both the administration and operations buildings and in the Employee Handbook. Additional copies of notification can be printed per request of the Human Resources department.
- Paid Sick Leave is accrued at the rate of one (1) hour for every forty (40) hours worked.

There is no cap on the number of paid sick leave hours that may be accrued in a year.

- A maximum of 40 hours of Paid Sick Leave can be carried over each year.
- The accrual year is a calendar year (January through December).

The amount of PTO available is recorded EACH PAYDAY ON YOUR PAY STUB OR OTHER REPORTING SYSTEM, NOT LESS THAN MONTHLY.

How to Use Paid Sick Leave:

- Employees are eligible to use accrued paid sick leave 90 days after starting employment.
- Paid Sick Leave can be used in 15-minute increments (.25 hours).

- Employees shall notify their supervisors that they are taking Paid Sick Leave and report the time on their Employee Self Serve timesheets or paper timesheets as "SICK" leave.
- Paid Sick Leave will be compensated at an employee's regular rate of pay.

Reasonable Notice for Use of Paid Sick Leave:

Employees are required to provide reasonable advanced notice for use of Paid Sick Leave. The District may require verification for absences that exceed three (3) days. If such verification requirement results in an unreasonable burden or expense, please contact HUMAN RESOURCES. Any information provided will be kept confidential.

If an employee's absence is foreseeable, the employee must provide notice to their department director at least 10 days, or as early as possible, before the first day Paid Sick Leave is used.

- If possible, notification should include the expected duration of the absence.

If an employee's absence is unforeseeable, the employee must contact department director as soon as possible.

- If the need for paid sick leave is unforeseeable, and arises before the required start of the employee's shift, notice should be provided no later than one (1) hour before the employee's required start time.
- In the event it is not possible to provide notice of an unforeseeable absence, a person, on the employee's behalf, may provide such notice.
- If possible, the notification should include the expected duration of the absence.

Reasonable Notice for Use of Paid Sick Leave for Domestic Violence Leave:

Foreseeable Use of Paid Sick Leave

- An employee must give advance oral or written notice to their department director as soon as possible for the foreseeable use of paid sick leave to address issues related to the employee or the employee's family member being a victim of domestic violence, sexual assault or stalking.

Unforeseeable Use of Paid Sick Leave

- If an employee is unable to give advance notice because of an emergent or unforeseen circumstance related to the employee or the employee's family member being a victim of domestic violence, sexual assault or stalking, the employee or a designee must give oral or written notice to their department director no later than the end of the first day that the employee takes such leave.

Reinstatement of Employment:

If an employee leaves employment and is rehired within 12 months of separation, any accrued, unused paid Sick Leave will be reinstated to the employee's Paid Sick Leave balance. If an employee is rehired within 12 months of separation, the employee will not be required to wait another 90 days to use the accrued paid sick leave if the employee met that requirement during the previous period of employment. If an employee did not meet the 90-day requirement for the use of paid sick leave prior to separation, the previous

period of time the employee worked for the District will count towards the 90 days for purposes of determining the employee's eligibility to use Paid Sick Leave.

Retaliation Prohibited:

Any discrimination or retaliation against an employee for lawful exercise of Paid Sick Leave rights is not allowed. Employees will not be disciplined for the lawful use of Paid Sick Leave. If an employee feels they are being discriminated or retaliated against, the employee may contact the District's Human Resources manager.

If an employee is not satisfied with the District's response, the employee may contact the Washington State Department of Labor & Industries. www.lni.wa.gov/workplacerrights

HOLIDAYS

MASON COUNTY PUD NO. 1 provides 10 paid holidays annually. The following are the paid holidays for regular full-time and part-time employees:

- New Year's Day (January 1)
- Martin Luther King, Jr. Day (third Monday in January)
- President's Day (third Monday in February)
- Memorial Day (last Monday in May)
- Independence Day (July 4)
- Labor Day (first Monday in September)
- Veteran's Day (November 11)
- Thanksgiving Day (fourth Thursday in November)
- Day after Thanksgiving
- Christmas Day (December 25)

Full-time employees receive eight hours straight time pay. Part-time employees receive holiday pay based on the number of hours they were scheduled to work.

Employees must be present for their entire scheduled workday prior to and on their entire scheduled workday following a holiday in order to receive pay for that holiday, unless on approved vacation or other excused absence.

A recognized holiday that falls on a Saturday will be observed on the preceding Friday. A recognized holiday that falls on a Sunday will be observed on the following Monday.

In the event that it is necessary to work on any of these holidays, employees working the holiday are compensated at their straight time rate for those hours worked on the holiday plus holiday pay. Holiday pay is not counted as time worked for computing overtime.

Employees paid on a salary basis receive holiday pay for any recognized holiday if the employee performs any work that week.

In addition to the recognized holidays previously listed, eligible employees will receive one annual floating holiday. These holidays must be scheduled with the prior approval of the employee's supervisor.

MILITARY LEAVE

A military leave of absence will be granted to employees who are absent from work because of service in the U.S. uniformed services in accordance with the Uniformed Services Employment and Reemployment Rights Act (USERRA). Advance notice of military service is required, unless military necessity prevents such notice, or it is otherwise impossible or unreasonable.

The leave will be unpaid. However, employees may use any available paid time off for the absence. Continuation of health insurance benefits is available as required by USERRA based on the length of the leave and subject to the terms, conditions and limitations of the applicable plans for which the employee is otherwise eligible.

Benefit accruals, such as vacation, sick leave, or holiday benefits, will be suspended during the leave and will resume upon the employee's return to active employment.

Employees on military leave for up to 30 days are required to return to work for the first regularly scheduled shift after the end of service, allowing reasonable travel time. Employees on longer military leave must apply for reinstatement in accordance with USERRA and all applicable state laws.

Employees returning from military leave will be placed in the position they would have attained had they remained continuously employed or a comparable one depending on the length of military service in accordance with USERRA. They will be treated as though they were continuously employed for purposes of determining benefits based on length of service.

Contact the Human Resources Department for more information or questions about military leave.

UNPAID LEAVE

The District provides leaves of absence without pay to eligible employees who have no Paid Time Off accrual and who wish to take time off from work duties to fulfill personal obligations. Employees in the following employment classification(s) are eligible to request unpaid personal leave as described in this policy:

- * Regular full-time employees

Eligible employees may request unpaid personal leave only after having completed 180 calendar days of service. As soon as eligible employees become aware of the need for a personal leave of absence, they should request a leave from their supervisor.

Unpaid personal leave may be granted at the sole discretion of the manager for a period of up to 30 calendar days every year. If this initial period of absence proves insufficient, consideration will be given to a written request for an extension.

Requests for unpaid personal leave will be evaluated based on a number of factors, including anticipated work load requirements and staffing considerations during the proposed period of absence.

Subject to the terms, conditions, and limitations of the applicable plans, health insurance benefits will be provided by PUD No.1 until the end of the month in which the approved unpaid personal leave begins. At that time, employees will become responsible for the full costs of these benefits if they wish coverage to continue. When the employee returns from unpaid personal leave, benefits will again be provided by PUD No.1 according to the applicable plans.

Benefit accruals, paid personal leave, or holiday benefits, will be suspended during the leave and will resume upon return to active employment.

When an unpaid personal leave ends, every reasonable effort will be made to return the employee to the same position, if it is available, or to a similar available position for which the employee is qualified. However, PUD No. 1 cannot guarantee reinstatement in all cases.

Unless prior arrangements have been agreed upon if an employee fails to report to work promptly at the expiration of the approved leave period, PUD No. 1 will regard the employee as having resigned and employment considered terminated.

Unpaid Leave for Faith, Conscience or Religious Activities

In accordance with state law, the District shall grant two unpaid holidays per calendar year to all employees for a reason of faith or conscience or an organized activity conducted under the auspices of a religious denomination, church or religious organization. The PUD shall allow the employee to take the unpaid holidays on the dates selected by the employee unless the employee's absence would impose an undue hardship on the District or the employee's position is necessary to maintain public safety as outlined in WAC 82-56-020 "Definition of Undue Hardship".

BEREAVEMENT

The District recognizes that employees may need unexpected time off due to the death of a family member. Employees are provided with Paid Time Off or Comp Time (both considered in this policy as PTO) for making arrangements, settling family affairs, bereavement, and/or attending the funeral or memorial service of a member of the immediate family.

Employees covered by Collective Bargaining Agreements should refer to the appropriate article in their contract regarding PTO. Non-union employees should refer to the policy in the Employee Handbook titled "*Paid Time Off (Annual Leave)*" for review of the leave guidelines.

Immediate family is defined as parent, sibling, spouse, child, grandparent, stepparent, parent-in-law, grandchild, and registered domestic partner. Also included in this definition are the equivalent relatives of the employee's spouse. Exceptions may be granted subject to approval by General Manager.

Time Allowances:

Employees may be granted a maximum of three (3) days off, with pay deducted from the employee's accrued PTO whenever there is a death in the immediate family. Any employee who does not have sufficient PTO available to cover the absences nonetheless may be granted time off in accordance with the District's policy titled "*Unpaid Personal Leave*".

Scheduling of Leave:

Scheduling of bereavement leave will be by mutual agreement between the employee and their Department Director. Bereavement leave pay shall be that amount the employee

would have earned had the employee worked his/her regular work schedule during the leave. It is not mandatory that the employee actually attend the funeral services to be eligible for any bereavement leave pay. It is expected, however, that the absence will be used for the purpose of bereavement and handling any business matters related to the death.

Additional Time Off:

The District understands the deep impact that death can have on an individual or a family, therefore additional time off may be granted by the General Manager. Additional leave may be granted depending on the circumstances such as distance and the individual's responsibility for funeral arrangements. The employee may make arrangements with his or her supervisor for additional days off in the instance of the death of an immediate family member. All supervisor/employee arrangements for leave must be approved by the General Manager prior to the employee taking the additional leave.

Non-family Member Funeral Leave:

All full-time employees may take up to one (1) day off with pay (PTO) to attend the funeral of a close, non-family member. This time off will be considered by the employee's Director on a case-by-case basis.

Bereavement leave days need not be taken consecutively.

PREGNANCY DISABILITY LEAVE

PUD 1 provides pregnancy disability leaves of absence without pay to eligible employees who are temporarily unable to work due to a disability related to pregnancy, childbirth, or related medical conditions.

Employees should make requests for pregnancy disability leave to their supervisors at least 30 days in advance of foreseeable events and as soon as possible for unforeseeable events.

A pregnant employee may continue active employment until the attending physician advises the employee they should be off work. A leave of absence is granted to the employee for the period of time the employee is temporarily disabled due to the pregnancy, as certified by a physician.

If there is concern regarding the pregnant employee's ability to safely and/or productively function at their job, a second opinion may be obtained by a qualified physician of the employer's choice. The employer will pay the full cost of this examination. An accurate job description, describing all of the employee's job duties, should be presented to the reviewing physician.

Following the date of delivery, the employee must keep the company informed of their condition and expected date of return. At least a two-week advance notice is required before the employee's return to work. An employee, who due to childbirth complications is unable to return to work on the prearranged return date, must present a signed statement from the attending physician. The physician must indicate the nature of the complication and the expected date of return to work. If the employee returns to work immediately upon the release from the physician, the employee will be returned to the same job or a similar job of comparable pay, unless business necessity prevents such reinstatement.

Subject to the terms, conditions, and limitations of the applicable plans, health insurance benefits will be provided by the District until the end of the disability period. At that time, employees will become responsible for the full costs of these benefits if they wish coverage to continue. When the employee returns from pregnancy disability leave, benefits will again be provided by the District according to the applicable plans.

Benefit accruals, such as vacation, sick leave, or holiday benefits, will be suspended during the unpaid leave and will resume upon return to active employment.

So that an employee's return to work can be properly scheduled, an employee on pregnancy disability leave is requested to provide the District with at least two weeks advance notice of the date she intends to return to work.

When a pregnancy disability leave ends, the employee will be reinstated to the same position, unless either the job ceased to exist because of legitimate business reasons for each means of preserving the job would substantially undermine the ability to operate the District safely and efficiently. If the same position is not available, the employee will be offered a comparable position in terms of such issues as pay, location, job content, and promotional opportunities.

Unless prior arrangements have been agreed upon if an employee fails to report to work promptly at the end of the pregnancy disability leave, the District will assume that the employee has resigned. The District will provide nursing employees with reasonable break time from work and a private space to express breast milk during the work day. Employees may use paid rest break time and additional unpaid break time if needed.

SHARED LEAVE POLICY & PROCEDURES

It is the policy of the District to allow employees to share their accrued annual leave with fellow employees in the event of a prolonged medical condition (or an employee's immediate family has a medical condition) that requires the employee to be absent from the workplace for a period of time which exceeds their accrued annual leave and/or sick leave bank (if available and applicable).

The policy will not ordinarily apply to short-term or sporadic conditions or illnesses. This would include such things as sporadic, short-term recurrences of chronic allergies or conditions; short-term absences due to contagious diseases; or short-term, recurring medical or therapeutic treatments. These examples are illustrative, not all inclusive. Each case must be examined and decided based on its conformity to policy intent and must be handled consistently and equitably.

To qualify for shared leave, the employee experiencing the situation must:

1. Deplete (or have scheduled depletion of) their total accrued annual leave and Sick Leave Bank according to the policy and procedures for use of Annual and Sick Leave Bank;
2. Provide verification of the situation which is occurring to the Director of Administrative Services and receive approval for the sharing;

3. Have abided by the District's policy and procedures for use of annual leave and Sick Leave Bank during his/her term of employment with the District; and the following procedures shall be followed in the determination of qualification for and administration of shared leave.
 - a) The department head will provide the Human Resources Department with evidence of the employee's need for shared annual leave.
 - b) Appropriate medical justification and documentation.
 - c) Amount of time, which the employee can reasonably be expected to be absent due to the condition.

Human Resources will present verification of the situation, evidence of prior use of annual leave, and Sick Leave as well as timing for the depletion of the employee's annual leave and Sick Leave Bank to the general manager for approval of sharing.

The employee shall not receive more than a total of eighteen (18) months of shared annual leave throughout the term of his/her employment with the District. To the extent possible, shared leave should be used on a consecutive basis.

The employee shall receive no more than four (4) weeks of shared annual leave at one time. At the end of each four-week period, a review of the situation will be conducted by Human Resources and report will be given to the general manager for consideration of continued sharing. Factors that may be considered in continuation of use of shared annual leave include but are not necessarily limited to:

- a) The estimated (if an estimation is possible) duration of the circumstances that gave rise to the situation, and
- b) The extent to which it is determined, in the sole discretion of the District, that further absence of the employee from his/her duties can be accommodated without hiring replacement personnel.

After written approval is given, Human Resources will inform other employees of the District that there is need for donations of Annual Leave for sharing. The personal situation of the employee in need of shared annual leave will be kept as confidential as possible during this process.

4. To be eligible to donate annual leave, an employee must comply with the following:
 - a) Have a balance of ten (10) days or more of accrued annual leave after the donation, and
 - b) Have taken a minimum of ten (10) days of annual leave within the prior calendar year or have a total of accrued and used annual leave of ten (10) days or more for the prior calendar year.

In no event shall a donation of annual leave be approved which will result in an employee reducing his/her accrued annual leave to less than ten (10) days.

All donations of annual leave shall be in increments of .25 hours and will be acknowledged by the donating employee in writing to Human Resources. All donation of annual leave shall

be voluntary and no amounts of annual leave will be transferred which have not been specifically authorized in writing by the donating employee.

Shared annual leave will be transferred each payroll cycle on a dollar-for-dollar basis. The value of the annual leave being donated shall be determined at the salary or hourly wage of the donating employee and the annual leave available to the receiving employee shall be calculated at there salary or hourly wage.

Human Resources shall be responsible for computing the value of donated annual leave and for adjusting the accrued annual leave balance of the receiving employee. Record of all annual leave donated shall be maintained for audit purposes.

The value of any annual leave donated, which remains unused, shall be returned at its original value to the employee or employees who have donated the annual leave. To the extent administratively feasible, the unused annual leave shall be returned on a prorated basis to all employees who have donated.

While an employee is on shared annual leave status, he/she will continue to be classified as a regular District employee and may maintain salary and benefits as if the employee was using their own accrued annual leave, except that additional annual leave will not be accrued by the receiving employee while that employee remains wholly on shared leave status. If the employee is only partially on paid leave status, their PTO accrual will be prorated to reflect that.

FAMILY & MEDICAL LEAVE

PUD 1 endeavors to provide a work environment that recognizes employees as an important part of the organization, as family members, and as individuals. PUD 1 recognizes that certain life events, such as the serious illness of the employee or employee's family member, the birth, adoption or foster care placement of a child, or a family member's military deployment or service-related injury are particularly significant and may require that the employee take time off from work. For this reason, the District strives to reasonably accommodate the needs of employees for periods away from work. PUD 1 has adopted human resources policies and benefits that support employees and their families.

It is Mason PUD 1's policy to authorize leaves of absence for eligible employees for qualifying circumstances, as specified in the federal Family and Medical Leave Act (FMLA), and other relevant statutes and regulations. Such leave shall include leave for the life events set forth in the purpose provision above, and as set forth in detail in the following sections. Administration of such leaves shall be conducted in accordance with applicable laws and regulations. Mason PUD 1 maintains posted notices summarizing employees' rights and responsibilities under the FMLA – contact Human Resources for information.

DEFINITIONS:

All terms used in this policy will be defined by the U.S. Department of Labor's regulations implementing the FMLA (see 29 CFR 825.800 – Definitions). The following terms are briefly summarized to assist employees in understanding the essential nature of applicable terms. Additional relevant terms and complete definitions are set forth at 29 CFR 825.800.

Child: A biological, adopted or foster child, stepchild, a legal ward or a child for whom the employee stands *in loco parentis* (in the place of a parent), where child is under the age of

18 or is 18 years of age or older and incapable of self-care because of a mental or physical disability at the time that the FMLA leave is to commence.

Covered Military Member: The employee's spouse, son, daughter or parent on active duty or call to active duty status.

Covered Service Member: A current member of the Armed Forces, including a member of the National Guard or Reserves, who is undergoing medical treatment, recuperation or therapy, is otherwise in outpatient status, or is otherwise on the temporary disability retired list, for a serious injury or illness incurred in the line of duty on active duty.

Exigency Leave: (See examples set forth in following paragraph) An approved absence due to a qualifying exigency arising out of the employee's spouse's, child's or parent's call to or active duty in the Reserves or National Guard by the federal government in support of a contingency operation.

Qualifying exigencies: Examples include short-notice deployment, attending certain military events and related activities, attending family support and assistance programs, arranging for temporary childcare and coverage for school activities, addressing financial and legal arrangements, attending counseling related to the deployment by a non-medical counselor, rest and recuperation with a covered member on leave from deployment, attending post-deployment activities such as post-deployment re-integration briefings, and additional activities not encompassed in the other categories, but agreed to by the employer and employee.

Group Health Plan: Any plan of, or contributed by, Mason PUD 1, to provide health care, including medical care, surgical care, hospital care, dental care, eye care, mental health counseling and substance abuse treatment.

Health Care Provider: A doctor of medicine or osteopathy who is authorized to practice medicine or surgery by the state in which the doctor practices; podiatrists, dentists, clinical psychologists, clinical social workers, optometrists, chiropractors (limited to treatment consisting of manual manipulation of the spine to correct a subluxation as demonstrated by x-ray to exist); physician assistants, nurse practitioners and nurse midwives performing within the scope of their practice as allowed by state law; Christian Science practitioners; or any other health care provider from whom Mason PUD 1's group health plan will accept certification for benefits claims.

Highly Compensated Employee: A salaried employee who is among the highest paid 10% of all employees within 75 miles of the employer's worksite.

Next of Kin of Covered Service Member: The nearest blood relative, other than the service member's spouse, parent, son, or daughter, in order of priority: a blood relative designated by the service member as "next of kin"; a relative granted legal custody of the service member; brothers; sisters; grandparents; aunts and uncles; and first cousins.

Parent: An employee's biological, adopted, step or foster parent. A person standing in *loco parentis* to the employee. This term does not include an employee's mother-in-law or father-in-law.

Qualifying exigencies: see "Exigency Leave"

Serious health condition: Mason PUD 1 intends to rely on the FMLA's regulations to determine whether an employee's or family member's condition is a "serious health condition," or whether a covered service member has a serious illness or injury incurred in the line of active duty. Each case will be evaluated individually in compliance with the FMLA. Employees are advised to contact the human resources department to obtain a detailed definition of a serious health condition, or a serious illness or injury incurred in the line of duty.

Spouse: A husband or wife as defined or recognized under applicable state law, including common law marriage. Employees needing leave to care for a domestic partner's serious health condition should contact Human Resources for assistance.

Eligibility:

The employee must have worked for the Mason PUD 1 for at least 12 months before taking leave and must have worked at least 1,250 hours for the Mason PUD 1 during the 12 consecutive months immediately prior to taking the leave. Time that is paid for but not worked (ex: sick leave, vacation, holidays, paid time off, extended illness benefits, etc.) and does not count toward the 1,250 hour total.

Employees who do not meet the foregoing FMLA eligibility requirements should contact Human Resources to determine how to proceed.

Types of FMLA Leave:

Employee Medical Leave: An approved absence due to an employee's serious health condition that renders the employee unable to perform the essential functions of his or her position.

Family Medical Leave: An approved absence due to the employee's need to care for a child, spouse or parent with a serious health condition.

Parental Leave: An approved absence due the employee's need to care for a newborn child, a newly adopted child or a newly placed foster child. When an FMLA-eligible female employee in Washington State takes an FMLA Employee Medical Leave due to disability caused by her serious health conditions of pregnancy and childbirth (usually 6-8 weeks), further time off to care for her newborn child falls under the FMLA Parental Leave category. To the extent allowed by law, all leaves will run concurrent.

D) Exigency Leave: An approved absence due to a qualifying exigency arising out of the employee's spouse, child, or parent's call to or active duty in the Reserves or National Guard by the federal government in support of a contingency operation.

E) Military Caregiver Leave: An approved absence to care for the employee's spouse, child, parent or next of kin who is a current member of the Armed Forces (including the National Guard or Reserves) and who is undergoing medical treatment, recuperation or therapy, is in outpatient status, or is on the temporary disability retired list, for a serious illness or injury incurred by the member in the line of active duty in the Armed Forces.

Amount of Leave:

A) Employee Medical Leave, Family Medical Leave, Parental Leave, Exigency Leave:

Up to 12 workweeks of leave unpaid may be granted in a rolling 12-month period to FMLA eligible employees as defined in the following categories: employee medical leave, family medical leave, parental leave, or exigency leave. The rolling 12-month period is measured backward from the date the employee uses any Employee Medical, Family Medical, Parental or Exigency Leave under the FMLA.

B) Military Caregiver Leave: An eligible employee's FMLA entitlement is limited to a total of 26 workweeks of leave during a single 12-month period to care for a covered service member's service-related serious injury or illness. This single 12 month period is measured forward from the date of an employee's first absence to care for the covered service member's injury. Additionally, during any single 12-month period, the employer's total FMLA leave entitlement is limited to a combined total of 26 weeks for all qualifying reasons under the FMLA, including Military Caregiver Leave.

NOTICE TO EMPLOYEE: Human resources will provide an employee with written notice at the onset of FMLA leave, advising the employee whether they are eligible employee, as well as a notice confirming whether the leave qualifies as FMLA and how much FMLA leave the employee has available and/or will be using during the approved absence.

General Notice to Employer:

30-DAY NOTICE: Where leave is foreseeable (ex: planned medical treatment; birth or adoption of a child), the employee shall provide at least 30-days' advance notice, make efforts to schedule the leave so as not to disrupt operations, and submit any required health care provider certification before the leave begins. Although the initial notice or request for FMLA leave may be verbal, whenever the need for FMLA is foreseeable, the employee is required to complete a written FMLA leave request and submit it to Human Resources.

30-DAY NOTICE EXCEPTION: If 30 days advance notice is not practicable, such as because of lack of knowledge of approximately when the leave will be required to begin, a change in circumstances, or a medical emergency, or whenever Exigency Leave is needed, an employee must provide notice of the need for leave as soon as practicable (generally on the same or next business day as the employee became aware of the need for such leave). If applicable, the employee must provide the health care provider or other required certification within 15 days of request. If the need for the leave is unforeseeable, including when FMLA is being used on an intermittent basis, the employee must still comply with normal call-in procedures that apply to the employee's specific position.

FMLA REQUEST CONTENT REQUIREMENTS: When requesting leave, employees must provide sufficient information for Mason PUD 1 to determine if the absence may qualify as FMLA leave, as well as information about the anticipated timing and duration of the leave. Sufficient information may include: that the employee is unable to perform job functions; the family member is unable to perform daily activities; the need for hospitalization or continuing treatment by a healthcare provider; or circumstances supporting the need for Exigency Leave or Military Caregiver Leave. Employees must also inform Mason PUD 1 if the absence is for a reason for which FMLA leave was previously taken or certified.

PERIODIC STATUS REPORTS: During the leave, the employee may be required to report periodically to Human Resources on his or her status, continuing need for leave and continued intention to return to work.

RETURN TO WORK REPORT: Employees whose leave is necessary because of their own serious health condition will be required to provide a release/fitness-for-duty report assessing the employee's current ability to perform the essential job functions, as a condition of their return to work. A current job description will be provided by Mason PUD 1 to the health care provider to assist in this process. In the case of Employee Medical Leave taken on an intermittent or reduced work schedule basis, a release/fitness for duty certification also may be required every 30 days if safety concerns exist regarding the employee's ability to perform the job without a significant risk of harm to the employee or others.

Additional Provisions – Employee or Family Medical Leave:

HEALTH CARE PROVIDER CERTIFICATION: Mason PUD 1 requires a health care provider certification to support a request for leave for an employee to care for the employee's own serious health condition or a seriously ill child, spouse or parent. For Employee Medical Leave, the certification must include a statement that the employee is unable to perform the essential functions of his or her position. For Family Medical Leaves, the certification must include a section completed by the employee describing the care that the employee will be providing to the family member and the employee's estimate of the leave needed to provide care for the family member. With either Employee Medical or Family Medical Leaves, the health care provider must include an estimate of the duration of leave. When a certification is requested it must be provided within 15 days, absent unusual circumstances. Mason PUD 1 may require, at its discretion and expense, a second medical opinion. If the first and second opinions differ, Mason PUD 1 may require, at its expense, the binding opinion of a third health care provider, who will be chosen jointly by Mason PUD 1 and the employee.

INTERMITTENT / REDUCED SCHEDULE REQUIREMENTS: If certified as medically necessary due to the serious health condition of the employee or the employee's spouse, child, or parent, FMLA leave may be taken on an intermittent or reduced leave schedule. Absences on an intermittent or reduced schedule basis will only be counted against the FMLA entitlement for such time actually absent from work. Whenever an employee needs intermittent leave or a reduced work schedule for the employee's or family member's planned medical treatment, the employee must make a reasonable effort to schedule the treatment(s) so not to disrupt unduly Mason PUD 1's operations. Additionally, if leave is requested on an intermittent or reduced work schedule basis because of foreseeable, planned medical treatment of the employee or family member, Mason PUD 1 may require the employee to temporarily transfer to an alternative position for which the employee is qualified and which better accommodates the recurring periods of absence or part-time schedule, provided that the position has or the employee receives equivalent pay and benefits.

USE OF ACCRUED LEAVE: Employees on an FMLA leave due to their own or a family member's serious health condition may be required to use their accrued leave (ex: sick leave, vacation, personal holidays, personal leave, paid time off, extended illness benefits, etc.) during the FMLA leave. When an employee's serious health condition is due to an on the job injury or illness, available paid leave will be coordinated with workers' compensation benefits to the extent allowed by state law. The smallest unit of paid leave which may be used is fifteen (15) minutes. If paid time is unavailable or exhausted, the FMLA leave is unpaid.

Additional Provisions – Parental Leave:

DOCUMENTATION OF FAMILY RELATIONSHIPS: Employees who request a Parental Leave may be required to provide reasonable documentation of family relationships. Parental Leave only may be taken on an intermittent or reduced leave schedule basis if Mason PUD 1 agrees. Absences on an intermittent or reduced schedule basis will only be counted against the 12-workweek entitlement for such time actually absent from work. Spouses who are both employed by Mason PUD 1 are limited to a combined total of 12 workweeks of FMLA leave to care for a newborn or newly placed child (both paid and unpaid).

Additional Provisions – Exigency Leave:

DOCUMENTATION OF DUTY STATUS: Where employee's spouse, son, daughter, or parent (if "covered military members") are on active duty or call to active duty status, Mason PUD 1 may require certification that the respective "covered military member" is in the National Guard or Reserves and has been called to or is on active duty in support of a contingency operation. Generally, providing a copy of the member's active duty orders when requested satisfies this certification requirement. An employee requesting Exigency Leave may also be required to provide a statement with supporting documentation about the nature and details of the specific exigency, the amount of leave being requested, and the employee's relationship to the military member. When either certification is requested it must generally be provided within 15 days, absent unusual circumstances.

LEAVE STRUCTURE: Subject to the following, leave due to a qualifying exigency may be taken in a block of time, on an intermittent or a reduced workweek basis. Short-term deployment Exigency Leaves are usually limited to seven days when the military member receives seven or less days' notice of a call to active duty. Exigency Leaves to make temporary child care arrangements and deal with school activities do not include time off to deal with ongoing child care. Exigency Leaves while the service member is on leave from deployment for rest and recuperation are permitted for up to five days while the service member is on temporary rest and recuperation leave from deployment.

USE OF ACCRUED LEAVE: During an Exigency Leave, employees may be required to use accrued leave (ex: sick leave, vacation, personal leave, personal holidays, paid time off, extended illness benefits, etc.). The smallest unit of paid time which may be used is fifteen (15) minutes. When available paid leave is exhausted, Exigency Leave is unpaid.

Additional Provisions – Military Caregiver Leave:

DOCUMENTATION FROM HEALTH CARE PROVIDER: Mason PUD 1 may require information from the service member's health care provider to support a request for Military Caregiver Leave. If the Department of Defense ("DOD") has issued an invitational travel order or authorization and a copy is provided to Human Resources it will be accepted as certification of the serious illness or injury of the service member for the duration specified on it. In the absence of an invitational travel order or authorization, medical certification of the service member's serious illness or injury must be completed by a DOD or VA health care provider, or a DOD TRICARE network or TRICARE authorized private health care provider.

DOCUMENTATION OF RELATIONSHIP: As part of the certification process, an employee may be required to verify their relationship to the covered service member and other information about the covered service member, such as military branch, medical treatment facility, a description of the care to be provided, and the duration of the leave.

LEAVE STRUCTURE: Military Caregiver Leave may be taken in a block of time. If certified as medically necessary, Military Caregiver Leave also may be taken intermittently or by working a reduced schedule. When it is used intermittently or by working a reduced schedule due to the service member's planned medical treatment, the employee must make a reasonable effort to schedule planned treatment so as to not unnecessarily disrupt Mason PUD 1's operations. Additionally, when such leave is foreseeable for planned medical treatment of the service member, the employee may be temporarily transferred during the intermittent leave or reduced work schedule period to an alternative position for which the employee is qualified and which better accommodates the reoccurring periods of absence, provided the alternative position has equivalent pay and benefits.

USE OF ACCRUED LEAVE: Employees on Military Caregiver Leave may be required to use accrued leave (ex: sick leave, vacation, personal holidays, personal leave, paid time off, extended illness benefits, etc.). The smallest unit of paid leave which may be used is fifteen (15) minutes. When available paid leave is exhausted, Military Caregiver Leave is unpaid.

Paid/Unpaid Leave and Benefits Continuation:

USE OF ACCRUED LEAVE: As set forth in the preceding sections, an employee who is granted leave under this policy may be required to first use all available accrued leave (ex: sick leave, vacation, personal holidays, personal leave, paid time off, extended illness benefits, etc.). After such leave is depleted, the remainder of the FMLA leave period shall be unpaid.

MEDICAL, DENTAL, LIFE & LONG TERM DISABILITY PREMIUM PAYMENT: During the leave period (including any unpaid portion), the Mason PUD 1 shall continue to pay premiums for medical, dental, life and long term disability insurance coverage as if the employee was an active worker.

SUPPLEMENTAL INSURANCE PREMIUM PAYMENT: If the employee has supplemental insurance coverage through payroll deduction, he/she shall be required to pay the premiums for that coverage to the Mason PUD 1 during the leave period.

COORDINATION WITH HUMAN RESOURCES: If the employee taking FMLA leave contributes a portion of his/her or a dependent's insurance premiums, the employee must make arrangements with Human Resources at the start of the leave for continuing the employee's portion of such premiums during any unpaid FMLA leave.

FAILURE TO RETURN TO WORK: If the employee fails to return to work after leave, Mason PUD 1 reserves the right to recover any premium payments paid to maintain benefit coverages during the leave period *unless* the employee cannot return for reasons beyond the employee's control, including:

1. Continuation, recurrence or onset of the employee's or immediate family member's serious health condition that would entitle the employee to leave under this policy (without regard to whether the employee has exhausted the allowable 12 weeks); or
2. Other circumstances *beyond the control of the employee.*

ACCRUAL OF PTO: Accrual of PTO will be prorated according to the amount of time the employee is on paid status during any month in which they are on medical or family leave.

UNION SENIORITY ACCRUAL: Seniority for union employees shall continue to accrue while an employee is on paid status. No seniority is accrued during any of the unpaid leave period.

Job Restoration:

GENERALLY: If the medical or family leave requires 12 weeks or less unpaid leave from the job, the employee will be returned to the position which was held at the time the leave began and to the same headquarters location. If, during the employee's leave the position is filled, the returning employee will be reinstated and the replacement employee will return to his/her former position or bid or apply for another position. Reinstatement may be denied to employees who fail to provide a required release/fitness-for-duty certificate.

If unpaid leave is granted in addition to the provided 12-week period, the employee has no job return rights. Once released, the employee may exercise seniority to bid (bargaining unit employee position) into other jobs or apply (non-union employee positions) for other Mason PUD 1 positions for which they may be qualified and has a medical release to perform.

Job return rights may be extended with the approval of the General Manager.

EXCEPTIONS: An employee has no greater right to reinstatement or to other benefits and conditions of employment during an FMLA leave, than if the employee had been continuously, actively employed during the FMLA leave period. Thus, if an employee's job is eliminated or hours are reduced while the employee is on leave, or if the employee would have been laid off even if the employee had not been on leave, the employee may be laid off while on leave or be assigned a reduced work schedule upon reinstatement. Similarly, if misconduct or performance problems are uncovered before or while an employee is on an FMLA leave, an employee may be subject to discipline while on or when returning from FMLA leave.

MODIFIED ASSIGNMENTS: If appropriate work is available and the employee's medical restrictions (as provided by the health care provider) permit him/her to perform the work, the employee may be offered a medically restricted modified-duty job assignment. When working in a modified-duty assignment, the employee is still on leave from the job and the maximum length of the job return rights provision of this procedure shall apply. If the employee does not accept a modified-duty assignment, he/she will remain on leave.

Employees will perform modified-duty work assignments to the best of their abilities and limitations. Good faith effort is the employee's obligation. While in a modified-duty assignment the employee will receive Mason PUD 1 benefits as provided to all active employees. The employee's pay will be adjusted to reflect the work he/she is performing while in modified-duty assignments.

LONG TERM DISABILITY: In certain situations where an employee is unable to perform an available Mason County PUD 1 job due to medical disabilities, the possibility of qualifying for long-term disability through the group LTD insurance program should be explored. The Human Resources Manager should be contacted for information.

Procedure Upon Exhaustion of FMLA:

Employees who have exhausted their FMLA entitlement and who need additional leave may request Personal Leave. Personal Leave may be granted on different terms and conditions than FMLA leaves. Generally, such employees will need to continue group health insurance at their own cost. Additionally, an employee's position may not be held during a Personal Leave unless required as a reasonable accommodation.

Coordination with Washington Law:

No FMLA provisions supersede any provision of State or local law that provide greater family or medical leave rights than those provided by FMLA. 29 CFR 825.701. In the absence of an employee's voluntary request for protected leave, the District may designate an employee's leave as FMLA leave or leave under State law, when appropriate.

According to applicable law, if leave qualifies for FMLA leave and leave under State law, the leave used may count against the employee's entitlement under both laws. Further details regarding FMLA's interaction with state law is set forth at 29 CFR 825.701.

WASHINGTON PAID FAMILY & MEDICAL LEAVE

Paid Family and Medical Leave (PFML) is a mandatory statewide insurance program, administered by the Washington State Employment Security Department, that provides almost every Washington employee with paid time off to give or receive necessary care. To be eligible for the State benefit, employees must have worked 820 hours in the qualifying period (defined as the first four of the last five calendar quarters), for any employer(s) in Washington State. The program is funded by premiums paid by both employees and employers. The employee portion will be deducted from your paycheck.

If you qualify, this program will allow you to take up to 12 weeks, as needed, if you:

- welcome a child into your family (through birth, adoption or foster placement),
- experience a serious illness or injury,
- need to care for a seriously ill or injured family member,
- need time to prepare for a family member's pre- and post-deployment activities, as well as time for childcare issues related to a family member's military deployment.

If you face multiple events in a year, you may be eligible to receive up to 16 weeks, and up to 18 weeks if you also experience a pregnancy-related serious health condition.

If the need for leave is foreseeable, you must provide Mason County PUD No. 1 at least 30 days' notice.

If approved by the State, you may be entitled to partial wage replacement while on leave. The benefit is a percent of your weekly wage, as determined by the State. You will file your claim with the Employment Security Department and, if approved, you will be paid by the Employment Security Department. Retaliation for requesting or taking Paid Family and Medical Leave is prohibited.

Employees may use paid time off to supplement wages while using PFML.

If you are eligible for the federal Family and Medical Leave Act (FMLA) and your FMLA and PFML leave run concurrently or overlap, you will be entitled to maintain your health

insurance while you are on leave. You must continue to pay your portion of the premium cost while on leave.

Chapter 49.76 RCW – Domestic Violence Leave

PURPOSE:

If you are a victim of actual or threatened domestic violence, sexual assault or stalking, Mason PUD 1 will provide you with reasonable safety accommodations. You may be asked for written verification that you are a victim of domestic violence, sexual assault, or stalking.

Mason PUD 1 provides reasonable leave for employees who are victims of domestic violence, sexual assault or stalking, or for employees whose family members are victims, to participate in legal proceedings, receive medical treatment or obtain other necessary services. To the extent allowed by law, Mason PUD 1 will maintain coverage under any health insurance plan for the employee for the duration of the leave.

An employee may take, reasonable unpaid leave, intermittent leave or leave on a reduced leave schedule to:

- a) Seek legal or law enforcement assistance or remedies to ensure the health and safety of the employee or employee's family members including, but not limited to, preparing for, or participating in, any civil or criminal legal proceeding related to or derived from domestic violence, sexual assault, or stalking;
- b) Seek treatment by a health care provider for physical or mental injuries caused by domestic violence, sexual assault, or stalking, or to attend to health care treatment for a victim who is the employee's family member;
- c) Obtain, or assist a family member in obtaining, services from a domestic violence shelter, rape crisis center, or other social services programs for relief from domestic violence, sexual assault, or stalking;
- d) Obtain, or assist a family member in obtaining, mental health counseling related to an incident of domestic violence, sexual assault, or stalking, in which the employee or employee's family member was a victim of domestic violence, sexual assault, or stalking; or
- e) Participate in safety planning, temporarily or permanently relocate, or take other actions to increase the safety of the employee or employee's family member from future domestic violence, sexual assault, or stalking.

DEFINITIONS:

"Child" means a biological, adopted or foster child, a stepchild, a legal ward, or a child of a person standing in loco parentis who is: (a) under eighteen years of age; or (b) eighteen years of age or older and incapable of self-care because of a mental or physical disability.

"Dating Relationship" means a social relationship of a romantic nature. Factors that the court may consider in making this determination include: (a) the length of time the

relationship has existed; (b) the nature of the relationship; and (c) the frequency of interaction between the parties.

“Domestic violence” means (a) physical harm, bodily injury, assault, or the infliction of fear of imminent physical harm, bodily injury or assault, between family or household members; (b) sexual assault of one family or household member by another; or (c) stalking as defined herein by one family or household member by another family or household member.

“Family member” means any individual whose relationship to the employee can be classified as a child, spouse, parent, parent-in-law, grandparent, or person with whom the employee has a dating relationship.

“Intermittent leave” means leave taken in separate blocks of time due to a single qualifying reason.

“Reduced leave schedule” means a leave schedule that reduces the usual number of hours per workweek, or hours per workday, of an employee.

“Sexual assault” means one or more of the following: (a) rape or rape of a child; (b) assault with intent to commit rape or rape of a child; (c) incest or indecent liberties; (d) child molestation; (e) sexual misconduct with a minor; (f) custodial sexual misconduct; (g) crimes with a sexual motivation; or (h) an attempt to commit any of the aforementioned offenses.

“Stalking” occurs where a person, without lawful authority and under circumstances not amounting to a felony attempt of another crime: (a) intentionally and repeatedly harasses or repeatedly follows another person; and (b) the person being harassed or followed reasonably fears that the stalker intends to injure the person, another person, or the property of the person or of another person; and the stalker either (i) intends to frighten, intimidate or harass the person, or (ii) knows or reasonably should know that the person is afraid, intimidated or harassed even if not intended by the stalker.

USE OF LEAVE: An employee who is absent from work pursuant to this policy may elect to use the employee's sick leave and other paid time off.

NOTICE REQUIREMENTS:

When the need for leave is foreseeable the employee must give as much advance notice as possible.

When advance notice is not possible because of emergency or unforeseen circumstances the employee or his/her designee must give notice no later than the end of the first day that the employee takes such leave.

DOCUMENTATION:

When an employee requests leave, the employer may require that the request be supported by verification that the employee or employee's family member is a victim of domestic violence, sexual assault or stalking; and the leave was/is for a purpose outlined in the “Purpose” section above.

ACCEPTABLE DOCUMENTATION:

When verification is required, it must be provided in a timely manner. In the event that advance notice of the leave cannot be given because of emergency or unforeseen circumstance verification must be provided to the employer within a reasonable time period during or after the leave.

An employee may satisfy the verification requirement by providing one or more of the following;

- a) A police report indicating that the employee or employee's family member was a victim of domestic violence, sexual assault or stalking.
- b) A court order protecting or separating the employee or employee's family member from the perpetrator. Or other evidence from the court or prosecuting attorney that the employee or employee's family member appeared or is scheduled to appear in court in connection with an incident of domestic violence, sexual assault, or stalking.
- c) Documentation that the employee or the employee's family member is a victim of domestic violence, sexual assault, or stalking, from any of the following persons from whom the employee or employee's family member sought assistance in addressing the domestic violence, sexual assault, or stalking: An advocate for victims of domestic violence, sexual assault, or stalking; an attorney; a member of the clergy; or a medical professional. Note that provision of documentation under this section has no impact on the confidential and/or privileged nature of such communications.
- d) An employee's statement that the employee or the employee's family member is a victim of domestic violence, sexual assault, or stalking and that the leave taken was for one of the purposes described RCW 49.90.020.

Documentation of familial relationship: If the victim of domestic violence, sexual assault, or stalking is the employee's family member, verification of the familial relationship between the employee and the victim may include, but is not limited to, a statement from the employee, a birth certificate, a court document, or other similar documentation.

CONFIDENTIALITY:

The employee is not required to produce or discuss any information with the employer that is beyond the scope of what is required in this policy or that would compromise the employee's safety or the safety of the employee's family member in any way.

The employer will maintain the confidentiality of all information provided by the employee and will maintain confidentiality of the fact that the employee or employee's family member is a victim of domestic violence, sexual assault or stalking and that the employee requested leave under this policy unless:

- a) The employee requests or consents to the employer releasing information; b) Release of information is ordered by the court of administrative agency; or c) The release of information is required by the applicable federal or state law;

BENEFITS / POSITION:

The taking of leave shall not result in the loss of any pay or benefits to the employee that accrued before the date on which the leave commenced.

The employer will restore the employee to the position of employment held by the employee when the leave commenced; or restore the employee to an equivalent position with equivalent employment benefits, pay and other terms and conditions of employment.

The prior section does not apply if the employment from which the individual takes leave is:

- a) With a staffing company and that individual is assigned on a temporary basis to perform work at or services for another organization to support or supplement the other organization's workforces, or to provide assistance in special work situations such as, but not limited to, employee absences, skill shortages, seasonal workloads or to perform special assignments or projects, all under the direction and supervision of the organization to which the individual is assigned; or
- b) If an employee was hired for a specific term or only to perform work on a discrete project, the employment term or project is over, and the employer would not otherwise have continued to employ the employee.

POSTING:

Mason PUD 1 maintains a posted version of a related notice pursuant to RCW 49.76.130.
Chapter 49.77 RCW – Military Family Leave

PURPOSE:

Mason PUD 1 provides for leave during a period of military conflict for employees who are spouses of members of the armed forces of the United States, national guard, or reserves, who have been notified of impending calls to order to active duty or who have been deployed. Employees are entitled to a total of fifteen (15) days of unpaid leave per deployment.

DEFINITIONS:

"Department" means the department of labor and industries.

"Employee" means a person who performs service for hire for an employer, for an average of twenty or more hours per week, and includes all individuals employed at any site owned or operated by an employer, but does not include an independent contractor.

"Employer" means (a) any person, firm, corporation, partnership, business trust, legal representative, or other business entity which engages in any business, industry, profession, or activity in this state; (b) the state, state institutions, and state agencies, and (c) any unit of local government including, but not limited to, a county, city, town, municipal corporation, quasi-municipal corporation, or political subdivision.

"Period of military conflict" means a period of war declared by the United States Congress, declared by executive order of the president, or in which a member of a reserve component of the armed forces is ordered to active duty pursuant to either sections 12301 and 12302 of Title 10 of the United States Code or Title 32 of the United States Code.

"Spouse" means a husband or wife, as the case may be, or state registered domestic partner.

TIMING OF LEAVE:

Leave may be taken after the notification or order, either before the spouse's deployment or when the spouse is on leave from deployment.

NOTICE:

An employee must provide the employer with notice of intent to take leave under this chapter, within five (5) business days of receiving the official notice of impending call or order to active duty.

USE OF LEAVE:

You may choose to apply applicable accrued paid leave benefits while taking military family leave.

BENEFITS / POSITION:

Health Insurance Benefits: Health insurance benefits may continue at the level and conditions as provided under applicable laws.

Benefit Retention/Accrual: The taking of leave under this policy may not result in the loss of any employment benefits accrued before the date on which the leave commenced. However, benefit accruals, such as seniority, vacation, sick leave, or holiday benefits, will be suspended during the leave and will resume upon return to active employment.

Return to Work: Any employee taking leave under this policy is entitled, upon return from leave, to be restored by the employer to the position of employment held by the employee at the time the leave commenced; or to be restored to an equivalent position with equivalent employment benefits, pay and other terms and conditions of employment, with certain exceptions as provided by law (see, for example, RCW 49.78.280(2)).

Failure to Return: Unless prior arrangements have been agreed upon, if an employee fails to return to work on the agreed upon return date, the employee will be deemed to have resigned.

JURY DUTY

PUD No.1 encourages employees to fulfill their civic responsibilities by serving jury duty when required. Employees in an eligible classification may request up to 2 weeks of paid jury duty leave over any 2 year period. Any jury duty pay received by the employee while in a paid status shall be remitted to PUD No. 1.

Jury duty pay will be calculated on the employee's base pay rate times the number of hours the employee would otherwise have worked on the day of absence. Employee classifications that qualify for paid jury duty leave are:

- * Regular full-time employees

* Regular part-time employees may take unpaid time off for jury duty.

If employees are required to serve jury duty beyond the period of paid jury duty leave, they may use any available paid time off (for example, vacation benefits) or may request an unpaid jury duty leave of absence. In such case the employee may retain the jury duty pay received.

Employees must show the jury duty summons to their supervisor as soon as possible so that the supervisor may make arrangements to accommodate their absence. If you are excused from jury duty, or if you are released when there are at least four hours of the normal workday remaining, you must report to work if you were scheduled to work.

Either the District or the employee may request an excuse from jury duty if, in the District's judgment, the employee's absence would create serious operational difficulties.

PUD 1 will continue to provide health insurance benefits for the full term of the jury duty absence. Benefit accruals shall continue.

WORKPLACE HEALTH AND INJURY

ACCIDENT REPORTING

Accidents are preventable and we take every possible precaution to make your working conditions safe. The final responsibility for an accident free workplace is up to you. All accidents, whether resulting in a personal injury or not, must be reported to your supervisor regardless of how minor they may be. Even minor accidents may indicate an unsafe condition, which should be corrected.

SAFETY

To assist in providing a safe and healthful work environment for employees, customers, and visitors, PUD 1 has established a workplace safety program. This program is a top priority for the District.

The General Manager and Safety Coordinator have the responsibility for implementing, administering, monitoring, and evaluating the safety program. Its success depends on the alertness and personal commitment of all.

PUD 1 provides information to employees about workplace safety and health issues through regular internal communication channels such as supervisor-employee meetings, bulletin board postings, memos, or other written communications. A labor-management safety committee, composed of representatives from throughout the organization, has been established to help monitor PUD 1 safety program and to facilitate effective communication between employees and management about workplace safety and health issues.

Employees and supervisors receive periodic workplace safety training. The training covers potential safety and health hazards and safe work practices and procedures to eliminate or minimize hazards.

Some of the best safety improvement ideas come from employees. Those with ideas, concerns, or suggestions for improved safety in the workplace are encouraged to raise them

with their supervisor, or with another supervisor or manager, or bring them to the attention of a member of the labor-management safety committee. Reports and concerns about workplace safety issues may be made without fear of reprisal.

Each employee is expected to obey safety rules and to exercise caution in all work activities. Employees must immediately report any unsafe condition to the appropriate supervisor. Employees who violate safety standards, who cause hazardous or dangerous situations, or who fail to report or, where appropriate, remedy such situations, may be subject to disciplinary action, up to and including termination of employment. (Reference the Accident Prevention Program.)

In the case of accidents that result in injury, regardless of how insignificant the injury may appear, employees should notify the Safety Chairman or the appropriate supervisor within a reasonable time. Such reports are necessary to comply with laws and initiate insurance and workers' compensation benefits procedures.

SMOKING

In keeping with PUD 1's intent to provide a safe and healthful work environment, for employees and members of the public who are conducting business at PUD 1 facilities, it is the purpose of this policy to minimize negative effects of second hand smoke on all personnel and the public.

Passage of Washington State Initiative Measure No. 901, approved November 8, 2005, prohibits smoking in buildings and vehicles open to the public and places of employment, including areas within twenty-five (25) feet of doorways, windows that open, and ventilation intakes. The use of tobacco and E-cigarettes/vapes is also prohibited by this policy.

Therefore, this non-smoking policy will apply to all PUD 1 employees, contractors, and visitors to the PUD 1 facilities.

As defined in RCW 70.160.020 (revised by Initiative 901):

"Smoke" or "Smoking" as used herein, means the carrying or smoking of any kind of lighted pipe, cigar, cigarette, or any other lighted smoking equipment.

"Public place" means that portion of any building or vehicle used by and open to the public, and includes a presumptively reasonable minimum distance of twenty-five (25) feet from entrances, exits, windows that open, and ventilation intakes that serve an enclosed area where smoking is prohibited.

"Place of employment" means any area under the control of a public or private employer which employees are required to pass through during the course of employment, including, but not limited to: entrances and exits to the places of employment and including a presumptively reasonable minimum distance of twenty-five (25) feet from entrances, exits, windows that open, and ventilation intakes that serve an enclosed area where smoking is prohibited; work areas; restrooms; conference and classrooms; break rooms and cafeterias; and other common areas.

No person may smoke in a public place or in any place of employment. (RCW 70.160.030)

Signs shall be posted conspicuously at each of the PUD 1 building entrances which state that smoking is prohibited.

Individuals intentionally violating the non-smoking policy by smoking in a public place or place of employment, or any person removing, defacing, or destroying a sign required by Chapter 70.160 RCW could be subject to a civil fine of up to one hundred dollars (\$100).

In addition, employees not observing the policy will become subject to the disciplinary procedures outlined in the PUD's Employee Handbook.

This policy applies equally to all employees, customers, and visitors.

USE OF EQUIPMENT & VEHICLES

Work related motor vehicle crashes are the leading cause of on-the-job injury and deaths in the United States. Therefore, no company's safety program is complete unless it incorporates vehicle safety. It is the management philosophy and commitment of Mason County PUD No. 1 to develop, implement and effectively direct a fleet vehicle/equipment safety and use policy.

This policy applies to the use and operation of all vehicles and work equipment for Mason County PUD No. 1. It also applies to all employees who may drive a company owned or leased vehicle while on company business, or who may drive their own vehicle (with management permission) in the conduct of company business.

A. Vehicle and Equipment Use Rules and Procedures

1. Safety restraints (seatbelts) are provided in all vehicles and equipment (where applicable) and are a proven tool for minimizing or eliminating injuries from motor vehicle or equipment accidents. Consequently, all drivers and passengers are required to wear safety restraints in the prescribed manner while operating or riding in a company owned or leased vehicle, or any other vehicle while on company business. The occupants in the vehicle will share the responsibility to enforce safety belt restraint use. Employees must ensure that all safety restraints are maintained in good operating condition and under no circumstances should any employee disable or interfere with the operation of the restraints. (In accordance with RCW 46.61.688.)

(Note - the presence of air bags in the vehicle does not negate the need to use seat belts. The two safety systems are designed to be most effective when used together).

2. Personal use of a company vehicle other than for business purposes, commuting to and from work or de minimis personal use (such as a stop for a personal errand between business' meetings) is prohibited.

3. Employees are to comply with all established vehicle traffic laws and regulations while operating a company vehicle or their own vehicle on company business at all times

4. All employees driving a company vehicle or driving their own vehicle while on company business are required to have a valid driver's license appropriate for the type of vehicle being driven and comply with all conditions and/or restrictions on that license.

5. Employees are prohibited from operation of any company vehicle or their own vehicle on company business while their judgment or faculties are impaired or reduced. As an example, such impairment or reduction of faculties may be due to consumption of alcoholic beverages, legal or illegal medications.
6. Firearms or any other "weapon" are not permitted in any company owned or leased vehicle or any personal vehicle used on company business. See employee handbook policy 522 for further definition.
7. Employees are strictly prohibited from the transportation of hitchhikers, strangers or other non-authorized personnel at all times. Note – "authorized personnel" are defined as employees, management, customers, and contractors or vendors conducting legitimate business with Mason County PUD 1. Employees may transport family members with prior management approval.
8. Employees who operate a medium or heavy duty company truck are required to possess the additional license as required of state and federal agencies as applicable for that vehicle. (CDL- Commercial Driver's License Class A or B).
9. Employees who operate a medium or heavy duty truck while on company business are required to adhere to both state and federal requirements for vehicle inspections.
10. Employees are required to operate any and all vehicles used for company business at a speed appropriate to the road, traffic and weather conditions as well as posted limits.
11. Drivers shall maintain their vehicles in a clean and orderly fashion and report any problems or needs to the supervisor.
12. Any employee that operates work equipment like a backhoe, cable plow, ditch witch and the like will be trained and qualified to do so by supervision and/or management.
13. Cell phones can be a valuable tool for servicing our clients. However, cell phones (whether company-provided or personal) may not be used to conduct company business while operating a vehicle. If you have a hands-free telephone device, you may use it while operating a vehicle; otherwise, should you need to use your cell phone, you must pull off the road, park, and make or receive the call. Reading, typing, or sending a text message, while driving, is strictly prohibited by law.

B. Vehicle Maintenance

1. All employees shall perform daily, weekly or monthly safety inspections to ensure the vehicle (or work equipment) is in a safe operating condition per the established schedule for that vehicle or piece of equipment. See your supervisor for additional information.
2. Employees are required at a minimum to maintain vehicles as recommended by manufacturer's specifications for preventative and scheduled maintenance. See your supervisor for additional information.
3. Suspected mechanical problems are to be repaired under the warranty whenever possible to help reduce overall costs.

C. Safety Awareness Training

The success of this fleet vehicle safety program requires that drivers be aware of the causes of motor vehicle accidents. To minimize employees' susceptibility to injury, and reduce

accidents, safe driver training will be provided to all drivers each year. This training may consist of videos, printed material and/or periodic safety meetings. In addition, an outside source for vehicle safety training may be utilized. Check with your supervisor for details.

IN THE EVENT OF AN ACCIDENT

1. Employees are to contact their immediate supervisor within a reasonable time after the accident.
2. The following information should be gathered at the accident scene and submitted to your supervisor. Use your accident reporting kit provided in the vehicle.
 - Name of vehicle owner - insurance information
 - Name of other driver(s)
 - Names of injured (if any)
 - Where injured were taken
 - Witnesses - for and against
 - Names and badge numbers of investigating officers
 - Time and location of accident
 - Weather conditions
 - Traffic conditions
 - Diagram and written description

Employee is required to fill out a state accident report. If the damage is estimated to be over \$750 the District will file the report with the WA State Patrol.

EMPLOYEES ARE NOT AUTHORIZED TO AND SHALL NOT EXPRESS OPINION AS TO FAULT OR LIABILITY, AGREE TO ANY SETTLEMENT ON BEHALF OF THE COMPANY OR SIGN ANY STATEMENTS OTHER THAN THE DOCUMENTS REQUIRED BY POLICE AUTHORITIES.

3. Management/ Safety Committee will review the circumstances of all reported accidents to determine cause and to take corrective actions as needed. "Preventability" will also be determined where applicable and the driver notified of the status.
4. Employees must comply with state laws and file written reports with state, county or city authorities in accordance with the laws of the applicable jurisdiction in the event of any accident.

D. Violations of Safety Policy

It is the responsibility of each employee to ensure that company vehicles are not driven or operated by anyone except in accordance with this policy.

Failure to comply with this vehicle safety policy or any part of the general safety policy may result in the revocation of driving privileges, as well as appropriate disciplinary action up to and including termination. All vehicle violations incurred on company business shall be borne by the employee.

RESPONSIBILITY

The supervisor has the responsibility to make sure his/her drivers understand and follow all provisions of this policy, provide preventive maintenance as needed and to report any vehicle problems or needs to the Director of Operations. While using a company vehicle

each driver has the responsibility to know and follow all the provisions of the vehicle safety program, including proper maintenance, periodic inspections of the vehicle to determine conditions, and reporting unsafe or unacceptable conditions to his/her supervisor.

EMERGENCY CLOSINGS

At times, emergencies such as severe weather, fires, power failures, or earthquakes, can disrupt company operations. In extreme cases, these circumstances may require the closing of a work facility.

When operations are officially closed due to emergency conditions, the time off from scheduled work will be unpaid unless approved by the General Manager.

ACKNOWLEDGMENT EMPLOYMENT RELATIONSHIP AND HANDBOOK RECEIPT

I have received a copy of the Employee Handbook outlining my responsibilities as an employee and the responsibilities of the Employer. I understand my obligation to read the information contained in this handbook.

If I have any questions, I will contact my supervisor. I understand that the employee handbook is merely a guide to acquaint myself with Mason PUD 1. It is not intended to be contractually binding nor is it intended to guarantee or promise specific employment benefits or duration of employment.

I understand I must comply with the guidelines, policies, and procedures of Mason PUD 1.

I understand my employment and compensation can be terminated at the option of either myself or Mason PUD 1 any time with or without reason or notice.

I understand the District reserves the right, at its discretion, to add, delete, or modify any provision in this handbook, with or without prior notice.

Signature of Employee: _____

Date: _____

Print Employee Name: _____

Bids for Water System Generators

Highland Estates & Wonderland Water Systems

Contractor	Bid Amount
Double D	\$105,320.95 (Non-responsive bidder)
Legacy	\$104,150.24

This project is to install back up generators at both the Highland Estates and Wonderland water system. Legacy Power System is the lowest responsible bidder.



Power Systems

A Division of Legacy Telecommunications, Inc.

September 20, 2021

PUD No. 1 Mason County
James Reyes EIT
21971 N. US Hwy 101
Shelton, WA. 98584
(360) 877-5249, x.215

Wonderland Well Site Generator Installation

Generator and ATS Install: 40KW generator, Cummins Model 50RS, 120/240V, 3-Phase (LP). ATS 200 Amp, 240 Volt, 3 Phase, 3-Pole, Nema 1R enclosure, exerciser clock

Scope of Work

- ✓ Acquire electrical and mechanical permits in accordance with local jurisdictions.
- ✓ Provide Locates for safe installation
- ✓ Furnish new pad with conduit(electrical) stubbed out under the generator(6" reinforced, expanded edge)
- ✓ Furnish and Install permanent standby generator. (40KW, model #RS40)
- ✓ Furnish and install conduit and appropriately rated wire between panel and generator.
- ✓ Furnish and install pad for the LP tank (includes ground prep, secure with straps/earth anchors)
- ✓ Furnish and install Automatic Transfer Switch. Cummins 200AMP, model OTEC
- ✓ Furnish and install 500 gallon LP tank and 1st fill
- ✓ Furnish and install 1" gas line to generator.
- ✓ Furnish and install regulators, black iron pipe, shut off valve, drip leg and required fittings to integrate fuel supply system to generator.(pressure tested)
- ✓ All work done will conform to jurisdictional building and electrical codes.
- ✓ Furnish and install 12 volt DC starting battery.
- ✓ Manufacturer certified start up, testing, training and warranty registration.
- ✓ Provide insurance certificate.
- ✓ All labor will be paid at applicable prevailing wage.

TOTAL Price..... \$49,546.53

Proposed Work Schedule for Wonderland Well Site

- The Work shall commence on or before October 1st, 2021.
- Upon award of work, order the generator & ATS
- 1 week before the equipment arrives, pour pads and set 500-gallon LP tank
- 1 week after arrival of the generator & ATS begin work
- Install will take 2-3 days
- Project work must be completed no later December 31, 2021.

Highland Estates Well Site Generator Installation

Generator and ATS Install: 60KW generator, Cummins Model 60RS, 120/240V, 1-Phase (LP). ATS 200 Amp, 240 Volt, single Phase, 3-Pole, Nema 3R enclosure, exerciser clock

Scope of Work

- ✓ Acquire electrical and mechanical permits in accordance with local jurisdictions.
- ✓ Provide Locates for safe installation
- ✓ Furnish new pad with conduit(electrical) stubbed out under the generator (6" reinforced, expanded edge)
- ✓ Furnish and install permanent standby generator. (60KW, model #RS60)
- ✓ Furnish and install conduit and appropriately rated wire between panel and generator.
- ✓ Furnish and install pad for the LP tank (includes ground prep, secure with straps/earth anchors)
- ✓ Furnish and install Automatic Transfer Switch. Cummins 200AMP, model RA200SE
- ✓ Furnish and install 500-gallon LP tank and 1st fill
- ✓ Furnish and install 1" gas line to generator.
- ✓ Furnish and install regulators, black iron pipe, shut off valve, drip leg and required fittings to integrate fuel supply system to generator. (Pressure tested)
- ✓ All work done will conform to jurisdictional building and electrical codes.
- ✓ Furnish and install 12-volt DC starting battery.
- ✓ Manufacturer certified start up, testing, training and warranty registration.
- ✓ Provide insurance certificate.
- ✓ All labor will be paid at applicable prevailing wage.

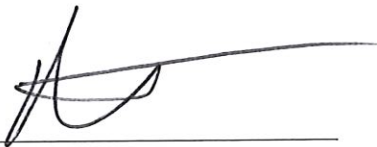
TOTAL Price..... \$54,603.71

Proposed Work Schedule for Highland Estates Well Site

- The Work shall commence on or before October 1st, 2021.
- Upon award of work, order the generator & ATS
- 1 week before the equipment arrives, pour pads and set 500-gallon LP tank
- 1 week after arrival of the generator & ATS begin work
- Install will take 2-3 days
- Project work must be completed no later December 31, 2021.

Dan Bergstrom
Legacy Power Systems
8102 Skansie Ave
Gig Harbor, WA. 98322
(253)858-0214

Signature

A handwritten signature in dark ink, appearing to be 'Dan Bergstrom', written over a horizontal line.

Date

09-20-2021



PUBLIC UTILITY DISTRICT NO. 1
OF MASON COUNTY
N. 21971 Hwy. 101
Shelton, Washington 98584

BOARD OF COMMISSIONERS

MIKE SHEETZ, Commissioner
JACK JANDA, Commissioner
RON GOLD, Commissioner

Sept 27, 2021

Sheila Richardson
Public Works Board Office
Olympia, WA

Re: Support for Jefferson County PUD's Discovery Bay East Project

Dear Ms. Richardson,

Mason County PUD No. 1 offers our support for Jefferson County PUD's request for funding to build fiber to over 200 homes and businesses along the eastern shore of Discovery Bay.

Most of the homes included within the boundaries of their Discovery Bay East project have no internet or outdated DSL connections. While some try to get by with cellular hotspots or satellite, these technologies are expensive and inadequate for video conferencing. Building fiber optic connections to this community will improve quality of life and increase economic opportunity.

Jefferson PUD has been a leader and champion for broadband expansion in their county. Mason PUD 1 serves a remote area in south Jefferson County, and we have been in close partnership with Jefferson PUD to ensure that all rural residents can access telehealth, telework, remote learning and other facets of daily life in America that are dependent upon reliable, high-speed internet.

We applaud their efforts to seek out federal and state funding to expand their network to our most underserved residents. We strongly urge you to support their request for funding.

Thank you for your consideration.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Mike Sheetz'.

Mike Sheetz
Board President

A handwritten signature in blue ink, appearing to read 'Jack Janda'.

Jack Janda
Vice President

A handwritten signature in blue ink, appearing to read 'Ron Gold'.

Ron Gold
Board Secretary



Media Release

For Immediate Release
September 23, 2021

CERB Approves Grant for Mason PUD 1's Hood Canal-101 Broadband Project

Olympia, WA –Washington's Community Economic Revitalization Board (CERB) unanimously approved Mason County PUD No. 1's Hood Canal-101 Broadband Project grant application in the amount of \$797,040. The grant will fund the second phase of a public-private partnership between PUD 1 and Hood Canal Communications (HCC) to extend access to broadband along Highway 101 on the west side of Hood Canal from Eldon to the Mason/Jefferson County line. The Mason County commission also approved a grant for phase one of the project through American Rescue Plan Act (ARPA) funding.

"The concept for this broadband project came about rather quickly over the summer," stated Kristin Masteller, general manager of PUD 1. "Our utility doesn't serve broadband, but our customers continue to ask for help getting it. Our neighboring PUDs that do serve broadband already have their plates full with projects in their own service areas. When Mike Oblizalo, from Hood Canal Communications, came to me with a plan to serve our electric customers along the canal, we realized that HCC was going to need our help to procure the grant funding to make this a reality, so my team and commission agreed to step up and partner with them."

Mason County also awarded ARPA funds to HCC to build out fiber in the Colony Surf development in Lilliwaup. PUD 1 has supported HCC's National Telecommunications and Information Administration grant, which if funded, will complete the buildout from where the CERB project ends at the county line, up to PUD 1's electric customers in south Jefferson County, all the way to Mount Walker. PUD 1 serves electricity to south Jefferson County as part of a longstanding interlocal agreement with Jefferson PUD, and their predecessor Puget Sound Energy. "About a third of our electric service area is unserved or underserved with regard to reliable, high-speed internet. This puts our community at a severe socioeconomic disadvantage because they lack access to telehealth, telework, remote learning, and general facets of everyday life that people experience through internet connectivity. We see it as our role as a utility service provider to help bring the resources and partners together to help make this happen for our community," Masteller said.

As part of the CERB funding, about 117 homes and businesses will be connected between Mike's Beach Resort and Forest Drive, just across the county line. Phase one, funded by ARPA, will also connect 58 homes and businesses between Eldon and Mike's Beach. The Colony Surf project will connect an additional 90 homes. "The pandemic really highlighted the need for high-speed internet and solidified it as an essential service. As a result, we're seeing this once-in-a-generation opportunity for grant funding to build out fiber to the home. HCC has received almost \$8 million in grant funds over the last 20 years for serving rural, underserved areas and we appreciate our partnership with PUD 1 to help us reach new unserved areas on the canal," said Mike Oblizalo, vice president and general manager for Hood Canal Communications.

Kevin Shutt, Mason County's District 2 Commissioner, joined the PUD's CERB community broadband committee and was a project champion for both the ARPA and CERB funding applications. "I am pleased the County commission was able to help fund the first phase of this project and support PUD 1 and HCC's request for additional state and federal grants to expand broadband access. Connecting rural residents is a priority for us as we work with public and private partners to ensure Mason County leads our regional economic recovery and remains competitive into the future," stated Shutt.

For this funding cycle, CERB approved \$1,975,000 in low-interest loans and \$8,272,040 in grants for 10 planning, economic development and rural broadband infrastructure construction projects.

###

Since 1935, PUD 1 has provided non-for-profit electric, water, and wastewater services to over 8,300 customers in Mason and Jefferson counties. The District's mission is to provide customers with safe, reliable and valued utility services.

For more information, contact:



Kristin Masteller
General Manager

21971 N. Hwy. 101, Shelton, WA 98584

(360) 877-5249- Office * (360) 877-9274- Fax

Pursuant to the Washington Public Records Act, RCW 42.56, this email, and any attachments, may be disclosed as a public record. This institution is an equal opportunity provider and employer.

