PLEDGE OF ALLEGIANCE

CONSENT AGENDA
1. Approval of Agenda 06/26/18
2. Approval of Minutes 05/22/18 Commission Meeting
3. Ratification of Vouchers 05/29/18, 06/05/18, 06/12/18, 06/19/18
4. Approval of Vouchers 06/26/18
5. Project Acceptance
   Sterling Hills National Fire Line (Burlington)
   Bay Baby Products, Inc. Agriculture Processing Facility (Mount Vernon Rural)
   Plat of Spring Breeze (Mount Vernon)
6. Recommendation to Award Utility Potholing to Interwest Construction for Judy
   Reservoir-Mount Vernon Transmission Line-Phase 2

STATUS OF BUDGET – 1st Quarter 2018

AUDIENCE COMMENTS

OLD BUSINESS
7. Manager’s Report
8. Draft Strategic Plan Revisions – Potential Action
9. IT Policy & Administrative Practice & Procedures (AP&Ps) – Potential Action
10. Gilligan Creek Watershed Land Management Plan - Discussion

NEW BUSINESS
11. Legislative Task Force on Water Supply
   Recommendation to Ratify Task Force Representative
12. Recommendation to Execute Cascade Natural Gas Agreement - Potential Action
13. Skagit River Diversion Pump and Motor Refurbishment Project
   Change Order No. 1 – Razz Construction – Potential Action

MISCELLANEOUS

COMMISSIONER COMMENTS

ADJOURNMENT

JUDY RESERVOIR ELEVATION
MINUTES OF THE REGULAR MEETING OF THE COMMISSION
PUBLIC UTILITY DISTRICT NO. 1 OF SKAGIT COUNTY, WASHINGTON

May 22, 2018

The regular meeting of the Commission of Public Utility District No. 1 was held in the Aqua Room of the utility located at 1415 Freeway Drive, Mount Vernon, Washington, on May 22, 2018.

The meeting was called to order at 4:30 PM. Those Commissioners in attendance were: Robbie Robertson, President; Eron Berg, Vice President; and Al Littlefield Secretary. Also in attendance were: George Sidhu, General Manager; Mark Handzlik, Engineering Manager, Sally Saxton, Treasurer, Peter Gilbert, Attorney; and Kim Carpenter, Clerk of the Board; Audience: Judy Littlefield, Brian Murphy and Natasha Dunlap, BERK Consulting, Les Walker, Dale Ragan, Joe Lindquist (District 2 PUD Commissioner Candidate) and District Employees: Mike Fox, Kathy White, Mark Semrau, Kevin Tate, Luis Gonzalez, Gary Chrysler, Angie Garza, Dean Myers, and Matt Walker.

Commissioner Littlefield led the Pledge of Allegiance.

Commissioner Littlefield moved to approve the Consent Agenda for May 22, 2018:

1. Approval of Agenda 05/22/18
2. Approval of Minutes
   05/08/18 Commission Meeting
   05/15/18 Special Joint Commission Meeting with Port of Skagit County
3. Ratification of Vouchers 05/15/18
   No. 2795 - Voucher Nos. 12507-12572, Payroll Check Nos. 22638-22720 ($581,324.52)
   No. 2796 - Voucher Nos. 12573-12573 ($1,170.10)
4. Approval of Vouchers 05/22/18
   No. 2797 – Voucher Nos. 12574-12640 ($1,365,060.09)
5. Recommendation to Award (Granite Construction)
   Repaving – Township Street, South of State Route 20

The motion passed.

There were no audience comments.

Under New Business:

6. Presentation of Draft Strategic Plan – BERK Consulting
   Manager Sidhu summarized the Strategic Plan process and intent and recognized the employee planning committee members; Mike Benton, Gary Chrysler, Mike Fox, Angie Garza, Mark Handzlik, Cody Haugstad, Rob Sager, Sally Saxton, Doug Streeter, Kevin Tate, Matt Walker, and Kathy White.

   Brian Murphy and Natasha Dunlap of BERK Consulting presented the draft strategic plan. Discussion ensued regarding various aspects of the information presented, including questions and suggestions. Manager Sidhu indicated that the intent is not for adoption today, but rather to allow time for the Commission to review the
document and submit comments or questions.

Manager Sidhu stated that staff will be working on implementation framework and as there are budget funds remaining, will continue to work with BERK regarding suggested changes. Mr. Murphy stated that they will work on the suggested language changes and present another draft for review.

The Commission felt the draft was good and thanked the consultants for their time and effort.

Treasurer Saxton presented the Treasurer’s Report for April 2018.

Under Old Business:

7. Manager’s Report
Manager Sidhu reported on the following items:

- Special Joint Meeting with the Port of Skagit County was held on May 15 and SkagitNET LLC was formed and filed for certification with the State.
- To coincide with American Water Works Association (AWWA) Drinking Water Week, community tours of the WTP and Judy Reservoir were held on May 16; good feedback was received from participants and a good response was also received from a survey sent to participants.
- Future meeting with BERK Consultants
- Draft Commission meeting schedule was presented to the Commission in January and the meeting of June 12 was cancelled due to lack of a quorum as Commissioners Robertson and Littlefield will be attending the AWWA Annual meeting. The next meeting of the Commission will be June 26.

Under Miscellaneous, Manager Sidhu stated that the Commission notebooks include a Skagit Valley Herald article and letter to the editor regarding a candidate for District 2 PUD Commissioner. Manager Sidhu stated that he has reached out to both candidates who have filed to run against Commissioner Robertson.

Under Commissioner Comments, Commissioner Robertson asked about issues with the District’s website; Manager Sidhu replied that an old version of the website is online so that data we have is not lost; however, the site needs upgrading and currently nothing can be uploaded. An outside consultant is working on the site.

Commissioner Roberson stated he would be presenting a 10-minute PowerPoint presentation from the WA PUD Association (WPUDA) Telecom Workshop and NoaNet Board of Commissioners meetings in Spokane.

Commissioner Berg asked if Commissioner Littlefield planned to attend the Public Utility Risk Management Services (PURMS) insurance meeting on June 6; Commissioner Littlefield replied he could attend if needed.
Commissioner Berg stated he received a letter from a person in Anacortes regarding fiber in the Anacortes waterline; Manager Sidhu replied he would contact Fred Buckenmeyer prior to responding; however, the issues are not specific to the PUD or SkagitNET.

Having no further business to come before the Board, Commissioner Littlefield moved for adjournment. The motion passed and the meeting of May 22, 2018 was adjourned at 6:05 PM.

Respectfully submitted:

________________________________________
Kim Carpenter
Clerk of the Board
June 26, 2018

Board of Commissioners
Public Utility District No. 1 of Skagit County
Post Office Box 1436
1415 Freeway Drive
Mount Vernon, WA 98273-1436

RE: Project Acceptance

Name of Project: Sterling Hills National Fire Line
Reference: Project # 3720
Location: Burlington
Developer: Sterling Hill National, LLC
Contractor: Welch Brothers Construction, Inc.

Gentlemen:

The District has approved the plans and specifications and has inspected the installation of the new water plant within the above project. The Engineering Department has received satisfactory pressure and bacteriological test results. All documentation for this project has been completed.

I recommend that the Commission of the District accept this project.

Respectfully submitted,

[Signature]

Mark C. Handzlik, P.E.
Engineering Manager

cc: George Sidhu, P.E., General Manager
    Michael E. Demers, Engineering Technician
Sterling Hills National, LLC Fire Line
Project Acceptance

<table>
<thead>
<tr>
<th>Meter</th>
<th>Main Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domestic</td>
<td>Existing</td>
</tr>
<tr>
<td>Fire</td>
<td>Waiting Acceptance</td>
</tr>
</tbody>
</table>

This map was created from available public records and existing map sources, not from field surveys. While great care was taken in preparing maps from different sources, they may not agree to the precise location of geographic features. The relative positioning of map features to one another results from combining different map sources without field verification.

The PUD #1 of Skagit County disclaims any warranty of merchantability or warranty of title of any of the data on this map for any particular purpose, either expressed or implied. No representation or warranty is made concerning the accuracy, currency, completeness or quality of the data on this map. The recipient assumes full responsibility for use thereof, and further agrees to hold the PUD #1 of Skagit County harmless from any damage, loss, or liability arising from the use of this map.

NAD 1983 StatePlane Washington North FIPS 4601 Feet
Author: wilson
6/4/2018
June 26, 2018

Board of Commissioners
Public Utility District No. 1 of Skagit County
Post Office Box 1436
1415 Freeway Drive
Mount Vernon, WA 98273-1436

RE: Project Acceptance

Name of Project: Bay Baby Produce, Inc. Agriculture Processing Facility
Reference: Project # 3664
Location: Mount Vernon Rural
Developer: Bay Baby Produce, Inc.
Contractor: Western Refinery Services, Inc.

Gentlemen:

The District has approved the plans and specifications and has inspected the installation of the new water plant within the above project. The Engineering Department has received satisfactory pressure and bacteriological test results. All documentation for this project has been completed.

I recommend that the Commission of the District accept this project.

Respectfully submitted,

Mark C. Handzlik, P.E.
Engineering Manager

cc: George Sidhu, P.E., General Manager
    Michael E. Demers, Engineering Technician
June 26, 2018

Board of Commissioners
Public Utility District No. 1 of Skagit County
Post Office Box 1436
1415 Freeway Drive
Mount Vernon, WA 98273-1436

RE: Project Acceptance

Name of Project: Plat of Spring Breeze
Reference: Project # 3695
Location: Mount Vernon
Developer: Jim N. Scott
Contractor: TRICO Companies, LLC.

Gentlemen:

The District has approved the plans and specifications and has inspected the installation of the new water plant within the above project. The Engineering Department has received satisfactory pressure and bacteriological test results. All documentation for this project has been completed.

I recommend that the Commission of the District accept this project.

Respectfully submitted,

Mark C. Handzlik, P.E.
Engineering Manager

cmp

Attachment

cc: George Sidhu, P.E., General Manager
    Michael E. Demers, Engineering Technician
June 26, 2018

TO: George Sidhu, P.E., General Manager
FROM: Mark Handzlik, P.E., Engineering Manager
BY: Mark Semrau, P.E., PMP, Capital Projects Manager

SUBJECT: Recommendation to Award
Interwest Construction, Inc.
Utility Potholing for JR-MV Transmission Line – Phase 2

Requested Action:
Authorize the General Manager to execute and enter into a contract with Interwest Construction, Inc., in the amount of $64,700.76, which includes Washington State sales tax, for utility potholing along the JR-MV Transmission Line route and McLean Road.

Background:
HDR has completed the 30% review drawings for the JR-MV Transmission Line – Phase 2. These drawings identify several utility crossings along the proposed pipeline route. It is recommended that these utilities be located and depths be determined before proceeding with the transmission line profile design. Determining these utility interferences now will reduce construction conflicts.

Bid Summary:
The District contacted several contractors that are listed on the Small Works Roster. Interwest Construction (ICI) and Whatcom Refinery Services (WRS) were the only contractors that provided an estimate. Other contractors contacted include:

- WRS – Provided a quote that was 45% higher than ICI bid.
- Trico Companies, LLC - Responded, but do not have the people to perform the work at this time.
- Ram Construction General Contractors, Inc. - Responded, but do not have the people to perform the work at this time.
- Puget Sound Utility Services – Sent bid package but did not give a response.
- TRIMAXX Construction, Inc. - Spoke with Todd Snyder, but they did not have the right equipment and did not give a response.

Fiscal Impact:
Funding for this contract and project will come from the 2018 Budget for the JR-MV Transmission Line – Phase 2. The work is consistent with the intended use of these funds.
## PUD NO 1 OF SKAGIT COUNTY

### STATEMENT OF NET POSITION (Unaudited)

### AS OF MARCH 31, 2018

### ASSETS

#### CURRENT ASSETS

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASH AND INVESTMENTS</td>
<td>$4,986,739</td>
<td>$6,616,103</td>
</tr>
<tr>
<td>CUSTOMER ACCOUNTS RECEIVABLE (NET)</td>
<td>2,568,686</td>
<td>2,202,741</td>
</tr>
<tr>
<td>ACCOUNTS RECEIVABLE, OTHER</td>
<td>193,137</td>
<td>169,208</td>
</tr>
<tr>
<td>MATERIALS INVENTORY</td>
<td>1,410,751</td>
<td>1,738,918</td>
</tr>
<tr>
<td>PREPAID EXPENSES</td>
<td>141,643</td>
<td>151,734</td>
</tr>
<tr>
<td>OTHER CURRENT ASSETS</td>
<td>163,031</td>
<td>197,551</td>
</tr>
<tr>
<td><strong>TOTAL CURRENT ASSETS</strong></td>
<td><strong>9,463,987</strong></td>
<td><strong>11,076,255</strong></td>
</tr>
</tbody>
</table>

#### RESTRICTED ASSETS

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASH AND INVESTMENTS</td>
<td>6,517,268</td>
<td>8,878,945</td>
</tr>
<tr>
<td>GRANTS AND FED STIMULUS RECEIVABLE</td>
<td>16,529</td>
<td>45,800</td>
</tr>
<tr>
<td><strong>TOTAL RESTRICTED ASSETS</strong></td>
<td><strong>6,533,797</strong></td>
<td><strong>8,924,745</strong></td>
</tr>
</tbody>
</table>

#### NONCURRENT ASSETS

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVESTMENTS</td>
<td>3,639,006</td>
<td>3,174,719</td>
</tr>
<tr>
<td>LUD ASSESSMENTS RECEIVABLE</td>
<td>850,964</td>
<td>695,089</td>
</tr>
<tr>
<td>PRECONSTRUCTION COSTS</td>
<td>816,087</td>
<td>1,593,122</td>
</tr>
</tbody>
</table>

#### CAPITAL ASSETS

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>NON OPERATING PROPERTY</td>
<td>29,521</td>
<td>29,521</td>
</tr>
<tr>
<td>LAND AND LAND RIGHTS</td>
<td>579,821</td>
<td>579,821</td>
</tr>
<tr>
<td>EARTHEN IMPOUNDING RESERVOIR</td>
<td>12,375,489</td>
<td>12,375,489</td>
</tr>
<tr>
<td>CONSTRUCTION IN PROGRESS</td>
<td>8,375,070</td>
<td>14,282,427</td>
</tr>
<tr>
<td>PLANT</td>
<td>209,806,226</td>
<td>218,396,524</td>
</tr>
<tr>
<td>EQUIPMENT</td>
<td>3,782,599</td>
<td>4,143,826</td>
</tr>
<tr>
<td>ACCUMULATED DEPRECIATION</td>
<td>(71,185,639)</td>
<td>(76,172,869)</td>
</tr>
<tr>
<td><strong>TOTAL NONCURRENT ASSETS</strong></td>
<td><strong>169,069,144</strong></td>
<td><strong>179,097,669</strong></td>
</tr>
</tbody>
</table>

**TOTAL ASSETS**

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TOTAL ASSETS</strong></td>
<td><strong>$185,066,928</strong></td>
<td><strong>$199,098,669</strong></td>
</tr>
</tbody>
</table>

### DEFERRED OUTFLOWS OF RESOURCES

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFERRED OUTFLOWS RELATED TO PENSIONS</td>
<td>1,136,027</td>
<td>780,492</td>
</tr>
<tr>
<td><strong>TOTAL DEFERRED OUTFLOWS OF RESOURCES</strong></td>
<td><strong>$1,136,027</strong></td>
<td><strong>$780,492</strong></td>
</tr>
</tbody>
</table>

---

PUD No 1 of Skagit County (Skagit PUD) has prepared these financial statements in accordance with generally accepted accounting principles. These financial statements should be read in conjunction with the notes to the financial statements included in Skagit PUD's Annual Report as of December 31, 2016. This information is provided for general information. Not all the information is intended for nor should it be relied upon for making investment decision by current or prospective investors.
## LIABILITIES

### CURRENT LIABILITIES:

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCOUNTS PAYABLE</td>
<td>$696,720</td>
<td>$292,457</td>
</tr>
<tr>
<td>RETAINAGE PAYABLE</td>
<td>206,752</td>
<td>104,165</td>
</tr>
<tr>
<td>TAXES PAYABLE</td>
<td>103,349</td>
<td>107,917</td>
</tr>
<tr>
<td>CUSTOMER DEPOSITS</td>
<td>150,901</td>
<td>148,024</td>
</tr>
<tr>
<td>ACCRUED INTEREST ON DEBT</td>
<td>191,913</td>
<td>301,048</td>
</tr>
<tr>
<td>BONDS AND LOANS PAYABLE</td>
<td>2,934,307</td>
<td>2,947,205</td>
</tr>
<tr>
<td>OTHER CURRENT LIABILITIES</td>
<td>144,066</td>
<td>148,427</td>
</tr>
<tr>
<td><strong>TOTAL CURRENT LIABILITIES</strong></td>
<td><strong>4,428,008</strong></td>
<td><strong>4,049,243</strong></td>
</tr>
</tbody>
</table>

### NONCURRENT LIABILITIES

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTHER POSTEMPLOYMENT BENEFITS</td>
<td>1,285,524</td>
<td>1,547,541</td>
</tr>
<tr>
<td>COMPENSATED ABSENCES</td>
<td>936,332</td>
<td>936,093</td>
</tr>
<tr>
<td>REVENUE BONDS OUTSTANDING,NET</td>
<td>10,186,166</td>
<td>13,046,585</td>
</tr>
<tr>
<td>PUBLIC WORKS TRUST FUND LOANS</td>
<td>7,525,123</td>
<td>6,168,922</td>
</tr>
<tr>
<td>DRINKING WATER STATE REV FUND LOANS</td>
<td>5,527,139</td>
<td>9,917,417</td>
</tr>
<tr>
<td><strong>TOTAL NONCURRENT LIABILITIES</strong></td>
<td><strong>25,460,284</strong></td>
<td><strong>31,616,558</strong></td>
</tr>
<tr>
<td>NET PENSION LIABILITY</td>
<td>6,078,187</td>
<td>4,189,495</td>
</tr>
<tr>
<td><strong>TOTAL LIABILITIES</strong></td>
<td><strong>$35,966,479</strong></td>
<td><strong>$39,855,296</strong></td>
</tr>
</tbody>
</table>

### DEFERRED INFLOWS OF RESOURCES

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFERRED INFLOWS RELATED TO PENSIONS</td>
<td>105,213</td>
<td>1,052,374</td>
</tr>
<tr>
<td><strong>TOTAL DEFERRED INFLOWS OF RESOURCES</strong></td>
<td><strong>$105,213</strong></td>
<td><strong>$1,052,374</strong></td>
</tr>
</tbody>
</table>

### NET POSITION

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVESTED IN CAPITAL ASSETS NET OF DEBT</td>
<td>$127,215,684</td>
<td>$128,407,510</td>
</tr>
<tr>
<td>RESTRICTED ASSETS</td>
<td>6,533,797</td>
<td>8,924,745</td>
</tr>
<tr>
<td>UNRESTRICTED ASSETS</td>
<td>16,381,782</td>
<td>21,639,236</td>
</tr>
<tr>
<td><strong>TOTAL NET POSITION</strong></td>
<td><strong>$150,131,263</strong></td>
<td><strong>$158,971,491</strong></td>
</tr>
</tbody>
</table>
PUD NO 1 OF SKAGIT COUNTY
REVENUES, EXPENSES AND CHANGES IN NET POSITION (Unaudited)
FOR THREE MONTHS ENDING MARCH 31, 2018

<table>
<thead>
<tr>
<th>OPERATING REVENUE</th>
<th>2017 1st Qtr Actual</th>
<th>2018 1st Qtr Actual</th>
<th>2018 1st Qtr Budget</th>
<th>Actual to Budget Favorable/Unfavorable</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESIDENTIAL-MULTIPLE</td>
<td>$3,274,321</td>
<td>$3,505,646</td>
<td>$3,608,677</td>
<td>($103,031) 97%</td>
</tr>
<tr>
<td>COMMERCIAL-INDUSTRIAL-FARMS-FIRE PROTECTION</td>
<td>1,119,475</td>
<td>1,148,429</td>
<td>1,134,447</td>
<td>13,982 101%</td>
</tr>
<tr>
<td>GOVERNMENTAL</td>
<td>147,662</td>
<td>126,706</td>
<td>137,599</td>
<td>(10,893) 92%</td>
</tr>
<tr>
<td>RESALE</td>
<td>18,919</td>
<td>17,011</td>
<td>17,024</td>
<td>(13) 100%</td>
</tr>
<tr>
<td>IRRIGATION</td>
<td>27,522</td>
<td>42,287</td>
<td>30,879</td>
<td>11,408 137%</td>
</tr>
<tr>
<td>TOTAL WATER SALES</td>
<td>4,587,899</td>
<td>4,840,079</td>
<td>4,928,626</td>
<td>(88,547) 98%</td>
</tr>
<tr>
<td>OTHER WATER REVENUES</td>
<td>72,240</td>
<td>73,162</td>
<td>56,122</td>
<td>17,040 130%</td>
</tr>
<tr>
<td>BROADBAND REVENUES, NET OF COSTS</td>
<td>(2,661)</td>
<td>(1,166)</td>
<td>(1,617)</td>
<td>451 72%</td>
</tr>
<tr>
<td>TOTAL OPERATING REVENUES</td>
<td>4,657,478</td>
<td>4,912,075</td>
<td>4,983,131</td>
<td>(71,056) 99%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPERATING EXPENSES</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SUPPLY</td>
<td>64,880</td>
<td>70,662</td>
<td>197,532</td>
<td>126,870 36%</td>
</tr>
<tr>
<td>TREATMENT</td>
<td>333,867</td>
<td>427,126</td>
<td>51,356</td>
<td>124,230 77%</td>
</tr>
<tr>
<td>TRANSMISSION AND DISTRIBUTION</td>
<td>221,055</td>
<td>212,780</td>
<td>313,384</td>
<td>100,604 68%</td>
</tr>
<tr>
<td>PURCHASED TELECOMMUNICATIONS S VCS</td>
<td>7,932</td>
<td>15,877</td>
<td>13,802</td>
<td>(2,075) 115%</td>
</tr>
<tr>
<td>CUSTOMER ACCOUNTS</td>
<td>360,933</td>
<td>376,799</td>
<td>427,595</td>
<td>50,796 88%</td>
</tr>
<tr>
<td>ADMINISTRATIVE AND GENERAL</td>
<td>1,374,416</td>
<td>1,355,882</td>
<td>1,611,082</td>
<td>255,200 84%</td>
</tr>
<tr>
<td>UTILITY TAXES</td>
<td>228,532</td>
<td>242,444</td>
<td>247,862</td>
<td>5,618 98%</td>
</tr>
<tr>
<td>DEPRECIATION EXPENSE</td>
<td>651,694</td>
<td>639,374</td>
<td>1,234,225</td>
<td>594,851 52%</td>
</tr>
<tr>
<td>TOTAL OPERATING EXPENSE</td>
<td>3,243,309</td>
<td>3,340,744</td>
<td>4,596,838</td>
<td>1,256,094 73%</td>
</tr>
</tbody>
</table>

| OPERATING INCOME (LOSS)                                | 1,414,169            | 1,571,331           | 386,293             | 1,185,038 407%                       |

<table>
<thead>
<tr>
<th>NON OPERATING REVENUE</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>INTEREST INCOME</td>
<td>25,636</td>
<td>59,799</td>
<td>19,550</td>
<td>40,249 306%</td>
</tr>
<tr>
<td>INTEREST AND PENALTY INCOME ON LUDS</td>
<td>4,555</td>
<td>9,367</td>
<td>8,176</td>
<td>1,191 115%</td>
</tr>
<tr>
<td>MISCELLANEOUS INCOME</td>
<td>5,769</td>
<td>6,366</td>
<td>11,250</td>
<td>(4,884) 57%</td>
</tr>
<tr>
<td>GAINS ON CAPITAL ASSET DISPOSITIONS</td>
<td>33</td>
<td>437</td>
<td>437</td>
<td>437 100%</td>
</tr>
<tr>
<td>TOTAL NON OPERATING REVENUE</td>
<td>35,993</td>
<td>75,969</td>
<td>38,976</td>
<td>36,993 195%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NON OPERATING EXPENSE</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MISCELLANEOUS EXPENSE</td>
<td>(80)</td>
<td>73</td>
<td>200</td>
<td>127 37%</td>
</tr>
<tr>
<td>INTEREST ON DEBT, NET</td>
<td>117,877</td>
<td>146,877</td>
<td>207,383</td>
<td>60,506 71%</td>
</tr>
<tr>
<td>TOTAL NON OPERATING EXPENSE</td>
<td>117,797</td>
<td>146,950</td>
<td>207,583</td>
<td>60,633 71%</td>
</tr>
</tbody>
</table>

| INCOME (LOSS) BEFORE CONTRIBUTIONS                     | 1,332,365            | 1,500,350           | 217,686             | 1,282,664 689%                       |

<table>
<thead>
<tr>
<th>CAPITAL CONTRIBUTIONS</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NON DONATED PLANT</td>
<td>58,100</td>
<td>158,000</td>
<td>75,000</td>
<td>83,000 211%</td>
</tr>
<tr>
<td>DONATED PLANT</td>
<td>40,865</td>
<td>48,093</td>
<td>100,000</td>
<td>(51,907) 48%</td>
</tr>
<tr>
<td>SYSTEM DEVELOPMENT FEES</td>
<td>365,098</td>
<td>430,923</td>
<td>275,000</td>
<td>155,923 157%</td>
</tr>
<tr>
<td>SERVICES</td>
<td>112,944</td>
<td>102,975</td>
<td>102,000</td>
<td>975 101%</td>
</tr>
<tr>
<td>PIPE REPLACEMENT</td>
<td>148,830</td>
<td>150,364</td>
<td>136,559</td>
<td>13,805 110%</td>
</tr>
<tr>
<td>LOCAL UTILITY DISTRICTS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 0%</td>
</tr>
<tr>
<td>GRANTS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 0%</td>
</tr>
<tr>
<td>TOTAL CAPITAL CONTRIBUTIONS</td>
<td>725,837</td>
<td>890,355</td>
<td>688,559</td>
<td>201,796 129%</td>
</tr>
</tbody>
</table>

| CHANGE IN NET POSITION                                 | 2,058,202            | 2,390,705           | $906,245            | $1,484,460 264%                      |

<table>
<thead>
<tr>
<th>NET POSITION, JANUARY 1</th>
<th>148,073,061</th>
<th>156,580,786</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NET POSITION, MARCH 31</td>
<td>$150,131,263</td>
<td>$158,971,491</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

PUD No 1 of Skagit County (Skagit PUD) has prepared these financial statements in accordance with generally accepted accounting principles. These financial statements should be read in conjunction with the notes to the financial statements included in Skagit PUD’s Annual Report as of December 31, 2016. This information is provided for general information. Not all the information is intended for nor should it be relied upon for making investment decision by current or prospective investors.
## Operating Revenues and Expense Tracking (Unaudited)

FOR THREE MONTHS ENDING MARCH 31, 2018

### Operating Revenue

**Water Sales**

<table>
<thead>
<tr>
<th>System</th>
<th>2017 YTD Actual</th>
<th>2018 YTD Actual</th>
<th>2018 YTD Budget</th>
<th>Actual to Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>JUDY SYSTEM</td>
<td>$4,439,709</td>
<td>$4,702,049</td>
<td>$4,749,189</td>
<td>$(47,140)</td>
</tr>
<tr>
<td>FIDALGO/SIMILK</td>
<td>61,017</td>
<td>65,683</td>
<td>106,143</td>
<td>$(40,460)</td>
</tr>
<tr>
<td>CEDARGROVE</td>
<td>27,395</td>
<td>30,293</td>
<td>21,398</td>
<td>8,895</td>
</tr>
<tr>
<td>ROCKPORT</td>
<td>9,304</td>
<td>10,692</td>
<td>7,699</td>
<td>2,993</td>
</tr>
<tr>
<td>MOUNTAIN VIEW</td>
<td>2,486</td>
<td>2,674</td>
<td>2,469</td>
<td>205</td>
</tr>
<tr>
<td>ALGER/SAMISH</td>
<td>21,883</td>
<td>448</td>
<td>18,400</td>
<td>(17,952)</td>
</tr>
<tr>
<td>POTLATCH</td>
<td>9,933</td>
<td>11,645</td>
<td>10,923</td>
<td>722</td>
</tr>
<tr>
<td>SKAGIT VIEW VILLAGE</td>
<td>11,405</td>
<td>12,243</td>
<td>9,139</td>
<td>3,104</td>
</tr>
<tr>
<td>MARBLEMOUNT</td>
<td>4,767</td>
<td>4,352</td>
<td>3,266</td>
<td>1,086</td>
</tr>
<tr>
<td><strong>Total Water Sales</strong></td>
<td>$4,587,899</td>
<td>$4,840,079</td>
<td>$4,928,626</td>
<td>$(88,547)</td>
</tr>
</tbody>
</table>

**Other Operating Revenue**

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
<th>2018</th>
<th>Actual to Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>MISC SERVICE CHARGES</td>
<td>72,240</td>
<td>73,162</td>
<td>56,122</td>
<td>17,040</td>
</tr>
<tr>
<td>BROADBAND SERVICES, NET OF COSTS</td>
<td>(2,661)</td>
<td>(1,166)</td>
<td>(1,617)</td>
<td>451</td>
</tr>
<tr>
<td><strong>Total Other Operating Revenue</strong></td>
<td>69,579</td>
<td>71,996</td>
<td>54,505</td>
<td>17,491</td>
</tr>
</tbody>
</table>

**Total Operating Revenue**

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2018</th>
<th>2018</th>
<th>Actual to Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>$4,657,478</td>
<td>$4,912,075</td>
<td>$4,983,131</td>
<td>$(71,056)</td>
</tr>
</tbody>
</table>

### Operating Expenses

<table>
<thead>
<tr>
<th>Description</th>
<th>2017</th>
<th>2018</th>
<th>2018</th>
<th>Actual to Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>SALARIES/WAGES/BENEFITS</td>
<td>1,802,730</td>
<td>1,876,125</td>
<td>2,137,525</td>
<td>261,400</td>
</tr>
<tr>
<td>WATER PURCHASED FROM OTHERS</td>
<td>32,027</td>
<td>31,871</td>
<td>46,250</td>
<td>14,379</td>
</tr>
<tr>
<td>ELECTRICITY PURCHASED FOR PUMPING</td>
<td>29,692</td>
<td>35,988</td>
<td>121,125</td>
<td>85,137</td>
</tr>
<tr>
<td>CHEMICALS FOR TREATMENT</td>
<td>71,176</td>
<td>112,579</td>
<td>106,638</td>
<td>(5,941)</td>
</tr>
<tr>
<td>GENERAL SUPPLIES AND SERVICES</td>
<td>184,239</td>
<td>172,806</td>
<td>294,582</td>
<td>121,776</td>
</tr>
<tr>
<td>UTILITIES</td>
<td>36,046</td>
<td>36,205</td>
<td>47,828</td>
<td>11,623</td>
</tr>
<tr>
<td>POSTAGE AND SHIPPING</td>
<td>24,126</td>
<td>11,411</td>
<td>23,740</td>
<td>12,329</td>
</tr>
<tr>
<td>EQUIP MAINT CONTRACTS</td>
<td>6,009</td>
<td>3,418</td>
<td>4,638</td>
<td>1,220</td>
</tr>
<tr>
<td>PURCHASED TELECOMMUNICATIONS SVCS</td>
<td>7,698</td>
<td>15,877</td>
<td>9,776</td>
<td>(6,101)</td>
</tr>
<tr>
<td>MEMBERSHIPS</td>
<td>24,431</td>
<td>22,382</td>
<td>20,767</td>
<td>(1,615)</td>
</tr>
<tr>
<td>TECHNOLOGY/SCADA/SUPPORT</td>
<td>40,378</td>
<td>122,783</td>
<td>115,723</td>
<td>(7,060)</td>
</tr>
<tr>
<td>PROFESSIONAL SERVICES</td>
<td>77,902</td>
<td>65,377</td>
<td>157,186</td>
<td>91,809</td>
</tr>
<tr>
<td>TRAVEL AND TRAINING</td>
<td>41,782</td>
<td>8,286</td>
<td>58,968</td>
<td>50,682</td>
</tr>
<tr>
<td>EQUIPMENT AND VEHICLE EXPENSE</td>
<td>13,428</td>
<td>25,751</td>
<td>48,544</td>
<td>22,793</td>
</tr>
<tr>
<td>INSURANCE EXPENSE</td>
<td>91,753</td>
<td>90,460</td>
<td>111,771</td>
<td>21,311</td>
</tr>
<tr>
<td>ADVERTISING EXPENSE</td>
<td>7,105</td>
<td>7,910</td>
<td>9,775</td>
<td>1,865</td>
</tr>
<tr>
<td>BAD DEBT EXPENSE</td>
<td>4,932</td>
<td>4,132</td>
<td>7,500</td>
<td>3,368</td>
</tr>
<tr>
<td>HEALTH PERMITS</td>
<td>34,010</td>
<td>34,010</td>
<td>34,265</td>
<td>255</td>
</tr>
<tr>
<td>MISCELLANEOUS EXPENSES</td>
<td>26,739</td>
<td>11,345</td>
<td>8,150</td>
<td>(3,195)</td>
</tr>
<tr>
<td>UTILITY TAXES</td>
<td>228,532</td>
<td>242,244</td>
<td>247,862</td>
<td>5,618</td>
</tr>
<tr>
<td>TRANSFERS TO CONSTRUCTION IN PROGRESS</td>
<td>(193,120)</td>
<td>(229,590)</td>
<td>(250,000)</td>
<td>(20,410)</td>
</tr>
<tr>
<td><strong>Total Operating Expenses</strong></td>
<td>2,591,615</td>
<td>2,701,370</td>
<td>3,362,613</td>
<td>661,243</td>
</tr>
</tbody>
</table>

**Net Operating Income Before Depreciation and OPEB Costs**

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2018</th>
<th>2018</th>
<th>Actual to Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>$2,065,863</td>
<td>$2,210,705</td>
<td>$1,620,518</td>
<td>$590,187</td>
</tr>
</tbody>
</table>
STRATEGIC PLAN
2018-2022
Final Draft 6/22/18
SKAGIT PUD COMMISSIONERS

Eron Berg
Al Littlefield
Robbie Robertson

PLANNING COMMITTEE

Mike Benton, Project Manager
Gary Chrysler, IT Manager
Mike Fox, Operations Manager
Angie Garza, Customer Service Representative
Mark Handzlik, Engineering Manager
Cody Haugstad, Construction Worker
Rob Sager, Water Treatment Plant Operator
Sally Saxton, Treasurer
George Sidhu, General Manager
Doug Streeter, Contracted Auditor and Interim Finance Manager
Kevin Tate, Community Relations Manager
Matt Walker, Meter Technician
Kathy White, Human Resources Manager
LETTER FROM SKAGIT PUD’S GENERAL MANAGER

Since 1936, Skagit PUD has committed to providing safe and reliable utility services to meet the current and future needs of Skagit County residents. As the largest water purveyor in Skagit County, we have a responsibility to serve our customers, but also to manage the water resources that have been placed in our trust. We strive to be a responsible steward of those resources by being a customer-focused, forward-looking, and fiscally responsible utility.

During the strategic planning process, we received a tremendous amount of valuable input from a broad range of people that helped determine plan objectives. Our local partners and employees were surveyed for their insights and a Strategic Planning Committee comprised of staff from all of our departments was created to help direct and guide the process.

Skagit PUD’s 5-year Strategic Plan establishes our strategic objectives in three main areas:

2. Communication with the Public and Partners.
3. Internal Operations, Communication, and Organizational Development.

The focus of the Strategic Plan is on the short-term horizon to help guide decisions that will define our organization going forward. The challenges that we face in Skagit County are similar to many of the challenges facing Washington State and the nation. Water system planning, aging infrastructure, increasing rates, strong communications, and hiring and retaining a high quality workforce are many of the complex issues we will address during this planning horizon.

It is critical for our organization to have a clear vision of where we want to be and a commitment on how we intend to get there. The completion of this Strategic Plan is the first step in outlining our commitments, and developing an implementation plan to achieve our strategic objectives.

I want to recognize everyone who worked on this Strategic Plan and the collaborative approach that was used. On behalf of the Strategic Planning Committee, we extend our thanks to the partners and District staff that participated in pre-planning surveys. Our team is excited about the challenges and opportunities that will result from the Strategic Plan, and we are eager to realize the continuous quality improvements coming to Skagit PUD.

George Sidhu, P.E.
General Manager
CONTENTS

Overarching Guidance: Mission, Vision, and Core Values......................................................... 2
Summary of Goals and Strategies ................................................................................................. 3
I. Customer-Focused Services ......................................................................................................... 4
   A. Water ..................................................................................................................................... 7
   B. Telecommunications ............................................................................................................. 11
   C. Sewer ................................................................................................................................. 15
II. Communication with the Public and Partners ......................................................................... 17
III. Internal Operations, Communication, and Organizational Development ........................... 21
Implementation Framework ......................................................................................................... 25
OVERARCHING GUIDANCE
VISION, MISSION, AND CORE VALUES

Our Vision is to be an outstanding regional leader and innovative utility provider.

Our Mission is to provide our customers with high-quality water services at an affordable price.

As we pursue our Vision and advance our Mission, we demonstrate and maintain balance among our Core Values:

- **Quality.** We seek to exceed customer expectations by providing exceptional service.
- **Environmental Stewardship.** We act to preserve our region’s natural resources.
- **Financial Prudence.** We strive to keep our rates as low as possible while making wise capital investments and strategic business decisions.
SUMMARY OF GOALS AND STRATEGIES

I. CUSTOMER-FOCUSED SERVICES

A. Water
   1. Make prioritized and strategic capital infrastructure investments to maintain existing assets and quality to serve the growing Skagit community.
   2. Steward partnership-based efforts that advance the strategic regional use of water resources.

B. Telecommunications
   1. Invest in the telecommunications infrastructure necessary to securely and efficiently manage our water system and facilitate the extension of broadband infrastructure within Skagit County.
   2. Stay current and decide whether we should enter the telecom industry as a retail provider if public utility districts are given the authority to do so.

C. Sewer
   1. Explore and understand the connection between sewage and reclaimed water.

II. COMMUNICATION WITH THE PUBLIC AND PARTNERS

1. Strengthen communications and engagements with our customers.
2. Seek opportunities to engage youth in water-related education.
3. Ensure our policy-setting and decision-making processes are transparent and easily accessible.
4. Strengthen our provision of high-quality customer service.
5. Strengthen our relationships with our partners.

III. INTERNAL OPERATIONS, COMMUNICATION, AND ORGANIZATIONAL DEVELOPMENT

1. Strengthen internal systems and the use of technology to create efficiencies.
2. Address our aging District headquarters facility.
3. Attract, retain, and develop a high-quality workforce.
4. Improve internal communications throughout the organization.
I. CUSTOMER-FOCUSED SERVICES
A. WATER

STATEMENT OF INTENT

Skagit PUD’s core focus is providing water to residential, business, and agricultural customers. We make strategic and sustainable investments to ensure our water rights, infrastructure, and other resources are managed for the benefit of our customers and for the long-term benefit of the region.

The most significant contribution we can make to environmental sustainability is by improving the efficiency of our system and by encouraging smart water use among our customers. By making strategic investments to reduce wasted water, we will also diminish our need for finding additional water sources and for making large capital improvements in the future.

The District will play a supportive role in addressing the legal availability of water for agriculture and rural land owners.
Make prioritized and strategic capital infrastructure investments to maintain existing assets and quality to serve the growing Skagit community.

a. Refine existing criteria for assessing, prioritizing, and selecting capital projects and operational improvements.
   • Implement and provide additional resources to our asset management system, including development of an economic risk model.
   • Reduce equipment failure rates.
   • Collect data from existing infrastructure at every opportunity, especially main breaks, leak repairs, and low pressure events.
   • Perform regular and routine maintenance on infrastructure to develop a database of information.

b. Expand the inputs that inform our capital planning.
   • Develop a GIS-based, extended-period, hydraulic model to be used for water system planning, flushing program development, and contaminant transport simulation.
   • Update our Customer Buildout Capacity Analysis.

c. Update our Water System Plan and Capital Improvement Program that:
   • Identifies major capital facilities and components.
   • Identifies maintenance procedures and replacement criteria.
   • Establishes a level of service for the system.
   • Establishes goals for preventative maintenance.

d. Implement SCADA systems to maintain security of our infrastructure [see development of internally-focused fiber network under B. Telecommunications].
2 Steward partnership-based efforts that advance the strategic regional use of water resources.

a. Engage local partners and stakeholders in implementing efficient solutions that meet the future water demands of Skagit County communities by utilizing an updated Coordinated Water System Plan.

b. Foster outreach to partners to identify synergy projects and community development programs [coordinate with efforts under II.5].

c. Reduce water waste by making strategic investments in District technology and infrastructure and by increasing our efforts to encourage smart water use among our customers.

d. Apply strategic resources to the issue of the legal availability of water for agriculture and rural land owners by continuing to advocate for a state level solution and exploring potential regional solutions.

5-YEAR RESOURCE NEEDS

Goal 2 includes significant investment in existing and potentially new infrastructure to serve current and future water customers as directed by our Capital Improvement Program. By focusing additional staff capacity in asset management and planning as directed by Goal 1, we will prioritize making smart long-term investments that maximize and prolong the value of our infrastructure, water rights, and other resources.
B. TELECOMMUNICATIONS

STATEMENT OF INTENT

Investment in telecommunications infrastructure is necessary to the security and effective management of Skagit PUD’s water systems. Skagit PUD is collaborating with the Port of Skagit County on the SkagitNet effort for development of telecommunications services to support the growth and prosperity of the Skagit County community. In these efforts, Skagit PUD will favor the development of wholesale capacity over becoming a retail provider.
1 Invest in the telecommunications infrastructure necessary to securely and efficiently manage our water system and facilitate the extension of broadband infrastructure within Skagit County.

   a. Develop a fiber and radio network focused on meeting District needs.
   b. Continue our SkagitNet partnership with the Port of Skagit County, seeking greater clarity in roles and responsibilities.
   c. Carefully consider additional opportunities to develop broadband infrastructure, favoring partnerships and a focus on the wholesale provision of backbone capacity.

2 Stay current and decide whether we should enter the telecom industry as a retail provider if public utility districts are given the authority to do so.

   a. Monitor policy and market changes and review case studies, lessons learned, and best practices from elsewhere in the state or country.

5-YEAR RESOURCE NEEDS

Beyond our current commitment to create a broadband network for a portion of the Skagit community in partnership with the Port, we do not foresee the need for substantial investment in this area based on the preceding Statement of Intent.
C. SEWER

STATEMENT OF INTENT

While Skagit PUD has the legal authority to provide sewer services, we are not seeking to develop this service area. We would, however, be willing to meet regional needs if directed to do so by state and local agencies.

We will more actively pursue opportunities to use sewage as a method of increasing water availability and reducing or deferring investment in our water system infrastructure through water reclamation and recycling.

1. Explore and understand the connection between sewage and reclaimed water.
   a. Conduct an annual review of policy changes, technology trends, and the state of the sewer field, particularly in connection to water rights.
   b. Attend industry conferences to maintain a sense of the sewer industry and how it relates to water rights.
   c. Develop a contingency plan for how we would provide sewer services if mandated to do so.

5-YEAR RESOURCE NEEDS

We do not foresee the need for substantial investment in this area during the coming five years.
II. COMMUNICATION WITH THE PUBLIC AND PARTNERS

STATEMENT OF INTENT

As a service provider and steward of public resources, it is incumbent on us to communicate effectively with our customers, members of the public, and partners.
1 Strengthen communications and engagements with our customers.
   a. Develop an agency-wide Communications Plan that includes:
      • Implementation of a focused and consistent mission-based message.
      • Specific tactics for print, web, social media, public relations, and broadcast channels.
      • Strategies to implement online tools that provide easy access to information for customers, generating efficiencies for customers and District staff.
      • Identification of value communications, such as pushing out messages rather than keeping all resources available on demand at all times.

2 Seek opportunities to engage youth in water-related education.
   a. Continue outreach to schools and tours of the Water Treatment Plant and source water intakes.
   b. Explore opportunities to have a presence and offer internships at regional higher educational institutions, expanding our partnerships over time.

3 Ensure our policy-setting and decision-making processes are transparent and easily accessible.
   a. Maintain current efforts for making Commission meetings accessible and transparent.
   b. Continue to assess public interest and calibrate our investments in this area.
4 Strengthen our provision of high-quality customer service.
   a. Improve wayfinding signage for the driveway and entrance to the building.
   b. Begin implementation of a regular customer satisfaction survey.
   c. Increase customer familiarity with payment channels.
   d. Monitor rate increases and consider options to minimize impacts on customers.

5 Strengthen our relationships with our partners.
   a. Establish a prioritized plan for strengthening our relationship with partners.
   b. Assess our channels for communicating and sharing information with partners and make strategic improvements to key communication channels.

5-YEAR RESOURCE NEEDS

Additional staff capacity may be required to develop and implement the communications plan directed by Goal 1.
III. INTERNAL OPERATIONS, COMMUNICATION, AND ORGANIZATIONAL DEVELOPMENT

STATEMENT OF INTENT

To provide high-quality services for our customers, it is imperative that we have strong staff and supporting systems.
1 Strengthen internal systems and the use of technology to create efficiencies.

   a. Identify needs and an appropriate solution for a document or content management system to increase efficiencies for contract approvals and other processes.
   b. Learn and implement the full capabilities of core software systems.
   c. Establish security and emergency response plans, policies, and procedures.
   d. Evaluate the most effective and resource-efficient use of in-house and contracted staffing and resources.
   e. Revisit our Strategic Plan on an annual basis, tracking our progress and ensuring it guides our budgeting and activities.

2 Address our aging District headquarters facility.

   a. Complete the feasibility study and determine whether the District headquarters should be housed in a new or existing building and at our current site or in a new location.
   b. Based on this plan, outline the scope, schedule, budget, and funding/financing plan with consideration of the impact on rate payers.
   c. Make repairs to the current building as necessary, or use temporary spaces until a permanent solution is in place.
Attract, retain, and develop a high-quality workforce.

a. Strengthen our ability to recruit highly capable employees.
   • Stay current on staffing trends to develop and update our hiring and recruitment practices, including compensation trends, benefits, and what is desired by the workforce.
   • Implement updates and best practices as appropriate while maintaining a level of consistency with hiring practices.

b. Anticipate and plan for pending retirements.
   • Identify likely staffing needs for the next five years and beyond considering anticipated retirements.
   • Develop a succession plan based on identified needs, which can be revised and updated as operations evolve at the District. The succession plan should include evaluation of current staff and opportunities to provide development opportunities where appropriate.
   • Continue to evaluate our needs when openings or retirements occur, seeking efficient solutions as conditions change.

c. Strengthen and systematize our focus on staff development.
   • Identify development opportunities by asking staff, reviewing needs identified in the evaluation process, and gathering input from management personnel.
   • Establish a staff development process that benefits both employees and the District.
4 Improve internal communications throughout the organization.

a. Increase transparency of internal communication throughout the District.

b. Use the content of this Strategic Plan to structure internal meetings and communications.

c. Continuing to gather input and suggestions from staff about internal communications.

5-YEAR RESOURCE NEEDS

The items listed above can be implemented with current resource levels.
IMPLEMENTATION FRAMEWORK

Skagit PUD will use this Strategic Plan to guide decision-making during the five-year period from 2018 to 2022. The direction established in this plan is at a high level and will be used to inform more detailed and actionable annual plans.

Using this Strategic Plan as a foundation, Skagit PUD will:

• Establish annual implementation steps, timelines, and performance metrics or milestones to guide and monitor implementation of the Goals and Strategies established in the Strategic Plan.

• Use the Strategic Plan to inform and frame:
  » Budget development.
  » Work unit work plans.
  » Meetings, including Commission meetings and all-staff meetings.
  » Communications with staff, customers, and partners.

• Provide regular progress reports, including:
  » Quarterly staff progress reports to the General Manager.
  » Annual General Manager progress reports to the Commission.
VISION

Our Vision is to be an outstanding regional leader and innovative utility provider.

MISSION

Our Mission is to provide our customers with high-quality water services at an affordable price.

VALUES

As we pursue our Vision and advance our Mission, we demonstrate and maintain balance among our Core Values:

- **Quality.** We seek to exceed customer expectations by providing exceptional service.
- **Environmental Stewardship.** We act to preserve our region’s natural resources.
- **Financial Prudence.** We strive to keep our rates as low as possible while making wise capital investments and strategic business decisions.

HOW THIS PLAN WILL BE USED

Skagit PUD will use this Strategic Plan to guide decision-making during the five-year period from 2018 to 2022. The direction established in this plan is at a high level and will be used to inform more detailed and actionable annual plans, budgets, Commission meetings, and communications with customers and partners. Progress will be reported regularly, with staff reporting to the General Manager quarterly, and the General Manager reporting to the Commission annually.

WANT TO LEARN MORE?

Skagit PUD welcomes the opportunity to share our plan with you. Visit our website www.skagitpud.org or contact our Community Relations Manager, Kevin Tate, at (360) 424-7104.
I. CUSTOMER-FOCUSED SERVICES

A. WATER
Skagit PUD’s core focus is providing water to residential, business, and agricultural customers. We make strategic and sustainable investments to ensure our water rights, infrastructure, and other resources are managed for the benefit of our customers and for the long-term benefit of the region. The most significant contribution we can make to environmental sustainability is by improving the efficiency of our system and by encouraging smart water use among our customers. By making strategic investments to reduce wasted water, we will also diminish our need for finding additional water sources and for making large capital improvements in the future. The District will play a supportive role in addressing the legal availability of water for agriculture and rural land owners.

1. Make prioritized and strategic capital infrastructure investments to maintain existing assets and quality to serve the growing Skagit community.
2. Steward partnership-based efforts that advance the strategic regional use of water resources.

B. TELECOMMUNICATIONS
Investment in telecommunications infrastructure is necessary to the security and effective management of Skagit PUD’s water systems. Skagit PUD is collaborating with the Port of Skagit County on the SkagitNet effort for development of telecommunications services to support the growth and prosperity of the Skagit County community. In these efforts, Skagit PUD will favor the development of wholesale capacity over becoming a retail provider.

1. Invest in the telecommunications infrastructure necessary to securely and efficiently manage our water system and facilitate the extension of broadband infrastructure to rural communities.
2. Stay current and decide whether we should enter the telecom industry as a retail provider if public utility districts are given the authority to do so.

C. SEWER
While Skagit PUD has the legal authority to provide sewer services, we are not seeking to develop this service area. We would, however, be willing to meet regional needs if directed to do so by state and local agencies. We will more actively pursue opportunities to use sewage as a method of increasing water availability and reducing or deferring investment in our water system infrastructure through water reclamation and recycling.

1. Explore and understand the connection between sewage and reclaimed water.

II. COMMUNICATION WITH THE PUBLIC AND PARTNERS
As a service provider and steward of public resources, it is incumbent on us to communicate effectively with our customers, members of the public, and partners.

1. Strengthen communications and engagements with our customers.
2. Seek opportunities to engage youth in water-related education.
3. Ensure our policy-setting and decision-making processes are transparent and easily accessible.
4. Strengthen our provision of high-quality customer service.
5. Strengthen our relationships with our partners.

III. INTERNAL OPERATIONS, COMMUNICATION, AND ORGANIZATIONAL DEVELOPMENT
To provide high-quality services for our customers, it is imperative that we have strong staff and supporting systems.

1. Strengthen internal systems and the use of technology to create efficiencies.
2. Address our aging District headquarters facility.
3. Attract, retain, and develop a high-quality workforce.
4. Improve internal communications throughout the organization.
June 22, 2018

TO: George Sidhu, P.E., General Manager
FROM: Gary Chrysler, IT Manager

SUBJECT: IT Policy and subordinate Administrative Practice and Procedure (AP&P) Documents.

Requested Action:
Approve and authorize the General Manager to sign District Policies #1060, #1061, and #1062.

Background:
The Commission has received review packets over the first half of the year including a complete replacement of all IT Policies and Procedures. With the completion of this project, and having heard no requests for changes from the Commission, all of the goals of the project have been met and all that remains is final approval.

There will be occasional new AP&P documents as business needs require, but for now, after much effort, we are ready to go.

Attached are District Policies #1060, #1061, and #1062.

Fiscal Impact:
There is no fiscal impact at this time.

kac
In accordance with the authority granted by Board Resolution #2160-09, an Information Technology Policy is hereby established for all employees, consultants, vendors, and contractors.

1. Purpose

The purpose of this Policy is to ensure an information technology infrastructure that promotes the basic mission of the District. In particular, this Policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and superior performance of Information Technology Systems;
- To protect privacy and maintain legally required restrictions to information as required by District policies and procedures, state and federal law, and industry best practices;
- To ensure that use of Information Technology Systems is consistent with the principles and values that govern use of other District facilities and services;
- To ensure that Information Technology Systems are used for their intended purposes; and
- To establish processes for addressing policy violations and sanctions for violators.

All hardware, software, and related technology systems and services are provided by the District for the sole purpose of enhancing and attaining the District’s stated and published mission, vision, and values, the District’s Code of Conduct, and other code of ethics / responsibilities documents as referenced in District policies and Administrative Practices and Procedures.

2. Definition

Information technology systems and electronic resources are provided by the District with the understanding that approved users will interact with them with a sense of compliance and adherence to all applicable laws and regulations, mutual respect, cooperation and collaboration. These resources are finite, and must be shared. With any established interconnection of electronic resources, the effect of one individual can have a dramatic effect on others within the network. As such, the use of District network and electronic resources is a revocable privilege. All constituents will benefit if all users of the District’s electronic systems avoid any activities that may cause interruptions or degradation of services for other users of the same systems.

The Information Technology Department proactively monitors the network for activity which violates District policies, practices, and procedures. Failure to comply with the terms of this policy may lead to disciplinary or legal action. Penalties for unacceptable use, as outlined in the accompanying Administrative Practices and Procedures, range from immediate deactivation of the user’s account, disciplinary action up to and including termination, and/or referral to law enforcement authorities for further investigation.

The District reserves the right to monitor, limit, and /or restrict any electronic messages, network and/or systems traffic, and public or private information stored on computers owned, maintained, or managed by the District. Computers, systems, or services not owned, maintained, or managed
by the District shall not be used to interact with District systems, unless granted, in writing, specific privilege on a case-by-case basis. Email, voice mail, web pages, and digital content are subject to archiving, monitoring, and review, and may be subject to public disclosure in accordance with RCW 42.56.

3. Enforcement

The District expects that all individuals using its electronic resources, including, but not limited to, employees, commissioners, consultants, vendors, contractors, and anyone else granted temporary or permanent access, will abide by this policy.

All access to the District’s systems must be authorized and pre-approved, and users must understand that laws currently exist prohibiting the following:

- Electronic libeling or defamation;
- Sending/Posting/Broadcasting messages that incite hate or discontent;
- Transmitting repeated unwanted advances;
- Falsifying information or impersonation;
- Unauthorized use, providing, or copying protected intellectual or copyrighted property;
- The unauthorized transmission, in any form, of legally protected information;

The District also states definitively that its networks are private, separate, and distinct from the public Internet. As such, access and use must comply with all District administrative practices and procedures, rules, and regulations, as well as compliance and adherence to all federal, state, and local laws.

4. Policy Management

The Information Technology Department, in cooperation with District Management and Staff, will continue to update, maintain, improve, and add to its Administrative Practices and Procedures as regulation, industry standards, and District procedures require. Information Technology Administrative Practices and Procedures are grouped under the following headings for clarity.

4.1 IT Staff Manual

The IT Staff Manual contains Administrative Practices and Procedures applicable to the technical and security operations of the IT Department. The IT Staff Manual is directed, primarily, at IT Department Staff.

4.2 Managers’ Manual

The Managers’ Manual contains Administrative Practices and Procedures applicable to the management of the District and its various departments in relation to Information Technology requirements. The Managers’ Manual is directed, primarily, at the District’s management team.
4.3 PCI Manual

The PCI Manual contains Administrative Practices and Procedures as required by Payment Card Industry Standards (PCI-DSS) for the protection of systems and data security, response plans, and training within the District. The PCI Manual is directed, primarily, at the IT, Finance, and Customer Service Department staff.

4.4 Operational Technology Manual

The Operational Technology Manual contains Administrative Practices and Procedures applicable to the management of the District’s Operational Technology, such as building security, supervisory control systems (SCADA). The Operational Technology manual is directed, primarily, at IT, Operations, and Water Treatment Plant staff.

4.5 End User Manual

The End User Manual Contains Administrative Practices and Procedures applicable to the use and day-to-day operation of the District’s Information and Operational Technology assets. The End User Manual is directed toward all District staff, contract employees, contractors, consultants, and anyone else who may be authorized to access and use District technology assets.

5. Updates

Information Technology will work with District leadership and staff to maintain and facilitate the distribution of all related Administrative Practices and Procedures under the authority of this policy. District Staff may revise, replace, or delete specific Administrative Practices and Procedures, as the law, District practices, industry standards, and/or circumstances require.

<table>
<thead>
<tr>
<th>Former Title/Policy #:</th>
<th>1060</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board Approval Date:</td>
<td></td>
</tr>
<tr>
<td>Effective Date: 8/26/18</td>
<td></td>
</tr>
<tr>
<td>Revision Date(s):</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. **Overview**
Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives the District a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

2. **Purpose**
This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by the District that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

3. **Scope**
This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

4. **Policy**
   
   **4.1 Contingency Plans**
   The following contingency plans must be created:
   
   - **Computer Emergency Response Plan:** Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
   - **Succession Plan:** Describe the flow of responsibility when normal staff is unavailable to perform their duties.
   - **Data Study:** Detail the data stored on the systems, its criticality, and its confidentiality.
   - **Criticality of Service List:** List all the services provided and their order of importance.
   - It also explains the order of recovery in both short-term and long-term timeframes.
   - **Data Backup and Restoration Plan:** Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
   - **Equipment Replacement Plan:** Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
   - **Mass Media Management:** Who is in charge of giving information to the mass media?
   - Also provide some guidelines on what data is appropriate to be provided.
After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

5. Policy Compliance

5.1 Compliance Measurement
The IT Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the IT Team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes
None.

7. Definitions and Terms
The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Disaster

8. Revision History

<table>
<thead>
<tr>
<th>Former Title/Policy #</th>
<th>1061</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board Approval Date:</td>
<td></td>
</tr>
<tr>
<td>Effective Date: 8/26/18</td>
<td></td>
</tr>
<tr>
<td>Revision Date(s):</td>
<td></td>
</tr>
</tbody>
</table>

General Manager Signature: ___________________________ Date: ___________________________
1. Overview
A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an SRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

2. Purpose
The purpose of this policy is to establish the requirement that all business units supported by the IT Team develop and maintain a security response plan. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

3. Scope
This policy applies any established and defined business unit or entity within the District.

Policy
The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific business unit for whom the SRP is being developed in cooperation with the IT Team. Business units are expected to properly facilitate the SRP for applicable to the service or products they are held accountable. The business unit security coordinator or champion is further expected to work with the IT Manager and IT Staff in the development and maintenance of a Security Response Plan.

4.1 Service or Product Description
The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

4.2 Contact Information
The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).
4.3 Triage
The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

4.4 Identified Mitigations and Testing
The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

4.5 Mitigation and Remediation Timelines
The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

5 Policy Compliance

5.1 Compliance Measurement
Each business unit must be able to demonstrate they have a written SRP in place, and that it is under version control and is available via the web. The policy should be reviewed annually.

5.2 Exceptions
Any exception to this policy must be approved by the IT Team in advance and have a written record.

5.3 Non-Compliance
Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP.

6 Related Standards, Policies and Processes
None.

7 Definitions and Terms
None.

8 Revision History

<table>
<thead>
<tr>
<th>Former Title/Policy #:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Board Approval Date:</td>
<td></td>
</tr>
<tr>
<td>Effective Date: 8/26/18</td>
<td></td>
</tr>
<tr>
<td>Revision Date(s):</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>

Policy #1062
1 Purpose
This APP describes the manner in which voice recording of phone and radio conversations is to be conducted in the District.

2 APP
This APP supersedes all previous APP statements concerning voice recording. Any questions regarding this APP should be directed to the District’s General Counsel. District employees should check with the General Counsel prior to any recording of a phone and/or radio conversation.

3 Customer Service Only:
The District has been and may continue to selectively record phone conversations in Customer Service. Voice recording is considered a necessary business tool to be used, among other things, for training and improved customer communications. The recordings may be reviewed with appropriate staff and are not retained unless necessary for legal or disciplinary inquiry. At the resolution of these inquiries, the recordings shall be deleted after one to two months unless otherwise required by law.

4 Commission Meetings Only:
The District began recording commission meetings in 2017. All commission meeting recordings are subject to public records law and are made available on the District website. Commission meeting recordings are stored with our Cloud Vendor as well as on District servers, with full replication to our offsite disaster recovery facility. All commission meeting recordings are to be retained indefinitely.

5 Contact Information
General Manager
Public Relations
Human Resources
Information Technology

6 Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>403</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. **Purpose**
In order to protect and manage the District’s computer systems and servers, the Information Technology Department (IT) has developed IT policies and APP’s regarding network security, change management, and general use of District computers, among others. The District’s network systems are the backbones that keep our core business processes running, providing operational excellence and customer service to our internal customers as well as our customer owners. One of the ways the IT Department strives to be a good steward of these technological resources is by developing IT policies and APP’s to keep systems running smoothly, allow District employees to conduct their work more efficiently, and keep the District on the cutting edge of today’s computer and network systems technology.

Technology is an ever-changing field. IT policies and APP’s need to be updated and changed regularly as technologies change. Due to the sensitive nature of the District’s computer and network systems and the need to protect them, IT policies and APP’s shall have the same force and effect as District administrative policies and APP’s.

2. **Policies and Procedures**
IT policies must be reviewed by the IT Steering Committee, also known as the Management Group, prior to submission for Commission approval.

IT APP documents must be reviewed by the IT Steering Committee prior to approval by the General Manager. All District employees must be aware of and abide by IT policies and APP’s which have gone through the IT Steering Committee approval process.

Employees are expected to know and comply with all IT policies and APP’s. Each employee is responsible to review IT policies and APP’s as posted on the internal public drive.

When a new IT policy is established or an older IT policy is updated, the IT Department will work with the Public Information Department to make sure the new or changed IT policy is communicated to District employees in a clear and timely manner.

All IT policies and APP’s shall be posted on the internal public drive and available for review by employees.
3. Contact Information
Information Technology Department

4. Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-501</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. Purpose

The purpose of this Information Technology (IT) department APP is to outline the process the department uses in retiring computer equipment. “Computer Equipment” includes desktop computers, laptop computers, Personal Digital Assistants (PDAs), or any other computer-related equipment. “Retiring” includes surplus, sale, auction or disposal of the equipment.

2. APP

The IT department is responsible for determining whether or not computer equipment is obsolete or available for surplus. Based on the current software and potential District-wide upgrades, computers will need to be replaced to make way for more up-to-date equipment. This cycle varies by type of equipment, technical standards and/or warranty periods.

When computer equipment is no longer needed by a department, the IT department will determine whether or not it is obsolete (outdated and unavailable for use in the District) according to the following criteria.

2.1. Determination of Obsolescence. The IT department will consider several criteria when determining whether computer equipment is obsolete:

- Age of the equipment
- Equipment warranty expiration
- Substandard technical performance
- Memory constraints
- Current value of equipment vs. the cost to maintain its usage
- No longer meets District’s technology or needs

Once computer equipment has been deemed obsolete by the IT department, it is no longer available for use in the District, per our Information Technology Change Management APP 503.

The IT department keeps records of the purchase of all District computer equipment as well as all the equipment capabilities. When computer equipment is considered obsolete, it is scheduled for replacement and the old equipment is retired.
2.2. **Retirement and Disposal Process.** When computer equipment is retired, the following information must be gathered:

- Description
- Make
- Manufacturer
- Serial Number

Equipment is to be tagged with the above information and stored in a safe and secure area in order to protect its value. The equipment is to be marked as “Retired” in the appropriate asset register.

2.2.1. If the computer equipment is **obsolete and functioning**, it is to be surplused according to Policy #1022 and the District’s Fixed and Tagged Assets Procedures. However, it is to be marked on the surplus list as not available for use in other departments of the District, as the equipment will not support current District standards. Retiring employees may purchase obsolete and functioning computer equipment that has been assigned to them at the fair market value of such equipment with the approval of the District’s Finance Manager.

2.2.2. If the computer equipment is **obsolete and scrap** (parts still usable and saleable), it is to be scrapped according to Policy #1022 and the District’s Fixed and Tagged Assets Procedures.

2.2.3. If the equipment is **broken and not repairable**, it has no fair market value and will be scheduled for disposal by the IT department in accordance with Hazardous Substances requirements.

3. **Contact Information**

Information Technology Department

4. **Reference**

District Fixed and Tagged Asset Procedures

5. **Revision History**

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-502</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. Overview
See Purpose.

2. Purpose
The purpose of this APP is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this APP provides direction to ensure Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

3. Scope
This APP applies to all District employees and affiliates.

4. APP
4.1 Algorithm Requirements
4.1.1 Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

4.1.2 Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

4.1.3 Signature Algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Key Length (min)</th>
<th>Additional Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDSA</td>
<td>P-256</td>
<td>Cisco Legal recommends RFC6090 compliance to avoid patent infringement.</td>
</tr>
<tr>
<td>RSA</td>
<td>2048</td>
<td>Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.</td>
</tr>
<tr>
<td>LDWM</td>
<td>SHA256</td>
<td>Refer to LDWM Hash-based Signatures Draft</td>
</tr>
</tbody>
</table>

4.2 Hash Function Requirements
In general, the District adheres to the NIST Policy on Hash Functions.
4.3 Key Agreement and Authentication

4.3.1 Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

4.3.2 End points must be authenticated prior to the exchange or derivation of session keys.

4.3.3 Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

4.3.4 All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

4.3.5 All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

4.4 Key Generation

4.4.1 Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

4.4.2 Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

5. Policy Compliance

5.1 Compliance Measurement
The IT team will verify compliance to this APP through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the APP owner.

5.2 Exceptions
Any exception to the APP must be approved by the IT team in advance.

5.3 Non-Compliance
An employee found to have violated this APP may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes
National Institute of Standards and Technology (NIST) publication FIPS 140-2.

NIST Policy on Hash Functions

7 Definitions and Terms
The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/
8 Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-502.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change/s</th>
<th>Author/s</th>
<th>Approver/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01/01/15</td>
<td></td>
<td>Gary Chrysler</td>
<td></td>
</tr>
</tbody>
</table>
1. **Overview**

A clean desk policy can be an import tool to ensure all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee’s awareness about protecting sensitive information.

2. **Purpose**

The purpose for this policy is to establish the minimum requirements for maintaining a “clean desk” – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

3. **Scope**

This policy applies to all District employees and affiliates.

4. **Policy**

   4.1 Employees are required to ensure all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

   4.2 Computer workstations must be locked when workspace is unoccupied.

   4.3 Computer workstations must be shut completely down at the end of the work day.

   4.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

   4.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when left unattended.

   4.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

   4.7 Laptops must be either locked with a locking cable or locked away in a drawer.

   4.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

   4.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

   4.10 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the locked confidential disposal bins.

   4.11 Whiteboards containing Restricted and/or Sensitive information should be erased.

   4.12 Lock away portable computing devices such as laptops and tablets.
4.13 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
4.14 All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure sensitive documents are not left in printer trays for the wrong person to pick up.

5. Policy Compliance

5.1 Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the IT team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes
None.

7 Definitions and Terms
None.

8 Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-502.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General Manager Signature:</th>
<th>Date:</th>
</tr>
</thead>
</table>
1. Overview
Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the network.

2. Purpose
The purpose of this guidelines is to provide best practices for the created of strong passwords.

3. Scope
This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

4. Statement of Guidelines
All passwords should meet or exceed the following guidelines

4.1. Strong passwords have the following characteristics:
- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:";'<>?,/).

4.2. Poor, or weak, passwords have the following characteristics:
- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these examples as passwords!)
5.0 Passphrases
Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

6. Policy Compliance
6.1. Compliance Measurement
The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

6.2. Exceptions
Any exception to the policy must be approved by the Infosec team in advance.

6.3. Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7. Related Standards, Policies and Processes
None.

8. Definitions and Terms
None.

9. Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>Effective Date:</th>
<th>Revision Date:</th>
<th>General Manager Signature:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2060-502.7</td>
<td>8/26/08</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PUBLIC UTILITY DISTRICT NO. 1 OF SKAGIT COUNTY
Password Protection APP

APP #2060-502.8

1. Overview
Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of the District's resources. All users, including contractors and vendors with access to District systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose
The purpose of this APP is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope
The scope of this APP includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any District facility, has access to the District network, or stores any non-public District information.

4. APP
4.1 Password Creation
4.1.1 All user-level and system-level passwords must conform to APP No. 2060-502
4.1.2 Users must not use the same password for District accounts as for other non-District access (for example, personal ISP account, option trading, benefits, and so on).
4.1.3 Where possible, users must not use the same password for various District access needs.
4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
4.1.5 Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

4.2 Password Change
4.2.1 All system-level passwords (for example, root, enable, Domain Admin, Local Admin, application administration accounts, and so on) must be changed, where practical means are available to change them, on at least a quarterly basis.
4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.
4.2.3 Password cracking or guessing may be performed on a periodic or random basis by
the IT Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential District information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not hint at the format of a password (for example, "my family name").

4.3.6 Do not share District passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

4.3.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.9 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."
A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5. APP Compliance

5.1 Compliance Measurement
The IT Team will verify compliance to this APP through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the APP owner.

5.2 Exceptions
Any exception to the APP must be approved by the IT Team in advance.

5.3 Non-Compliance
An employee found to have violated this APP may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

- Password Construction Guidelines

7 Definitions and Terms
The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Simple Network Management Protocol (SNMP)

8 Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-502.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General Manager Signature:</th>
<th>Date:</th>
</tr>
</thead>
</table>
Guideline for Transmission of Social Security Numbers and Other Legally Protected Information
APP #2060-502.9

Introduction

The model approach for access to information is based upon the lowest required level of access. The model approach for the release of any information is to release the least amount of information required. As an example, in the case of a collection agency,

1. What, specifically, are they requesting
2. Signed verification by Authorized District Personnel that the requesting person/agency/entity is legally allowed access to the requested information.
3. If allowed access to information by law, use an approval work flow that has, at the minimum,
   a. the requesting agency,
   b. the requesting person,
   c. the reason for the request,
   d. a checklist of what is being requested
   e. itemized description of what is transmitted with notation of what was refused, why, and by whom.
   f. Acknowledgement of Transmission with the following:
      i. Preparers Position, signature, and date,
      ii. Receivers Position, signature, and date, and
      iii. Approver’s Position, signature, and date.
   g. How the information was transmitted
   h. Who transmitted the data
   i. Who received the data
   j. Acknowledgement of the receipt of data.
      i. Legally protected information should never be transmitted via email.
4. There are two ways to request information
   a. Public Records Request
      i. Follow the process in place to address these requests
      ii. All requests must be made in accordance with currently legal standards.
   b. Other requests
      i. No information should be transmitted via requests by telephone
      ii. All requests must be made in writing
      iii. Protected information must not be transmitted unless legally required.
      iv. Collection agencies do not have a legal right to protected information.
5. Revision History:

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-502</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General Manager Signature:</th>
<th>Date:</th>
</tr>
</thead>
</table>
1. Purpose

This APP defines how changes are made to the District’s IT technology, including servers, network, applications and data. When this APP is followed, incidents risk is reduced and the integrity of the business operations and reporting is preserved. Without APP formality, the risk of incidents would be higher and accountability for IT changes would be insufficiently documented. Change Management is an IT Service Management discipline whose goal is to reduce the risk of incidents when changes are made to the IT infrastructure and applications. Change Management reduces the risk through standardized procedures to document, communicate and implement changes.

2. Scope

All District APP’s involving the purchase, management, and maintenance of software and technology equipment operated within the District’s facilities or for the District are within the scope of this APP. If there is variance between departmental expectations and the approach described through District procedures, the District will look to IT Staff and the General Manager to support the spirit and the objectives of District APP’s.

3. APP

3.1. Software Governed by This APP

The word “change” applies to new, modified, and decommissioned software, servers, applications, systems, and data.

The Information Technology Change Management APP applies to all District software and technology connected to or operating in, on, or within the District’s network, servers, and systems. It includes software and systems maintained by IT or by any other department or staff member; this includes vendor-supplied software, in-house developed software and scripting, as well as all hardware connected to, or capable of being connected to District owned infrastructure.

Software and other technology installations that are administered, developed, or maintained by non-IT department staff shall comply with this APP.

3.2. Application Change Tracking

IT uses helpdesk software as a tool for change tracking. Users submit a helpdesk request ticket when they need support for any software changes, including application, access, or production data changes.

The helpdesk ticket is routed for approval and assigned to the appropriate person who will make the change, or manage the vendor making the change.

All proposed changes shall be submitted for approval routing through the helpdesk system and shall be reviewed with appropriate IT Staff prior to approval. Documentation of approved changes and successful testing shall be submitting through the helpdesk for final approval.
3.3. Network Systems and Services Scheduled Maintenance

IT staff must patch and update software equipment regularly to protect the District's IT environment. Although IT works hard to minimize the impact to the District, our water customers, and our end users, we also occasionally need vendor support during maintenance cycles.

As not all vendors are available 24/7, we have created a schedule with various types of maintenance windows that may include system outages.

3.4. Maintenance Schedules

3.4.1. Planned Maintenance

Scheduled maintenance, including, but not limited to the following examples:

- Microsoft patches automatically applied after hours by Group Policy
- Installation of Core System Software patches
- Other vendor security patches for known vulnerabilities as made available.

3.4.2. Unplanned Maintenance

Unscheduled maintenance may be the result of a system or software failure, or vulnerability or other similar situation, resulting in or requiring immediate downtime which may directly impact business operations.

4. Procedures

All IT Staff are responsible for documenting changes to District software, Third Party software, application configuration, and systems configuration. The IT Manager and the General Manager are responsible for enforcing the IT Change Management APP.

5. Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>503</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. Overview
IT’s intention for publishing an Acceptable Use APP is not to impose restrictions contrary to Skagit PUD’s established culture of openness, trust and integrity. IT is committed to protecting the District's employees, partners, customers, and the company, from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the District. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies and procedures for further details.

Effective security is a team effort involving the participation and support of every District employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose
The purpose of this APP is to outline the acceptable use of computing, network, and software of and at the District. These rules are in place to protect the employee and the District. Inappropriate use exposes the District to risks including malware attacks, compromise of network systems, security, and services, as well as legal issues.

3. Scope
This APP applies to the use of information, electronic and computing devices, and network resources, and software, to conduct District business or interact with internal networks and business systems, whether owned or leased by the District, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at the District and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with District policies and standards, and local laws and regulation. Exceptions to this APP are documented in section 5.2.
This APP applies to employees, contractors, consultants, temporary, and other workers at the District, including all personnel affiliated with third parties. This APP applies to all equipment owned or leased by the District.

4. APP

4.1 General Use and Ownership

4.1.1 District proprietary information stored on electronic and computing devices whether owned or leased by the District, the employee or a third party, remains the sole property of the District. You must ensure through legal or technical means, proprietary information is protected in accordance with the Data Protection Standard.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of District proprietary, or any legally protected information.

4.1.3 You may access, use or share District proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use in accordance with District Policy 1010 – Ethics in the Workplace. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within the District may monitor equipment, systems and network traffic at any time, per IT's Audit APP.

4.1.6 The District reserves the right to audit networks and systems on a periodic basis to ensure compliance with this APP.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access APP.

4.2.2 System level and user level passwords must comply with the Password APP. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
4.2.4 Postings by employees from a District email address to newsgroups should contain a
disclaimer stating the opinions expressed are strictly their own and not necessarily those
of the District, unless posting is in the course of business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from
unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these
restrictions during the course of their legitimate job responsibilities (e.g., systems administration
staff may have a need to disable the network access of a host if the host is disrupting production
services).

Under no circumstances is an employee of the District authorized to engage in any activity
deemed illegal under local, state, federal or international law while utilizing District-owned
resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities
which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret,
   patent or other intellectual property, or similar laws or regulations, including, but not
   limited to, the installation or distribution of "pirated" or other software products not
   appropriately licensed for use by the District.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization
   and distribution of photographs from magazines, books or other copyrighted sources,
   copyrighted music, copyrighted video, and the installation of any copyrighted software
   for which the District or the end user does not have an active license, is strictly
   prohibited.

3. Accessing data, a server, or an account, for any purpose other than conducting District
   business, even with authorized access, is prohibited.

4. Exporting software, technical information, encryption software, or technology in
   violation of international or regional export control laws is illegal. The appropriate
   management should be consulted prior to export of any material in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms,
   Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a District computing asset to actively engage in procuring or transmitting material in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction. Reference District APP 2040-Discrimination, Harassment and Bullying.

8. Making fraudulent offers of products, items, or services originating from any District account or computer.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties or otherwise specifically authorized. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning by employees or by third parties or vendors is expressly prohibited unless prior notification to IT is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the District network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, District employees to parties outside the District.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.

1. Sending unsolicited email messages, including the sending of 'junk mail' or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages. Reference District APP 2040-Discrimination, Harassment and Bullying

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within the District's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the District or connected via the District's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using the District’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this APP. Limited and occasional use of the District’s systems to engage in blogging is acceptable, provided it is done in a professional and responsible manner, does not otherwise violate the District’s appropriate APP’s, is not detrimental to the District’s best interests, and does not interfere with an employee's regular work duties. Blogging from the District’s systems is subject to monitoring.

2. The District’s Confidential Information APP also applies to blogging. As such, Employees are prohibited from revealing any District confidential or proprietary information, trade secrets or any other material covered by the District’s Confidential Information APP when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of the District, and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the District’s AP&P 2040-Discrimination, Harassment and Bullying.

4. Employees may also not attribute personal statements, opinions or beliefs to the District when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the District. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the District’s trademarks, logos and any other District intellectual property may not be used in connection with any blogging activity.
5. **APP Compliance**

5.1 Compliance Measurement
The IT team will verify compliance to this APP through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the APP owner.

5.2 Exceptions
Any exception to the APP must be approved by the IT Policy Review Board in advance.

5.3 Non-Compliance
An employee found to have violated this APP may be subject to disciplinary action, up to and including termination of employment.

6. **Related Standards, Policies and Processes**
- Data Classification APP
- Data Protection Standard
- Social Media APP
- Minimum Access APP
- Password APP

7. **Definitions and Terms**
The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/
- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

8. **Revision History**

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-505</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. **Overview**
Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can pose many legal, privacy and security risks, thus it’s important for users to understand the appropriate use of electronic communications.

2. **Purpose**
The purpose of this email APP is to ensure the proper use of the District email system and make users aware of what the District deems as acceptable and unacceptable use of its email system. This APP outlines the minimum requirements for use of email within the District Network.

3. **Scope**
This APP covers appropriate use of any email sent from a District email address and applies to all employees, vendors, and agents operating on behalf of the District.

4. **APP**
4.1 All use of email must be consistent with District policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
4.2 District email account should be used primarily for District business-related purposes; personal communication is permitted on a limited basis, but non-District related commercial uses are expressly prohibited.
4.3 All District data contained within an email message or an attachment must be secured according to the *Data Protection Standard*.
4.4 Email should be retained only if it qualifies as a District business record. Email is a District business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
4.5 Email that is identified as a District business record shall be retained according to the District’s Record Retention Schedule.
4.6 The District email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any District employee should report the matter to their supervisor immediately.
4.7 Users are prohibited from automatically forwarding District email to a third party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain District confidential or above information.
4.8 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct District business, to create or memorialize any binding transactions, or to store or retain email on behalf of the District. Such communications and transactions should be conducted through proper channels using District-approved documentation.

4.9 Using a reasonable amount of District resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a District email account is prohibited.

4.10 District employees shall have no expectation of privacy in anything they store, send or receive on the company’s email system.

4.11 The District may monitor messages without prior notice. The District is not obliged to monitor email messages.

5 APP Compliance

5.1 Compliance Measurement
The IT team will verify compliance to this APP through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the APP owner.

5.2 Exceptions
Any exception to the APP must be approved by the IT team in advance.

5.3 Non-Compliance
An employee found to have violated this APP may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes
- Data Protection Standard

7 Definitions and Terms
None.

8 Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-506.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. Purpose
This policy addresses access to, use, and disclosure of electronic mail (e-mail). “E-mail” includes all technologies used to transfer messages, including electronic mail and any form of “chat” (i.e., instant messaging and/or peer-to-peer file exchange).

E-mail is a business tool that is provided by the District to employees to facilitate the timely and efficient conduct of District business. To help ensure that e-mail is used appropriately, the District has developed this policy.

2. Policy
1. Acceptable Use and General E-Mail Guidelines

   The District provides electronic mail to employees, and to contractors who have appropriate authorization, at District expense for their use on District business. Incidental and occasional personal use of electronic mail is permitted; however, such messages will be treated no differently from other messages, and the employees should not consider the messages private or confidential. Personal e-mail use shall not interfere with the performance of job duties. Users of the District’s e-mail system shall adhere to the following guidelines:

   a) Be careful about sending confidential information by e-mail. E-mail is not private. Generally speaking, do not put anything in an e-mail message that you would not want everybody to read.

   b) Do not flood other mailboxes (systems) with messages.

   c) Do not participate in chain e-mails.

   d) All-User emails are to be sent only by supervisors. Employees that must send all-user emails must do so at the direction of or the approval of their respective supervisors or the General Manager.

   e) Do not “reply all” to all user emails.

   d) Do not attempt to obscure the true identity of the sender of messages or forge messages from another user.
e) If you receive a message addressed to another user (and not to you) please let the sender know, and contact the IT Help Desk.

a) Be aware of system capacities. Your e-mail account has a limited storage capacity. To prevent an interruption of service, ensure that e-mail that has no further reference value is deleted or stored off-line to a Personal File Folder. This includes messages in your Inbox, Sent Items, or other on-line e-mail folders.

b) Avoid the initial impulse to send "flame" mail (a message that is uncomplimentary or insulting to the recipient). You cannot retract a message once it has been sent. Take time out to consider your actions, and the potential reaction; then compose your message or choose another method of communication.

c) E-mail is a delivery mechanism not only for general correspondence, but also for Official Public Records. It can transmit both unofficial and official business, close a transaction, or authorize work. Refer to the District’s Records Management Policy for more information on the storage, retention, and disposition of electronic mail.

d) E-mail that is deleted from your Deleted Items folder is recoverable for up to thirty (30) days. After that period, it is not recoverable.

e) Employees should not open e-mails or attachments unless they know the sender, know the attachment, and are expecting the attachment. Some file types are restricted to be included as an attachment. Contact the IT Help Desk for more information.

f) When using e-mail for personal use, consider the content. E-mail communications leaving the District come from "skagitpud.org" and not only imply Skagit PUD representation, but are, in fact, District property and may be subject to public disclosure. Delete e-mail used for personal use at the earliest opportunity.

g) E-mail can be considered junk mail or “spam” (unsolicited advertisements). Avoid unnecessary proliferation of messages. Do not send frivolous or excessive messages.

2. Restrictions on E-mail Usage

a) Users must not send through email credit card numbers, procurement card numbers, social security numbers, log-in passwords, payments information, or any confidential information.

b) The electronic display or transmission of sexually explicit images, messages or cartoons is prohibited.

c) The use of ethnic slurs, racial epithets, or any material that offensively addresses someone’s age, sex, sexual orientation, religion, national origin, ancestry or disability, or any language that might be construed as harassment is prohibited. The use of any kind of offensive, abusive, harassing or threatening words or documents sent either internally or externally that might be construed as harassment is prohibited. Harassment is defined as the creation of an intimidating, hostile, or offensive working environment. See District
APP 2040-Discrimination, Harassment and Bullying for further information on the District’s prohibition against harassment.

d) The use of electronic mail to solicit or proselytize others for commercial ventures, religious or political causes is prohibited.

e) The use of the District’s e-mail system to develop or send any virus or otherwise destructive program is prohibited.

f) The use of e-mail for political purposes, such as using e-mail to circulate advertising for political candidates or issues, is prohibited.

3. Prohibition on the Use of External E-mail and Internet E-mail Accounts

The District has in place extensive security measures for our computer systems and servers. The District utilizes the very best antimalware and filtering solutions; however, they only check for e-mail viruses on our corporate email server. The system does not, and cannot, monitor outside email/Internet accounts. Checking a personal Internet email account from a District workstation bypasses our security and can cause serious problems, including a complete network outage. For the purpose of protecting the security of District computer systems and networks, and with no exception, employees shall not access external email accounts from District workstations. Any email account that does not end in “@skagitpud.org” is considered an outside email account.

4. Use of District E-mail System by Non-Employees

If there is a legitimate business reason, certain customers, suppliers, and other third parties may use the District electronic mail system under special circumstances and only if they agree to abide by all applicable rules. The District reserves the exclusive right to administer and maintain user capabilities in the District e-mail system.

In order to provide a non-employee with District e-mail access, a Technology Resources Request Form must be filled by the sponsoring District supervisor or manager and provided to the IT Help Desk Coordinator. The Technology Resources Request Form is located on the IT Homepage on the Intranet.

5. All Employee Messages

Approval of “All Employees” (allusers@skagitpud.org) e-mail messages is the responsibility of the General Manager or Department managers. No message is to be sent to the “All Employees” group without review and authorization by the employee’s Department manager.

6. Activity Monitoring

The e-mail system at the District is the property of the District. The District reserves the right to review, access, monitor and/or disclose any message or any material, including attachments, created, received or sent, or files downloaded over the District’s e-mail system. The monitoring system of the District is capable of tracking and recording e-mail messages.
sent and received. The purpose of such monitoring by the District is to provide quality control, ensure compliance with District policies, and for other business purposes.

It is a violation of District policy for any employee, including Network and E-mail Administrators, to use the electronic mail system to satisfy idle curiosity, with no legitimate business purpose for obtaining access to the files or communications of others. Such electronic "snooping" is prohibited.

7. Privacy and Public Records

Pursuant to the Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510 et seq.), notice is hereby given there are no facilities provided by this system for sending or receiving truly private or confidential electronic communications. Pursuant to Washington Public Disclosure laws Act (RCW 42.17.250 et seq.) e-mail, depending on its content and/or attachment(s), may be considered to be an “Official Public Record.” As such, e-mail may be subject to disclosure to the public and/or news media upon request. Please refer to District Policy No. 405 regarding disclosure of documents and information. Further, e-mails that have been properly identified as Official Public Records, as defined in the District’s Record Management Policy (No. 402), should not be deleted, but rather retained in accordance with the policy.

8. Control Procedures

Network and/or E-mail Administrators may establish control procedures impacting the e-mail configurations of all employees. These may include limits on message file size, number of retained messages, individual message size, number and size of attachments, and other restrictions.

9. Questions and/or Reporting Violations

If you have information about a violation of this policy by another employee of the District, you may discuss the same with your supervisor or contact Human Resources or the Security Department.

If you have any questions about this policy, restrictions or guidelines, you may contact the IT Help Desk.

3. Contact Information

Records Management
Information Technology Department
Human Resources Department
4. Reference
Policy 2040-Discrimination, Harassment and Bullying
APP 2060-505 Use of Internet Access and Network Resources
APP 2060-506.1 Use of Email

5. Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-506.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
Public Utility District No. 1 of Skagit County
Payment Card Industry
Data Security Standards
Administrative Practice and Procedure (APP) Set
PCI DSS APP
SAQ A
# Table of Contents

<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Security APP</td>
<td>3</td>
</tr>
<tr>
<td>Data Classification APP</td>
<td>6</td>
</tr>
<tr>
<td>Data Retention APP</td>
<td>14</td>
</tr>
<tr>
<td>Data Disposal APP</td>
<td>18</td>
</tr>
<tr>
<td>Third-Party Access and Management APP</td>
<td>22</td>
</tr>
</tbody>
</table>
Backup Security Section 1

Introduction

Backups are made for systems transmitting, processing, and/or storing sensitive data in order to be able to reinstitute data and configurations should the system become compromised or in the event of a disaster. The District’s cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

As backup media may contain cardholder data, it needs to be protected from unauthorized access and/or use just like for any other electronic media containing this content. Unauthorized access and use of the contents of the media can potentially lead to a security breach, possibly causing harm to the District finances, operations, customers, and public image.

Purpose

This Backup Security APP details the requirements for the safeguarding of backup media containing cardholder data in the District’s cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to the District employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at the District, whether conducting activities on District premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by the District whether located on District premise or off-site, and all District locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at the District, to include District employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible. A digital copy will be stored in the Policy & Procedure folder under the District’s “Public” drive.
Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the District’s PCI Review Committee for review and approval on a case by case basis. A single exception does not constitute a permanent change in practice. If a permanent change in practice is required, a revision of the PCI policy will be required.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action, up to and including termination.

Review Schedule

The PCI Review Committee shall meet no less than 4 times per year on the last work day of each quarter. PCI Review Committee

Section 1 Detail

Cardholder Data Storage

Cardholder data must be encrypted or in an unreadable protected format wherever it is stored. Therefore, should backups be made of systems transmitting, processing, and storing this data, careful reviews should be made on a periodic basis to determine if cardholder data is being stored on the media.

Handling

Backup media containing cardholder data are to be treated according to the Confidential data labeling, handling, retention, and disposal policies. Backup media may be reused as long as the content is deleted using triple overwrite technology, otherwise it is to be physically destroyed by drilling per the District’s disposal policy.

Third-Party or Alternate Location Storage

In the event that cardholder data must be retained by the District, it shall, under no circumstances be transmitted to a third party for review or retention. If backup media(s) containing cardholder data are legally required to be retained at a third-party or another District location, they are to be tracked and protected against loss of theft. A certified and insured third-party must be used to pick up and deliver said media. The media must be counted and tracked at the point of departure and also at the point of arrival, in the case of inconsistencies, the PCI Review Committee will be notified in due time. A PCI-compliant service provider is recommended when using a third-party storage facility.
Tracking Logs

A log is to be maintained of the transports with the District Auditor’s signature. Transport logs are to be retained for a minimum of 2 years. The media must be counted and tracked at the point of departure and also at the point of arrival, in the case of inconsistencies, the PCI Review Committee will be notified in due time.
Data Classification Section 2

Introduction

The purpose of classifying data is to be able to define and implement the appropriate level of security controls to protect it from unauthorized access and use. The higher the level of classification, the more intensive and comprehensive the security controls should be in place to protect it. Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment. The District’s cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Printed and electronic data is to be classified in terms of its value to the District, sensitivity, legal requirements, and impact if it is lost or falls into the ‘wrong hands’. When performing a data classification exercise, it is critical to review the methods in which this data can be transmitted, stored, or used. Electronic data can be emailed, faxed, transmitted via instant message and/or other messaging technologies. Printed data can be faxed, hand delivered, scanned, and mailed. Data can be stored on systems, in code, workstations, devices, mobile media, backup tapes, and similar. Electronic data can be printed or copied to another workstation or system. Printed data can be retained in file cabinets and on desks.

Classifying data can help protect District data from unauthorized access and usage, and help safeguard the District’s finances, operations, customers, and public image.

Purpose

This Data Classification APP details the requirements for the classification of assets and data in the District’s cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to the District employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at the District, whether conducting activities on District premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by the District whether located on District premise or off-site, and all District locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at the District, to include District employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible. A digital copy will be stored in the Policy & Procedure folder under the District’s “Public” drive.
Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the District’s PCI Review Committee for review and approval on a case by case basis. A single exception does not constitute a permanent change in practice. If a permanent change in practice is required, a revision of the PCI policy will be required.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is September 1st, 2015 by the District’s PCI Review Committee, to be approved by the General Manager.

Section 2 Detail

Asset and Data Identification

Any asset (system, workstation, removable media, mobile media, backup tape, etc.) and data being processed, transmitted, and/or stored in the cardholder environment is to be identified and documented, along with the asset owner’s name, location, and contact information.

Asset and Data Evaluation

A risk assessment exercise should be performed to determine level of risk associated with each asset and data set. The list should be documented and assigned a classification of High, Medium, or Low in terms of its value to the District, sensitivity, legal requirements, and impact if lost or misused. Once this is completed, the evaluation should be reviewed and approved by the PCI Review Committee.

Classification Terminology

Should the asset or data set receive one or more High results during the evaluation exercise, it should be labeled as “Confidential”. If there are no High results and the asset or data set carries one or more Medium results, it should be labeled as “Confidential”. If the asset or data set receives no High or Medium results, it may be labeled as “Sensitive”.

Security Controls

The level of security controls to be in place to safeguard the asset or data set from unauthorized access and misuse will increase with its classification level. For example, a database storing encrypted cardholder data should still be classified as High and therefore “Confidential”, even though the contents are encrypted, as the loss of this data may still cause non-compliance with legal requirements and harm the District’s reputation. This database would require the highest level of security controls to be in place, to include, but not limited to, being placed behind a
firewall and an intrusion detection/prevention system, have restricted access permissions, maintain file integrity software, and have active logging enabled. An asset or data set classified as Confidential may be freely released externally and communicated, and may be readily accessible to both internal and external users.

**Data Handling**

Once the asset or data set have been classified, it is to be transmitted, processed, used, and/or stored following the methods outlined in the Data Handling APP. An asset or data set without an assigned classification is to be treated as “Confidential” until it is properly classified.

**Incident Response**

Should a Confidential asset or data set be intentionally or unintentionally accessed, viewed, or used by an unauthorized party, the incident response plan is to be initiated. Should it be a Sensitive asset or data set, the PCI Review Committee should evaluate the repercussions of the event and initiate the incident response plan as appropriate.

**Classification Details**

Confidential

This type of classification is assigned to assets and data sets which, if lost, would cause serious harm to the District, the District’s customers, the District’s third-parties, and others. Harmful effects can be from a financial, competitive, compliance, legal, branding, and/or reputation perspectives. Subsequently, it must be kept confidential.

Examples include cardholder data, financial plans, business and strategic plans, and customer lists.

Sensitive

This type of classification is assigned to assets and data sets which, if lost, could potentially cause harm to the District, the District’s customers, the District’s third-parties, and others; however it would not be unrepairable. Subsequently, it should be kept confidential as much as possible.

Examples include intranet content, performance evaluations, and internal communications (unless they contain confidential information).
Public

This type of classification is assigned to assets and data sets which are readily available and part of the public domain so would not cause any harm to the District, the District’s customers, the District’s third-parties, and others. Subsequently, it does not require specific security controls.

Examples include the District’s website, marketing materials, press releases, and external announcements.

Requests for Access to Confidential or Sensitive Assets or Data

The system owner is ultimately responsible for individuals and applications which have access to their assets, and are to review all access requests. The system owner is to review the access permissions on a quarterly basis in tandem with the quarterly access control review exercise.

Awareness

Users are to be trained and made aware of the classifications and their handling requirements. Users who have business requirements to view, access, and use Confidential and Sensitive assets and data are to receive specialized training on how to properly handle those items.
Data Handling Section 3

Introduction

Assets and data sets need to be handled by users according to their classification in order to properly safeguard it from unauthorized access and usage (see Data Classification APP). Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment. The District’s cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Electronic data can be emailed, faxed, transmitted via instant message and other messaging technologies. Printed data can be faxed, hand delivered, scanned, and mailed. Data can be stored on systems, in code, workstations, devices, mobile media, backup tapes, and others. Electronic data can be printed or copied to another workstation or system. Printed data can be retained in file cabinets and on desks.

Handling assets and data according to its classification level can help protect the District data from unauthorized access and usage, and help safeguard the District’s finances, operations, and brand name.

Purpose

This Data Handling APP details the requirements for the transmission, storing, and usage of assets and data in the District’s cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to the District employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at the District, whether conducting activities on District premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by the District whether located on District premise or off-site, and all District locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at the District, to include District employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.
The most current version of this policy is to be readily available and accessible. A digital copy will be stored in the Policy & Procedure folder under the District’s “Public” drive.

**Exceptions**

There are no exceptions to this policy. Requests for exceptions may be submitted to the District’s PCI Review Committee for review and approval on a case by case basis. A single exception does not constitute a permanent change in practice. If a permanent change in practice is required, a revision of the PCI policy will be required.

**Violations**

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action, up to and including termination.

**Review Schedule**

The next scheduled review date is September 1st, 2015 by the District’s PCI Review Committee, to be approved by the General Manager.

**Section 3 Detail**

**Cardholder Data**

Cardholder data must never be stored in electronic format. Sensitive authentication data may never be stored under any circumstances.

Cardholder data may never be transmitted using any end-user methodologies unless specifically approved by the PCI Review Committee with a valid business need. If required to transmit cardholder data, it must be in unreadable format (for example, encrypted, masked, truncated). Users may also not store cardholder data without specific approval to do so from the PCI Review Committee at which point it must also be retained in a protected format. The only exception is for users who need to view cardholder numbers for business reasons; these users must be approved by the PCI Review Committee and may only view the number individually (meaning one by one).

**Handling Requirements for Assets and Data Sets Labeled as Confidential:**

- **Access:** Business need-to-know only. Reviewed quarterly.
- **Non-Disclosure (NDA):** The District’s third-parties and employees may only access these assets and data after signing an NDA. The system owner must then approve the distribution.
- **Changes:** Changes made to these assets and data sets must be approved by the PCI Review Committee and the system owner prior to the change, recorded and retained for minimum of one year.
Email: Only individuals approved by the PCI Review Committee to transmit this data may do so, and then only if the email and its attachments are approved using a District-approved encryption method. A receipt request should be used or requested.

Internet: This data may never be transmitted using a non-District email system or posted/communicated via the internet. This includes posting to websites or using internet email and messaging technologies.

Fax: The person sending the fax with this data is required to be present at the fax machine to verify that it has been sent and is not stored in the memory. A receipt request should be used or requested.

Internal Mail: This type of data should not be delivered over internal District mail, unless absolutely necessary and then a return receipt should be used or requested. It is preferable to deliver the item in-person.

External Mail: This type of data is to be packaged in a secure manner and delivered by a commercial delivery service which can be tracked. A return receipt should be used or requested, such as a delivery signature.

Printing: This type of data should not be printed unless absolutely needed for business purposes, and after approval from the PCI Review Committee. The printing must be supervised.

Print Storage: Printed data is required to be within eyesight or within possession at all times, or locked up in a secure manner or location.

Electronic Storage: Stored data may not be retained in a readable format and is to be truncated, masked, or encrypted using a District-approved method. This includes data storage on workstations, systems, backup tapes, etc.

Handling Requirements for Assets and Data Sets Labeled as Sensitive:

Access: Business need-to-know only. Reviewed quarterly.

Non-Disclosure (NDA): The District’s third-parties and employees may only access these assets and data after signing a NDA.

Changes: Changes made to these assets and data sets must follow the District’s Change Management APP.

Email: Only individuals approved by the PCI Review Committee to transmit this data may do so, and then only if the email and its attachments are approved using a District-approved encryption method. A receipt request should be used or requested.

Internet: This data may never be transmitted using a non-District email system or posted/communicated via the Internet. This includes posting to websites or using Internet email and messaging technologies.

Fax: The person sending the fax with this data is required to be present at the fax machine to verify that it has been sent and is not stored in the memory. A receipt request should be used or requested.

Internal Mail: This type of data should not be delivered over internal District mail, unless absolutely necessary and then a return receipt should be used or requested. It is preferable to deliver the item in-person.

External Mail: This type of data is to be packaged in a secure manner and delivered by a commercial delivery service which can be tracked. A return
receipt should be used or requested, such as a delivery signature.

**Printing:**
This type of data should not be printed unless absolutely needed for business purposes, and after approval from the PCI Review Committee. The printing must be supervised.

**Print Storage:**
Printed data is required to be within eyesight or within possession at all times, or locked up in a secure manner or location.

**Electronic Storage:**
Stored data may not be retained in a readable format and is to be truncated, masked, or encrypted using a District-approved method. This includes data storage on workstations, systems, backup tapes, etc.

**Handling Requirements for Assets and Data Sets Labeled as Public:**

| Access: | Access is available to everyone Non-Disclosure (NDA): No NDA is required to distribute these assets or data |
| Changes: | Changes should follow the Change Management APP |
| Email: | May be readily emailed |
| Internet: | May be readily transmitted; however caution should be used if posting to an external website to ensure that the District’s reputation will not be harmed. |
| Fax: | May be readily faxed |
| Internal Mail: | May be delivered freely via internal mail |
| External Mail: | Mail be readily mailed outside of the District |
| Printing: | May be readily printed |
| Print Storage: | Does not need to be stored securely |
| Electronic Storage: | Does not need to be stored securely |
Data Retention Section 4

Introduction

The retention period for assets and data sets may be affected by legal, industry, financial, and/or regulatory requirements. In order to reduce risk, however, assets and data sets should not be retained longer than absolutely required in the cardholder environment. The District’s cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage phase(s) of cardholder data.

Each asset and data set (both electronic and printed formats) should be reviewed by a Legal point-of-contact to assess the District’s legal, industry, and regulatory requirements for its length of retention. The same exercise should be performed by the system owner as well as management to assess its industry requirements for retention. When completed, an analysis should be performed with the guiding principle that the item should be retained for the least amount of time as is possible.

The retention of assets and data for the minimum length of time possible under law and to support business operations can help protect the District’s data from unauthorized access and usage, and help safeguard the District’s finances, operations, and brand name.

Purpose

This Data Retention APP details the requirements for the retention of assets and data in the District’s cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to the District’s employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at the District, whether conducting activities on District premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased the District, whether located on District premise or off-site, and all District locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at the District, to include District employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible. A digital copy will be stored in the Policy & Procedure folder under the District’s “Public” drive.

Exceptions
There are no exceptions to this policy. Requests for exceptions may be submitted to the District’s PCI Review Committee for review and approval on a case by case basis. A single exception does not constitute a permanent change in practice. If a permanent change in practice is required, a revision of the PCI policy will be required.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action, up to and including termination.

Review Schedule

The scheduled meeting of the PCI Review Committee shall be on or near the 2nd Wednesday of the 1st month of each quarter, or more often, as required, to be approved by the General Manager.

Section 4 Detail

Retention of Cardholder Data

Cardholder data should only be retained for the minimum length of time as is possible, once legal, industry, financial, and regulatory requirements are reviewed and applied. Representatives from the Legal and Management groups, as well as the system owner, should assess these requirements and define the retention period for each asset and data set, following the guiding principle that the item should be retained for the least amount of time as is possible.

The form in Appendix A of this APP must be completed for each data set being retained.

Retention of Sensitive Authentication Data

Sensitive Authentication Data (the magnetic strip, PIN blocks, CVV) may never be stored.

Retention Periods

Data is to be deleted, at a minimum, quarterly or preferably more frequently, unless defined during the assessment exercise that it is required to be retained for a longer period of time. If it must be retained for longer than 90 days, a review should be performed quarterly to ensure that the data has not been retained past its defined storage period.

Responsibilities

The system owner or the data owner is ultimately responsible for ensuring that assets and data sets under their ownership are not retained past the defined periods. The PCI Review Committee is responsible for personally witnessing performing the physical destruction or deletion of data.
Third-Parties

Third-parties must receive a copy of District’s data labeling, handling, retention, and disposal policies and follow them exactly. Periodic, unannounced reviews should be made by District staff to ensure that the third-party does not violate the policies.
Appendix A: Retention Assessment

Data Set or Asset: ________________________________

Purpose/Function: ________________________________

Owner: ________________________________

Assessment Performed by: ________________________________

Assessment Date: ________________________________

Retention Requirements (as applicable):

Legal: ________________________________

Industry: ________________________________

Financial: ________________________________

Regulatory: ________________________________

Other: ________________________________

Data to be deleted on quarterly basis: Yes☐ No☐

Data to be reviewed on quarterly basis: Yes☐ No☐

Legal Signature: ________________________________

Management Signature: ________________________________

System/Data Owner Signature: ________________________________
Data Disposal Section 5

Introduction

Assets and data sets need to be safeguarded from unauthorized access and use throughout the lifecycle. When no longer needed for business reasons, care should be taken to ensure that the asset and its data cannot be accessed or regenerated by an unauthorized user when disposed of or transferred to a new party. Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment. District’s cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Secure disposal and deletion methods are required for assets and data sets which are classified as Confidential or Sensitive. Items classified as Public may be reused freely.

The secure disposal and deletion of assets and data according to its classification level can help protect District data from unauthorized access and use, and continue to safeguard District’s finances, operations, and brand name.

Purpose

This Data Disposal APP details the requirements for the disposal of assets and deletion of data in District’s cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to the District employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at the District, whether conducting activities on District premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by District whether located on District premise or off-site, and all District locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at the District, to include District employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible. A digital copy will be stored in the Policy & Procedure folder under the District’s “Public” drive.
Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the District’s PCI Review Committee for review and approval on a case by case basis. A single exception does not constitute a permanent change in practice. If a permanent change in practice is required, a revision of the PCI policy will be required.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action, up to and including termination.

Review Schedule

The next scheduled review date is ______________________, 2018 by the District’s PCI Review Committee, to be approved by the General Manager.

Section 5 Detail

Disposal Requirements for Electronic Data on:

Assets Labeled as Confidential

Confidential assets are to be securely wiped using an industry-strength wiping tool or format prior to being transferred to another party. If the asset is not going to be reused, the item should be physically destroyed in addition to taking the extra precaution of being securely wiped. Checks should be made of each asset to ensure that the data has successfully been deleted prior to the asset being provided to another party. The deletion or destruction schedule should be documented and reviewed by DAN Number on a quarterly basis. Users should be made aware of the importance of safely destroying and deleting these assets and data.

Cardholder data must be securely erased when it no longer meets its retention requirements (see Data Retention APP). If this period of time is longer than 90 days, an audit must be performed on a quarterly basis to ensure that it has not exceeded its defined retention period.

Assets Labeled as Sensitive

Sensitive assets are to be physically destroyed, and recorded, in the same manner as for those labeled as Confidential.
Assets Labeled as Public

Public assets are not required to be securely wiped using an industry-strength wiping tool or format prior to being transferred to another party; however it is recommended as a best practice. If the data is not securely deleted, then checks of each asset must be made to ensure that there is no sensitive data retained prior to the asset being provided to another party. The deletion or destruction schedule should be documented and reviewed by the PCI Review Committee on a quarterly basis.

Disposal Requirements for Printed Data:

Labeled as Confidential

Printed documentation labeled as Confidential assets are required to be shredded using a cross-cut shredder. All areas handling documentation with sensitive information must have such a shredder located nearby or a locked bin if a third-party is used to pick up the documentation for shredding. These documents are to be securely retained up to their destruction. Third-party vendors used to shred documentation must have provided a signed Non-Disclosure Agreement and agree to the District’s terms and conditions of protecting the sensitive data. The destruction schedule should be documented and reviewed by the PCI Review Committee on a quarterly basis. Users should be made aware of the importance of safely destructing these documents.

Cardholder data must be securely destructed when it no longer meets its retention requirements (see Data Retention APP). If this period of time is longer than 90 days, an audit must be performed on a quarterly basis to ensure that it has not exceeded its defined retention period.

Assets Labeled as Sensitive

Sensitive assets are to be destroyed, and recorded, in the same manner as for those labeled as Confidential.

Assets Labeled as Public

Public assets are not required to be securely destroyed. If the data is not securely deleted, then checks must be made of each asset to ensure that there is no sensitive data retained prior to the asset being provided to another party. The destruction schedule should be documented and reviewed by the PCI Review Committee on a quarterly basis.
Responsibilities

The system owner or the data owner is ultimately responsible for ensuring that electronic and printed media is disposed of in a secure manner, and the users’ managers are responsible for ensuring that their employees follow these policies. The PCI Review Committee is responsible for performing the actual destruction or deletion of data.

Third-Parties

Third-parties must receive a copy of District’s data labeling, handling, retention, and disposal policies and follow them. Periodic checks should be made by District to ensure that the third-party does not violate the policies.
Third-Party Access and Management Section 6

Introduction

Threats can be introduced to the District’s environment simply by connecting a third-party without efficient security practices and controls in place. Should an attacker penetrate the third-party’s network, they may route their way via the connected third-party into the District’s network. In some cases, third-parties have privileged access (meaning they have direct access to cardholder data in the production environment), thus gaining unauthorized access to the cardholder data environment. District’s cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Should an unauthorized user obtain access to the District’s network via this route, they may do so under the pretense of being the third-party and therefore potentially penetrate systems, applications, and other networks unnoticed to gain additional access to sensitive data. This can lead to a security breach, causing harm to the District’s finances, operations, and brand name.

A third-party, in Payment Card Industry (PCI) terms, may either transmit, process, and/or store cardholder data on behalf of District, but also may be connected to perform non PCI-related functions. Therefore, it is important to safeguard District from attackers masquerading as an authorized third-party, as well as proactively validating the security controls and practices in place at connected third-parties.

There are several types of third-parties, the most common being resellers, point of sale (POS) providers, Information Technology support companies, software application developers and vendors, shopping cart vendors, off-site storage vendors, data center and Web hosting providers, and Service Providers (those companies which transmit, process, and store cardholder data on District’s behalf).

Purpose

This Third-Party Access and Management APP details the requirements for the evaluation, connection, compliance, and management of third-parties to the District’s cardholder data environment.

Scope

This policy applies to the District employees, third-parties, service providers, contractors, temporary employees, and other staff members at the District, whether conducting activities on District premises or off-site.
This policy applies to all systems, applications, and equipment owned or leased by District whether located on District premises or off-site, and all District locations where cardholder data is present.

**Distribution**

This policy is to be distributed to all those with responsibilities for maintenance and management of security controls and practices at the District, to include District employees, third-parties, service providers, contractors, and temporary employees.

The most current version of this policy is to be readily available and accessible. A digital copy will be stored in the Policy & Procedure folder under the District’s “Public” drive.

**Exceptions**

There are no exceptions to this policy. Requests for exceptions may be submitted to the District’s PCI Review Committee for review and approval on a case by case basis. A single exception does not constitute a permanent change in practice. If a permanent change in practice is required, a revision of the PCI policy will be required.

**Violations**

Individuals found to have violated this policy, whether intentionally or non-intentionally, may be subject to disciplinary action, up to and including termination.

**Review Schedule**

The next scheduled review date is ________________, 2018 by the District’s PCI Review Committee, to be approved by the General Manager.

**Section 6 Detail**

**Assessment of Risk**

Third-parties must be given a risk assessment prior to being connected to the District cardholder data environment. No third-party may be connected to the District environment prior to receiving this assessment. Should a third-party have not received this risk assessment and is currently connected, the risk assessment is to be performed before they may be reconnected. This assessment is to include discovery of threats which may lead to potential vulnerabilities,

Once the review has been performed, the third-party is to close gaps found, and the remaining findings and description of risk are to be reviewed and accepted by the General Manager.
Compliance with the PCI Data Security Standards (PCI DSS) is required for all Level 1 connected third-parties. These entities must have been assessed by an on-site Qualified Security Assessor (QSA), have a Report on Compliance accepted by either their acquiring bank or VISA, and have quarterly passing external scans. Levels 2 - 4 connected third-parties may perform a self-assessment and may be required to have quarterly passing external scans, depending on instruction from their acquiring banks. Should the connected third-party have evidence of their annual PCI compliance passing assessment, they are not required to have a risk assessment performed. Level 1 connected third-parties may provide District with their acceptance letter from their acquiring bank or VISA as well as their Attestation of Compliance (AoC). Levels 2 - 4 may provide their Self Assessment Questionnaire (SAQ) and external scans (if performed).

**Network Diagram**

A network diagram is to be maintained which accurately depicts all connected third-parties, along with networking equipment, systems, applications, wireless networks, and other applicable components of the cardholder data environment.

**List of Third-Parties**

District is to maintain a current list of connected third-parties with details of whether they have direct access to the cardholder environment. This is to clearly denote which third-parties have privileged access and so special attention may be paid to them during session monitoring. The list of third-parties is to also include their PCI compliance status and date of, whether they have accepted by their acquiring bank or VISA or have performed a SAQ (whichever is applicable to their Level as defined above). The list must contain information about which PCI DSS Requirements, if any, are managed by each third-party.

**PCI Compliance Status**

The status of connected third-parties achieving PCI compliance is to be reviewed annually. All third-parties with direct access to the cardholder environment must obtain PCI compliance or have an official exception provided by their acquiring bank or VISA. Should a third-party with privileged access not have obtained this compliance status, they are to document in writing their efforts in doing so with the target completion date. District is to monitor the compliance efforts of these third-parties.

**Terms and Conditions**

All connected third-parties are to sign a Non-Disclosure Agreement (NDA). Contracts with Service Providers are to contain terms and conditions, as well as an agreement to safeguard District’s cardholder data in all its formats from generation to its destruction, and signed by the third-party prior to connection to the District’s network. No third-party may be connected to the District environment prior to signing their agreement with District’s terms and conditions. Should a third-party have not signed their agreement and is currently connected, they are required to do so before they may be reconnected.

Terms and conditions should contain the following, but not limited to, the third-party’s obligation to:
• Protect District’s cardholder data and environment.
• Follow District’s policies and procedures at all times, unless there is specific approval from the General Manager.
• Use only District-approved security controls and practices.
• Communicate any suspected compromise of third-party systems connected to the District’s network.
• Escalate suspected breaches and incidents to the District within 2 hours.
• Retain and dispose of electronic and paper cardholder data media in a secure manner.
• Comply with federal and industry laws and regulations.
• Train individuals with access to the District systems and data on effective safeguard measures.
• Maintain security awareness amongst personnel.
• Conduct criminal background checks on all individuals with access to the District’s network, systems, and data. Background checks are to be performed prior to granting individuals access.
• Removing access permissions immediately upon termination of the individual.
• Maintaining appropriate access control methods, including two-factor remote access.
• Only attempting to connect to the District’s network during authorized periods, and disconnecting when the work is completed.
• Permitting District to perform periodic reviews, and forensic investigations upon District General Maanger determination.
• Physically and logically segregating District systems, networks, and data from those belonging to any other clients.
• Implementing logging and audit trail requirements.
• Permitting District to perform periodic reviews, and forensic investigations upon District General Maanger determination.

Change Management

Any changes made by the third-party in regards to their security controls and practices as well as organizational process changes must be communicated to the District. District is to review the change as to its potential impact on District. This is to help protect against the possibility of inadvertently introducing open avenues for attack. Once the review has been performed, the change documentation and description of any residual risk from the third-party performing the change is to be reviewed and accepted by the General Manager.

The change management process must be used to track changes from their initial request stage through review to documentation of residual risk to approval by the General Manager.

Any system or application changes with impact on District are to be tested by the third-party in a test environment prior to being placed into the production environment.

Event Management and Response

Logs for District systems, applications, and equipment managed by the third-parties are to be generated, reviewed, and maintained to provide an audit trail. Logs are to be synced to a safeguarded central location.
Incidents, whether suspected or actual, are to be reported to the District within 2 hours so they may be responded to in accordance with the Incident Response Plan. Determination of the third-party’s role in incident response and containment should be clearly defined.

**Security Awareness**

Training is to be provided by the third-party at an appropriate level by function. Individuals with access to the District’s cardholder environment are to be provided with more detailed training upon hire and then on an annual basis, with a focus on the protection of District’s cardholder environment and technical training. Other company individuals are to receive general security awareness training upon hire and then annually.

**Background Checks**

Criminal background checks (within the constraints of local laws) are to be performed by the third-party of each individual with access to the District’s cardholder environment. Background checks should be nation-wide in scope, or at the very least, of each state the individual has resided in.

**Access Controls**

Access to the District’s cardholder environment is to be limited to only those individuals with a business need-to-know. Individual authentication, meaning a unique userID and unique password, is to be used.

Remote access may only be performed using a secure network protocol, such as SSH, and users must use two-factor authentication (the user must possess something they have and something they know in addition to their userID).

Password management is to follow the password requirements specified in APP’s 2060-502.7 and 2060-502.8.

**Monitoring and Managing Third-Party Access**

Third-party access may only be permitted with prior authorization through the District’s Multi Level Approval Change Process, and is to be disconnected and disabled immediately after use. If possible, it is preferred that time of use is disabled automatically. Senior IT Staff are to monitor the access at all times. In some cases, access is granted to third-parties on a 24/7/365 basis. These types of access should be approved in accordance with the District’s Multi Level Approval Change Process prior to access being granted, and IT Staff is to periodically monitor the connection without prior notification to the third-party.

The third-party may not attempt to access District’s network without prior authorization at anytime, and doing so may result in the initiation of the incident response plan.

**Testing and Scanning**

The third-party is to agree to periodic security controls and practices review by District, and to
be included in the vulnerability scanning initiatives performed by District and relevant external support services. Additional testing procedures, such as penetration testing and application assessments, may also be performed as needed.

In the instance of a breach to the District’s cardholder environment, District reserves the right to perform forensic activities on the third-party’s environment.

**Segregation**

The third-party is to logically and physically separate District’s systems, network, and data from any other clients (if applicable). There may not be any shared environments without the explicit permission of District.

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-701</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
The PCI Review Committee shall include a minimum of three persons assigned by the following Department Managers:

- Finance
- Administration
- Information Technology.
- Customer Service

More than one member may be appointed by each Department Manager, and may include themselves.

At least one member shall be a qualified person with appropriate financial and accounting skills. In addition, at least one member shall be a qualified person with appropriate information technology security and technical skills.

The PCI Review Board shall meet no less than 4 times per year on the last work day of each quarter.

The Role of the PCI review board is outlined in the six part PCI-DSS APP number 2060-701.

The decisions made by the PCI review board shall be made with the goal of maintaining PCI-DSS compliance and shall, upon acceptance, immediately become part of, and be subject to the requirements of the PCI-DSS APP.
Cyber Security - Employee Awareness Training Program
Administrative Practice and Procedures (APP)
Table of Contents

Introduction ........................................................................................................................................... 3

Cyber Security Employee Awareness Training Program ................................................................. 4

Overview/Purpose ................................................................................................................................. 4

Scope.................................................................................................................................................... 4

Standards and Regulatory Requirements.......................................................................................... 4

ISO/IEC 27001 & 27002 §8.2.2 .............................................................................................................. 4

PCI DSS §12.6 ................................................................................................................................... 5

Health Insurance Portability and Accountability Act (HIPPA) §164.308.(a),(5),(i) ............... 5

Red Flag Rules §16 CFR 681.1(d)-(e) ................................................................................................. 5

RUS Emergency Restoration Plan (ERP) ........................................................................................... 5

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standard. §CIP-004-3(B)(R1) ................................................................. 5

Program ............................................................................................................................................. 6

Related Standards ............................................................................................................................... 9

Definition of Terms Revision History ...............................................................................................9
Introduction

Effective Cyber Security begins with awareness. A comprehensive Cyber Security program focuses on:

- Physical security practices and methods
- Technical security practices and methods
- The human aspects of cyber security

These areas of risk are often exploited by malicious parties to take advantage of the inherent risk represented by humans with inadequate awareness and training.
Cyber Security
Employee Awareness Training Program
Overview/Purpose

Public Utility District No. 1 of Skagit County (the “District”) recognizes the need to protect the District, our customers, employees and data, and systems, from growing cybersecurity threats. This document establishes a formal program for ongoing Employee Awareness Training within the District to ensure employees are adequately trained to recognize, appropriately act upon, and mitigate threats and protect those customer, employee and company resources.

Scope

All full time and temporary employees and other workers at the District and its subsidiaries must receive identified introductory and ongoing Cyber Security Awareness Training. Human Resources will include Cyber Security Awareness Training notification in the new employee orientation process.

Standards and Regulatory Requirements

A formal Cyber Security Training program is required for compliance with many standards, regulatory requirements, and Cyber Security Best Practices. Requirements applicable to the District are listed below, along with NERC CIP and PCI-DSS standards. The District, at this time, is not bound by NERC CIP standards but they are included herein for reference and consideration of use. Other standards and regulations may be developed and/or implemented subsequent to this program acceptance and should be adopted and implemented as necessary.

**ISO/IEC 27001 & 27002 §8.2.2**

All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
PCI DSS §12.6

Make all employees aware of the importance of cardholder information security.

Educate employees (for example, through posters, letters, memos, meetings and promotions).

Require employees to acknowledge in writing that they have read and understood and will comply with the company’s security policy and procedures.

Health Insurance Portability and Accountability Act (HIPPA) §164.308.(a).(5).(i)

Implement a security awareness and training program for all members of its workforce (including management).

Red Flag Rules §16 CFR 681.1(d)-(e)

Employees should be trained about the various red flags to look out for, and/or any other relevant aspect of the organization’s Identity Theft Prevention Program.

RUS Emergency Restoration Plan (ERP)

Note relevant cyber security regulations.

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standard. §CIP-004-3(B)(R1)

The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.)
Program

Roles and Responsibilities

1. **Manager of Information Technology (IT Manager)**

   Ensures that high priority is given to effective security awareness training for all employees. This will include implementation of a viable IT Cyber Security program with a strong awareness and training component. The Manager of Information Technology will:

   - Assign responsibility for IT Security;
   - Ensure that a District wide IT Cyber Security program is implemented, is well-supported by resources and budget, revised on a periodic basis (annually or a different basis) to reflect lessons learned, actual events, and available technology, and is effective;
   - Ensure that the District has enough sufficiently trained personnel to protect its IT resources;
   - Establish the overall strategy for the IT security awareness and training program;
   - Ensure that the Board of Commissioners, General Manager, Managers, system and data owners, and others understand the concepts and strategy of the security awareness and training program, and are informed of the progress of the program’s implementation;
   - Ensure Board of Commissioner meeting minutes reflect the ongoing discussion of cyber security issues;
   - Promote the development and certification of the IT security program staff, full-time- or part-time security officers, and others with significant security responsibilities;
   - Ensure that the District’s IT security awareness and training program is funded and staffed;
   - Ensure that all users are sufficiently trained in their security responsibilities and only have access to the systems and information they need to perform their job;
   - Ensure that effective tracking and reporting mechanisms are in place.

2. **IT Manager**

   Functions in the role of Information Technology Security Manager and has tactical level responsibility for the IT security and awareness training program. The IT Manager will:

   - Ensure that awareness and training material developed and presented is appropriate and timely for the intended audiences;
   - Ensure that awareness and training material is effectively deployed to reach the intended audiences;
   - Ensure that users and managers have an effective way to provide feedback on the awareness and training material and its presentation;
   - Ensure that awareness and training material is reviewed periodically and updated when necessary; and
   - Assist in establishing a tracking and reporting strategy.
3. **Department Managers**

Have responsibility for complying with IT security awareness and training requirements established for their users. Managers will:

- Work with the IT Manager and department staff to meet shared responsibilities;
- Serve in the role of system/data owner, where applicable;
- Consider developing individual development plans (IDP’s) for users in roles with significant security responsibilities;
- Ensure that all users (including contractor’s) of their systems (i.e., general support systems and major applications) are appropriately trained in how to fulfill their security responsibilities before allowing them access;
- Ensure that users (including contractor’s) understand specific rules of each system and application they use; and
- Work to reduce errors and omissions by users due to lack of awareness and/or training.

4. **Users**

Users comprise the largest audience and are the single most important group of people that can help reduce unintentional errors and IT vulnerabilities. Users may include employees, contractors, other agency personnel, visitors, guests, and other collaborators or associates requiring access. Users must:

- Understand and comply with District security policies and procedures;
- Be appropriately trained in the rules of behavior for the systems and applications to which they have access;
- Work with management to meet training needs;
- Be aware of actions they can take to better protect the District’s information. The actions include, but are not limited to: strong password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks and rules to deter spread of spam or viruses and worms.

**Training Needs Assessment**

1. A needs assessment will be conducted to determine the District’s awareness and training needs. As a minimum, the following roles will be involved and addressed to identify any special training needs:

   - **Executive Management** – Identify directives and laws (including data breach) that form the basis of the security program. Ensure comprehension of leadership roles in effecting full compliance by users within their departments;
   - **Identified Security Personnel** – Ensure cooperative staff and individuals who are acting as consultants to the District are well educated on security policy and accepted best practices;
   - **System Owners** – Ensure a broad understanding of security policy and a high degree of
understanding regarding security controls and requirements applicable to the systems they manage;
• System Administrators and IT Support Personnel – Ensure a high degree of technical knowledge in effective security practices and implementation;
• Operational Managers and System Users – Ensure a high degree of security awareness and training on security controls and rules of behavior for systems they use to conduct business operations.

Awareness Training

1. IT security awareness will be used to focus attention on security and should not be confused with Security Training. Various methods will be utilized to promote awareness of security to include, but not be limited to the following methods:
   • Utilization of security awareness posters and banners throughout all District campuses;
   • Targeted email’s with an Awareness message appropriate to the group;
   • All employee emails with an appropriate message to the group;
   • Presentations by IT security managers at employee meetings; and
   • Scheduled online security awareness training.

Security Training

1. All Technical Services staff involved with IT systems will attend security basics and literacy training courses relative to their areas of oversight and level of security responsibility.
2. The District will seek to hire and/or to provide education for IT staff who hold, or to obtain, degrees from accredited universities, or industry recognized certifications in IT Security. Examples of such include but are not limited to:
   • Bachelor’s/Master’s Degree in Information Systems Security
   • Certified Information Systems Security Manager (CCISO)
   • Certified Information Systems Security Professional (CISSP)
   • Certified Ethical Hacker (CEH) Certification
   • Global Information Assurance Certification (GIAC)

New Employee Orientation Training

Newly hired full-time and part-time employees, contractors and consultants, will be provided Cyber Security orientation training to consist of the following:

1. Overview of District employed computing technology.

This should include covering of major aspects of the policies with a signed acknowledgment that the employee has read and understood the District’s security policies and procedures.
Related Standards


Definition of Terms Revision

History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2026-701.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
</tbody>
</table>

General Manager Signature:  Date:
1.0 Purpose
The purpose of the APP is to establish the goals and the vision for the breach response process. This APP will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The APP shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Skagit PUD Information Technology's intentions for publishing a Data Breach Response APP are to focus significant attention on data security and data security breaches and how the District’s established culture of openness, trust and integrity should respond to such activity. District Information Security is committed to protecting the District's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.0 Background
This policy mandates that any individual who suspects that a theft, breach or exposure of District Protected data or District Sensitive data has occurred must immediately provide a description of what occurred via e-mail to Helpdesk@skagitpud.org, or by calling (360) 848-4435. This e-mail address and phone number are monitored by the District’s IT Staff. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

3.0 Scope
This APP applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of District employees and/or customers. Any agreements with vendors will contain similar language to protect District information assets.

4.0 APP Confirmed theft, data breach or exposure of District Protected data or District Sensitive data
As soon as a theft, data breach or exposure containing District Protected data or District Sensitive data is identified, the process of removing all access to that resource will begin.

The General Manager will chair an incident response team to handle the breach or exposure.
The team will include members from:

- IT
- Finance (if applicable)
- Legal
- Communications
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the General Manager

### 5.0 Confirmed theft, breach or exposure of District data

The General Manager will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

#### 5.1 Work with Forensic Investigators

As provided by District cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

#### 5.2 Develop a communication plan.

Work with District communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

### 6.0 Ownership and Responsibilities

#### 6.1 Roles & Responsibilities:

- **Sponsors** are those members of the District community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any District Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

- **Network Systems Administrator** is that member of the District community, designated by the General Manager or the Manager, Information Technology (IT), who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
• **Users** include virtually all members of the District community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.

This is covered in the section above so I don’t think we need to duplicate here

### 7.0 Enforcement

Any District personnel found in violation of this APP may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

### 8.0 Definitions

- **Encryption or encrypted data** – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;
- **Plain text** – Unencrypted data.
- **Hacker** – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).
- **Protected Health Information (PHI)** - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.
- **Personally Identifiable Information (PII)** - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered
- **Protected data** - See PII and PHI
- **Information Resource** - The data and information assets of an organization, department or unit.
- **Safeguards** - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.
- **Sensitive data** - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

### 9.0 Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-702</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
1. Overview
Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities by remediated prior to production deployment.

2. Purpose
The purpose of this policy is to define web application security assessments within the District. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of District services available both internally and externally as well as satisfy compliance with any relevant policies in place.

3. Scope
This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at the District.

All web application security assessments will be performed by delegated security personnel either employed or contracted by the District. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of the District is strictly prohibited unless approved by the General Manager or required as part of a Public Records Request.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

4. Policy
4.1 Web applications are subject to security assessments based on the following criteria:

   a) **New or Major Application Release** – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

   b) **Third Party or Acquired Web Application** – will be subject to full assessment after which it will be bound to policy requirements.

   c) **Point Releases** – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
d) **Patch Releases** – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

e) **Emergency Releases** – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the IT Manager or an appropriate manager who has been delegated this authority.

4.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

a) **High** – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.

b) **Medium** – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

c) **Low** – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

a) **Full** – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.

b) **Quick** – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

c) **Targeted** – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4 The current approved web application security assessment tools in use which will be used for testing are:

- Outside Scanning Agency: Comodo

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.
5. Policy Compliance

5.1 Compliance Measurement
The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the IT Manager.

6. Related Standards, Policies and Processes

- OWASP Top Ten Project
- OWASP Testing Guide
- OWASP Risk Rating Methodology

7. Definitions and Terms
None.
## 8 Revision History

<table>
<thead>
<tr>
<th>Former Title/AP&amp;P #:</th>
<th>2060-803</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>8/26/08</td>
</tr>
<tr>
<td>Revision Date:</td>
<td></td>
</tr>
<tr>
<td>General Manager Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
June 18, 2018

TO: George Sidhu, P.E., General Manager

FROM: Mark Handzlik, P.E., Engineering Manager

BY: Bill Trueman, Engineering Manager

SUBJECT: Property Management Plan for Gilligan Creek Watershed Property

Requested Action:
No requested action at this time. The final property management plan related to the Gilligan Creek Watershed Property Project is attached for informational purposes.

Background:
The District completed the Gilligan Creek Watershed Property acquisition in December 2017. Funding for this purchase has been provided through a loan by Washington State Department of Ecology’s (Ecology) Clean Water State Revolving Fund (CWSRF). This funding source will provide the District with a 20-year loan for 75% of the land acquisition costs. The remaining 25% of the District’s costs will be “forgiven” through an action of the funding source.

The last two deliverables due to Ecology before the District can invoice for this funding source, consist of a property management plan and a deed of right to Ecology recorded on the property. The deed of right and majority of the content for the property management plan were negotiated with Ecology prior to execution of the funding agreement. Final revisions to the property management plan have been made and Ecology has confirmed their approval of the changes. A copy of the final property management plan is attached.

We are working to complete the final steps of the funding agreement, and then will invoice Ecology.

Fiscal Impact:
No changes to the project budget are requested.

kac
EXECUTIVE SUMMARY

This Property Management Plan (plan) is related to property Public Utility District No. 1 of Skagit County (District) purchased in 2017 to protect surface water diversion facilities at Gilligan Creek, a tributary to the Skagit River in Skagit County, Washington. The plan provides a basic framework along with a general description of goals, objectives, and actions to be taken while managing the property. Intensive land use activities such as road construction and timber harvesting are described in greater detail to describe the extent to which these activities are anticipated to be allowed on the property.

The primary purpose of the property will be to continue operations of a surface water diversion facility at Gilligan Creek and to protect water quality by maximizing suitable vegetation and riparian protection from nonpoint sources of pollution.

TABLE OF CONTENTS

1. Property Description ........................................ Page 2
2. Connection to Cultus Mountain Watershed Management Plan ... Page 3
3. Overall Management Goals and Objectives ............... Page 4
4. Vegetation Management ...................................... Page 4
5. Roads .......................................................... Page 5
6. Public Access and Recreation ............................... Page 6
7. Public Education ............................................. Page 6
8. Monitoring ................................................... Page 7
9. Amendments .................................................. Page 7

ATTACHMENTS

Attachment A – Property Map .................................. Attachment C – Property Deed
Attachment B – Property Survey ......................... Attachment D – Access Easements
1. PROPERTY DESCRIPTION

Boundary Description
The property is approximately 250 acres in size and a portion of Section 2, Township 34 North, Range 5 East, W.M.

See Attachment A – Property Map for additional details related to the property.

See Attachment B – Property Survey for the legal boundaries of the property (AFN 201712050031); the subject property is “Parcel A” and is identified by Skagit County as parcel P134099.

History
The property was owned by private industrial forestland owners prior to the District’s purchase from Weyerhaeuser Company in 2017. See Attachment C – Property Deed (AFN 201712200038).

Resources
The property contains merchantable timber and pre-merchantable forest cover.

Gilligan Creek, a Shoreline of the State, crosses through the property. The District possesses water rights for the withdrawal of surface water from Gilligan Creek at a diversion facility on the property. This surface water withdrawal is used as a source of supply for the District’s Judy Reservoir Group A water system (“Judy System”; DOH ID#79500E).

Uses and Values
The property has historically been used as commercial forest land. The existing forest cover and potential for commercial timber production have continued financial value to the owner of the property. The property also has value to the District as a location for a source of supply to the Judy System.

Surrounding Land Uses
Surrounding properties are used as commercial forest land.

Existing Improvements
The District operates a surface water diversion facility on the property at Gilligan Creek. An underground pipeline is routed across the property from the intake to eventually discharge at the District’s Judy Reservoir to the west.

There are numerous existing gravel-surfaced access roads on the property in various levels of maintenance condition. These roads have been historically used to access the District’s surface water diversion facility and pipelines and to facilitate commercial forest management activities.
Risks and Hazards
The property is mountainous and contains some steep slopes and areas of natural slope instability.

Access
Access to the property is obtained through a number of easements granted to the District.
Prior to purchasing the property, the District possessed an easement for the surface water diversion facility at Gilligan Creek and source water pipeline to Judy Reservoir which is located across the property. As a part of the property acquisition, the District was granted additional access easements to the property. See Attachment D – Access Easements for copies of the easements acquired with the property.
The District’s easements to the property do not include public access.

Encumbrances
See Attachment C – Property Deed for a list of recorded encumbrances on the property.
Mineral rights were reserved by Great Northern Railway Company in 1920.
According to the provisions of a funding agreement with Washington State Department of Ecology (Ecology) that was utilized to support purchase of the property, a Deed of Right to Ecology will be recorded on the property. The purpose of the Deed of Right is to record certain aspects of this agreement.

2. CONNECTION TO THE CULTUS MOUNTAIN WATERSHED MANAGEMENT PLAN

District water rights and watershed control
The District holds several water rights at Gilligan Creek for municipal water supply. District water rights are described in detail in the most recent update of the District’s Water System Plan.
Gillian Creek is one of four streams that are discussed in the District’s Cultus Mountain Watershed Management Plan (most recently updated in 2013). This watershed management plan is used by the District to document the watershed control program for the Judy Reservoir Group A water system.

Importance of Gilligan Creek to source water supply
Gillian Creek is a major source of supply to the District’s Judy Reservoir Group A water system.
Critical Areas Designation
The District has designated “Critical Areas” in the Cultus Mountain Watershed Management Plan. These critical areas are locations within the watershed where human or animal activity could degrade water quality at the intake.

The subject property has been designated by the District as a “Level 1 Priority” critical area due to the large volume of water withdrawn from Gilligan creek and the proximity to the intake facility.

3. OVERALL MANAGEMENT GOALS AND OBJECTIVES

Continued operation of surface water diversion facility:
- Intake facility located within the bed and banks of Gilligan Creek
- Buried source water pipeline and appurtenances for the transport of diverted water to Judy Reservoir
- Stream gauging equipment (in-stream gauges, overland conduits, antenna sites)
- Access roads

Protect source water to surface water diversion facility:
- Maximized area of mature forest cover and protected riparian areas within the Gilligan Creek Watershed boundaries to reduce sediment loads from upland sources and buffer from nonpoint sources of pollutants and fluctuations in flows and water temperature.
- Road maintenance (e.g., functional ditches and drainage, proper surfacing, abandonment as determined necessary by the District)

Comply with Department of Ecology Deed of Right:
- Ecology approval of Property Management Plan revisions
- Ecology approval of activities not allowed by the Property Management Plan or Deed of Right

4. VEGETATION MANAGEMENT

Existing conditions:
With the exception of areas cleared for roads or utilities, the property is covered by varying ages of forest following a long history of industrial forest management.

The majority of the property is within the Gilligan Creek Watershed. Minor areas of the property, located in the northwest and northeast corners of the property, are not within the Gilligan Creek Watershed (see attached map).
Management Actions:

- Vegetation will be managed as necessary to support operation of the District’s surface water diversion facilities (e.g., roadside brushing, danger tree removal, clearing for relocated facilities and new roads).

- Areas within and outside (see attached map) the Gilligan Creek Watershed and not affecting the operation of the utility infrastructure will be managed to maximize the area of mature forest cover. In general, this will consist of passive forest management (e.g. allowing for the forest to age and mature naturally).

Depending on funding availability, the District may consider more active management (e.g., forest thinning). “Clear-cut” timber harvesting within the Gilligan Creek Watershed will not be allowed unless site-specific circumstances support this type of action (e.g. forest disease, fire damage). The Property Management Plan will be revised in accordance with section nine (9) of the plan prior to timber harvesting in the Gilligan Creek Watershed. These revisions would describe the proposed timber harvesting activities. Timber harvesting will not be allowed in the Gilligan Creek Watershed except when in accordance with the goals and objectives of the Property Management Plan.

- Removal of vegetation and debris within stream channels will be performed as needed to protect the surface water diversion facilities.

5. ROADS

Existing conditions:

There is an existing gravel road network on the property in varying conditions:

- Roads actively used by the District to access infrastructure; maintained in good condition.
- Forest management roads maintained by the previous landowner prior to acquisition.
- Roads overgrown with vegetation, not accessible by vehicle, and likely require maintenance or abandonment.

Management Actions:

- The District will continue to maintain roads currently used to access infrastructure and facilitate use of the surface water diversion facility. Other existing roads on the property will be maintained to provide continued vehicular access throughout the property for condition assessment, forest fire protection, and other administrative needs. This maintenance may include clearing vegetation from overgrown roads to allow for vehicular access.

- Depending on specific conditions, some existing roads on the property may be inactivated or abandoned in the future following adequate assessment by the District.
• Depending on easement and title exceptions, some roads may be maintained or used by easement holders.
• New roads may be required in the future to facilitate use of the surface water diversion facility (e.g., relocation of facilities, re-routing around slope instability)
• New roads may be required in the future to facilitate management of the acquired property (e.g., fire protection, forest management)
• Areas outside of the Gilligan Creek Watershed would be managed according to existing federal, state, and local rules and regulations. For example, new forest roads may be necessary for timber harvesting.

6. PUBLIC ACCESS AND RECREATION

Existing conditions:
There is no existing public vehicular access to the property. The District’s easements to the property do not include public access. Drivable roads that access the property are gated and motorized access is restricted to authorized personnel.
Non-motorized recreation (e.g., hiking) is allowed by neighboring landowners, and one neighboring landowner has a fee access program that allows motorized recreation by permit. Two existing roads that access the property from the east are within the fee access program area, but these roads are currently overgrown with vegetation and are not accessible by vehicle. Areas in close proximity to the surface water diversion facilities are currently restricted from public entry by the District.

Management Actions:
Public recreation on the acquired property may be allowed by the District in the future. Public access in close proximity to tributary streams and the surface water diversion facilities would be restricted based on the District’s assessment of threats to water quality.
The District will continue to coordinate with neighboring landowners to maintain restrictions to public motorized access on roads that access the property.
If the District chooses to open the two access routes from the east that are within the neighboring fee access program, the District would install gates at the property boundary to restrict unapproved vehicle entry.

7. PUBLIC EDUCATION

Management Actions:
The District may incorporate the acquired property into public outreach and educational activities (e.g., tours for schools).
8. MONITORING

Management Actions:
The District conducts regular turbidity testing at the surface water diversion facility in Gilligan Creek. A stream gauging station is also in operation at the diversion site which collects regular stream level data for flows downstream of the point of diversion. Diverted flows to Judy Reservoir are metered. Currently there are no plans for additional testing or monitoring on the property.

9. AMENDMENTS

Process
This Property Management Plan will be revised as necessary to address changing conditions, regulation, or scientific research. Revisions will be subject to approval by Washington State Department of Ecology in accordance with the future Deed of Right, which shall not be unreasonably withheld.

Review/update schedule
This property management plan will be reassessed in conjunction with updates to the Cultus Mountain Watershed Management Plan, or sooner if warranted by specific circumstances.
ATTACHMENT A
PROPERTY MAP
This map was created from available public records and existing map sources, not from field surveys. While great care was taken in this process, maps from different sources rarely agree as to the precise location of geographic features. The relative positioning of map features to one another results from combining different map sources without field verification.

The PUD #1 of Skagit County disclaims any warranty of merchantability or warranty of fitness of this map for any particular purpose, either expressed or implied. No representation or warranty is made concerning the accuracy, currency, completeness or quality of data depicted on this map. Any user of this map assumes all responsibility for use thereof, and further agrees to hold the PUD #1 of Skagit County harmless from any damage, loss, or liability arising from the use of this map.
Agenda Item #10

ATTACHMENT B
PROPERTY SURVEY
ATTACHMENT C
PROPERTY DEED
FOR VALUABLE CONSIDERATION, receipt of which is hereby acknowledged, WEYERHAEUSER COMPANY, a Washington corporation, successor by merger to Weyerhaeuser Columbia Timberlands LLC, which was successor by merger to Longview Timberlands, LLC, hereby conveys and warrants to PUBLIC UTILITY DISTRICT NO. 1 OF SKAGIT COUNTY, a Washington public utility district, the real property located in the County of Skagit, State of Washington, more particularly described in Exhibit No. 1, attached hereto.

SUBJECT TO: Only the permitted exceptions set forth in Exhibit No. 2 attached hereto.

TO HAVE AND TO HOLD the same unto the said Grantee and unto its successors and assigns forever, with all appurtenances thereunto belonging.

Grantor covenants with Grantee that it will forever warrant and defend said title to said lands against all lawful claims and encumbrances done or suffered by it, but against none other.
DATED: December 5, 2017

GRANTOR:

WEYERHAEUSER COMPANY, a Washington corporation

By

Name James R. Johnston
Title Vice President

ACKNOWLEDGMENT

STATE OF WASHINGTON )
COUNTY OF KING ) ss.

On this 5th day of December, 2017 before me, the undersigned, a Notary Public in and for the State of Washington, duly commissioned and sworn, personally appeared James R. Johnston, the Vice President of Weyerhaeuser Company, the Washington corporation that executed the foregoing instrument, and acknowledged the said instrument to be the free and voluntary act and deed of said corporation, for the uses and purposes therein mentioned, and on oath stated that he is authorized to execute the said instrument.

Witness my hand and official seal hereto affixed the say and year first above written.

Printed Name: Paul A. Hill
Notary Public in and for the State of Washington
Residing at Seattle
My Commission Expires: 10/29/2018
EXHIBIT No. 1

TO DEED

LEGAL DESCRIPTION

PARCEL A

A portion of Section 2, Township 34 North, Range 5 East, W.M., being more particularly described as follows:

BEGINNING at a point on the west line of the northwest quarter of said Section 2, said point being South 01° 23' 43" West 647.28 feet from the northwest corner thereof;
thence South 89° 01' 12" East along a line lying south 650 feet and parallel with the south line of Section 35, Township 35 North, Range 5 East, W.M., for a distance of 3714.00 feet;
thence South 01° 05' 14" West 2198.58 feet;
thence South 01° 41' 24" West for a distance of 604.05 feet;
thence South 58° 25' 14" West 1317.64 feet to the southeast corner of the northeast quarter of the southwest quarter of said Section 2;
thence North 88° 18' 20" West along the south line of said northeast quarter for a distance of 1314.17 feet to the southwest corner thereof;
thence North 01° 40' 10" East along the west line of said northeast quarter for a distance of 1332.87 feet to the northwest corner thereof;
thence North 88° 09' 56" West along the south line of the northwest quarter of said Section 2 for a distance of 1309.49 feet to the southwest corner thereof;
thence North 01° 23' 43" East along the west line of said northwest quarter for a distance of 2143.08 feet to the POINT OF BEGINNING.

Situate in the County of Skagit, State of Washington,
EXHIBIT No. 2

TO DEED

PERMITTED EXCEPTIONS

SUBJECT TO:

(i) liens for taxes, assessments and other governmental charges which are not yet due and payable as of the recordation of this deed;

(ii) all land use (including environmental and wetlands), building and zoning laws, regulations, codes and ordinances affecting the Property;

(iii) any rights of the United States of America, the State in which the Property is located or others in the use and continuous flow of any brooks, streams or other natural water courses or water bodies within, crossing or abutting the Property, including, without limitation, riparian rights and navigational servitudes;

(iv) title to that portion of the Property, if any, lying below the mean high water mark of abutting navigable rivers;

(v) all easements, rights-of-way, water rights, licenses and other such similar encumbrances apparent or of record;

(vi) all existing public and private roads and streets and all railroad and utility lines, pipelines, service lines and facilities;

(vii) all encroachments, overlaps, boundary line disputes, shortages in area, persons in possession, cemeteries and burial grounds and other matters not of record which would be disclosed by an accurate survey or inspection of the Property;

(viii) prior reservations or conveyances of mineral rights or mineral leases of every kind and character;

(ix) any loss or claim due to lack of access to any portion of the Property; and further
SCHEDULE "B-1"

EXCEPTIONS:

A. RESERVATIONS CONTAINED IN DEED:

Executed By: Great Northern Railway Company
Recorded: October 13, 1920
Auditor's No.: 145258
As Follows:

"Reserving all iron, ore, coal and other minerals together with the right to explore for, mine and remove the same"

A purported partial assignment of said mineral reservations, affecting a portion of the subject property, was made by document recorded as Auditor's File No. 200907240052.

B. AN EASEMENT AFFECTING THE PORTION OF SAID PREMISES AND FOR THE PURPOSES STATED HEREIN AND INCIDENTAL PURPOSES.

For: Pipe line or conduits, etc.
In Favor of: Clear Lake Water Corporation
Recorded: July 9, 1940
Auditor's File No. 327300

Said easement was assigned to Public Utility District No. 1 by document dated November 14, 1940, recorded November 16, 1940, under Auditor's File No. 332004.

C. RESERVATIONS CONTAINED IN DEED:

Executed By: Atlas Lumber & Shingle Company
Recorded: April 6, 1912
Auditor's No.: 90743
As Follows:

Excepting and reserving therefrom the rights to build, construct and locate and maintain on, over and across said Lot 3 of Section 2, a water flume, water pipe, reservoir, for use in connection with the water works plant, it being understood however, that no standing timber shall be cut, destroyed or removed in the work of the building, maintaining or repairing of said pipe, flume or reservoir, and in case any timber is so cut, destroyed or removed, the parties so cutting, destroying or removing such timber, shall pay to the grantee herein, a reasonable value therefore and license is hereby reserved to go upon said land for the purpose of building, constructing and locating said pipe, flume and reservoir at any time.
D. AN EASEMENT AFFECTING THE PORTION OF SAID PREMISES AND FOR THE PURPOSES STATED HEREIN AND INCIDENTAL PURPOSES.

For: 
Pipe line

In Favor of: 
Skagit Improvement Company

Auditor’s File No. 
92148

Affects: 
A portion of the subject property.

E. RESERVATIONS CONTAINED IN DEED:

Executed By: 
John Hancock Mutual Life Insurance Company

Recorded: 
November 7, 1994

Auditor’s No.: 
9411070066

As Follows:

EXCEPTING and reserving in Grantor hereof, its successors and assigns, a permanent, assignable, non-exclusive access easement for the purposes of construction, reconstruction, use by pedestrian and vehicular traffic, including but not limited to specialized logging equipment, logging trucks or other equipment used for growing, harvesting, or managing timber, and maintenance of roads for forestland and natural resource management, 60 feet in width, unless indicated otherwise, over and across existing roadways delineated on the maps annexed hereto as hereinafter identified and referenced and made a part hereof.

F. AN EASEMENT AFFECTING THE PORTION OF SAID PREMISES AND FOR THE PURPOSES STATED HEREIN AND INCIDENTAL PURPOSES.

For: 
A perpetual nonexclusive easement

In Favor of: 
Weyerhaeuser

Recorded: 
August 15, 1986

Auditor’s File No. 
8608150015

G. AGREEMENT, AND THE TERMS AND PROVISIONS THEREOF:

Between: 
Longview Fibre Company

And: 
The Washington Dept. of Natural Resources

Recorded: 
January 30, 2004

Auditor’s No.: 
200401300177

Regarding: 
Road easement exchange

Affects: 
An Easterly portion of the subject property

H. AGREEMENT, AND THE TERMS AND PROVISIONS THEREOF:

Between: 
PUD #1 of Skagit County

And: 
Georgia-Pacific Corporation

Recorded: 
November 18, 1969

Auditor’s No.: 
733103

Regarding: 
Watershed Agreement

Guardian Northwest Title and Escrow, Agent for
First American Title Insurance Company
I. EASEMENT, INCLUDING TERMS AND PROVISIONS THEREOF:

Grantee: Grandy Lake Forest Associates Limited Partnership
Recorded: July 27, 1988
Auditor's No.: 8807270016
Purpose: Road for hauling forest products and related uses
Area Affected: A portion of Road B

J. EASEMENT AND PROVISIONS CONTAINED THEREIN AS CREATED OR DISCLOSED INSTRUMENT:

In Favor Of: Puget Sound Power & Light Company
Recorded: March 18, 1936
Auditor's No.: 277225
For: Electric transmission lines and related purposes

K. EASEMENT, INCLUDING TERMS AND PROVISIONS THEREOF:

Grantee: Skagit Improvement Company
Recorded: July 12, 1912
Auditor's No.: 92148
Purpose: Pipeline and related purposes


N. ANY AND ALL OFFERS OF DEDICATIONS, CONDITIONS, RESTRICTIONS, EASEMENTS, FENCE LINE/Boundary DISCREPANCIES, NOTES, PROVISIONS AND/OR ANY OTHER MATTERS AS DISCLOSED AND/OR Delineated ON THE FACE OF THE FOLLOWING PLAT/SHORT PLAT/SURVEY:

Name: Survey
Recorded: April 20, 2017
Auditor's No.: 201704200048
Shows: Line between East ¼ corner and Southeast corner of Section 35, Township 35 North, Range 5 East, W.M.

O. DECLARATION OF EASEMENT, INCLUDING THE TERMS AND PROVISIONS THEREOF:

Recorded: April 24, 1989
Auditor's No.: 8904240007
Purpose: Roads as set forth therein
Area Affected: Portions of Road B

Guardian Northwest Title and Escrow, Agent for
First American Title Insurance Company
P. EASEMENT, INCLUDING TERMS AND PROVISIONS THEREOF:

Grantee: Georgia-Pacific Corporation
Recorded: November 13, 1985
Auditor's No.: 8511130019
Purpose: Roads as set forth therein

Q. EASEMENT, INCLUDING TERMS AND PROVISIONS THEREOF:

Grantee: State of Washington
Recorded: April 5, 1993
Auditor's No.: 9304050156
Purpose: Roads as set forth therein
Area Affected: Road established by Auditor's File No. 9311170093

R. EASEMENT, INCLUDING TERMS AND PROVISIONS THEREOF:

Grantee: John Hancock Mutual Life Insurance Co.
Recorded: November 17, 1993
Auditor's No.: 9311170093
Purpose: Roads as set forth therein

S. EASEMENT, INCLUDING TERMS AND PROVISIONS THEREOF:

Grantee: John Hancock Mutual Life Insurance Co.
Recorded: October 28, 1994
Auditor's No.: 9410280040
Purpose: Roads as set forth therein

T. EASEMENT, INCLUDING TERMS AND PROVISIONS THEREOF:

Grantee: Longview Fibre Co.
Recorded: February 5, 1998
Auditor's No.: 9802050035
Purpose: Roads as set forth therein
U. EASEMENT AND PROVISIONS CONTAINED THEREIN AS CREATED OR DISCLOSED INSTRUMENT:

In Favor Of: Dan Hinds, et ux
Recorded: January 5, 1996
Auditor's No.: 9601050070
For: Ingress, egress and utilities
Affects: Road established by Auditor's File No. 9802050035

V. EASEMENT, INCLUDING TERMS AND PROVISIONS THEREOF:

Grantee: Puget Sound Power & Light Co.
Recorded: November 13, 1989
Auditor's No. 8911130053
Purpose: Electric transmission and/or distribution system and related purposes
Area Affected: Road established by Auditor's File No. 9802050035

W. Question of the exact locations and widths of the Easement roads established by Auditor's File Nos. 9311170093, 9410280040, 9802050035 and 8511130019.
ATTACHMENT D
ACCESS EASEMENTS
June 21, 2018

TO: Commission

FROM: George Sidhu, P.E., General Manager

SUBJECT: Skagit Water Supply Task Force – Recommendation of Representative

Requested Action:
Recommend that the Commission ratify the selection of Tom Mortimer as the District’s representative on the Skagit Water Supply Task Force.

Background:
During the 2018 session, the Legislature passed ESSB 6095 (supplemental capital budget) creating a Joint Legislative Task Force on Water Supply in Skagit County to review surface water and groundwater needs and uses as they relate to agricultural uses, domestic potable water uses, and instream flows, and to develop and recommend studies.

The Task Force will focus on Water Resource Inventory Area (WRIA) 3 and 4 and will include members from the House of Representatives and the Senate, as well as other state agencies. In addition, the Task Force will include representatives from many local agencies, organizations and Indian tribes that will be appointed by the Legislative members serving on the Task Force. Skagit PUD has been asked to recommend a representative to serve on the Task Force by Friday June 22.

I have recommended that the District’s representative on the Water Supply Task Force be Tom Mortimer, Attorney at Law. Mr. Mortimer is an attorney licensed in Washington State with 29 years of experience in water resource management, water right permitting, watershed planning, securing new water rights, municipal water right legislation and many other items. He has worked in Whatcom, Skagit and Snohomish County for over 25 years and has been utilized by the District for different water related issues. I think Mr. Mortimer would be a good choice as our representative on the Water Supply Task Force as he understands the issues in Skagit County and can also provide a regional and state wide perspective during the discussions.

Fiscal Impact:
The Skagit Water Supply Task Force was not planned or budgeted for in the 2018 Budget. Mr. Mortimer’s time will be funded from the Professional Services Budget, which currently is at 42% of the annual budget after the first quarter ($65,377 spent out of $157,186 budgeted). Attempts will be made to have the Task Force reimburse the District for these costs, but if that is unsuccessful a budget amendment may be necessary.

kac
June 18, 2018

George Sidhu, P.E., General Manager
Skagit Public Utility District
P.O. Box 1436
Mount Vernon, WA 98273

Dear Mr. Sidhu:

During the 2018 session, the Legislature passed ESSB 6095 (supplemental capital budget), creating a Joint Legislative Task Force on Water Supply (Task Force) "to review surface water and groundwater needs and uses as they relate to agricultural uses, domestic potable water uses, and instream flows, and to develop and recommend studies."

The Task Force must consist of four members each from the House of Representatives and the Senate, as well as agency representatives from the Department of Ecology, the Department of Fish and Wildlife, and the Department of Agriculture.

Additionally, the Task Force must also include the following members, appointed by consensus of the co-chairs of the Task Force:

- Two representatives from organizations representing the farming industry in Washington;
- One representative designated by each county within Water Resource Inventory Areas (WRIAs) 3 and 4;
- One representative designated by each city within WRIAs 3 and 4;
- Two representatives from an environmental advocacy organization or organizations;
- One representative designated by each public utility district in WRIAs 3 and 4;
- One representative from an organization representing business interests; and
- Representatives from federally recognized Indian tribes with reservations and treaty fishing rights located within WRIAs 3 and 4.

Pursuant to ESSB 6095, we are writing to respectfully request that Skagit PUD submit a recommendation for a representative to serve on the Task Force.
The Legislative members of the Task Force are planning the first meeting of the Task Force, during which co-chairs will be elected. The first meeting of the Task Force will take place at 10:00 a.m. on Monday, June 25, at Skagit Valley College in Mount Vernon. Once the first meeting occurs and co-chairs are elected, the co-chairs will appoint representatives from the organizations, jurisdictions, and tribes listed above. Once additional Task Force members have been appointed, the first meeting of the full Task Force will be scheduled in due course.

Pursuant to ESSB 6095, the Task Force must immediately focus on WRIA 4, and may not meet regarding WRIA 3 before January 1, 2019. Studies and selection of scientists or organizations to implement these studies must be based on the recommendations of the Task Force and must be made by a seventy-five percent majority of the members of the Task Force. The 2018 supplemental capital budget includes $2 million for studies identified by the Task Force.

The Legislative members would like to have recommendations from the organizations for recommended representatives to the Task Force prior to the first meeting, so that the co-chairs will have the recommendations and can appoint representatives from organizations in a timely fashion. We respectfully request that you submit your recommendations by Friday, June 22 to Karen Epps, Senate Committee Services staff (karen.epps@leg.wa.gov) and Rob Hatfield, House of Representatives Office of Program Research staff (robert.hatfield@leg.wa.gov).

Thank you for your interest in the Joint Legislative Task Force on Water Supply.

Kind regards,

Representative Vincent Buys
Representative Kristine Lytton
Representative Strom Peterson
Senator Keith Wagoner

Senator Marko Liias
Senator John McCoy
Representative David Taylor
Senator Judy Warnick
June 22, 2018

TO: George Sidhu, P.E. – General Manager
FROM: Mark Handzlik, P.E. - Engineering Manager
BY: Mike Benton, Project Manager

SUBJECT: Recommendation to Execute Agreement/Bill of Sale with Cascade Natural Gas (CNG)

Requested Action:
Authorize the General Manager to execute the attached agreement between the District and Cascade Natural Gas turning over ownership of an abandoned steel gas main to the District for reuse as an internal fiber optic communication conduit.

Background:
Through the District’s ongoing agency coordination efforts, staff learned of the plan by CNG to construct a new transmission line in close proximity to the District’s 12 inch ductile water line on East Jones Road in Sedro-Woolley. This new gas line’s cathodic protection would likely corrode the District’s waterline.

Rather than paying the District for the relocation, CNG has offered to give the District ownership of one of its retired gas lines along the BNSF right of way from the intersection of Magnolia and Spruce Street, Burlington, to North Hill Blvd (see attached map).

Through this agreement, the District is agreeing to relocate 419 LF of existing water main along East Jones Road in Sedro-Woolley that is in conflict with a planned high pressure gas main. The waterline relocation cost is estimated at $99,860.00. The calculated value of the existing in place conduit to the District is $143,879.68 resulting in a net benefit to the District of $44,049.68.

Fiscal Impact:
Funding for the East Jones Road Pipeline Relocation project was designated to come from budget Line Item 60, Mandated by Other Agencies.

kac
AGREEMENT AND BILL OF SALE

This AGREEMENT AND BILL OF SALE (this “Agreement”) dated as of May 17, 2018 (the “Closing Date”), is made by and between Cascade Natural Gas Corporation, a Washington corporation, with offices at 8113 West Grandridge Boulevard, Kennewick, WA 99336 (“Seller”), and Skagit Public Utility District, with offices at 1415 Freeway Dr., Mt Vernon, WA 98273 (“Buyer”) (Seller and Buyer may be referred to herein, individually, as a “Party” or, collectively, as the “Parties”).

RECITALS

WHEREAS, Buyer has offered to purchase all of Seller’s right, title, and interest in and to the 3” high pressure main pipe more particularly described on Exhibit A attached hereto (hereinafter the “Assets”); and

WHEREAS, Seller has agreed to sell and convey to the Buyer all of Seller’s right, title and interest in and to the Assets; and

WHEREAS, Buyer has agreed to relocate the Sedro Woolley 12” water main described in Exhibit B in exchange for transfer of the Assets.

AGREEMENT

NOW, THEREFORE, in consideration of the foregoing premises and for other good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, the Parties hereto hereby agree as follows:

1. Conveyance. Subject to the terms and conditions of this Bill of Sale, the Seller does hereby sell and convey to the Buyer all of the Seller’s right, title and interest in and to the Assets. The conveyance to Buyer of the Assets is on an AS-IS WHERE-IS basis, with all faults and defects, with no representations or warranties of any kind or nature, whether statutory, written, oral, express or implied (including warranties of fitness for a particular purpose or merchantability). Conveyance includes all rights and responsibilities under any existing franchise agreements or easements with other parties, whether implied or explicit. Buyer hereby accepts the Assets.

2. Taxes and Fees. Buyer shall be responsible for any applicable sales taxes or other fees under applicable state or local law associated with the sale and transfer of the Assets.

3. Incorporation of Recitals/Exhibit. The recitals set forth above and Exhibit A are each incorporated into this Agreement by this reference.

4. No Third Party Beneficiaries. Nothing contained in this Agreement, expressed or implied, is intended or shall be construed to confer upon or give to any third party, whether a governmental authority, private entity or person, other than the Parties and their successors or assigns, any rights or remedies under or by reason of this Agreement.
5. **Successors and Assigns.** Except as restricted herein, this Agreement shall be binding upon and shall inure to the benefit of Seller and Buyer and their respective successors and assigns.

6. **Counterparts/Signatures.** This Agreement may be executed in one or more counterparts, each of which will be deemed an original.

7. **Governing Law.** This Agreement shall be governed by, construed, enforced and performed according to the laws of the State of Washington without regard to principles of conflicts of law.

8. **Amendment.** This Agreement may not be amended, modified, or waived except by written instrument executed by officers or duly authorized representatives of the Parties.

9. **Severability.** The invalidity or unenforceability of any portion or provision of this Agreement shall in no way affect the validity or enforceability of any other portion or provision hereof. Any invalid or unenforceable portion or provision will be deemed severed from this Agreement and the balance of this Agreement will be construed and enforced as if this Agreement did not contain such invalid or unenforceable portion or provision.

10. **Headings.** The headings of the Sections and subsections of this Agreement are for convenience only and shall not be used in the interpretation of this Agreement.

11. **Authority.** Each Party represents to the other that it has the power and authority to execute and deliver this Agreement and to perform its respective obligations under this Agreement and that the person or persons signing for each Party have been duly authorized by such Party to do so.

12. **Entire Agreement.** This Agreement constitutes the entire agreement and understanding of the Parties with respect to its subject matter and supersedes all oral communication and prior writings with respect thereto.

(Signature Page Follows)
Agenda Item #12

IN WITNESS WHEREOF, Seller and Buyer have executed this Agreement to be effective as of the Closing Date.

SELLER:

Cascade Natural Gas Corporation

By: ___________________________
Name: Eric Martuscelli
Title: V.P. - Operations

STATE OF WASHINGTON )
COUNTY OF Benton ) ss.

Subscribed and sworn to before me on May 24th, 2018.

(seal)

BUYER:

Skagit Public Utility District

By: ___________________________
Name: George Sidhu, P.E
Title: General Manager
EXHIBIT A – 3” High Pressure Main Pipe

[See attached map]

EXHIBIT B – E. Jones Rd., Sedro Woolley, WA - 12” Water Main

[See attached pdf drawing]
June 22, 2018

TO: George Sidhu, P.E., General Manager
FROM: Mark Handzlik, P.E., Engineering Manager
BY: Mike Benton, Project Manager

SUBJECT: Change Order No. 1 - Razz Construction
Skagit River Diversion Pump and Motor Refurbishment Project

Requested Action:
Authorize the General Manager to execute Change Order No. 1 with RAZZ Construction in the amount of $170,767.32 including sales tax, for the recommended pump repairs and upgrades to the District’s Skagit River Diversion (SRD) and authorize the use of up to $220,000 of System Development Funds to augment budget Line Item 20 SRD Pump Rebuilds.

Background:
At the beginning of the 2017 pumping season, only one of the five SRD pumps (P-105) was functioning properly which does not meet the District’s supply requirements. In April 2017 bids were received for pump and motor assessment, and in June 2017 three of the pumps (P-101, P-102, & P-104) were removed.

At the December 12, 2017 regular meeting of the Commission Razz Construction was awarded a multi-year contract in the amount of $473,277.00 to refurbish all five pumps. Three of the pumps were to be completed in 2018 and the remaining two pumps were to be completed in 2019.

Through value engineering and an aim to meet the objective of complete refurbishment of the SRD pumps, additional work outside the original scope of the project was identified. This work includes replacement of three pump shafts that cannot be repaired at a cost that is less than the replacing the shafts, complete refurbishment of the pump bowls and suction bells, adding steady bushings, and adding an improved mechanical (potable water) shaft seal system.

These additional improvements will have significant impact on the longevity of the pumps in the following ways:
- The seal water system start pressures have been reduced from 280 psi to 220 psi.
- The pump start pressure has been reduced from 260 psi to 200 psi.
- The mechanical seal will prevent silty river water from coming in contact with the shaft bearings.
- Through repair of the pump bowls now a second removal of the pump shafts and bowls will not be required to conduct the work separately in future years. This efficiency will save costs in future years.

The original schedule provided for three of the pumps to be installed and operational for the 2018 pumping term. The lead-time on these materials has delayed that schedule to the end of the 2018 pumping term. If all work planned for 2018 and 2019 is conducted before the end of the year all five
Agenda Item #13

Memo re: Change Order No. 1-Razz Construction
Skagit River Diversion Pump and Motor Refurbishment
June 22, 2018
Page 2

Pumps will be operational for the 2019 pumping term. This would bring the project back on schedule and would be most efficient from an operational standpoint. Therefore, an additional $220,000 is being sought from System Development Funds to complete the entire project, including contingency, this year. The requested $250,000 in 2019 will not be requested for the completion of this project. Overall the project will be delivered at a cost that is below the proposed budgeted amount which is shown below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Including WSST</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018 Budget</td>
<td>$550,000.00</td>
</tr>
<tr>
<td>2019 Budget (planned)</td>
<td>$250,000.00</td>
</tr>
<tr>
<td><strong>Total Project Budget</strong></td>
<td><strong>$800,000.00</strong></td>
</tr>
<tr>
<td>RAZZ Contract (2018 &amp; 2019)</td>
<td>$473,277.00</td>
</tr>
<tr>
<td>Change Order No. 1 including WSST</td>
<td>$170,767.33</td>
</tr>
<tr>
<td><strong>Subtotal</strong></td>
<td><strong>$644,044.33</strong></td>
</tr>
<tr>
<td>Other Contracts</td>
<td></td>
</tr>
<tr>
<td>RH2 – Seal Water Design</td>
<td>$25,000.00</td>
</tr>
<tr>
<td>QCC – SCADA Design and Programming</td>
<td>$33,247.50</td>
</tr>
<tr>
<td><strong>Design Subtotal</strong></td>
<td><strong>$58,247.50</strong></td>
</tr>
<tr>
<td>District Labor (estimated)</td>
<td>$20,000.00</td>
</tr>
<tr>
<td><strong>Total Project Cost Estimate</strong></td>
<td><strong>$722,291.83</strong></td>
</tr>
<tr>
<td>Remaining Budget</td>
<td>77,708.17</td>
</tr>
</tbody>
</table>

Sales Tax Included in all above figures

**Fiscal Impact:**
Funding for this contract and project will come from the project budget Line Item 20 – SRD Pump Rebuilds. The original project budget was approved for $550,000 in fiscal year 2018. An additional $250,000 in funding was planned for fiscal year 2019. Through the approval of this change order and budget augmentation with System Development Funds the project will be completed this year and no additional funding will be requested in 2019. The work is consistent with the intended use of the requested funding.

kac
Project Name: SKAGIT RIVER DIVERSION PUMP STATION PUMP AND MOTOR REFURBISHMENT PROJECT

Contractor: RAZZ CONSTRUCTION, INC.  
Address: 1415 Freeway Drive  
           PO Box 1436  
           Mount Vernon, WA 98273

Attention: Don Rassmussen – Owner/Project Manager  
Address: 4055 Hammer Dr.  
           Bellingham, Washington 98226

| Original Contract Amount – Schedule A – FY 2018 | $250,700.00 | Days | 104 |
| Original Contract Amount – Schedule B – FY 2019 | $185,500.00 | Days | 104 |
| Previously Approved Changes | $0.00 | Days | 0 |
| This Change Order | $157,389.24 | Days | 191 |
| Subtotal | $593,589.24 | Days |
| Sales Tax 8.5% | $50,455.08 | Days |
| New Contract Amount (incl. Tax): | $644,044.32 | Days | 295 |

Original Substantial Completion Date: April 15, 2018

New Substantial Completion Date: October 31, 2018

This Change Order covers the contract modification hereunder described. All other terms and conditions remain unchanged.

<table>
<thead>
<tr>
<th>Description of Changes</th>
<th>Increase in Bid Item Amount ($)</th>
<th>(Decrease) in Bid Item Amount ($)</th>
<th>Contract Time Change (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCO 001 – Repair Damaged Line Shafts – Schedule A pumps</td>
<td>43,355.76</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCO 002 – Seal Water Flushing System Additions – All 5 Pumps</td>
<td>17,415.41</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCO 003 – Add Steady Bushings to Pump Motors – 5 EA</td>
<td>15,744.29</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCO 005 – Damaged Bowl Replacement – 2 refurbished + 1 new</td>
<td>95,873.78</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCO 006 – Credit to Refurbish Schedule B pumps in place</td>
<td></td>
<td>$15,000.00</td>
<td>15,000.00</td>
</tr>
<tr>
<td>Delay to complete Seal Water System Design &amp; SCADA Integration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Contractor to schedule and coordinate work to ensure the pumps and motors identified in schedule A are tested and functional on or before October 31, 2018. Pumps are not allowed to be started or tested between October 31 and April 1st due to PUD/Puget Sound Energy Agreement provisions.</td>
<td></td>
<td></td>
<td>191</td>
</tr>
<tr>
<td>General Contractor to coordinate with all parties to provide an updated overall project schedule with each monthly pay request.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Totals: (w/o Tax) | $172,389.24 | $15,000.00 | 191 |

Total This Change w/o Tax | $157,389.24 |
Agenda Item #13

With this Change Order, the Contract Amount shall be increased or decreased by the sum of $157,389.24 plus WSST and the Contract Time shall be extended by 191 Calendar days.

It is understood and agreed that the acceptance of this Change Order by the Contractor constitutes an accord and satisfaction and represents payment in full both as to time and money for all costs arising out of, or incidental to, the above described change to the Contract including any and all delay and impact resulting from this change in Work.

<table>
<thead>
<tr>
<th>RAZZ CONSTRUCTION, INC.:</th>
<th>PUD No. 1 OF SKAGIT COUNTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>By:</td>
<td>By: George Sidhu, P.E.</td>
</tr>
<tr>
<td>Title:</td>
<td>Title: General Manager</td>
</tr>
<tr>
<td>Date:</td>
<td>Date:</td>
</tr>
<tr>
<td>Signature</td>
<td>Signature</td>
</tr>
</tbody>
</table>

SKAGIT RIVER DIVERSION PUMP STATION PUMP AND MOTOR REFURBISHMENT PROJECT

6/21/18
Agenda Item #13

2018 BUDGET REQUEST FORM

(PLEASE ATTACH SUPPORTING DOCUMENTATION FOR AMOUNT REQUESTED)

ITEM/PROJECT NAME: SRD Pump Replacements

Brief Description of Item: Routine Capital Maintenance of SRD Pumps, Motors, & Control

Is this a carryover? □ Yes □ No

REQUESTING DEPARTMENT (Check the appropriate department box):

□ Administration
□ Comm Relations
□ Operations
□ Engineering
□ HR
□ Cust Svc
□ WTP
□ Assets
□ Finance
□ Mtr Dept
□ Const
□ Information Tech

Requestor's Name: Mark Handzlik Date: 7/9/2017

Requested Amount (Please include any shipping and sales tax): $ 900,000

Purpose / Benefits (What will this do for the District?): The District's pumps at the Skagit River Diversion require significant maintenance to be operational. Over the course of 3 years, beginning in 2017, this project will result in the complete refurbishment of all 5 SRD pumps, motors, and control valves.

Why is this purchase needed now? What will happen if we defer it to another year? The SRD has zero operational redundancy and failure to replace the pumps before summer of 2018 will likely cause the District to rely on the stream diversions or Anacortes for supply of water to District customers.

Please rate the importance of this Item/Project (Circle the appropriate number)

1 Absolutely critical
2 Really need it
3 Really want it; it will make life easier
4 It would be nice, but don't absolutely need it
5 If there is money to spare

Is this a multi-year project?: □ Yes □ No

If yes, how many years is the project spread over?: 3

What percentage of the project is to be completed each year?:

1st Year $ 45,000 (2017)
2nd Year $550,000 (2018)
3rd Year $250,000 (2019)

4th Year
5th Year
6th Year

General Manager: ___________________________ Date Reviewed: ____________

Comments: _____________________________

□ Approved $ ___________ □ Postpone

For Use by Auditor
General Ledger Code: _____________________________
Tracking number: _____________________________
## 2018 Capital Budget Requests - Attachment A

<table>
<thead>
<tr>
<th>DEPT DESCRIPTION</th>
<th>REQUESTED AMOUNT</th>
<th>2018 Revised Proposed</th>
<th>Funding Source</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Carry over from 2017 (includes carry over)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>REQUESTS FROM CONSTRUCTION DEPARTMENT</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Const Variable Message Sign Boards</td>
<td>$33,000</td>
<td>$ -</td>
<td>-</td>
<td>This item will not be funded.</td>
</tr>
<tr>
<td>2 Const Paving Machine</td>
<td>$130,000</td>
<td>$ -</td>
<td>-</td>
<td>This item will not be funded.</td>
</tr>
<tr>
<td><strong>Ops</strong> Architect Services for Building</td>
<td>$250,000</td>
<td>$250,000</td>
<td>Revenue</td>
<td>An allowance for Architect Services for services related to a new building.</td>
</tr>
<tr>
<td><strong>Ops</strong> Mountain View Treatment Systems and Generator</td>
<td>$30,000</td>
<td>$30,000</td>
<td>Revenue</td>
<td>Needs motor, rewiring, treatment system and generator.</td>
</tr>
<tr>
<td><strong>Ops</strong> Mailroom Conversion</td>
<td>$25,000</td>
<td>$25,000</td>
<td>Revenue</td>
<td>With the District's billing and mailing being conducted off site, the space is available for other purposes. Recognizing an increasing need for office space this item will repurpose the mailroom for engineering construction contract management personnel.</td>
</tr>
<tr>
<td><strong>Ops</strong> Ram 3500 - 1 Ton Service Truck for Construction - Flat Bed</td>
<td>$38,000</td>
<td>$38,000</td>
<td>Revenue</td>
<td>Scheduled Fleet Replacement.</td>
</tr>
<tr>
<td><strong>Ops</strong> Base Station and Radios</td>
<td>$15,000</td>
<td>$15,000</td>
<td>Revenue</td>
<td>Current truck radio system is decades old, past useful life</td>
</tr>
<tr>
<td><strong>Ops</strong> F150 1/2 Ton Pickup for Distribution</td>
<td>$43,000</td>
<td>$43,000</td>
<td>Revenue</td>
<td>Scheduled Fleet Replacement.</td>
</tr>
<tr>
<td><strong>Ops</strong> Meter Department Truck Replacement</td>
<td>$37,000</td>
<td>$29,000</td>
<td>Revenue</td>
<td>Scheduled Fleet Replacement.</td>
</tr>
<tr>
<td><strong>10-a</strong> Ops Meter Department Truck Replacement</td>
<td>$37,000</td>
<td>$29,000</td>
<td>Revenue</td>
<td>Scheduled Fleet Replacement.</td>
</tr>
<tr>
<td><strong>10-b</strong> Ops F150 Construction Manager Truck Replacement</td>
<td>$29,075</td>
<td>$36,000</td>
<td>Revenue</td>
<td>Scheduled Fleet Replacement.</td>
</tr>
<tr>
<td><strong>10-c</strong> Ops Taurus Ram 150 Truck Replacement</td>
<td>$29,075</td>
<td>$36,000</td>
<td>Revenue</td>
<td>Scheduled Fleet Replacement.</td>
</tr>
<tr>
<td><strong>10-d</strong> Ops F150 Construction Foreman Replacement</td>
<td>$29,075</td>
<td>$36,000</td>
<td>Revenue</td>
<td>Scheduled Fleet Replacement.</td>
</tr>
<tr>
<td><strong>10-e</strong> Ops F150 Locator Truck Replacement</td>
<td>$29,075</td>
<td>$36,000</td>
<td>Revenue</td>
<td>Scheduled Fleet Replacement.</td>
</tr>
<tr>
<td><strong>11</strong> Ops Vector Truck</td>
<td>$480,000</td>
<td>$534,000</td>
<td>Revenue</td>
<td>Replacement of current Vector truck</td>
</tr>
<tr>
<td><strong>REQUESTS FROM OPERATIONS DEPARTMENT</strong></td>
<td>$1,075,400.00</td>
<td>$1,129,000.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 WTP Water Purification System for Lab</td>
<td>$7,500</td>
<td>$7,500</td>
<td>Revenue</td>
<td>The ability to make deionized pure water for lab testing. Current purification system was installed when the WTP was built and had to be repaired numerous times. This year the amount of lab tests have tripled, which has increased the need of DI water.</td>
</tr>
<tr>
<td>13 WTP Ammonia Monochloramine analyzer</td>
<td>$26,000</td>
<td>$26,000</td>
<td>Revenue</td>
<td>Necessary for PO4 trigger monitoring.</td>
</tr>
<tr>
<td>14 WTP SRD arsenic ASCO replacement</td>
<td>$7,500</td>
<td>$7,500</td>
<td>Revenue</td>
<td></td>
</tr>
<tr>
<td>15 WTP Streaming Current Monitor</td>
<td>$14,000</td>
<td>$14,000</td>
<td>Revenue</td>
<td>Cogulation monitor, current one is failing</td>
</tr>
<tr>
<td>16 WTP Reversal walkway</td>
<td>$7,500</td>
<td>$7,500</td>
<td>Revenue</td>
<td>Safety concern walking on large rocks to current walkway.</td>
</tr>
<tr>
<td>17 WTP Gutters</td>
<td>$16,500</td>
<td>$16,500</td>
<td>Revenue</td>
<td>Past their useful life, damaged, leaking on ground and then freezing in winter. Safety concern.</td>
</tr>
<tr>
<td>18 WTP HVAC System for control room and electrical room</td>
<td>$25,000</td>
<td>$25,000</td>
<td>Revenue</td>
<td>Climate control for Superintendent office and control room at WTP.</td>
</tr>
<tr>
<td>19 WTP Operations Manual Update</td>
<td>$50,000</td>
<td>$165,000</td>
<td>$165,000</td>
<td>Revenue</td>
</tr>
<tr>
<td><strong>20</strong> WTP SRD Pump Rebuilds</td>
<td>$100,000</td>
<td>$550,000</td>
<td>$550,000</td>
<td>Revenue</td>
</tr>
</tbody>
</table>

**REQUESTS FROM WATER TREATMENT PLANT** $19,000.00 $811,500.00