

AGENDA
SHAKOPEE PUBLIC UTILITIES COMMISSION
REGULAR MEETING
August 4, 2025
at 5:00 PM

1. **Call to Order** at 5:00pm in the SPU Service Center, 255 Sarazin Street
 - 1a) Roll Call
2. **Communications**
3. **Consent Agenda**
 - C=> 3a) Approval of July 7, 2025 Minutes (GD)
 - C=> 3b) Approval of August 4, 2025 Agenda (JK)
 - C=> 3c) August 4, 2025 Warrant List (KW)
 - C=> 3d) Monthly Water Dashboard for June 2025 (BC)
 - C=> 3e) MMPA July 2025 Meeting update (GD)
 - C=> 3f) Res #2025-21 Resolution approving of the Estimated Cost of Pipe Oversizing on the Watermain Project: Elliana Estates (JA)
 - C=> 3g) Res# 2025-22 Resolution setting the amount of the Trunk Water Charge, Approving of its Collection and Authorizing Water Service to Certain Property Described as: Elliana Estates (JA)
 - C=> 3h) June Financial Reports (KW)
 - C=> 3i) Amend Purchasing Policy (KW)
 - C=> 3j) Tower No. 3 (BC)
 - C=> 3k) IT Information Security Policy (PD)

***** Motion to approve the Consent Agenda**

4. **Public Comment Period.** Please step up to the table and state your name and address for the record.
5. **Liaison Report** (JD)
6. **Reports: Operations Items**
 - 6a) Operations Report – Verbal (BC)
 - 6b) Nitrate Testing and Operations Policy (RH)

***** Motion to approve the Nitrate Testing and Operations Policy and the temporary Nitrate Testing and Operations Policy (Well 23 Only), both dated 8/4/25*****

7. **Reports: General**

7a) Marketing/Key Accounts Report – Verbal (SW)

7b) Crisis Communication Plan (SW)

***** Motion to approve the Crisis Communications Plan *****

7c) General Manager Report – Verbal (GD)

7d) NES WTP Site Search Update: Shakopee Hawkins potential site plans (GD) **

** A portion of this meeting may be closed under Minnesota Statutes, Section 13D.05, subdivision 3(c) to review confidential or protected nonpublic appraisal data and to develop or consider offers or counter offers for the purchase of property at 1776 Mystic Lake Drive S **

8. **Items for Future Agendas**

9. **Tentative Dates for Upcoming Meetings**

- September 2, 2025 (Tuesday) - Changed
- October 6, 2025
- October 20, 2025 Workshop

10. **Adjournment**

MINUTES OF THE
SHAKOPEE PUBLIC UTILITIES COMMISSION
July 7, 2025
Regular Meeting

1. Call to Order. President Letourneau called the July 7, 2025 meeting of the Shakopee Public Utilities Commission to order at 5:00 P.M. President Letourneau, Vice President Mocol, Commissioner DuLaney, Commissioner Fox, and Commissioner Krieg were present.
2. Consent Agenda. Vice President Mocol moved to approve the consent agenda:
 - 3a. Approval of June 2, 2025 Minutes;
 - 3b. Approval of July 7, 2025 Agenda;
 - 3c. July 7, 2025 Warrant List;
 - 3d. Annual Elections for the 2025-2026 Insurance Policy;
 - 3e. Monthly Water Dashboard for May 2025;
 - 3f. 2025 Flushing Program Progress Map;
 - 3g. Nitrate Results;
 - 3h. MMPA May 2025 Meeting Update;
 - 3i. Res #2025-17 Resolution Approving of the Estimated Cost of Pipe Oversizing on the Watermain Project: Highview Park 5th Addition;
 - 3j. Res #2025-18 Resolution Setting the Amount of the Trunk Water Charge, Approving of its Collection and Authorizing Water Services to Certain Property Described as: Highview Park 5th Addition;
 - 3k. Tank 9 Utilities Facilities Easement Agreement;
 - 3l. Res #2025-19 Resolution Approving of the Estimated Cost of Pipe Oversizing on the Watermain Project: Bluff View – Phase 1;
 - 3m. Res #2025-20 Resolution Setting the Amount of the Trunk Water Charge, Approving of its Collection and Authorizing Water Services to Certain Property described as: Bluff View – Phase 1; and
 - 3n. Phased Retirement for Sheri Bergeland.Commissioner DuLaney seconded the motion. Ayes: Letourneau, Mocol, DuLaney, Fox, and Krieg. Nays: None.
3. Public Comment Period. No public comments were offered.
4. Liaison Report. Commissioner DuLaney noted that the MMUA legislative update was very informative. He also reported that the City issued a stop work order involving Black Rock/AT&T due to hitting SPU underground facilities. Greg Drent, General Manager, thanked City staff for the assistance in protecting facilities.
5. Water Report. Brad Carlson, Director of Field Operations, reported that Pumphouse #23 is resolving punch list items. He noted that staff are going door to door to complete AMI meter changeouts. Mr. Carlson reported that SPU has completed painting approximately 100 hydrants. The Riverview booster station generator is hooked up. Mr. Carlson reported that SPU has

completed the lead and copper testing for 2025; with the new well, SPU will be required to test again in 2026. He also reported that SPU completed the Minnesota Department of Health sanitary testing, which is required every 18 months.

6. Electric Report. Mr. Carlson provided an update on projects, including replacing all the electric in the Bonnevista Terrace manufactured home park; installing a 3-phase transformer on LaTour Drive for the new tank and pumphouse; continued sampling of oil in all switchgear; completed High Stakes and Prairie Point Apartments; underground installed at the CDA; replacing hydrants at Stagecoach Trail; and replacing rejected poles from the pole inspections. Mr. Carlson reported that fourteen outages occurred in the last month, three from fiber contractor hits; one failed transformer due to the heat, with approximately 100 customers out for two hours; and one primary fault at the Canterbury distribution system.

7. Marketing/Key Account Report. Sharon Walsh, Director of Key Accounts/Marketing, provided an update on the water tower painting, which should be completed by early August. SPU's website will provide updates. Ms. Walsh reported that SPU will promote paperless billing at the Rhythm on the Rails and will attend the Summer Carnival on August 1st. On the conservation front, Ms. Walsh will provide energy-saving information at Bonnevista. For AMI, she reported that 482 total water and electric meters remain to be replaced; 177 are located in Bonnevista. Ms. Walsh noted that two weeks ago, SPU staff began door knocking to arrange AMI meter replacements; a written notice was left if no one answered. Ms. Walsh suggested providing a second, final notice, noting disconnection within the week for failure to replace meters. Mr. Drent emphasized that SPU does not want to disconnect service, and that all customers not in compliance have already received three \$100 penalties, in addition to multiple written notices.

8. Director and General Manager Reports. Mr. Drent provided a finance update on behalf of Ms. Willemssen. Philip Dubbe, Director of IT & Technical Services, reported that an email security breach, which originated outside of SPU, was promptly identified and contained within about one hour. Joseph Adams, Director of Planning & Engineering, provided an update of the major water and electric projects in the capital improvement plan for 2025, along with budget impacts. Mr. Drent provided an update on pending projects, including SPU's assistance in drilling at Miracle Field, a revised draft regarding the Hawkins site purchase, Well #23 water quality and pumping levels, drafting the crisis communication policy, and individual meetings with staff. Mr. Drent attended the APPA national conference and noted pending issues of direct pay, as well as FEMA funding, which affects mutual aid. On the state level, Mr. Drent explained recent legislation, which requires public electric vehicle chargers, for which users pay, to issue a fee to the state. This legislation does not affect SPU because it currently does not charge for the use of its EV chargers.

9. Adjourn. Motion by Commissioner Fox, seconded by Commissioner Krieg, to adjourn. Ayes: Letourneau, Mocol, DuLaney, Fox and Krieg. Nays: None.

Greg Drent, Commission Secretary

AGENDA
SHAKOPEE PUBLIC UTILITIES COMMISSION
REGULAR MEETING
August 4, 2025
at 5:00 PM

1. **Call to Order** at 5:00pm in the SPU Service Center, 255 Sarazin Street
 - 1a) Roll Call
2. **Communications**
3. **Consent Agenda**
 - C=> 3a) Approval of July 7, 2025 Minutes (GD)
 - C=> 3b) Approval of August 4, 2025 Agenda (JK)
 - C=> 3c) August 4, 2025 Warrant List (KW)
 - C=> 3d) Monthly Water Dashboard for June 2025 (BC)
 - C=> 3e) MMPA July 2025 Meeting update (GD)
 - C=> 3f) Res #2025-21 Resolution approving of the Estimated Cost of Pipe Oversizing on the Watermain Project: Elliana Estates (JA)
 - C=> 3g) Res# 2025-22 Resolution setting the amount of the Trunk Water Charge, Approving of its Collection and Authorizing Water Service to Certain Property Described as: Elliana Estates (JA)
 - C=> 3h) June Financial Reports (KW)
 - C=> 3i) Amend Purchasing Policy (KW)
 - C=> 3j) Tower No. 3 (BC)
 - C=> 3k) IT Information Security Policy (PD)

***** Motion to approve the Consent Agenda**

4. **Public Comment Period.** Please step up to the table and state your name and address for the record.
5. **Liaison Report** (JD)
6. **Reports: Operations Items**
 - 6a) Operations Report – Verbal (BC)
 - 6b) Nitrate Testing and Operations Policy (RH)

***** Motion to approve the Nitrate Testing and Operations Policy and the temporary Nitrate Testing and Operations Policy (Well 23 Only), both dated 8/4/25*****

7. **Reports: General**

7a) Marketing/Key Accounts Report – Verbal (SW)

7b) Crisis Communication Plan (SW)

***** Motion to approve the Crisis Communications Plan *****

7c) General Manager Report – Verbal (GD)

7d) NES WTP Site Search Update: Shakopee Hawkins potential site plans (GD) **

** A portion of this meeting may be closed under Minnesota Statutes, Section 13D.05, subdivision 3(c) to review confidential or protected nonpublic appraisal data and to develop or consider offers or counter offers for the purchase of property at 1776 Mystic Lake Drive S **

8. **Items for Future Agendas**

9. **Tentative Dates for Upcoming Meetings**

- September 2, 2025 (Tuesday) - Changed
- October 6, 2025
- October 20, 2025 Workshop

10. **Adjournment**

SHAKOPEE PUBLIC UTILITIES COMMISSION

WARRANT LISTING

August 4, 2025

By direction of the Shakopee Public Utilities Commission, the Secretary does hereby authorize the following warrants drawn upon the Treasury of Shakopee Public Utilities Commission:

WEEK OF 7/03/2025

AAR BUILDING SERVICE CO.	\$4,468.51 JULY CLEANING SERVICE
ARAMARK REFRESHMENT SERVICES INC	\$223.38 COFFEE BREAKROOM
B & B TRANSFORMER INC	\$7,969.00 RETANK TRANSFORMER
BERGERSON-CASWELL INC	\$1,025.00 SVC CALL BAL OF MOTORS VALL CRK BOOSTER
BORDER STATES ELECTRIC SUPPLY	\$106,445.80 500W WATER PIT MODULE
KATHERINE BRASTAD	\$175.00 ENERGY STAR CLOTHES WASHER REBATE
DAWN BZOSKIE-COLEMAN	\$175.00 ENERGY STAR CLOTHES WASHER REBATE
CITY OF SHAKOPEE	\$219,280.00 WO#2581 TANK #9
CITY OF SHAKOPEE	\$354,000.00 WO#2844 E SHAKO SUB
CITY OF SHAKOPEE	\$71,197.51 WO#2683 BLDC-027027-2025
CITY OF SHAKOPEE	\$16,328.00 WO#2844 PERMIT FEE
CORE & MAIN LP	\$1,053.80 WO #2984 6" WITH 2"/3" FEMALE NPT
DAILY PRINTING, INC.	\$11,180.00 ANNUAL RPT/YR IN REVIEW
SHAHEEN DAWOOD	\$500.00 ENERGY STAR COOLING/HEATING REBATE
DSI/LSI	\$562.11 JULY GARBAGE SERVICE
CATHY DUSSIK	\$500.00 ENERGY STAR COOLING/HEATING REBATE
EMERGENCY AUTOMOTIVE TECHNOLOGIES	\$642.67 WO 2972 WESTIN PUBLIC SAFETY HDX DROP NE
FERGUSON US HOLDINGS, INC.	\$9,167.04 FLG X FIP BRZ MTR
G & L TANK SANDBLASTING & COATINGS LLC	\$425,212.87 WO2769 TANK#3 - PYMT #3
GRAINGER INC	\$94.15 BUCKET HOOK(E)
INT'L UNION OF OPER ENGINEERS LOCAL 49	\$816.00 JUNE UNION HOURS WORKED
IRBY - STUART C IRBY CO	\$1,420.80 SAFETY HARD HATS(E&W)
PONTERIO JOHN	\$105.00 BACKFLOW INSPECTION REFUND
JORDAN KIVEL	\$25.00 REBATE - TRIMMER
LANO EQUIPMENT INC	\$1,925.74 BOBCAT REPAIR
LOFFLER COMPANIES - 131511	\$1,511.54 LOCKOUT LETTER FOR WATER DEPT.
SARA MARAS	\$175.00 ENERGY STAR CLOTHES WASHER REBATE
MINN VALLEY TESTING LABS INC	\$365.90 WATER TESTING COLIFORM
NCPERS GROUP LIFE INS.	\$176.00 JUNE PREMIUMS
NOTT COMPANY	\$166.39 WO#2899 COUPLERS
JON OLSON	\$500.00 ENERGY STAR COOLING/HEATING REBATE
AMY RAMNARACE	\$73.86 IRRIGATION CONTROLLERS REBATE
RESCO	\$1,078.05 SWITCH IN-LINE DISCONNECT 38KV 600A
JAKE RISHEL	\$152.99 IRRIGATION CONTROLLERS REBATE
ERIK SCHAEFER	\$50.00 REBATE - PUSHMOWER
MARK TESKE	\$500.00 ENERGY STAR COOLING/HEATING REBATE
EDWARD THOMPSON	\$200.00 IRRIGATION CONTROLLERS REBATE
VIVID IMAGE, INC.	\$650.00 ESSENTIAL+PLAN 7/1-7/30 2025
WESCO RECEIVABLES CORP.	\$4,390.21 HEX UTILITY
WSB & ASSOCIATES INC.	\$50,746.50 WO#2581 PROF SVCS FEB 2025
XCEL ENERGY	\$2,621.55 5/22-6/2 VALLEY PARK ACT 51-5636204-8
CENTERPOINT ENERGY - ACH	\$899.66 10TH AVE GAS USAGE 5/6-6/6 2025
VERIZON WIRELESS SERVICES LLC	\$396.89 MONTHLYPEPWAVE POTSOLVE 5/6-6/5 2025
MINNESOTA LIFE	\$1,062.90 JUNE PREMIUMS FOR LIFE INS.
HEALTHPARTNERS	\$74,223.87 JULY PREMIUMS, JUNE CHARGE MONTH
DELTA DENTAL PLAN OF MN	\$5,750.69 DELTA DENTAL JUNE PREMIUMS
PRINCIPAL LIFE INS. COMPANY	\$5,180.18 JUNE LTD AND STD PREMIUMS

Total Week of 07/03/2025

\$1,385,364.56

WEEK OF 07/11/2025**CREDIT REFUNDS**

ABDO LLP
 ALTEC INDUSTRIES INC
 AMARIL UNIFORM COMPANY
 APPLE FORD OF SHAKOPEE
 BIRD'S LAWN CARE LLC
 BORDER STATES ELECTRIC SUPPLY
 MICHAEL BRUGIONI
 CHOICE ELECTRIC INC
 CITY OF PRIOR LAKE
 CITY OF SHAKOPEE
 CITY OF SHAKOPEE
 CITY OF SHAKOPEE
 CORVAL CONSTRUCTORS, INC.
 DAILY PRINTING, INC.
 DARYL EIDEN
 EMERGENCY AUTOMOTIVE TECHNOLOGIES
 FARWEST LINE SPECIALTIES LLC
 FASTENAL IND & CONST SUPPLIES
 FLYTE HCM LLC
 FRONTIER ENERGY, INC.
 GOPHER STATE ONE-CALL
 GRAINGER INC
 GRAYBAR ELECTRIC COMPANY INC
 HUY HA
 HAWKINS INC
 STACI HEICHERT
 CATHY HENDRICKSON
 HENRICKSEN PSG
 MARIAH HUMMEL
 IDEAL SERVICE
 INNOVATIVE OFFICE SOLUTIONS
 IRBY - STUART C IRBY CO
 JT SERVICES
 DIPESH KARKI
 LOCATORS & SUPPLIES INC
 LOFFLER COMPANIES - 131511
 MATHESON TRI-GAS INC
 MINN VALLEY TESTING LABS INC
 MN OCCUPATIONAL HEALTH - LOCKBOX 135054
 NAPA AUTO PARTS
 GERRY NEVILLE
 NISC
 NOVAK COMPANIES, LLC
 ORACLE AMERICA INC.
 DYLAN PASS
 PIONEER INDUSTRIES, INC.
 PRIORITY 1 SPRINKLERS LLC
 RESCO
 RW BECK GROUP, INC, LEIDOS ENG. LL
 SHORT ELLIOTT HENDRICKSON INC
 SPENCER FANE LLP
 JOE THEIS
 TOM KRAEMER, INC
 JOHN TRUTNAU
 SATHISH VANKAYALA
 SCOTT WEBER
 WESCO RECEIVABLES CORP.
 XCEL ENERGY
 AMERICAN NATL BANK_MASTERCARD_ACH
 FIRST DATA CORPORATION
 HEALTH EQUITY INC.
 HEALTH EQUITY INC.
 HEALTH EQUITY INC.
 MMPA C/O AVANT ENERGY
 MN DEPT OF REVENUE ACH PAYMENTS
 VERIZON WIRELESS SERVICES LLC
 PAYROLL DIRECT DEPOSIT 07.11.25
 BENEFITS & TAXES FOR 07.11.25

\$123,879.76 CREDIT REFUNDS

1,550.00 JUNE 2025 FS ACCOUNTING SERVICES
 1,416.18 HOT STICKS
 55.00 SPU UNIFORM ORDER T.BREZINA
 109.90 WATER DEPT TRUCK#651 OIL CHG
 4,082.03 LAWN CARE JUNE
 378,406.36 9S-36S ITRON METERS Z150511
 20.00 REBATE - LEAFBLOWER
 4,350.00 WO 2984 INSTALLATION OF VFD AT PH 4
 705.15 2ND QTR 2025
 547,799.30 JUNE SW \$418,637.58 & SD \$129,161.72
 351,483.00 JUNE PILOT TRANSFER FEE
 1,080.04 JUNE STORM DRAINAGE/SPU PROPERTIES
 587.00 HVAC REPAIR
 93.64 BUSINESS CARDS NORMA SWANSON
 500.00 ENERGY STAR COOLING/HEATING REBATE
 446.29 LIGHTBAR AMBER LED
 178.30 TEFLON DRILL BIT
 134.78 3/8-16x1 NYL HCS FHN WASHER(E)
 10.00 JUNE COBRA
 9,172.95 JUNE 2025 C&I IMPLEMENTATION
 1,351.35 JUNE TICKETS
 622.76 MARKING FLAG BLK/RED
 55.01 PIPE 2" PVC SWEEP ELBOW 45 DEGREES
 175.00 ENERGY STAR CLOTHES WASHER REBATE
 12,362.04 HYDROFLUOSILICIC ACID/CHLORINE
 25.00 REBATE - CHAINSAW
 152.10 IRRIGATION CONTROLLERS REBATE
 4,059.49 WO2981 STANDING DESK FOR TONY M
 62.44 REIMB MILEAGE 4/1/25-7/7/25 89.20 MILES
 7,162.61 INSTALL POWER SUPPLY WELL#17
 527.82 OFFICE SUPPLIES
 285.00 ALFO AF2346-1/2 BOLT,
 8,772.96 PIPE 1 1/4" INNERDUCT
 25.00 REBATE - TRIMMER
 2,635.80 RED FLAG-BLACK PRINT
 1,430.75 OVERAGE PERIOD 4/1/25-6/30/25
 10.17 ACETYLENE-LG/MED
 136.80 WATER TESTING COLIFORM
 39.00 DRUG TESTING WATER DEPT INV497131
 104.02 BELTS FOR A/C UNIT
 161.70 REIMB 116 MILES 6/20-6/26 2025
 11,829.98 JUNE PRINT SERVICES
 247.15 WO2978 ALUM KEY RACK FOR TRUCK(W)
 41,724.34 2ND QTR 2025 OPOWER CLOUD SERVICE
 500.00 ENERGY STAR COOLING/HEATING REBATE
 585.00 DOCUMENT SHREDDING SERVICE
 424.95 SERVICE CALLS
 2,740.12 ELBOW ARRESTER/CONNECTOR
 36,111.50 JUNE SPU ARC FLASH/COORD STUDIES
 414.88 WO SEH WELLHEAD PROTECTION PLAN PART 1
 7,464.00 JUNE LEGAL SERVICES
 25.00 REBATE - CHAINSAW
 346.80 WO#2769 TANK SITE3-75/25 AMI GL923
 75.00 ENERGY STAR REFRIGERATOR REBATE
 24.99 LED LIGHT BULB REBATE
 500.00 ENERGY STAR COOLING/HEATING REBATE
 22,758.45 BOLTS 5/8 X 12
 27.53 5/26-6/25 AMBERGLEN ACT 51-0012640573-3
 26,670.83 JUNE CC STMT
 11,309.89 JUNE CC FEES
 350.19 FLEX MEDICAL CLAIM REIMB D.H.
 107.00 MEDICAL FLEX CLAIM REIMB J/ADAMS
 192.00 DAYCARE FLEX CLAIM RIMB. C.S.
 4,539,996.86 JUNE POWER BILL
 341,796.00 JUNE SALES & USE TAX PAYABLE
 4,436.27 JUNE CELL PHONE BILL 5/24-6/23
 \$142,410.80
 \$146,586.67

Total Week of 07/11/2025**\$6,805,872.70**

WEEK OF 07/18/2025

BART ABBAN
APPLE FORD OF SHAKOPEE
B & B TRANSFORMER INC
BARNA GUZY & STEFFEN LTD
BORDER STATES ELECTRIC SUPPLY
CALIAN CORP.
CITY OF SHAKOPEE
CONFERENCE TECHNOLOGIES, INC.
ANGELICA CONTRERAS
CORE & MAIN LP
CORVAL CONSTRUCTORS, INC.
RISHIKESH DATHA ALGOLE
DITCHWITCH OF MINNESOTA
FASTENAL IND & CONST SUPPLIES
FERGUSON US HOLDINGS, INC.
GRAINGER INC
HAWKINS INC
JOHN HURKMAN
INNOVATIVE OFFICE SOLUTIONS
IRBY - STUART C IRBY CO
KENNETH KEWATT
DAI LE
LLOYD'S CONSTRUCTION SERVICES
LOCATORS & SUPPLIES INC
KATHERINE MILLER
MINN VALLEY TESTING LABS INC
NISC
NORTHERN STATES POWER CO
CATHY ODENTHAL
OFFICE OF MNIT SERVICES
OLSEN CHAIN & CABLE, INC.
PLUNKETT'S PEST CONT, INC.
DARCY POUTI
POWERPLAN BF
BRUCE REBER
RESCO
SCOTT COUNTY TREASURER
SHORT ELLIOTT HENDRICKSON INC
STAR ENERGY SERVICES
STINSON LLP
ULINE, INC.
UNLIMITED SUPPLIES INC.
VERIZON
WESCO RECEIVABLES CORP.
WINSTON COMPANY
LAUREN REITTER
GERRY NEVILLE
HEALTH EQUITY INC.
HEALTH EQUITY INC.
HEALTH EQUITY INC.

\$50.00 PUSHMOWER REBATE
\$1,174.41 REPLACE BLOWER FAN TRK611(E)
\$3,000.00 VFI-9 SWITCHGEAR REPAIR RP
\$4,240.00 WO#2844 E SUBSTATION PROPERTY 77283-001
\$351,326.29 600A SWITCHGEAR/RVAC11
\$1,049.07 BROADBAND SYSMANTEC RENEWAL 2025
\$6,272.19 JUNE FUEL BILL
\$769.48 SERVICE LABOR TRUCK TOOLS IMATS
\$75.00 ENERGY STAR REFRIGERATOR REBATE
\$174.42 4X2 TAPT BLIND FLG(W)
\$2,225.00 HVAC VALVE REPLACEMENT
\$95.00 PUSHMOWER REBATE
\$346.48 LEVER VALVE(E)
\$105.69 DRILL BIT(E)
\$207.12 RITE HITE ADPT SLIP TYP(W)
\$136.06 PINTLE HOOK(E)
\$360.00 CHLORINE CYLINDERS DEMURRAGE
\$200.00 IRRIGATION CONTROLLERS REBATE
\$373.06 OFFICE SUPPLIES
\$1,680.70 GLOVE TESTING
\$50.00 PUSHMOWER REBATE
\$50.00 ENERGY STAR DISHWASHER REBATE
\$513.50 DEMO & CONSTR RENTAL PD 5.30.25-7.01.25
\$1,502.30 RED MARKING PAINT(E)
\$500.00 ENERGY STAR COOLING/HEATING REBATE
\$365.90 WATER TESTING NITRATES
\$34,168.48 MAY PRINT SERVICES
\$3,385.82 JUNE POWER BILL
\$500.00 ENERGY STAR COOLING/HEATING REBATE
\$734.01 JUNE (WAN) MONTHLY SERVICE
\$735.33 3/8" X 7' QOO SLING G100
\$147.75 GENERAL PEST CONTROL P.H.15&16
\$25.00 TRIMMER REBATE
\$708.25 REPAIR ON BACKHOE
\$200.00 IRRIGATION CONTROLLERS REBATE
\$820.00 GUARD ARRESTER MULTIPORT
\$2,100.00 JULY 2025 MONTHLY FIBER CHG
\$5,081.35 WO#2581 PH23 NITRATE MODELING
\$800.00 NOVA PORTAL BLOCK 2 APPLICATIONS(#51-75)
\$870.00 JUNE LABOR MATTER FILE#3522418.0002
\$229.89 HEAVY DUTY HANDWRAPPER(E)
\$1,440.68 LOCK WASHERS/HEX BOLT
\$621.49 JUNE TRUCK TRACKING
\$1,957.18 UNDERGROUND PULLING GRIP
\$174.57 PROKNIT WIPES(E)
\$40.00 INACTIVE REFUND
196.70 REIMBURSE 281 MILES
\$1,950.00 MEDICAL FLEX CLAIM REIMB C.S.
\$714.00 DAYCARE FLEX CLAIM REIMB R.H.
\$219.50 JUNE ADM. FEE

Total Week of 07/18/2025

\$434,661.67

WEEK OF 07/25/2025

ALL ELEMENTS INC.
ALTEC INDUSTRIES INC
AMAZON.COM SALES INC.
CHRIS ANDERSON
ARAMARK REFRESHMENT SERVICES INC
ANDREW BETHEL
BORDER STATES ELECTRIC SUPPLY
TY BOWLING
AARON BOYCE
DONALD BRANDEL
NATE BRAUNHUT
COMCAST CABLE COMM INC.
CUSTOMER CONTACT SERVICES
FASTENAL IND & CONST SUPPLIES
FERGUSON US HOLDINGS, INC.
GRAINGER INC
CLOID GREEN
HENNEN'S AUTO SERVICE INC.
HIGH POINT NETWORKS, LLC
INNOVATIVE OFFICE SOLUTIONS
IRBY - STUART C IRBY CO
RONALD JACOBSON
JOHNSON CONTROLS FIRE PROTECTION LP
JT SERVICES
KWIK TRIP INC & SUBSIDIARIES
DAI LE
LEAGUE OF MINN CITIES INS TRUST
PAT LINDER
LOCATORS & SUPPLIES INC
LOFFLER COMPANIES - 131511
MID AMERICA METER INC
MINN VALLEY TESTING LABS INC
MINNESOTA SECURITY CONSORTIUM
MMUA
RYAN MOEN
MP NEXLEVEL LLC
NAGEL COMPANIES LLC
OLD 169 LLC
ESTELLE OPHEIM
JOE SUEL
TECH PRODUCTS, INC
LAI ONG TEO
USABUEBOOK
MIKE WASSMUND
WATERLY LLC
WESCO RECEIVABLES CORP.
WSB & ASSOCIATES INC.
HEALTH EQUITY INC.
HEALTH EQUITY INC.
PAYROLL DIRECT DEPOSIT 07.25.25
BENEFITS & TAXES FOR 07.25.25

\$628.67 LEAK REPAIR @ 1804 SARAZIN(W)
\$3,288.86 WIRE HOLDER/CONDUCTOR HOLDER
\$22,810.00 LIGHTING CONTROLS REBATE
\$500.00 ENERGY STAR COOLING/HEATING REBATE
\$317.47 COFFEE BREAKROOMS
\$500.00 ENERGY STAR COOLING/HEATING REBATE
\$1,157.36 SPLICING KIT II 2 STR-1/0 SOL 15KV
\$500.00 ENERGY STAR COOLING/HEATING REBATE
\$25.00 REBATE - TRIMMER
\$50.00 ENERGY STAR CLOTHES WASHER REBATE
\$500.00 ENERGY STAR COOLING/HEATING REBATE
\$2.29 CABLE IN BREAKROOMS
\$436.75 ANSWERING SERVICE 7/22-8/18/2025
\$52.12 3/8"MEDSPLIT/HCS3/8-16X1(E)
\$2,320.78 VLV BX TOP SECT DOM
\$1,682.94 BATTERY CHARGER PORT(E)
\$50.00 REBATE - PUSHMOWER
\$74.73 ENG TRUCK#629 OIL CHANGE
\$19,555.32 INFRASTRUCTURE SVCS ANNUAL BILLING
\$40.61 WALL CLOCK
\$1,784.68 METER SOCKET 3PH 200AMP 7 TERM W/BYPASS
\$150.00 ENERGY STAR DISHWASHER REBATE
\$552.00 CUST#-01300 105832214 JCI SYSTEM INSTALL
\$4,800.00 PIPE 2" INNERDUCT
\$734.00 EXTERIOR LIGHTING REBATE
\$100.00 ENERGY STAR DISHWASHER REBATE
\$6,869.54 CLAIM # LMC CA 00000444879 6/18/25
\$75.00 ENERGY STAR REFRIGERATOR REBATE
\$1,586.21 POLY PULLING TAPE
\$204.51 CONTRACT CHG 7/1-7/31 2025 MAINT AGREEM
\$648.00 TEST PROPELLER/NEW CASE O RING(W)
\$885.25 WATER TESTING COLIFORM
\$10,095.00 QUALYS INTERNAL VM LIC 1-YR 2025
\$14,566.25 Q3 2025 SAFETY PROGRAM/ELEC SAFETY
\$25.00 REBATE - CHAINSAW
\$1,176.39 HYDRANT METER#454624 RETURN REFUND
\$31,760.00 WO#2832 BORING MICRO SOURCE
\$12,325.05 WO2881 GATEWAY TOWNHOMES-WM PR&I REFUND
\$500.00 ENERGY STAR COOLING/HEATING REBATE
\$175.00 ENERGY STAR CLOTHES WASHER REBATE
\$463.65 SIGNS LOOK UP CAUTION
\$500.00 ENERGY STAR COOLING/HEATING REBATE
\$2,494.85 HACH DR900 COLORIMETER 9385100(W)
\$500.00 ENERGY STAR COOLING/HEATING REBATE
\$5,000.00 WATERLY UPGRADE TO MDH
\$1,600.20 HOT LINE CLAMP
\$436.00 WO#2581 PUMPHOUSE #23 JUN SVCS 2025
\$3,218.50 MEDICAL FLEX CLAIM REIMB B.C.
\$192.00 DAYCARE FLEX CLAIM REIMB C.S.
\$142,652.81
\$141,256.48

Total Week of 07/25/2025**\$441,819.27****Grand Total****\$9,067,718.20**

Keelby Willemssen
Presented for approval by: Director of Finance & Administration

Approved by General Manager

Approved by Commission President

Monthly Water Dashboard

As of: June 2025

Shakopee Public Utilities Commission

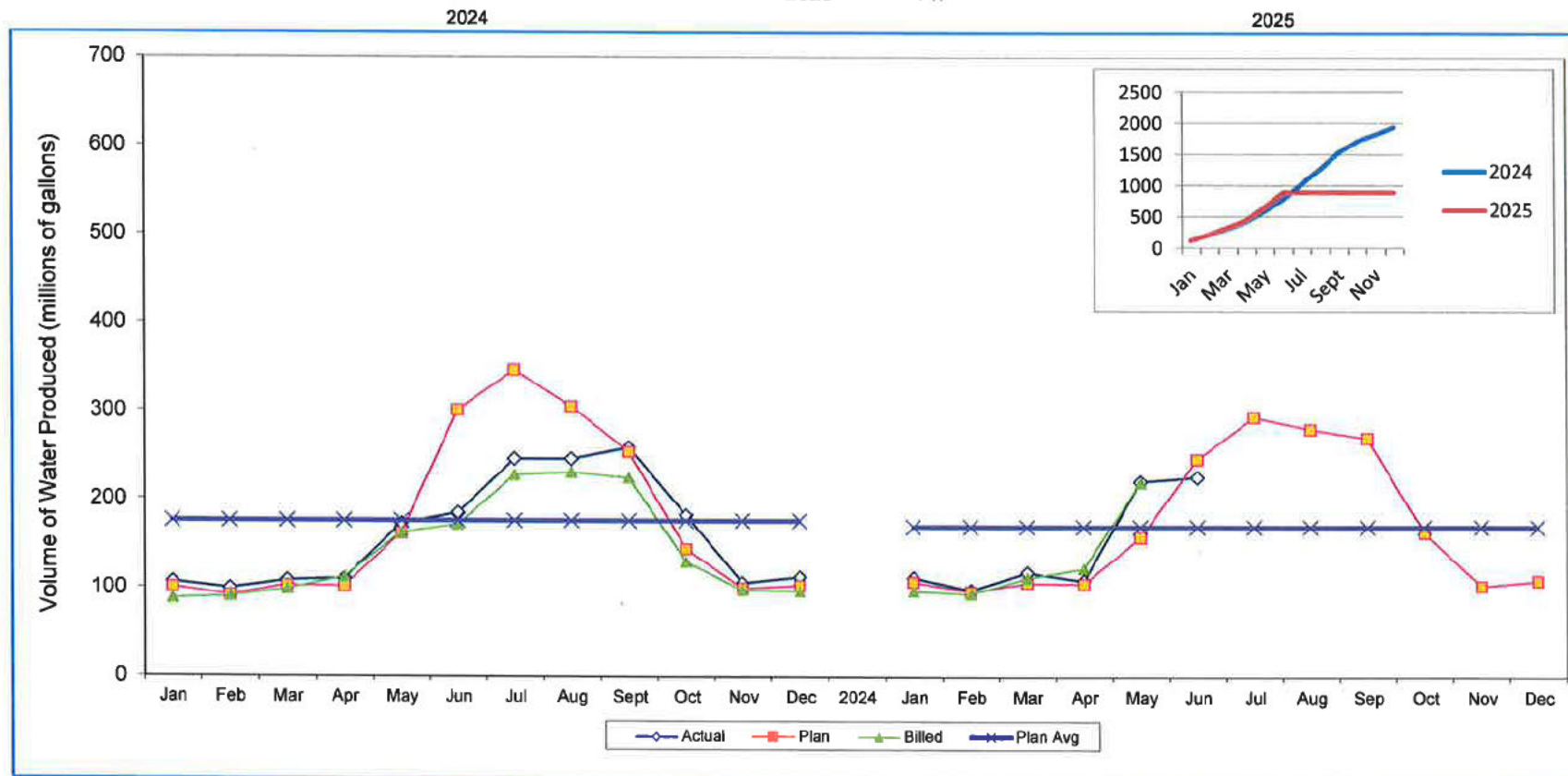
ALL VALUES IN MILLIONS OF GALLONS

Element/Measure

Water Pumped/Metered

Monthly Avg
 2023 187
 2024 161
 2025 147

Last 6 months actuals 112 98 118 109 221 226




2023	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec
	107	100	109	111	173	185	246	246	259	182	106	113
	101	92	103	102	162	301	346	305	254	144	100	103
	88	91	99	113	163	172	228	231	225	130	98	97
2024	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec
	112	98	118	109	221	226						
	107	96	106	105	158	246	294	280	270	163	103	109
	105%	103%	106%	106%	115%	108%						
2025	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec
	97	94	112	123	220							

* Actual gallons pumped vs. Plan



PO Box 470 • 255 Sarazin Street
Shakopee, Minnesota 55379
Main 952.445-1988 • Fax 952.445-7767
www.shakopeeutilities.com

To: SPU Commissioners

From: Greg Drent, General Manager 

Date: July 25, 2025

Subject: MMPA July 2025 Meeting Update

The Board of Directors of the Minnesota Municipal Power Agency (MMPA) met on July 22, 2025, at Canterbury Park in Shakopee, Minnesota, and via videoconference.

The Board reviewed the Agency's financial and operating performance for June 2025.

Participation in the residential Clean Energy Choice program increased by 65 customers. Customer penetration for the program is 6.5%.

The Board discussed the status of renewable projects the Agency is pursuing.

The Board discussed the Federal Budget Reconciliation Bill and the effect it will have on MMPA's projects.

Thanks

RESOLUTION #2025-21

RESOLUTION APPROVING OF THE ESTIMATED COST OF
PIPE OVERSIZING ON THE WATERMAIN PROJECT:

ELLIANA ESTATES

WHEREAS, the Shakopee Public Utilities Commission has been notified of a watermain project, and

WHEREAS, the pipe sizes required for that project have been approved as shown on the engineering drawing by JAMES R. HILL, INC., and

WHEREAS, a part, or all, of the project contains pipe sizes larger than would be required under the current Standard Watermain Design Criteria as adopted by the Shakopee Public Utilities Commission, and

WHEREAS, the policy of the Shakopee Public Utilities Commission calls for the payment of those costs to install oversize pipe above the standard size, and

NOW THEREFORE, BE IT RESOLVED, that the total amount of the oversizing to be paid by the Shakopee Public Utilities Commission is approved in the amount of approximately \$28,129.00 and

BE IT FURTHER RESOLVED, the payment of the actual amount for said oversizing will be approved by the Utilities Commission when final costs for the watermain project are known, and

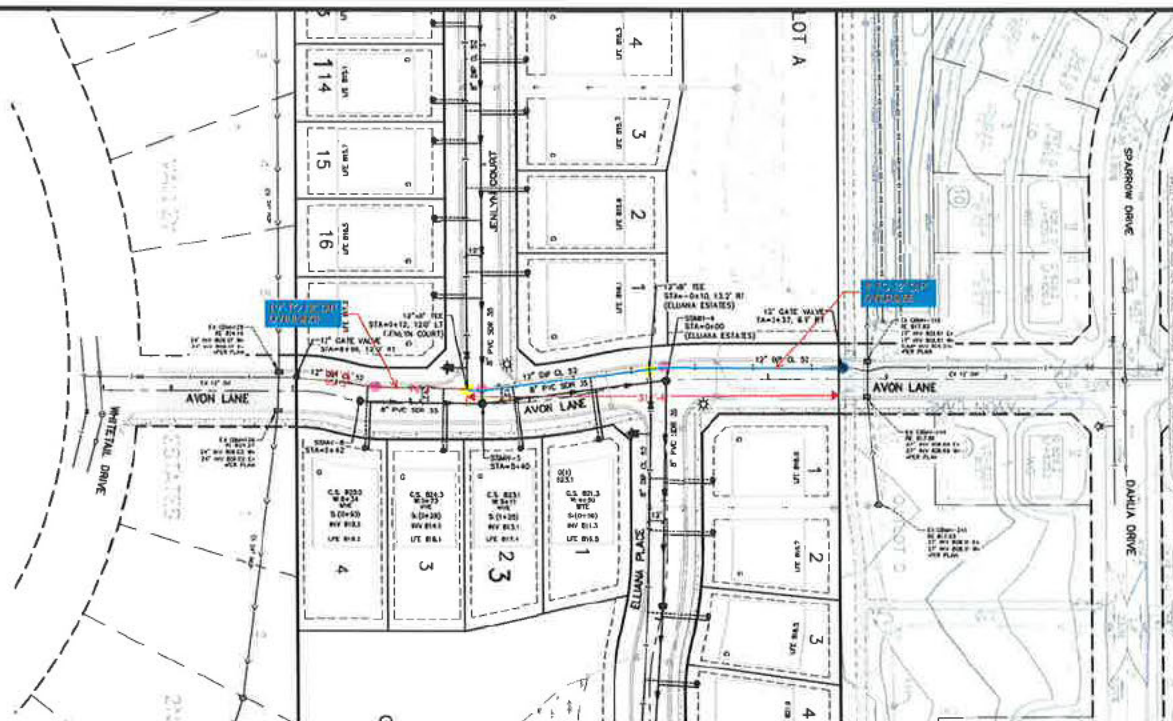
BE IT FURTHER RESOLVED, that all things necessary to carry out the terms and purpose of this Resolution are hereby authorized and performed.

Passed in regular session of the Shakopee Public Utilities Commission, this 4th day of August, 2025.

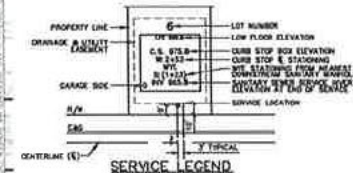
Commission President: BJ Letourneau

ATTEST:

Commission Secretary: Greg Drent



- LEGEND**
- PROPOSED WATERMAIN
 - PROPOSED SANITARY SEWER
 - PROPOSED WATER SERVICE
 - 1" COVER TYPE K
 - PROPOSED SANITARY SERVICE
 - 4" PVC SDR 26
 - PROPOSED STORM SEWER
 - PROPOSED CURB & GUTTER
 - PROPOSED CONCRETE
 - PROPOSED SEDIMENT BASIN
 - PROPOSED INFILTRATION BASIN



- SPU NOTES**
1. ALL WATERMAIN TO BE INSTALLED PER SPU WATER POLICY MANUAL.
 2. ALL PVC SHALL BE SDR 35 UNLESS OTHERWISE NOTED.
 3. ALL WATERMAIN SHALL BE DIP CLASS 52 AND WRAPPED IN V-BIO ENHANCED POLYETHYLENE ENCASING.
 4. ALL WATERMAIN SHALL HAVE MINIMUM 7.5 FT OF COVER.
 5. FLAG HYDRANTS
 6. ALL SANITARY SEWER SERVICE SHALL BE 4" PVC SDR UNLESS OTHERWISE NOTED
 7. THE UTILITY CONTRACTOR SHALL PROVIDE 18" MINIMUM SEPARATION BETWEEN WATERMAIN AND SANITARY SEWER AND SERVICES, ALONG WITH 3" MINIMUM SEPARATION BETWEEN STORM SEWER AND WATERMAIN AND SERVICES.
 8. SURVEYOR MUST WRITE CUT/FILL GRADE AND THE BURY LINE OF ALL HYDRANTS

GENERAL SERVICE NOTES

1. ALL WATER SERVICES SHALL BE 1" COVER TYPE K AND INSTALLED PER SPU DETAIL NO. WAT-003
2. ALL SANITARY SERVICES AND RISERS SHALL BE 4" PVC SDR 26 AND INSTALLED PER CITY DETAIL NO. 2003 AND 2004.

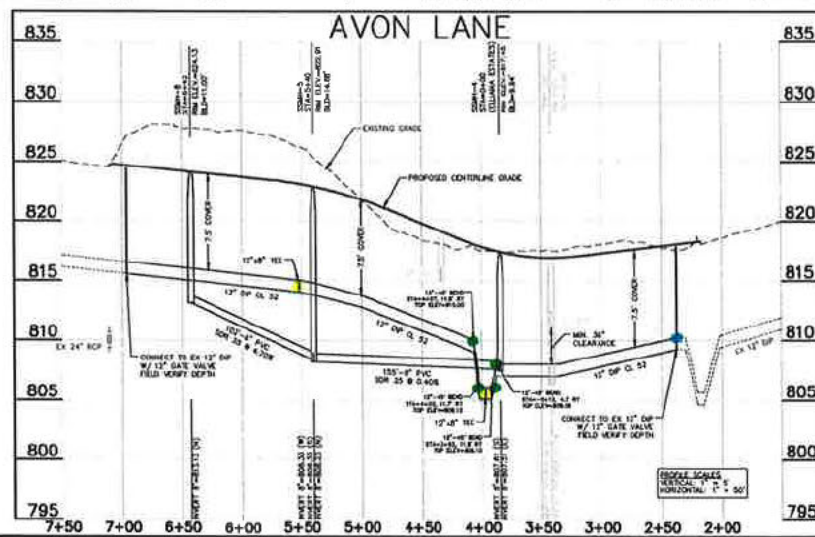
BENCHMARKS

1. SANITARY SEWER MANHOLE, WEST SIDE MYSTIC LAKE ELVD R-0-W, APPROX 53 LF SOUTH OF BOUNDARY LINE ELEV=815.11
2. SANITARY SEWER MANHOLE, CENTERLINE OF AVON LANE AND SPARROW DRIVE/DAHLIA DRIVE ELEV=832.38

APPROVED FOR ONE YEAR FROM THIS DATE

SHAKOPEE PUBLIC UTILITIES COMMISSION DATE

All materials and construction methods shall comply with the latest edition of the Minnesota Public Utilities Code, Chapter 216B, Revised 2014.



James R. Hill, Inc.
PLANNERS / ENGINEERS / SURVEYORS
2999 W. City Ave. 42, Suite 300, Burnsville, MN 55336
PHONE: (612) 890-6644 FAX: (612) 890-4244

ELLIANA ESTATES
SHAKOPEE, MINNESOTA
SANTARY SEWER & WATERMAIN CONSTRUCTION
AVON LANE
ELLIANA ESTATES
1000 COUNTY ROAD 42 WEST, SUITE 100, BURNSVILLE, MN 55337

ELLIANA ESTATES
SHAKOPEE, MINNESOTA
SANTARY SEWER & WATERMAIN CONSTRUCTION
AVON LANE
ELLIANA ESTATES
1000 COUNTY ROAD 42 WEST, SUITE 100, BURNSVILLE, MN 55337

DRAWN BY
JSO
DATE
05/20/2025
REVISIONS
NO. DESCRIPTION
CAD FILE
2363455
PROJECT NO.
23634
9

RESOLUTION #2025-22

RESOLUTION SETTING THE AMOUNT
OF THE TRUNK WATER CHARGE, APPROVING OF ITS COLLECTION
AND AUTHORIZING WATER SERVICE TO CERTAIN PROPERTY
DESCRIBED AS:

ELLIANA ESTATES
LOTS 1-17 Block 1, LOTS 1-10 Block 2, LOTS 1-4 Block 3, and Outlots A and B

WHEREAS, a request has been received for City water service to be made available to certain property, and

WHEREAS, the collection of the Trunk Water Charge is one of the standard requirements before City water service is newly made available to an area, and

WHEREAS, the standard rate to be applied for the Trunk Water Charge has been set by separate Resolution,

NOW THEREFORE, BE IT RESOLVED, that the amount of the Trunk Water Charge is determined to be \$54,580.84 based on 9.43 net acres, and that collection of the Trunk Water Charge is one of the requirements to be completed prior to City water service being made available to that certain property described as:

ELLIANA ESTATES
LOTS 1-17 Block 1, LOTS 1-10 Block 2, LOTS 1-4 Block 3, and Outlots A and B

BE IT FURTHER RESOLVED, that all things necessary to carry out the terms and purpose of this Resolution are hereby authorized and performed.

Passed in regular session of the Shakopee Public Utilities Commission, this 4th day of August, 2025.

Commission President: BJ Letourneau

ATTEST:

Commission Secretary: Greg Drent



PO Box 470 • 255 Sarazin
 Shakopee, Minnesota 55379
 Main 952.445-1988 • Fax 952.445-7767
www.shakopeeutilities.com

DATE: July 28, 2025
TO: Greg Drent, General Manager *GD*
FROM: Kelley Willemssen, Director of Finance & Administration *KW*
SUBJECT: June Financial Reports

As part of the June financial reports, we continued the practice of providing a component of analytical review. For the Water and Electric Operating Revenue and Expense budget to actual you will see comments at the bottom of each page. The budget is projected on an annual basis rather than a monthly basis so the information in the June financial reports equates to 50% of the annual budget.

Key Takeaways for YTD Actuals to Budget

- Electric revenues were 8.1% under budget, mainly due to lower than budgeted power cost adjustment revenue from lower purchased power costs.
- Electric expenses were 10.9% under budget, with major savings in purchase power costs.
- Water revenues were 18.9% under budget due to seasonal usage patterns and should stabilize beginning in July.
- Water expenses were under budget by 0.02%.
- Change in Net Position for the electric division as of 06/30/25 is \$2.4M.
- Change in Net Position for the water division as of 06/30/25 is \$2.1M.

Key Takeaways for YTD Actuals to Prior Year

- YTD electric operating revenues are up 3.52% from the prior year.
- YTD electric expenses are up 4.32% from the previous year.
- YTD water revenues are up 21.6% from the prior year.
- YTD water expenses are up 2.9% from the previous year.

Included in this report are the following statements:

- Combined Statement of Revenues, Expenses and Changes in Fund Net Position
- Electric Operating Revenue and Expense – Budget to Actual (with analytics)
- Water Operating Revenue and Expense– Budget to Actual (with analytics)
- Electric Operating Revenue and Expense – 2024 to 2025
- Water Operating Revenue and Expense – 2024 to 2025

Request

The Commission is requested to accept the Financial Reports for the period ending 06/30/25.

SHAKOPEE PUBLIC UTILITIES
COMBINED STATEMENT OF REVENUES, EXPENSES AND CHANGES IN FUND NET POSITION

	Year to Date Actual - June 30, 2025			Year to Date Budget - June 30, 2025			Electric		Water		Total Utility	
	Electric	Water	Total Utility	Electric	Water	Total Utility	YTD Actual v. Budget B/(W) \$ %		YTD Actual v. Budget B/(W) \$ %		YTD Actual v. Budget B/(W) \$ %	
OPERATING REVENUES	\$ 28,176,591	3,221,808	31,398,399	30,649,835	3,971,167	34,621,001	(2,473,244)	-8.1%	(749,358)	-18.9%	(3,222,602)	-9.3%
OPERATING EXPENSES												
Operation, Customer and Administrative	23,157,497	1,981,307	25,138,804	26,374,169	2,432,644	28,806,812	3,216,672	12.2%	451,337	18.6%	3,668,009	12.7%
Depreciation	2,084,976	1,833,053	3,918,029	1,968,414	1,382,389	3,350,803	(116,562)	-5.9%	(450,664)	-32.6%	(567,227)	-16.9%
Total Operating Expenses	25,242,472	3,814,360	29,056,833	28,342,582	3,815,033	32,157,615	3,100,110	10.9%	672	0.02%	3,100,782	9.6%
Operating Income	2,934,118	(592,552)	2,341,566	2,307,253	156,134	2,463,386	626,866	27.2%	(748,686)	479.5%	(121,820)	-4.9%
NON-OPERATING REVENUE (EXPENSE)												
Rental and Miscellaneous	100,206	281,547	381,753	166,009	93,131	259,139	(65,803)	-39.6%	188,417	202.3%	122,614	47.3%
Interdepartment Rent from Water	45,000	-	45,000	45,000	-	45,000	-	0.0%	-	0.0%	-	0.0%
Investment Income	1,278,080	898,805	2,176,885	907,716	302,572	1,210,289	370,363	40.8%	596,233	197.1%	966,597	79.9%
Interest Expense	(35,528)	(1,670)	(37,197)	(40,440)	(2,317)	(42,757)	4,912	12.1%	647	27.9%	5,559	13.0%
Gain/(Loss) on the Disposition of Property	18,037	-	18,037	28,336	-	28,336	(10,299)	0.0%	-	-	(10,299)	-
Total Non-Operating Revenue (Expense)	1,405,795	1,178,663	2,584,478	1,106,621	393,366	1,500,007	299,174	27.0%	785,297	199.6%	1,084,471	72.3%
Income Before Contributions and Transfers	4,339,913	586,131	4,926,044	3,413,874	549,520	3,963,393	926,040	27.1%	36,611	6.7%	962,651	24.3%
CAPITAL CONTRIBUTIONS	62,555	1,784,665	1,847,221	369,236	2,179,350	2,548,586	(306,681)	83.1%	(394,685)	-18.1%	(701,366)	-27.5%
MUNICIPAL CONTRIBUTION	(1,944,397)	(238,272)	(2,182,669)	(1,870,627)	(238,270)	(2,108,897)	(73,770)	-3.9%	(2)	0.0%	(73,772)	-3.5%
CHANGE IN NET POSITION	\$ 2,458,071	2,132,524	4,590,596	1,912,483	2,490,600	4,403,083	545,589	28.5%	(358,076)	-14.4%	187,513	4.3%

SHAKOPEE PUBLIC UTILITIES
ELECTRIC OPERATING REVENUE AND EXPENSE

	YTD Actual 6/30/2025	YTD Budget 6/30/2025	YTD Actual v. Budget Increase (decrease)	
			\$	%
OPERATING REVENUES				
Sales of Electricity				
Residential	\$ 10,411,391	11,111,634	(700,243)	93.7
Commercial and Industrial	17,178,795	18,866,045	(1,687,249)	91.1
Total Sales of Electricity	27,590,186	29,977,678	(2,387,492)	92.0
Forfeited Discounts	102,218	160,439	(58,221)	63.7 (1)
Free service to the City of Shakopee	73,771	66,182	7,589	111.5
Conservation program	410,416	445,536	(35,120)	92.1
Total Operating Revenues	28,176,591	30,649,835	(2,473,244)	91.9
OPERATING EXPENSES				
Operations and Maintenance				
Purchased power	19,314,417	21,233,833	(1,919,415)	91.0
Distribution operation expenses	327,831	409,606	(81,775)	80.0
Distribution system maintenance	510,594	653,223	(142,628)	78.2
Maintenance of general plant	217,890	241,924	(24,034)	90.1
Total Operation and Maintenance	20,370,732	22,538,585	(2,167,853)	90.4
Customer Accounts				
Meter Reading	10,767	37,334	(26,567)	28.8 (2)
Customer records and collection	267,384	364,643	(97,258)	73.3 (3)
Energy conservation	19,635	445,535	(425,900)	4.4 (4)
Total Customer Accounts	297,787	847,511	(549,724)	35.1
Administrative and General				
Administrative and general salaries	588,145	649,424	(61,279)	90.6
Office supplies and expense	290,708	414,490	(123,782)	70.1 (5)
Outside services employed	225,503	217,476	8,027	103.7
Insurance	83,385	87,752	(4,367)	95.0
Employee Benefits	983,114	1,246,607	(263,493)	78.9 (6)
Miscellaneous general	318,122	372,324	(54,202)	85.4
Total Administrative and General	2,488,978	2,988,073	(499,095)	83.3
Total Operation, Customer, & Admin Expenses	23,157,497	26,374,169	(3,216,672)	87.8
Depreciation	2,084,976	1,968,414	(116,562)	105.9
Total Operating Expenses	\$ 25,242,472	28,342,582	(3,100,110)	89.1
Operating Income	\$ 2,934,118	2,307,253	626,866	127.2

Item Explanation of Items Percentage Received/Expended Less than 80% or Greater than 120% and \$ Variance Greater than \$15,000.

- (1) YTD penalty fees are lower than budgeted, possibly due to enhanced digital tools through NISC; automatic payments and reminders.
- (2) YTD variance due to lower than budgeted meter reading expenses as AMI is close to fully deployed.
- (3) YTD variance is primarily due to a budgeted FTE that is not filled as of April.
- (4) YTD budget variance is mainly due to timing of rebates.
- (5) YTD budget variance is timing of when software dues and subscriptions are paid in the year. Variance should stabilize.
- (6) YTD budget variance is primarily from more PTO being budgeted through current period & an unfilled FTE position.

SHAKOPEE PUBLIC UTILITIES

WATER OPERATING REVENUE AND EXPENSE

	YTD Actual 6/30/2025	YTD Budget 6/30/2025	YTD Actual v. Budget Increase (decrease)	
			\$	%
OPERATING REVENUES				
Sales of Water	\$ 3,210,305	3,947,619	(737,314)	81.3
Forfeited Discounts	11,504	23,548	(12,044)	48.9 (1)
Total Operating Revenues	3,221,808	3,971,167	(749,358)	81.1
OPERATING EXPENSES				
Operations and Maintenance				
Pumping and distribution operation	399,927	404,588	(4,660)	98.8
Pumping and distribution maintenance	205,073	506,894	(301,821)	40.5 (2)
Power for pumping	174,509	183,038	(8,529)	95.3
Maintenance of general plant	19,140	33,294	(14,153)	57.5 (3)
Total Operation and Maintenance	798,650	1,127,814	(329,164)	70.8
Customer Accounts				
Meter Reading	6,710	28,345	(21,635)	23.7 (4)
Customer records and collection	87,359	87,721	(362)	99.6
Energy conservation	1,576	3,177	(1,601)	49.6 (5)
Total Customer Accounts	95,644	119,242	(23,598)	80.2
Administrative and General				
Administrative and general salaries	296,139	310,668	(14,529)	95.3
Office supplies and expense	103,758	121,369	(17,611)	85.5
Outside services employed	62,878	99,700	(36,822)	63.1 (6)
Insurance	27,795	29,260	(1,465)	95.0
Employee Benefits	476,478	472,840	3,638	100.8
Miscellaneous general	119,966	151,752	(31,786)	79.1
Total Administrative and General	1,087,013	1,185,588	(98,575)	91.7
Total Operation, Customer, & Admin Expenses	1,981,307	2,432,644	(451,337)	81.4
Depreciation	1,833,053	1,382,389	450,664	132.6 (7)
Total Operating Expenses	\$ 3,814,360	3,815,033	(672)	100.0
Operating Income	\$ (592,552)	156,134	(748,686)	(379.5)

Item Explanation of Items Percentage Received/Expended Less than 80% or Greater than 120% and \$ Variance Greater than \$15,000.

- (1) YTD penalty fees are lower than budgeted, possibly due to enhanced digital tools through NISC; automatic payments and reminders.
- (2) YTD budget variance is due to higher than projected pumping and distribution expenses through June, should stabilize throughout the year.
- (3) YTD budget variance is due to higher than projected general maintenance expenses through June, should stabilize throughout the year.
- (4) YTD variance due to lower than budgeted meter reading expenses as AMI is close to fully deployed.
- (5) YTD budget variance is mainly due to timing of rebates.
- (6) YTD budget variance is due to higher than projected outside services through June, should stabilize throughout the year.
- (7) YTD variance is due to higher than budgeted depreciation expenses for meters through the AMI implementation booked in Jan, should stabilize.

SHAKOPEE PUBLIC UTILITIES
ELECTRIC OPERATING REVENUE AND EXPENSE

	2025	2024	2024-2025 Increase (decrease)	
			\$	%
OPERATING REVENUES				
Sales of Electricity				
Residential	\$ 10,411,391	9,552,284	859,107	109.0
Commercial and Industrial	17,178,795	17,069,163	109,633	100.6
Total Sales of Electricity	27,590,186	26,621,447	968,739	103.6
Forfeited Discounts	102,218	129,099	(26,882)	79.2
Free service to the City of Shakopee	73,771	72,031	1,740	102.4
Conservation program	410,416	396,179	14,237	103.6
Total Operating Revenues	28,176,591	27,218,756	957,834	103.5
OPERATING EXPENSES				
Operations and Maintenance				
Purchased power	19,314,417	18,217,837	1,096,580	106.0
Distribution operation expenses	327,831	305,253	22,578	107.4
Distribution system maintenance	510,594	509,957	637	100.1
Maintenance of general plant	217,890	285,718	(67,828)	76.3
Total Operation and Maintenance	20,370,732	19,318,764	1,051,968	105.4
Customer Accounts				
Meter Reading	10,767	78,296	(67,529)	13.8
Customer records and collection	267,384	301,971	(34,587)	88.5
Energy conservation	19,635	63,516	(43,881)	30.9
Total Customer Accounts	297,787	443,783	(145,997)	67.1
Administrative and General				
Administrative and general salaries	588,145	456,741	131,404	128.8
Office supplies and expense	290,708	259,655	31,053	112.0
Outside services employed	225,503	226,083	(580)	99.7
Insurance	83,385	83,590	(205)	99.8
Employee Benefits	983,114	983,706	(591)	99.9
Miscellaneous general	318,122	307,700	10,422	103.4
Total Administrative and General	2,488,978	2,317,474	171,503	107.4
Total Operation, Customer, & Admin Expenses	23,157,497	22,080,022	1,077,474	104.9
Depreciation	2,084,976	2,117,324	(32,348)	98.5
Total Operating Expenses	\$ 25,242,472	24,197,346	1,045,126	104.3
Operating Income	\$ 2,934,118	3,021,410	(87,292)	97.1

SHAKOPEE PUBLIC UTILITIES

WATER OPERATING REVENUE AND EXPENSE

			2024-2025	
			Increase (decrease)	
	2025	2024	\$	%
OPERATING REVENUES	\$			
Sales of Water	3,210,305	2,640,762	569,543	121.6
Forfeited Discounts	11,504	8,436	3,067	136.4
Total Operating Revenues	3,221,808	2,649,198	572,610	121.6
OPERATING EXPENSES				
Operations and Maintenance				
Pumping and distribution operation	399,927	375,918	24,009	106.4
Pumping and distribution maintenance	205,073	337,080	(132,007)	60.8
Power for pumping	174,509	200,398	(25,889)	87.1
Maintenance of general plant	19,140	37,637	(18,497)	50.9
Total Operation and Maintenance	798,650	951,033	(152,383)	84.0
Customer Accounts				
Meter Reading	6,710	38,287	(31,577)	17.5
Customer records and collection	87,359	87,051	307	100.4
Energy conservation	1,576	1,606	(30)	98.1
Total Customer Accounts	95,644	126,944	(31,300)	75.3
Administrative and General				
Administrative and general salaries	296,139	266,343	29,796	111.2
Office supplies and expense	103,758	87,479	16,279	118.6
Outside services employed	62,878	102,037	(39,159)	61.6
Insurance	27,795	27,893	(98)	99.6
Employee Benefits	476,478	457,623	18,854	104.1
Miscellaneous general	119,966	113,780	6,186	105.4
Total Administrative and General	1,087,013	1,055,155	31,857	103.0
Total Operating Expenses	1,981,307	2,133,133	(151,826)	92.9
Depreciation	1,833,053	1,573,470	259,583	116.5
Total Operating Expenses	3,814,360	3,706,603	107,757	102.9
Operating Income	\$ (592,552)	(1,057,405)	464,853	56.0



PO Box 470 • 255 Sarazin Street
Shakopee, Minnesota 55379
Main 952.445-1988 • Fax 952.445-7767
www.shakopeeutilities.com

DATE: July 29, 2025

TO: Greg Drent, General Manager *GD*

FROM: Kelley Willemssen, Director of Finance & Administration *KW*

SUBJECT: Amend Purchasing Policy

Overview

To improve clarity and ensure consistent compliance, we are recommending specific updates to the Purchasing Policy regarding change orders and related procedural requirements. These updates aim to enhance understanding across departments and strengthen internal controls.

To assist with your review, both the **original version** of the policy and a **redlined** version showing all tracked changes are attached to this memo.

Action Requested:

Approve the amended Purchasing Policy



Purchasing/Contracts Policy

The Operating budget and Capital Improvement Plan (CIP) allocates funds for the purchase or payment of personnel, supplies, material, and contractual services. The Purchasing/Contract Policy is provided to all departments of the utility to provide guidance and direction to employees involved in the purchasing process. It is the policy of the utility to make purchases utilizing a competitive process to receive the best value. The competitive process may include verbal/written quotes, requests for proposals (RFP), and a formal bidding process. Requests cannot be made for items outside the budget except under special circumstances, which must be approved by the General Manager. The General Manager is the Purchasing Agent. Any deviation from this Purchasing and Contracts Policy must be approved by the commission. Purchasing authorization thresholds are summarized below:

- < \$2,500 – Supervisors
- < \$50,000 – Department Director or Superintendent
- < \$175,000 – General Manager
- ≥ \$175,000 – Commission (Follow Formal Bid Process)

PURCHASING AUTHORIZATION PROCESS

Purchasing: A purchase is defined as buying, renting, leasing or otherwise acquiring any goods and/or services for public purposes in accordance with laws, regulations, statutes, policies, and approved budgets. Non-inventory purchases up to \$2,500 do not require a purchase order. Non-inventory purchases over \$2,500 are procured via purchase order and need to follow the procedures and approvals outlined in Table 1. All inventory items are procured via purchase order and need to follow the procedures and approvals outlined in Table 1. Within the meaning of the definition of a purchase, the following are purchases that would **NOT** require a purchase order (some examples, not limited to the ones listed, that fall under this situation):

- Non – inventory purchases under \$2,500
- Recurring invoices in the normal course of business
- Public communications, i.e. telephone, newspaper ads etc.
- All Costs associated with education, training, workshops and conferences
- Professional Services
- Credit Card purchases (In accordance with the approved credit card policy and budget)
- Tuition reimbursement
- Lawyers (professional services)
- Accountants/Engineers/Consultants
- Healthcare providers (insurance contracts)

Recurring purchases – Purchases that recur in the normal course of business that may exceed dollar thresholds require two approvals from within the finance department for payment and do not require a purchase order. These are contractual accounts for services that are approved by the commission as part of the budget process. Some vendors, not limited to the ones listed, that fall under this situation include MMPA, Xcel Energy, PERA, League of MN Cities, health care providers and the State of Minnesota.

Professional services - Shakopee Public Utilities (SPU) is not required to use the competitive bidding process when contracting for professional services, such as those of engineers, lawyers, architects, and accountants, as well as other services requiring technical or professional training like lawn care services and janitorial services. Contracts for professional services will require review and approval by department directors and the general manager, within the dollar thresholds established in Table 1. Professional services do not require a purchase order as they are approved by the commission as part of the budget process.

Insurance contracts - SPU is not required to use the competitive bidding process for insurance contracts; however, SPU must seek requests for proposals for group insurance.

Table 1: Purchase & Bidding Authorizations and Requirements

Amount of Purchase:	Type of Quote Required:	Approval required by:	Written Specifications:	Sealed Bids Required:	Contract Required:	Purchase Order Required:
Purchases under \$2,500	Two telephone quotes are required when a good or service is available from more than 1 source or supplier, or when standardization or compatibility is not an overriding consideration, or in the open market.	Supervisor and above	As required based on type of purchase	No	No	No
Purchases between \$2,500 – \$25,000	Two written quotes are required when a good or service is available from more than 1 source or supplier, or when standardization or compatibility is not an overriding consideration, or in the open market.	Dept. Director or Superintendent	As required based on type of purchase	No	No	Yes
Purchases between \$25,000 – \$50,000	Three written quotes required when a good or service is available from more than 1 source or supplier, or when standardization or compatibility is not an overriding consideration or purchases through cooperative purchasing agreement.	Dept. Director or Superintendent	As required based on type of purchase	No	No	Yes
Purchases between \$50,000 – \$175,000	Three written quotes required when a good or service is available from more than 1 source or supplier, or when standardization or compatibility is not an overriding consideration or purchases through cooperative purchasing agreement.	General Manager provided purchase amount does not exceed amount authorized by CIP (See section D)	As required based on type of purchase	No	Construction Projects: Yes Commodities: At the discretion of General Manager	Yes
Purchases over \$175,000	General Manager or designee must advertise in SPU's legal newspaper.	Commission	Required	Yes	Yes	Yes
Capital Improvement Plan (CIP) Purchases – See section C						

A. Responsible Contractor Compliance:

- A contractor responding to a solicitation document of a contracting authority shall submit to the contracting authority a signed statement under oath by an owner or officer verifying compliance with each of the minimum criteria in subdivision 3 of Minnesota Statutes, Section 16C.285 at the time that it responds to the solicitation document, and from subcontractors as provided in Section 16C.285, subdivision 4. A contracting authority may accept a signed statement under oath as sufficient to demonstrate that a contractor is a responsible contractor and shall not be held liable for awarding a contract in reasonable reliance on that statement. A prime contractor, subcontractor, or motor carrier that fails to verify compliance with any one of the required minimum criteria or makes a false statement under oath in a verification of compliance shall be ineligible to be awarded a construction contract on the project for which the verification was submitted. A false statement under oath verifying compliance with any of the minimum criteria may result in termination of a construction contract that has already been awarded to a prime contractor or subcontractor or motor carrier that submits a false statement. A contracting authority shall not be liable for declining to award a contract or terminating a contract based on a reasonable determination that contractor failed to verify compliance with the minimum criteria or falsely stated that it meets the minimum criteria. A verification of compliance need not be notarized. An electronic verification of compliance made and submitted as part of an electronic bid shall be an acceptable verification of compliance under this section, provided that it contains an electronic signature as defined in Minnesota Statutes, Section 325L.02, paragraph (h).

B. Cooperative Purchasing Contracts:

- For contracts estimated to exceed \$25,000, SPU may consider the availability, price, and quality of supplies, materials, or equipment available through the state cooperative purchasing venture before buying through another source.
- If SPU is not utilizing the state's cooperative purchasing venture, SPU may consider another national municipal association's purchasing alliance or cooperative created by a joint powers agreement that purchases items from more than one source on the basis of competitive bids or competitive quotations.

C. Bidding Requirements:

- When supplies or equipment are competitive in nature, specifications cannot exclude all but one type of equipment or supplies. Proposals and specifications must allow free and full competition. Bidding requirements cannot be avoided by splitting a contract into several contracts, each of which is below the minimum amount requiring sealed bids. For example, SPU cannot purchase \$200,000 of lumber in several transactions, each involving an expenditure of less than \$100,000. However, if materials or work logically fall into two separate contracts because they involve separate transactions, as for the service of contractors specializing in different kinds of work, there is no reason why SPU cannot negotiate the contracts individually without sealed bids if the bids do not exceed the \$175,000 minimum.
- Capital Improvement Plan (CIP) purchases – The CIP is approved by the Commission and is an adopted budget document; therefore, the expenditure has been formally authorized.
- Sales tax – Beginning January 1, 2015, purchases made by Shakopee Public Utilities are generally exempt from sales tax. Certain other exclusions are listed in Statute and should be reviewed on a regular basis. Bidders should specify whether their bid includes sales tax or not. After the work is completed and a purchase order is processed, if the invoice does not itemize sales tax, you must obtain a corrected invoice from the vendor if sales tax is applicable on the item purchased.
- Consultant services - State law does not require SPU to competitively bid contracts for professional services (i.e. attorney, architect, engineer, accountant, cleaning company, or other person with technical, scientific, or professional training such as refuse hauling).

- Sealed bids are required for purchases exceeding \$175,000, and bids must be advertised by the General Manager or designee in SPU's legal newspaper (Notice to Bidders) and publicly opened and approved by the Commission. In addition to the legal notice, SPU must prepare instructions to bidders and general specifications for sealed bids. Attaching a copy of the proposed contract to the instructions to bidders is required. Sealed bids, including the number of bids received prior to bid opening, are nonpublic. Once opened, the name of the bidder and the dollar amount of the bid are public (all other data is private until completion of the selection process).
- Bids vs. Quotes terminology – always use term quotation unless referring to a sealed bid.
- Bid security (for sealed bids for purchases over \$175,000) in the amount of five percent (5%) of the bid shall be submitted to the General Manager. The bid security guarantees that in the event the bidder's offer is accepted, the bidder will enter into a contract in accordance with the proposal. Bid security of the successful bidder will be returned upon execution of the contract documents. Bid securities of unsuccessful bidders will be returned within a reasonable time period (Minnesota Statutes § 574.27). Failure of the successful bidder to execute the contract and furnish applicable bonds within ten (10) days after receiving written notice of the award shall cause the bid security to be forfeited as liquidated damages to SPU. The Commission at this time may award the contract to the next lower responsible bidder unless the Commission determines that public interest will be better served by accepting a higher bid, or the contract may be re-advertised.
- Rejecting Bids (and related Data Practices laws) - SPU has the right to reject any and all bids (requests for proposals, requests for bids, sealed bids). All data submitted in response to bid requests are private until bids are opened. If bids are rejected prior to the completion of the evaluation or selection process, all data, other than that made public at the bid opening, remain private until a re-solicitation of bids results in completion of the selection process. If the rejection occurs after the completion of the selection process, the data remain public. If a re-solicitation of bids does not occur within one year of the bid opening date, the remaining data become public.

D. Amendment

The contract cost, once established by the Commission, shall represent the maximum obligation to SPU. Any change orders that affect the cost of the contract shall be reviewed by the General Manager and SPU representative managing the contract. The General Manager has the authority to authorize a change order without Commission approval up to a maximum of 15% or \$150,000 of the contract price provided the original contract plus the change order does not exceed the authorized budget. If the change order exceeds this amount, then the General Manager and SPU representative managing the contract will forward the justification for the change order to the Commission for approval. In no event will payment in excess of the authorized budget be made until such approval has been obtained.

E. Bond Requirements

The vendor must execute to SPU a performance bond and a payment bond for public work over \$175,000 to protect SPU and all people furnishing work, equipment, materials, or supplies. An irrevocable letter of credit may be accepted in lieu of a performance bond.

No SPU contract is valid, nor may work commence on a bid contract, until the contractor provides a Performance Bond and a Labor and Materials Bond to SPU in accordance with state statute.

F. Certificate of Insurance

Before beginning work on a contract, the Contractor must submit to SPU, and obtain SPU's approval, on a certificate of insurance. This certificate shall be composed of a Standard Form C.I.C.C.-701 or an ACORD 25 form. The certificate of insurance shall list SPU as an additional insured, and shall be maintained at all times and survive termination or expiration of the contract, and provide for the following minimum coverage, unless mutually agreed otherwise:

- *Comprehensive General Liability:*

\$2,000,000.00 per occurrence;

\$4,000,000 aggregate

- *Automobile Liability for All Automobiles:* *\$2,000,000.00 combined single limit*
- *Workman's Compensation:* *Statutory Amounts*

The insurance cancellation language should state that the company will provide SPU 30 days' written notice of cancellation (include this requirement in bid specifications if applicable).

G. Guaranteed Energy Savings Agreements:

State Statutes authorize SPU to enter into a guaranteed energy savings agreement with a qualified provider for the purpose of implementing comprehensive utility cost-saving measures to improve the energy efficiency of various municipal facilities within SPU so long as the implementation costs will not exceed the amount to be saved in utility and maintenance costs over a twenty year period with said utility and maintenance cost savings guaranteed in writing by the qualified provider. SPU shall follow all requirements as prescribed in Statute related to this authority to enter into Guaranteed Energy Savings Agreements.



Purchasing/Contracts Policy

The Operating budget and Capital Improvement Plan (CIP) allocates funds for the purchase or payment of personnel, supplies, material, and contractual services. The Purchasing/Contract Policy is provided to all departments of the utility to provide guidance and direction to employees involved in the purchasing process. It is the policy of the utility to make purchases utilizing a competitive process to receive the best value. The competitive process may include verbal/written quotes, requests for proposals (RFP), and a formal bidding process. Requests cannot be made for items outside the budget except under special circumstances, which must be approved by the General Manager. The General Manager is the Purchasing Agent. Any deviation from this Purchasing and Contracts Policy must be approved by the commission. Purchasing authorization thresholds are summarized below:

- < \$2,500 – Supervisors
- < \$50,000 – Department Director or Superintendent
- < \$175,000 – General Manager
- ≥ \$175,000 – Commission (Follow Formal Bid Process)

PURCHASING AUTHORIZATION PROCESS

Purchasing: A purchase is defined as buying, renting, leasing or otherwise acquiring any goods and/or services for public purposes in accordance with laws, regulations, statutes, policies, and approved budgets. Non-inventory purchases up to \$2,500 do not require a purchase order. Non-inventory purchases over \$2,500 are procured via purchase order and need to follow the procedures and approvals outlined in Table 1. All inventory items are procured via purchase order and need to follow the procedures and approvals outlined in Table 1. Within the meaning of the definition of a purchase, the following are purchases that would **NOT** require a purchase order (some examples, not limited to the ones listed, that fall under this situation):

- Non – inventory purchases under \$2,500
- Recurring invoices in the normal course of business
- Public communications, i.e. telephone, newspaper ads etc.
- All Costs associated with education, training, workshops and conferences
- Professional Services
- Credit Card purchases (In accordance with the approved credit card policy and budget)
- Tuition reimbursement
- Lawyers (professional services)
- Accountants/Engineers/Consultants
- Healthcare providers (insurance contracts)

Recurring purchases – Purchases that recur in the normal course of business that may exceed dollar thresholds require two approvals from within the finance department for payment and do not require a purchase order. These are contractual accounts for services that are approved by the commission as part of the budget process. Some vendors, not limited to the ones listed, that fall under this situation include MMPA, Xcel Energy, PERA, League of MN Cities, health care providers and the State of Minnesota.

Professional services - Shakopee Public Utilities (SPU) is not required to use the competitive bidding process when contracting for professional services, such as those of engineers, lawyers, architects, and accountants, as well as other services requiring technical or professional training like lawn care services and janitorial services. Contracts for professional services will require review and approval by department directors and the general manager, within the dollar thresholds established in Table 1. Professional services do not require a purchase order as they are approved by the commission as part of the budget process.

Insurance contracts - SPU is not required to use the competitive bidding process for insurance contracts; however, SPU must seek requests for proposals for group insurance.

Table 1: Purchase & Bidding Authorizations and Requirements

Amount of Purchase:	Type of Quote Required:	Approval required by:	Written Specifications:	Sealed Bids Required:	Contract Required:	Purchase Order Required:
Purchases under \$2,500	Two telephone quotes are required when a good or service is available from more than 1 source or supplier, or when standardization or compatibility is not an overriding consideration, or in the open market.	Supervisor and above	As required based on type of purchase	No	No	No
Purchases between \$2,500 – \$25,000	Two written quotes are required when a good or service is available from more than 1 source or supplier, or when standardization or compatibility is not an overriding consideration, or in the open market.	Dept. Director or Superintendent	As required based on type of purchase	No	No	Yes
Purchases between \$25,000 – \$50,000	Three written quotes required when a good or service is available from more than 1 source or supplier, or when standardization or compatibility is not an overriding consideration or purchases through cooperative purchasing agreement.	Dept. Director or Superintendent	As required based on type of purchase	No	No	Yes
Purchases between \$50,000 – \$175,000	Three written quotes required when a good or service is available from more than 1 source or supplier, or when standardization or compatibility is not an overriding consideration or purchases through cooperative purchasing agreement.	General Manager provided purchase amount does not exceed amount authorized by CIP (See section D)	As required based on type of purchase	No	Construction Projects: Yes Commodities: At the discretion of General Manager	Yes
Purchases over \$175,000	General Manager or designee must advertise in SPU's legal newspaper.	Commission	Required	Yes	Yes	Yes
Capital Improvement Plan (CIP) Purchases – See section C.						

A. Responsible Contractor Compliance:

- A contractor responding to a solicitation document of a contracting authority shall submit to the contracting authority a signed statement under oath by an owner or officer verifying compliance with each of the minimum criteria in subdivision 3 of Minnesota Statutes, Section 16C.285 at the time that it responds to the solicitation document, and from subcontractors as provided in Section 16C.285, subdivision 4. A contracting authority may accept a signed statement under oath as sufficient to demonstrate that a contractor is a responsible contractor and shall not be held liable for awarding a contract in reasonable reliance on that statement. A prime contractor, subcontractor, or motor carrier that fails to verify compliance with any one of the required minimum criteria or makes a false statement under oath in a verification of compliance shall be ineligible to be awarded a construction contract on the project for which the verification was submitted. A false statement under oath verifying compliance with any of the minimum criteria may result in termination of a construction contract that has already been awarded to a prime contractor or subcontractor or motor carrier that submits a false statement. A contracting authority shall not be liable for declining to award a contract or terminating a contract based on a reasonable determination that contractor failed to verify compliance with the minimum criteria or falsely stated that it meets the minimum criteria. A verification of compliance need not be notarized. An electronic verification of compliance made and submitted as part of an electronic bid shall be an acceptable verification of compliance under this section, provided that it contains an electronic signature as defined in Minnesota Statutes, Section 325L.02, paragraph (h).

B. Cooperative Purchasing Contracts:

- For contracts estimated to exceed \$25,000, SPU may consider the availability, price, and quality of supplies, materials, or equipment available through the state cooperative purchasing venture before buying through another source.
- If SPU is not utilizing the state's cooperative purchasing venture, SPU may consider another national municipal association's purchasing alliance or cooperative created by a joint powers agreement that purchases items from more than one source on the basis of competitive bids or competitive quotations.

C. Bidding Requirements:

- When supplies or equipment are competitive in nature, specifications cannot exclude all but one type of equipment or supplies. Proposals and specifications must allow free and full competition. Bidding requirements cannot be avoided by splitting a contract into several contracts, each of which is below the minimum amount requiring sealed bids. For example, SPU cannot purchase \$200,000 of lumber in several transactions, each involving an expenditure of less than \$100,000. However, if materials or work logically fall into two separate contracts because they involve separate transactions, as for the service of contractors specializing in different kinds of work, there is no reason why SPU cannot negotiate the contracts individually without sealed bids if the bids do not exceed the \$175,000 minimum.
- Capital Improvement Plan (CIP) purchases – The CIP is approved by the Commission and is an adopted budget document; therefore, the expenditure has been formally authorized.
- Sales tax – Beginning January 1, 2015, purchases made by Shakopee Public Utilities are generally exempt from sales tax. Certain other exclusions are listed in Statute and should be reviewed on a regular basis. Bidders should specify whether their bid includes sales tax or not. After the work is completed and a purchase order is processed, if the invoice does not itemize sales tax, you must obtain a corrected invoice from the vendor if sales tax is applicable on the item purchased.
- Consultant services - State law does not require SPU to competitively bid contracts for professional services (i.e. attorney, architect, engineer, accountant, cleaning company, or other person with technical, scientific, or professional training such as refuse hauling).

- o Sealed bids are required for purchases exceeding \$175,000, and bids must be advertised by the General Manager or designee in SPU's legal newspaper (Notice to Bidders) and publicly opened and approved by the Commission. In addition to the legal notice, SPU must prepare instructions to bidders and general specifications for sealed bids. Attaching a copy of the proposed contract to the instructions to bidders is required. Sealed bids, including the number of bids received prior to bid opening, are nonpublic. Once opened, the name of the bidder and the dollar amount of the bid are public (all other data is private until completion of the selection process).
- o Bids vs. Quotes terminology – always use term quotation unless referring to a sealed bid.
- o Bid security (for sealed bids for purchases over \$175,000) in the amount of five percent (5%) of the bid shall be submitted to the General Manager. The bid security guarantees that in the event the bidder's offer is accepted, the bidder will enter into a contract in accordance with the proposal. Bid security of the successful bidder will be returned upon execution of the contract documents. Bid securities of unsuccessful bidders will be returned within a reasonable time period (Minnesota Statutes § 574.27). Failure of the successful bidder to execute the contract and furnish applicable bonds within ten (10) days after receiving written notice of the award shall cause the bid security to be forfeited as liquidated damages to SPU. The Commission at this time may award the contract to the next lower responsible bidder unless the Commission determines that public interest will be better served by accepting a higher bid, or the contract may be re-advertised.
- o Rejecting Bids (and related Data Practices laws) - SPU has the right to reject any and all bids (requests for proposals, requests for bids, sealed bids). All data submitted in response to bid requests are private until bids are opened. If bids are rejected prior to the completion of the evaluation or selection process, all data, other than that made public at the bid opening, remain private until a re-solicitation of bids results in completion of the selection process. If the rejection occurs after the completion of the selection process, the data remain public. If a re-solicitation of bids does not occur within one year of the bid opening date, the remaining data become public.

D. Amendment

The contract cost, once established by the Commission, shall represent the maximum obligation to SPU. ~~Any All~~ change orders that affect the cost of the contract shall be reviewed by the General Manager and SPU representative managing the contract. The General Manager has the authority ~~to authorize an individual change order without Commission approval up to a maximum of 15% of the contract price or \$150,000 of the contract price, whichever is less, as long as provided the sum of all change orders plus the original contract plus the change order does not exceed the authorized budget. The General Manager may require additional bonds in connection with a change order. If the change order exceeds this amount, If Commission approval is required, then the General Manager and SPU representative managing the contract will provide will forward the justification for the change order to the Commission for approval.~~ In no event will payment in excess of the authorized budget be made until such approval has been obtained.

E. Bond Requirements

The vendor must execute to SPU a performance bond and a payment bond for public work over \$175,000 (including any increase that the General Manager determines in connection with an authorized change order under Section D) to protect SPU and all people furnishing work, equipment, materials, or supplies. An irrevocable letter of credit may be accepted in lieu of a performance bond.

No SPU contract is valid, nor may work commence on a bid contract, until the contractor provides a Performance Bond and a Labor and Materials Bond to SPU in accordance with state statute.

F. Certificate of Insurance

Before beginning work on a contract, the Contractor must submit to SPU, and obtain SPU's approval, on a certificate of insurance. This certificate shall be composed of a Standard Form C.I.C.C.-701 or an ACORD 25 form. The certificate of insurance shall list SPU as an additional insured, and shall be maintained at all times and survive termination or expiration of the contract, and provide for the following minimum coverage, unless mutually agreed otherwise:

- *Comprehensive General Liability:* *\$2,000,000.00 per occurrence;
\$4,000,000 aggregate*
- *Automobile Liability for All Automobiles:* *\$2,000,000.00 combined single limit*
- *Workman's Compensation:* *Statutory Amounts*

The insurance cancellation language should state that the company will provide SPU 30 days' written notice of cancellation (include this requirement in bid specifications if applicable).

G. Guaranteed Energy Savings Agreements:

State Statutes authorize SPU to enter into a guaranteed energy savings agreement with a qualified provider for the purpose of implementing comprehensive utility cost-saving measures to improve the energy efficiency of various municipal facilities within SPU so long as the implementation costs will not exceed the amount to be saved in utility and maintenance costs over a twenty year period with said utility and maintenance cost savings guaranteed in writing by the qualified provider. SPU shall follow all requirements as prescribed in Statute related to this authority to enter into Guaranteed Energy Savings Agreements.



Proposed As Consent Item

3j

PO Box 470 • 255 Sarazin Street
Shakopee, Minnesota 55379
Main 952.445-1988 • Fax 952.445-7767
www.shakopeeutilities.com

TO: Greg Drent, General Manager *GD*
FROM: Brad Carlson, Director of Field Operations *BTC*
SUBJECT: Tower No.3 Recondition
DATE: July 24, 2025

Water Tower No. 3 is nearing completion. If you have the chance to catch a glimpse of the reconditioning project of Tower #3, it looks amazing. Staff wanted to touch base with the SPU Commission regarding the overall contract costs, which include contract change orders. The original contract price of \$1,336,990.00 was held with G&L Tanks Sandblasting and Coating, which has changed with approved change orders. The current contract price has increased to \$1,506,990.00. We remain within the \$2,000,000.00 budgeted amount for the Tower No.3 project. The following change orders are in addition to the original contract.

Original Contract Amount	\$1,336,990.00	(original contract bid)
Upgrade Add. Alternate No.1	\$40,000.00	(upgraded full wrap logo)
Change Order No.2	\$120,000.00	(interior dry full replacement)
Change Order No.3	\$8,000.00	(replace 2-overflow elbow)
Change Order No.4	<u>\$2,000.00</u>	(logo design add. stenciling)
New Contract Balance	\$1,506,990.00	

At this time, we are not looking for any approvals due to change orders, but we wanted to inform the Commission about the overall costs.

July 31st, 2025

TO: Greg Drent, General Manager *GD*

FROM: Philip Dubbe, IT Director *PD*

SUBJECT: IT Information Security Policy

Overview

Attached is the proposed policy for Information Security. This policy covers a wide array of topics which are important to the overall cybersecurity stance of the Utility. Many of these items have been done at the utility but without a formal policy. This policy will give the Utility consistent guidelines to follow moving forward.

Action Requested

Staff is requesting commission approval of the attached Information Security Policy to continue to standardize and enhance SPU's cybersecurity posture.

Shakopee Public Utilities (SPU) Information Security Policies



Pre-Commission Approval

July 31, 2025

Update to the Most Recent SPU Approval Date

(version 1.2)

Contents

Preambles	4
Purpose of this Policy	4
Definition of Information Security	5
Role and Responsibilities	5
Executive Management	5
IT Director:	6
IT Department.....	6
All Employees, Contractors, and Other Third-Party Personnel	7
Risk Management Program	7
Policy Maintenance.....	8
Revision History	8
Access Control.....	9
Purpose	9
Session Lockout:.....	10
Account Lockouts:.....	10
Password Criteria:	10
Remote Access and Virtual Escorting:	10
Account Management	12
Administrator/Special Access	13
Asset Management	14
Purpose	14
Hardware, Software, Applications, and Data.....	14
Backups	15
Change Management.....	15
Cloud Service Providers	16
Purpose:	16
Definitions and Terms:.....	16
Cloud Data Security.....	17
Encryption Policy.....	18

Purpose	18
Policy	18
SPU Encryption Standards (as of December 2024):	19
Human Resource Onboarding and Terminations	20
Onboarding	20
Terminations	20
Role Changes	20
Onboarding/Role Change/Termination Checklists	20
Identity Management	20
SPU Data Systems:	21
Unique Identification:	21
Authentication	21
Authentication Setup:	22
Multi-Factor Authentication:	23
Incident Response Procedures.....	24
Log Management, SIEM, MDR & Security Alerts	24
Audit Log Criteria	24
Response to Audit Processing Failures	25
Audit Monitoring, Analysis, and Reporting	25
Time Stamps.....	26
Protection of Audit Information	26
Audit Record Retention	26
Media Protection	26
Definition of Removable Media:	26
Policies concerning the Protection of Removable Media:	27
Encryption for Devices in Unsecure Locations:	27
Media Destruction & Re-Use:	27
Mobile Devices.....	29
General Mobile Security Controls:	29
Bluetooth Technologies:	Error! Bookmark not defined.
Mobile Hot Spots:	29
Mobile Device Management (MDMs) and Compensating Controls:	29
Network Security	31

Patch Management.....	32
Personally Identifiable Information (PII).....	32
Physical Security.....	33
Purpose	33
General.....	33
Access Cards.....	34
Housekeeping	34
Cabling Security.....	34
Surveillance Cameras and Recording Equipment	35
Maintenance & Utility Systems.....	35
Other Misc. Physical Security.....	35
Remote Access	37
System Configuration.....	37
Malicious Code and Spyware Protection:	37
Email Security:.....	38
Database Access and Database Password Management:	38
SNMP:	38
Additional Windows Security:.....	39
Change Management and Major Change Controls:	39
Vulnerability Management:	40
Wireless Security.....	41

Preambles

Purpose of this Policy

This policy stack has been created to comply with the NIST 800-53 and the Cybersecurity Framework (CSF) information security standards. These NIST standards require a wider range of executive management participation to enforce these Information Technology Security policies, in addition to the traditional involvement of the Information Technology Department and Information Security team(s).

Definition of Information Security

Information security, often referred to as InfoSec, refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection.

Application security is a broad topic that covers software vulnerabilities in web and mobile applications and application programming interfaces (APIs). These vulnerabilities may be found in authentication or authorization of users, integrity of code and configurations, and mature policies and procedures. Application vulnerabilities can create entry points for significant InfoSec breaches. Application security is an important part of perimeter defense for InfoSec.

Cloud security focuses on building and hosting secure applications in cloud environments and securely consuming third-party cloud applications. “Cloud” simply means that the application is running in a shared environment. Businesses must make sure that there is adequate isolation between different processes in shared environments.

An effective information security program should cover key elements such as management's commitment to information security, the need to comply with information security requirements, personal accountability, basic information on security procedures, and key contact points (for additional information and incident reporting).

Role and Responsibilities

Role	Responsibilities to this Policy
IT Director	<ul style="list-style-type: none">Review Draft Policy Requirements
IT Staff	<ul style="list-style-type: none">Implement Policy Requirements
General Manager	<ul style="list-style-type: none">Approve Policy Requirements
vCISO	<ul style="list-style-type: none">Develop Draft Policy Requirements
Board of Commissioners	<ul style="list-style-type: none">Final Approval, if appropriate

Executive Management

- Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of the SPU.
- Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.
- Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.
- Ensure that the IT Department is given the necessary authority to secure the Information Resources under their control within the scope of the SPU Information Security Program.

- Designate an IT Director and delegate authority to that individual to ensure compliance with applicable information security requirements.
- Ensure that the IT Director, in coordination with the IT Department, reports annually to Executive Management on the effectiveness of the SPU Information Security Program.

IT Director:

- Chairs the IT Department and provide updates on the status of the Information Security Program to Executive Management.
- Manage compliance with all relevant statutory, regulatory, and contractual requirements.
- Participate in security related forums, associations and special interest groups.
- Assess risks to the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of SPU.
- Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.
- Ensure that SPU has trained all personnel to support compliance with information security policies, processes, standards, and guidelines. Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities.
- Ensure that appropriate information security awareness training is provided to SPU personnel, including contractors.
- Implement and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of SPU.
- Develop and implement procedures for testing and evaluating the effectiveness of the SPU Information Security Program in accordance with stated objectives.
- Develop and implement a process for evaluating risks related to vendors and managing vendor relationships.
- Report annually, in coordination with the IT Department, to Executive Management on the effectiveness of the SPU Information Security Program, including progress of remedial actions.
- Conduct or Analyze Information Technology Risk Assessments
- Advise IT Department and Executive Management on applicable Compliancy Requirements (e.g. CJIS, HIPAA, PCI, etc)
- Prioritize and Remediate identified Remediation projects and tasks from various Risk Assessments
- Accelerate Information Security Tasks to preserve valuable staff time for routine Information Technology Tasks
- To help prevent and assist in the handling of Information Technology Security Incidents
- To research and act upon security matters that are relevant to the SPU before they become addressed in security standards (e.e NIST 800-53, CSF, CJIS, etc)

IT Department

- Ensure compliance with applicable information security requirements.
- Formulate, review and recommend information security policies.
- Approve supporting procedures, standards, and guidelines related to information security.
- Provide clear direction and visible management support for information security initiatives.

- Assess the adequacy and effectiveness of the information security policies and coordinate the implementation of information security controls.
- Ensure that ongoing security activities are executed in compliance with policy.
- Review and manage the information security policy waiver request process.
- Review information security incident information and recommend follow-up actions.
- Promote information security education, training, and awareness throughout SPU, and initiate plans and programs to maintain information security awareness.
- Report annually, to Executive Management on the effectiveness of the SPU Information Security Program, including progress of remedial actions.

All Employees, Contractors, and Other Third-Party Personnel

- Understand their responsibilities for complying with the SPU Information Security Program.
- Use SPU Information Resources in compliance with all SPU Information Security Policies.
- Seek guidance from the Information IT Department for questions or issues related to information security.

Risk Management Program

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the SPU Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we conduct business. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

- Confidentiality – Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the classic “need-to-know” principle.
- Integrity – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
- Availability – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

SPU has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which other information security policies may be developed to ensure that the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to SPU by its stakeholders, partners, customers and other third-parties.

The SPU Information Security Program is built around the information contained within this policy and its supporting policies.

Policy Maintenance

This entire policy should be reviewed on an annual basis by the vCISO and IT Director. Recommendations for changes shall be made to the SPU Manager for approval before the end of each calendar year. Changes shall be updated to the SPU's Information Security Risk Assessment on an annual basis, to comply with the NIST standards.

Revision History

Version	Date	Role	Description of Change
1.0	12/9/24	vCISO	Original Draft
1.1	1/24/25	IT Director, vCISO	Review of Draft
1.2	7/10/25	IT Director, Network Admin, vCISO	2 nd formal review
1.3 (TBD)	TBD	General Manager	Final Review
1.4 (TBD)	TBD	SPU Board of Commissioners	If needed

Access Control

Purpose

The purpose of this procedure is to limit the access to SPU Data to only those that are authorized and need it to complete their job duties. To accomplish this, the following procedures shall be followed:

1. Users shall be granted access to SPU Data according to the Identity and Authentication Procedure set forth below.
2. Access and Permissions to SPU Data shall be maintained by system administrators, information system security officers, maintainers, and system programmers, as determined by the SPU IT Director or designee.
3. Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by The SPU to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.
4. The SPU IT Department shall limit access to SPU Data to only authorized personnel with the need-to-know.
5. Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the SPU IT Department record retention policy, whichever is greater.

Access Control can be achieved by one or more of the following Criteria and Mechanisms:

1. Job assignment or function (e.g., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given SPU may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.
6. Access Control Lists (ACLs).
7. Application user rights/roles.

Session Lockout:

1. All Devices shall have an automatic lockout after a maximum of 30 minutes of inactivity;
2. Devices that are located in a Secure Location (e.g., Squad Car Mobile Data Communicator (MDC)) shall be exempt from this criteria for the purposes of officer safety;

Account Lockouts:

1. Systems shall enforce an automatic lockout after 5 unsuccessful login attempts, which shall last for a minimum of 30 minutes;
2. An account administrator may unlock the account with just cause;

Password Criteria:

Minimum: 12 characters

Last 10 passwords can't be repeated

Suggested complexity requirements and no dictionary words

Remote Access and Virtual Escorting:

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort;
2. The escort shall be familiar with the system/area in which the work is being performed;
3. The escort shall have the ability to end the session at any time;
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path; and
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session.
6. All remote access connections to the SPU networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.
7. Remote users may connect to the SPU networks only after formal approval by the requestor's manager or SPU Management.
8. The ability to print or copy confidential information remotely must be disabled.
9. Users granted remote access privileges must be given remote access instructions and responsibilities.
10. Remote access to Information Resources must be logged.
11. Remote sessions must be terminated after a defined period of inactivity.
12. A secure connection to another private network is prohibited while connected to the SPU network unless approved in advance by SPU IT management.

13. Non-SPU computer systems that require network connectivity must conform to all applicable SPU IT standards and must not be connected without prior written authorization from IT Management.
14. Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.

Account Management

- All personnel must sign the SPU Information Security Policy Acknowledgement before access is granted to an account or SPU Information Resources.
- All accounts created must have an associated, and documented, request and approval.
- Segregation of duties must exist between access request, access authorization, and access administration.
- Information Resource owners are responsible for the approval of all access requests.
- User accounts and access rights for all SPU Information Resources must be reviewed and reconciled at least annually, and actions must be documented.
- All accounts must be uniquely identifiable using the username assigned by SPU IT and include verification that redundant user IDs are not used.
- All accounts, including default accounts, must have a password expiration every 90 days
- Only the level of access required to perform authorized tasks may be approved, following the concept of “least privilege”.
- Whenever possible, access to Information Resources should be granted to user groups, not granted directly to individual accounts.
- Shared accounts must not be used. Where shared accounts are required, their use must be documented and approved by the Information Resource owner.
- User account set up for third-party cloud computing applications used for sharing, storing and/or transferring SPU confidential or internal information must be approved by the resource owner and documented.
- Upon user role changes, access rights must be modified in a timely manner to reflect the new role.
- Creation of user accounts and access right modifications must be documented and/or logged.
- Any accounts that have not been accessed within a defined period will be disabled.
- Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
- System Administrators or other designated personnel:
 - Are responsible for modifying and/or removing the accounts of individuals that change roles with SPU or are separated from their relationship with SPU.
 - Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.
 - Must have a documented process for periodically reviewing existing accounts for validity.
 - Are subject to independent audit review.
 - Must provide a list of accounts for the systems they administer when requested by authorized SPU IT management personnel.
 - Must cooperate with authorized SPU Information Security personnel investigating security incidents at the direction of SPU executive management.

- privileged user account management approval, use, and removal of privileged user accounts. All users of such accounts should be briefed on the policy and formally trained. Additional guidance for the use of privilege can be found in NIST SP 800-53 AC-6 (<https://nvd.nist.gov/800-53/Rev4/control/AC-6>)

Administrator/Special Access

- Administrative/Special access accounts must have account management instructions, documentation, and authorization.
- Personnel with Administrative/Special access accounts must refrain from abuse of privilege and must only perform the tasks required to complete their job function.
- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Shared Administrative/Special access accounts should only be used when no other option exists.
- The password for a shared Administrative/Special access account must change when an individual with knowledge of the password changes roles, moves to another department or leaves SPU altogether.
- In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency.

Asset Management

Purpose

The purpose of the SPU Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by SPU.

The SPU Asset Management Policy applies to individuals who are responsible for the use, purchase, implementation, and/or maintenance of SPU Information Resources

Asset inventories should be formally reconciled on no less than an annual basis; however, the shorter the time between reconciliation, the better. The sooner that an asset can be identified as lost or stolen, the sooner a response can be initiated.

Hardware, Software, Applications, and Data

- All hardware, software and applications must be approved by SPU IT.
- Installation of new hardware or software, or modifications made to existing hardware or software must follow approved SPU procedures and change control processes.
- All purchases must follow the defined SPU Purchasing Policy.
- Software used by SPU employees, contractors and/or other approved third-parties working on behalf of SPU, must be properly licensed.
- Software installed on SPU computing equipment, outside of that noted in the SPU Standard Software List, must be approved by IT Management and installed by SPU IT personnel.
- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
- The use of cloud computing applications must be done in compliance with all laws and regulations concerning the information involved, e.g. personally identifiable information (PII), protected health information (PHI), corporate financial data, etc.
- Two-factor authentication is recommended for external cloud computing applications with access to any confidential information for which SPU has a custodial responsibility.
- Contracts with cloud computing applications providers must address data retention, destruction, data ownership and data custodian rights.
- Hardware, software, and application inventories must be maintained continually and reconciled no less than annually.
- A general inventory of information (data) must be mapped and maintained on an ongoing basis.
- All SPU assets must be formally classified with ownership assigned.
- Maintenance and repair of organizational assets must be performed and logged in a timely manner and managed by SPU IT Management.
- SPU assets exceeding a set value, as determined by management, are not permitted to be removed from SPU's physical premises without management approval.
- All SPU physical assets exceeding a set value, as determined by management, must contain asset tags or a similar means of identifying the equipment as being owned by SPU.

- If a SPU asset is being taken to a High-Risk location, as defined by the FBI and Office of Foreign Asset Control, it must be inspected and approved by IT before being taken offsite and before reconnecting to the SPU network.
- Confidential information must be transported either by an SPU employee or a courier approved by IT Management.
- Upon termination of employment, contract, or agreement, all SPU assets must be returned to SPU IT Management.

Backups

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the information owner.
- The SPU backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for SPU must be formally approved to handle the highest classification level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest SPU sensitivity level of information stored.
- A process must be implemented to verify the success of the SPU electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of data damage or loss.
- Procedures between SPU and the offsite backup storage vendor(s) must be reviewed at least annually, preferably as part of a Disaster Recover (DR) Plan
- Backups containing confidential information must be encrypted.
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
 - System name
 - Creation Date
 - Sensitivity Classification
 - SPU Contact Information

Change Management

- Change documentation must include, at a minimum:
 - Date of submission and date of change,
 - Include Owner and custodian contact information,
 - Nature of the change,
 - Change requestor,
 - Roll-back plan, if appropriate
 - Change approver,
 - Change implementer, and
 - An indication of success or failure, after the change is completed

- Changes with a significant potential impact to SPU Information Resources must be scheduled.
- SPU Information Resource owners must be notified of changes that affect the systems they are responsible for.
- Authorized change windows must be established for changes with a high potential impact.
- Changes with a significant potential impact and/or significant complexity must have usability, security, and impact testing and back out plans included in the change documentation.
- Change control documentation must be maintained in accordance with the SPU Information Retention Schedule.
- Changes made to SPU customer environments and/or applications must be communicated to customers, in accordance with governing agreements and/or contracts.
- All changes must be approved by the Information Resource Owner, Director of Information Technology, or Change Control Board (if one is established).
- Emergency changes that require an immediate implementation (i.e. break/fix, incident response, etc.) may be implemented without following the formal change control process, but may not circumvent documentation requirements, even if documented after the change.

Cloud Service Providers

Purpose:

This policy is provided to define and describe cloud computing, discuss compliancy, detail security and privacy, and provide general recommendations. Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Common examples of cloud computing applications are OneDrive, SharePoint, Dropbox, Facebook, Google Drive, Salesforce, and Box.com, canva.com.

With many local government organizations looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is viable business solution. But the unique security and legal characteristics of local government organizations means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be done with policy compliance concerns such as HIPAA, DHS, IRS, CJIS, PCI and/or PII.

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection,
perhaps on behalf of a subscriber
Cloud provider – An organization that provides cloud services

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service, and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- a. readiness of existing applications for cloud deployment
- b. transition costs
- c. life-cycle costs
- d. maturity of service orientation in existing infrastructure
- e. security and privacy requirements – federal, state, and local

Cloud Data Security

- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
- The use of cloud computing applications must be done in compliance with all laws and regulations concerning the information involved, e.g. (PCI, HIPAA, CJIS, PII, etc).
- Two-factor authentication is recommended for external cloud computing applications with access to any confidential information for which SPU has a custodial responsibility.
- Contracts with cloud computing applications providers must address data retention, destruction, data ownership and data custodian rights.

Encryption Policy

Purpose

The purpose of the Encryption Policy is to establish the rules for acceptable use of encryption technologies relating to SPU's Information Resources.

Policy

1. All encryption technologies and techniques used by SPU must be approved by SPU IT Department.
2. SPU IT Department is responsible for the distribution and storage of all encryption keys.
3. All use of encryption technology should be managed in a manner that permits properly designated SPU personnel to promptly access all data, including for purposes of investigation and business continuity.
4. Only encryption technologies that are approved, managed, and distributed by SPU IT may be used in connection with SPU Information Resources.
5. SPU IT Department will create and publish the SPU Encryption Standards, which must include, at a minimum:
 - a. The type, strength, and quality of the encryption algorithm required for various levels of protection.
 - b. Key lifecycle Department, including generation, storing, archiving, retrieving, distributing, retiring, and destroying keys.
6. All SPU information classified as confidential must be encrypted when:
 - a. Transferred electronically over public networks.
 - b. Stored on mobile storage devices.
 - c. Stored on laptops or other mobile computing devices.
 - d. At rest.
7. The use of proprietary encryption algorithms is not permitted, unless approved by SPU IT Department
8. The use of encryption for any data transferred outside of the United States must be formally approved by SPU IT Department prior to transfer.

SPU Encryption Standards (as of July 2025):

Whenever possible:

Firewall VPN's: AES-128 (preferably AES-256)

IPSec: IKEv2

HTTPS: TLS 1.2

SSL Certs: RSA-2048

WiFi:

Minimum: WPA2 (Preferably WPA3)

Preferable:

At Rest Data Encryption: Bitlocker or similar

Human Resource Onboarding and Terminations

Onboarding

Preparing new hires for their jobs takes many steps, and many of them set the entire tone for your employer/employee relationship going forward. Using an onboarding checklist lets you tick those steps off your to-do list as you go so you don't omit crucial items during those first busy days, weeks and months. Let's take a comprehensive look at the topic of onboarding so you know what the process entails and what steps to include on your onboarding checklist.

Terminations

Hiring managers should inform HR promptly when termination occurs. As soon as possible, HR should send a list summarizing termination and instruct IT to suspend their access within the requested amount of business days. For any High-Risk Terminations, this should be done immediately.

As much as possible, these steps should be triggered by automation and should not require manual intervention.

Removing access is especially important for any members of the IT and security staff. Users often have network-wide access and could make quickly make significant changes in the environment very quickly. Revoking their access from all systems immediately upon termination is critical.

Role Changes

When an employee changes roles within the organization, their account access and permission levels should change accordingly. Too often, when users get promoted within the organization, they retain access rights from their previous position, which may be excessive or inappropriate for their new job. Like the onboarding process, hiring managers should inform HR of any role change. Then HR and IT will follow the same steps for onboarding and offboarding to provision new access.

Onboarding/Role Change/Termination Checklists

HR and IT should develop an Onboarding/Role Change/Termination Checklist to document these steps and ensure access control is granted/changed and terminated in a consistent and effective manner.

Identity Management

The purpose of this procedure is to ensure that the SPU IT Department can identify each unique user who is authorized to access SPU Data through any of the SPU Data Systems that the SPU IT Department uses. The second purpose of this procedure is to prove that the unique person accessing SPU Data is really them, by using authentication methods such as passwords, PINs, and other Multi-Factor Authentication methods.

SPU Data Systems:

The SPU's Account Administrator for each application shall be responsible for adding new users and disabling/deleting users once their access has been revoked.

Unique Identification:

Username must be unique. They can take the form of a full name, email address, employee number, or other unique alphanumeric identifier.

Authentication

- Personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- Password history must be kept to prevent the reuse of passwords.
- Unique passwords should be used for each system, whenever possible.
- Where other authentication mechanisms are used (i.e. security tokens, smart cards, certificates, etc.) the authentication mechanism must be assigned to an individual, and physical or logical controls must be in place to ensure only the intended account can use the mechanism to gain access.
- Stored passwords are classified as confidential and must be encrypted.
- All vendor-supplied default passwords should be immediately updated and unnecessary default accounts removed or disabled before installing a system on the network.
- User account passwords must not be divulged to anyone. SPU support personnel and/or contractors should never ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with SPU, if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- Administrators/Special Access users must not circumvent the SPU Authentication Standard for the sake of ease of use.
- Users should not circumvent password entry with application remembering embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the SPU IT Management.
- With a password management system employed, it must be used in compliance with the SPU Authentication Standard.
- Computing devices should not be left unattended without enabling a password protected screensaver or logging off of the device.
- SPU IT Support password change procedures must include the following:
 - authenticate the user to the helpdesk before changing password
 - change to a strong password
 - require the user to change password at first login.
- In the event that a user's password is compromised or discovered, the password must be immediately changed, and the security incident reported to SPU IT support.

Authentication Setup:

- Temporary Password for setup, then the user shall change it to a unique password of their own.
- Where multifactor authentication is employed, user identification must be verified in person before access is granted.

Multi-Factor Authentication:

When accessing SPU data from an unsecure location, and using VPN Access, users should also use Multi-Factor Authentication:

1. Access the SPU systems via a VPN tunnel using the SPU provided VPN solution;
2. Human Resources and/or Department Head, determines business need for the use of the VPN and level of access before a token can be issued;
3. VPN setup shall be carried out by IT Department
4. Each user shall get a unique VPN username and password;
5. Revocation shall be approved from Human Resources and/or Department Head, upon termination, lost token (if applicable), or other reason(s);
6. VPN disablement shall be carried out by IT Department

Incident Response Procedures

Refer to SPU's IR Plan (or more recent version).

DRAFT SPU Incident Response Plan July 2025.docx

Log Management, SIEM, MDR & Security Alerts

SPU shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. SPU shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components. Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the SPU. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with the SPU assessment of risk.

SPU's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. SPU shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems. SPU's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. SPU shall periodically review and update the list of SPU-defined auditable events. In the event SPU does not use an automated system, manual recording of activities shall still take place.

Audit Log Criteria

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
 - a. access permission on a user account, file, directory or other system resource;
 - b. create permission on a user account, file, directory or other system resource;
 - c. write permission on a user account, file, directory or other system resource;
 - d. delete permission on a user account, file, directory or other system resource;
 - e. change permission on a user account, file, directory or other system resource.

3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
 - a. access the audit log file;
 - b. modify the audit log file;
 - c. destroy the audit log file.

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

[Response to Audit Processing Failures](#)

SPU's information system shall provide alerts to appropriate SPU officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

[Audit Monitoring, Analysis, and Reporting](#)

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of and SPU's processing

indicates an elevated need for audit review. SPU shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to SPU operations, SPU assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Time Stamps

SPU's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. SPU shall synchronize internal information system clocks on an annual basis.

Protection of Audit Information

SPU's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

Audit Record Retention

SPU shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, SPU shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.

Media Protection

The purpose of this procedure is to protect SPU Data that may be found on computer and server hard drives, removable storage devices (e.g. USB drives or flash drives, mobile tablets or laptops and smartphones). For the same reason that if you delete a file by accident, you can often recover it using data recovery software, also makes it difficult to truly destroy protected data when disposing of these devices.

Definition of Removable Media:

Media includes computer hard drives, SAN or NAS media, removable storage USB drives, backup tapes, Multi-Function Printer hard drives, Printer hard drives, CDs, and floppy disks.

Policies concerning the Protection of Removable Media:

- The use of removable media for storage of SPU Information must be supported by a reasonable business case.
- All removable media use must be approved by SPU IT Department prior to use.
- Personally owned removable media use is not permitted for storage of SPU information.
- Users are not permitted to connect removable media from an unknown origin, without prior approval from SPU IT Department.
- Confidential and internal SPU information should not be stored on removable media without the use of encryption.
- The loss or theft of a removable media device that may have contained SPU information must be reported to the SPU IT Department.
- SPU will maintain inventory logs of all media and conduct media inventories at least annually.
- The transfer of information to removable media will be monitored.
- All staff that handles paper media that contains SPU Data shall ensure that these documents are stored in Secured Locations so that people that are not authorized to handle the SPU Data cannot access it;
- Any loss or theft of Paper Media and/or Mobile Devices shall be immediately reported to the SPU IT Department.

Encryption for Devices in Unsecure Locations:

Any device that contains SPU Data must be encrypted if it is in an unsecure location. The SPU IT Department shall accomplish this in the following manners:

- Servers / Workstations
- Mobile Devices – shall use hard drive encryption [e.g. BitLocker].
- Smartphone or Mobile Tablets shall use an MDM solution [e.g. Meraki or MS Intune].

Media Destruction & Re-Use:

- Media that may contain confidential or internal information must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
- All decommissioned media must be stored in a secure (locked) area prior to destruction.
- All information must be destroyed when no longer needed, included encrypted media.

- SPU IT shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.).
- SPU IT shall maintain written documentation of the steps taken to sanitize or destroy electronic media.
- SPU IT shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.
- SPU IT Department shall consult NIST Guidelines for Media Sanitation for further information:
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

Mobile Devices

The purpose of this procedure is to give the SPU IT Department the necessary procedure needed when dealing with mobile devices such as iPads, tablets, mobile laptops, MDCs, and other similar mobile devices that contain or access SPU Data.

General Mobile Security Controls:

At a minimum, all mobile devices shall have the same security controls as non-mobile devices that are connected to the SPU Network via physical connect (e.g. Ethernet cable). In addition, there will be additional controls or limitations, based on the nature of the non-physical connection type.

Mobile Hot Spots:

Isolated Mobile Hotspots (e.g. Verizon MiFi) that provide isolated internet cellular access, shall implement all Mobile Device Security Controls, whenever possible.

Tethered Mobile Hot Spots (e.g. a laptop wired to a SPU network, that also allows 802.11 connections through the laptop to the SPU Network) shall have these additional Security Control in place, whenever possible:

1. Enable encryption on the hotspot, WPA-2 or stronger.
2. Change the hotspot's default SSID
3. Ensure the hotspot SSID does not identify the device make/model or SPU ownership
4. Create a wireless network password (Pre-shared key) consistent with the Wireless 802.11 requirements described above;
5. Enable the hotspot's port filtering/blocking features if present; and
6. Only allow connections from SPU controlled devices

Mobile Device Management (MDMs) and Compensating Controls:

Use an MDM Solution for securing your mobile devices that handle SPU Data, whenever possible. When doing so, the MDM should handle as many of the following items as possible:

1. Remote locking of device;
2. Remote wiping of device;
3. Setting and locking device configuration;
4. Detection of "rooted" and "jailbroken" devices;
5. Enforcement of folder or disk level encryption;
6. Application of mandatory policy settings on the device;
7. Detection of unauthorized configurations;
8. Detection of unauthorized software or applications;

9. Ability to determine the location of SPU controlled devices;
10. Automatic device wiping after a specified number of failed access attempts.

Network Security

- SPU IT Department owns and is responsible for the SPU network infrastructure and will continue to manage further developments and enhancements to the infrastructure.
- To provide a consistent network infrastructure capable of leveraging new networking developments, all cabling must be installed by SPU IT Department or an approved contractor.
- Information security requirements must be included in any new information system or enhancements to the existing system.
- Appropriate technical solutions must be implemented to protect Confidential information from unauthorized transfer, modification, or disclosure (i.e. next-gen firewalls, IDS/IPS, DLP).
- A map or diagram of the network and data flow, including external connections, must be maintained. This map or diagram must be updated after any changes to the network occur. This diagram should be reviewed every 6 months to ensure it continues to represent the network architecture
- All systems on the network must be authenticated. Connections to the network must be authorized by IT Department.
- All hardware connected to the SPU network is subject to SPU IT management and monitoring standards.
- Resource usage should be monitored to ensure the required system performance.
- Information processing facilities must address redundancy sufficient to meet availability requirements.
- Changes to the configuration of active network management devices must be made according to the Change Control Policy.
- The SPU network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by SPU IT Management.
- All connections of the network infrastructure to external third-party networks are the responsibility of SPU IT Department.
- Groups of information services, users and information systems must be segregated on the network. The perimeter of each domain should be well defined and based on the relevant security requirements.
- Network devices must be installed and configured following SPU implementation standards.
- The use of departmental network devices is not permitted without the written authorization from SPU IT Management.
- Non-IT Department Personnel are not permitted to access or alter existing network hardware in any way.

Patch Management:

1. Applications and Network devices shall be patched on a monthly basis (or as close to monthly as possible);
2. Wherever possible, patches shall be installed in a test environment first with the ability to roll back if it breaks the OS or any application;
3. Regular scans should be run to detect missing updates. Patch management software should be reviewed for missing updates.
4. A patch management that is handled by their trusted third party Managed Service Provider, shall be used to centrally manage the patching of all devices;
5. Additional patching shall occur when warranted by a critical vulnerability or results of a vulnerability assessment;

Personally Identifiable Information (PII)

The purpose of this procedure is to ensure that SPU protects the Personally Identifiable Information (PII) that resides in its data stored in computer systems.

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any provided data maintained by SPU, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. .

The SPU shall ensure that the following Security Controls are in place:

1. Access to PII shall be restricted by "need only" basis;
2. Access Control and Authentication Policies to PII shall be the same as required by the Access Control and Authentication Procedure.

For Additional Requirements for Minnesota Statutes on Personal Identifiable Information (PII):

<https://www.revisor.mn.gov/statutes/cite/325e.61>

<https://www.revisor.mn.gov/statutes/2018/cite/325E.59>

<https://www.revisor.mn.gov/statutes/cite/13>

What data is PII?

Any combination of two or more of the following items can be used to compromise a person's identity:

- Name
- DOB/Place of Birth
- Home Address/Telephone Number/Email Address
- Social Security Number

- Financial Data
- Employment History
- Mother's Maiden Name
- Driver's License Number
- Vehicle License Number
- Non Public Photos
- Fingerprints, DNA, Iris Scans
- Health Information
- Criminal History

Physical Security

Purpose

Physical security keeps SPU employees, facilities, and assets safe from real-world threats. These threats can arise from internal or external intruders that question data security. Physical attacks can cause a safe area to break into or the invasion of a restricted area part.

General

- Physical security systems must comply with all applicable regulations including but not limited to building codes and fire prevention codes.
- Physical access to all SPU restricted facilities must be documented and managed.
- All Information Resource facilities must be physically protected in proportion to the criticality or importance of their function at SPU.
- Access to Information Resources facilities must be granted only to SPU support personnel and contractors whose job responsibilities require access to that facility.
- All facility entrances, where unauthorized persons could enter the premises, must be controlled.
- Secure areas must be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. This includes:
 - information processing facilities handling confidential information should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;
 - controls should be adopted to minimize the risk of potential physical and environmental threats;
 - environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities.
- Directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.
- Equipment must be protected from power failures and other disruptions caused by failures in utilities.
- Restricted access rooms and locations must have no signage or evidence of the importance of the location.
- All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.

- Card access records and visitor logs for Information Resource facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- Visitors in controlled areas of Information Resource facilities must be accompanied by authorized personnel at all times.
- Personnel responsible for Information Resource physical facility management must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

Access Cards

- The process for granting card and/or key access to Information Resource facilities must include the approval of a member of the IT Department.
- Each individual that is granted access rights to an Information Resource facility must sign the appropriate access and non-disclosure agreements.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to personnel responsible for Information Resource physical facility management. Cards must not be reallocated to another individual, bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for Information Resource physical facility management physical security administrator as soon as possible.
- IT Department must remove the card and/or key access rights of individuals that change roles within SPU or are separated from their relationship with SPU.
- IT Department must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

Housekeeping

- No combustible materials are to be stored in the Critical IT Space.
- Equipment racks cannot be used for storage.
- Notes and/or miscellaneous papers or network documentation cannot be taped to walls or racks.
- Parts and other items that need to be in the Critical IT Space must be stored in an enclosed cabinet.

Cabling Security

- Cabling, Racks and equipment are clearly labeled.
- Cabling in public hallways is concealed in ceiling or covered and protected by conduit
- All cabling in Critical IT Space is routed neatly in overhead ladder trays, where available, or neatly otherwise.

- All cabling in cabinets/racks is neatly routed along the side of the cabinet/rack.
- All abandoned and/or unused cabling is removed when a piece of equipment is removed or decommissioned.
- If cable locking racks is not feasible, a camera is set up to monitor each aisle 24x7x365
- cabling suppliers, cabling installation and authorized installers are approved by management and have the appropriate background checks in place

Surveillance Cameras and Recording Equipment

- Cameras monitoring the Critical IT Space must have a full coverage view of the infrastructure. Full coverage means there is no reasonable way an individual can move through the equipment without being seen by the monitoring system.
- The cameras must be monitored on a 24x7x365 basis by [video administrator]
- The cameras must record whenever they sense motion in the Critical IT Space. These recordings must be kept for a minimum of 45 days.
- If there is a need to take photos or videos of the Critical IT Space, there must be documented pre-approval. The pre-approval must come from ITS FTS management. Approval will only be granted for valid business justifications. Additional, documented approval is required to publish these photos or videos. This approval must also come from ITS FTS management.

Maintenance & Utility Systems

- Maintenance of Critical IT Space should be documented.
- Sensors for Environmental controls should be installed and monitored including: temperature, humidity, and water sensors
- Any water presence in a Critical IT Space that is noticed should be recorded and a ticket submitted to the correct responsible group.
- Cleaning schedule is maintained.
- Food and drink are not permitted in the Critical IT Space.
- An assurance check is performed on a quarterly basis to ensure all Minimum Physical Security Standards for Highly Critical IT Spaces are in place.
- Lighting is adequate to ensure activities can be performed safely.
- All physical safety and emergency procedures are visibly posted.
- Maintenance contractors and personnel have to be authorized and approved by management and have the appropriate background checks in place.

Other Misc. Physical Security

- All entrances to the Critical IT Space must have a sign that states this a “Authorized Personnel Only.”
- A sign must be posted stating no photography or video permitted without consent.

- A sign must be posted stating that no food or drink is permitted in the Critical IT Space.
- All power sources are clearly labeled.

Remote Access

1. All remote access connections to the SPU networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.
2. Remote users may connect to the SPU networks only after formal approval by the requestor's manager or SPU Management.
3. Users granted remote access privileges must be given remote access instructions and responsibilities.
4. Remote access to Information Resources must be logged.
5. Remote sessions must be terminated after a defined period of inactivity.
6. A secure connection to another private network is prohibited while connected to the SPU network unless approved in advance by SPU IT management.
7. Non-SPU computer systems that require network connectivity must conform to all applicable SPU IT standards and must not be connected without prior written authorization from IT Management.
8. Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.
9. If privately-owned teleworking equipment use is permitted, document policies and procedures to prevent disputes concerning rights to intellectual property developed on privately-owned equipment.
10. Confidential conversations should only take place in controlled environments. Ensure that personnel are reminded regularly to not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.

System Configuration

These policies apply to SPU owned devices. Personal devices, with or without SPU MDM security software, will be addressed in the SPU's future BYOD Policy.

Malicious Code and Spyware Protection:

1. All devices on the SPU network, or connecting to the SPU network, shall have endpoint protection against malicious code (typically referred to as Anti-Virus Software);
2. Common sense precautions should be taken. Users shall practice caution when visiting websites, downloading files and opening email attachments. Also, users shall not change their system's configuration or take other steps to defeat virus protection devices or systems.
3. Anti-Virus software shall be kept updated with automatic updates;
4. Anti-Ransomware monitoring shall also be in place for the network;
5. Host and/or network-based Intrusion Protection Software/application
6. Security Alerts shall be setup to alert the SPU IT Department when malware is detected

Email Security:

1. Email is to be processed through antivirus/malware filtering software before being delivered to the SPU's.
2. Anti-SPAM software shall be used to filter incoming email systems used by devices in a SPU network (i.e. ProofPoint or O365 SPAM filtering service);
3. Emails with common attachments known to carry viruses/malware, e.g. .exe, must be eliminated from the email.
4. Outbound SMTP email must be eliminated from all non-email servers.
5. Email servers must be tested and verified that open relay is shut off on the server.
6. Email being sent cannot violate any Federal or State laws.
7. Web access to SPU's email systems must utilize SSL certificates for encryption.
8. Email should be filtered through an email filtering product to help eliminate SPAM email
9. Web access to SPU's email systems should utilize an SSL certificate from a vendor that is in the default CA list of a home user's browser.
10. Add DNS TXT SPF (Sender Policy Framework) records to limit forged spam effects.
11. Add DNS TXT DKIM (Domain Keys Identified Mail) and Configure DKIM Encryption Keys / Selector records to limit forged spam effects.
12. Implementation of Domain based Message Authentication, Reporting and Conformance (DMARC).
13. Where possible, MFA for email web access should be utilized.
14. Internet email web access servers installed at the SPU site should be installed in a DMZ to help protect the internal network environment.

Database Access and Database Password Management:

All SQL database users must have passwords defined. All DBA user passwords must conform to the system-level password requirements. All DBA passwords are only to be known by the IT staff and DBAs. Database administrators must have separate users and passwords defined for tracking purposes.

All client database users' passwords must conform to the previously listed password requirements.

SNMP:

SNMP (Simple Network Management Protocol) is used on all network devices for monitoring of resources and preventative maintenance. Community strings serve as access passwords in SNMP. The following is a list of procedures regarding the management of this resource:

1. Community strings must conform to the system-level password requirements, except as listed below.
2. Community strings must be different from the passwords used to log in to the devices.
3. A keyed hash must be used where available (e.g., SNMPv3).
4. SNMPv2 or higher shall be used
5. Community strings must be changed on a yearly basis or upon separation of an IT staff SPU.

6. SNMP access must be configured to only devices that do the monitoring on the network.
7. The SNMP service should be configured to only accept connections from IT or authorized SNMP management devices.

Additional Windows Security:

1. Disable GUEST account access in domain policy.
2. Setup hidden shares when possible.
3. Setup group access to directories and remove access to the groups of EVERYONE, DOMAIN USERS.
4. Mobile devices containing confidential information should use whole-disk encryption, preferably pre-boot authentication
5. Setup a login banner to clarify that access to the system is for authorized users only and may be monitored.
6. Disable or rename the default Admin\$, C\$ and D\$ shares when possible.
7. Use Center for Internet Security (CIS) operating system hardening guidelines.
8. Install all security patches within two weeks of release date.
9. Track and update non-Microsoft user applications when security patches are released.
10. Enable the Windows or third-party firewall to block unexpected incoming traffic
11. Purge workstation magnetic hard drives by overwriting all disk space with binary zeros or random data (not just formatting), using a drive's internal whole-disk Secure Erase function, or degaussing.
12. Purge solid state drives by overwriting all disk space twice with binary zeros or random data (not just formatting), or physically destroy.
13. Only grant administrator rights access to users who require it to perform their job functions.
14. Disable inactive user accounts which have not been used in over 90 days, unless required.
15. Disable vulnerable cryptographic protocols (SSLv2, SSLv3, TLS 1.0, TLS 1.1) on servers (especially DMZ web servers)
16. Configure RDP on server: Force NLA and/or SSL signed by SPU CA, Set encryption to High.
17. Remove "Anonymous Logon" from the Active Directory "Pre-Windows 2000 Compatible Access" group, to help limit Active Directory read access to internal users.

Change Management and Major Change Controls:

A change management procedure shall be utilized to make authorized changes to the SPU's network environment. This procedure shall include documentation and formal approval of all changes. These items include, but not limited to, firewalls, routers, network switches, wireless controllers, access points, security appliances, directory services, servers, virtualization environments, storage devices (e.g. SANS), Voice over Internet Protocol (VoIP) systems, computers, mobile devices, and smartphones.

Vulnerability Management:

1. External Vulnerability Scans shall be conducted Monthly to detect firewall misconfigurations and high-risk ACL's.
2. Internal Vulnerability Scans shall be run Quarterly to detect unpatched systems
3. External Web Application Scans shall be run Quarterly on critical web sites including:
4. External Web Application Scans shall be run annually on critical web sites including:

These scans will require scan notification to each third party host.

5. Failed Vulnerability scan results rated at Critical or High (and some Medium external) will be remediated and re-scanned until all Critical and High risks are resolved.

Wireless Security

802.11 Wireless Protocols:

If the SPU Network has 802.11 Wireless Network access, then the following controls shall be implemented:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture;
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices within the wireless controller;
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation;
4. Enable user authentication and encryption mechanisms for the management interface of the AP, via Active Directory integration, whenever possible;
5. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed from their defaults upon installation;
6. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized;
7. Enable all security features of the wireless product, including the cryptographic authentication, IP Privacy, firewall, and other available privacy features;
8. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys, preferably via Active Directory authentication;
9. Ensure that the ad hoc mode has been disabled;
10. Disable all nonessential management protocols on the AP's;
11. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface;
12. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly;
13. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs;
14. When disposing of access points that will no longer be used by the SPU, clear access point configuration to prevent disclosure of network configuration (keys, passwords, etc).

Shakopee Public Utilities (SPU) Information Security Incident Response Plan

Draft: July 9, 2025

Approved: TBD

Purpose: This plan is to serve as guidance in the handling of a potential information security incident at SPU. A formal incident response plan is an industry best practice and is required for the Minnesota Department of Health (MDH) for their public water system compliance but can be used for any other cybersecurity Incident in SPU.

Roles: The SPU Security Policy requires all personnel to report suspected breaches of SPU security. These potential security incidents must be immediately reported to SPU IT Director or your appropriate Manager for investigation.

Communication: Internal communication should be limited to appropriate staff during the incident to not compromise the investigation. Communication with outside entities regarding the incident must be approved by SPU Management, except for 911 for immediate danger to lives.

Incident Response Procedure: SPU Incident Response adopts a high-level process like SANS guidelines and NIST 800-61: Prepare (already done), Identify (verify it is a security incident), Contain (remove device from the network & backup), Eradicate / Recover (remove malware or restore from system backup and prevent re-occurrence), and Lessons Learned (improve future responses or security). These processes are detailed in the template below.

NIST: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Shakopee Public Utilities (SPU) Incident Response Guideline Template

Start Date: _____

Description of Incident: _____

Step 1: Identify

Overview: This process must be followed if staff suspects a security incident has occurred and is used to notify and identify the type of incident that occurred.

#	Step	Handler	Date	Time	Actions Taken
1	If there is immediate danger to lives, dial 911 and then notify SPU IT Director, or your immediate Manager who will notify the IT Director.				
2	The IT Director will assign staff to assess the potential security incident* and determine if it is a security incident or if it is an unrelated event such as user error.				
3	If the report was not a security incident, no further work is needed, otherwise document the results of the investigation in a help desk ticket assigned to the IT Director.				
4	The IT Director will communicate with the appropriate SPU staff that an investigation is being conducted.				

* Note that some security devices produce a large number of suspicious event alerts, in which case it may be prudent for the incident handler to recommend the device be further tuned instead and only proceed if there is a reasonable likelihood of an incident

Step 2: Contain

Overview: Remove device from network, communicate outside, and backup

#	Step	Handler	Date	Time	Actions Taken
1	The IT Director will assign the appropriate staff to perform containment of the security event				
2	The assigned staff will disconnect the compromised device/s from SPU network.				
3	If Credit Card (PCI) data was likely compromised, the system affected <u>must not be powered down</u> per PCI Payment Brand procedures (referenced in appendix).				
4	Research how the incident occurred and perform the following steps to further contain it:				
.A	Make appropriate firewall/access list changes to restrict the ability for the threat to further compromise the systems.				
.B	Any passwords that were potentially compromised should be changed as appropriate.				
5	Outside notification should be reviewed by Management consulting with HR and Legal, as listed below and detailed in the Appendix.				
.A	If Credit Card (PCI) data was likely compromised, no further action should be taken on the system until the Credit Card brands listed in the appendix and the US Secret Service have been notified <u>by Management</u> , and we have been given further instructions from the Credit Card brands (e.g. Visa, MC) listed in the appendix.				

.B	If citizen data is compromised, <u>Management</u> should be alerted to handle communication with the citizens as appropriate.				
6	Back up the data for evidence by swapping out a mirrored drive or running a backup on the device if this incident is likely to result in a court case or if additional research is needed. If the incident is malware on a workstation not exposing Restricted data, a backup does not need to be done.				
.A	Start a “chain of evidence” form detailing how the evidence was stored, who had access, how used, and when.				
.B	Keep the evidence locked and only work with copies of the evidence.				
7	If a Mobile Device is involved, and is managed by a Mobile Device Management (MDM) solution, the device shall be locked or wiped in order to protect the protected data that may be store on that device. This shall be done rapidly given the higher risk mobile devices may pose.				

Step 3: Eradicate / Recover

Overview: Clean the system or rebuild/restore from a clean backup, prevent reoccurrence

#	Step	Handler	Date	Time	Actions Taken
1	Determine the root cause of incident.				
2	Clean the system or rebuild/restore from backup as appropriate.				
3	Apply fixes for root cause to prevent re-occurrence.				

4	Evaluate applying fix to prevent similar occurrences elsewhere if appropriate.				
5	Monitor SPU for similar events.				
6	For a major incident (e.g. web defacement, etc), Management must approve whether the systems go back online. This will be determined if Management is satisfied that the root cause is determined and resolved.				
7	Review and monitor systems for reoccurrence.				

Step 4: Lessons Learned

Overview: Formally document incident and make future recommendations

#	Step	Handler	Date	Time	Actions Taken
1	For incidents involving restricted data (PCI, SCADA, PII), complete the reporting required by the outside entities, to be sent <u>by Management after consulting HR/Legal.</u>				
2	For a major incident (e.g. web defacement, etc) a formal document of the incident should be written up and put in the file share which includes the following: <ul style="list-style-type: none"> ○ One to three paragraph summary with screen shot if applicable ○ Short background information on system / environment ○ Incident timeline, how discovered, steps taken by who (this template) ○ Future recommendations: Typically involves possible changes to improve 				

	incident handling process or harden the environment				
2	For a non-major incident put this form in the SPU Incident Response file share, labeled with the date and description.				
3	Review future recommendations with Management to implement if appropriate.				

Critical Contact Phone Numbers:

SPU IT Director

Philip Dubbe

[REDACTED]

SPU Network Administrator

Dan Pierre

[REDACTED]

SPU General Manager

Greg Drent

[REDACTED]

WATER-ISAC

1-866-426-4722

EI-ISAC

202-790-6000

MS-ISAC (Security Operations Center)

866-787-4722

Minnesota Security Consortium

Dimitrios Hilton (vCISO Security Consultant)


[REDACTED]


218-955-3110 (option “0” for emergency assistance)

Chirs Krieger (Forensics)

[REDACTED]

**SHAKOPEE PUBLIC UTILITIES
MEMORANDUM**

TO: Greg Drent, General Manager
Joseph Adams, Engineering Director 

FROM: Ryan Halverson, Water Engineering Supervisor 

SUBJECT: Approve an updated Nitrate Testing and Operations Policy

DATE: August 4, 2025

ISSUE

An update to the SPU Nitrate Testing and Operations Policy is necessary since organization personnel changes have been made, and new production and storage facilities have been added to the public water system since last adoption.

BACKGROUND

On May 2, 2005, the SPU Commission adopted a policy titled Water Department Testing and Operational Procedures for Nitrates (See attachment A). This policy was created to memorialize the testing schedules, operational protocols and response and reporting procedures of the department to ensure that the water provided by SPU not only meets but exceeds all applicable drinking water standards and regulations.

The Maximum Contaminant Level (MCL) for nitrate in drinking water, as established by the Safe Drinking Water Act (SDWA), and adopted by both the US Environmental Protection Agency and MN Department of Health is 10.0 mg/L.

Specifically of concern to the Commission in 2005, was the elevated nitrate levels related to Wells 4, 5, 6 and 7 in the Normal Elevation Service Zone. While SPU wells were not over the 10.0 mg/L MCL, the Commission was sensitive to the elevated nitrate levels which ranged from 6.0 mg/L to 8.5 mg/L at the time.

When individual wells have elevated nitrate levels over the MCL, per Minnesota Department of Health regulations, the well can be blended with other wells at the wellhead and before

distribution to the system. The current SPU nitrate policy uses the practice of blending wells prior to distribution, with the desired goal of providing water with nitrates below 5.0 mg/L, which is 50% of the regulatory MCL.

Since the previous policy adoption, SPU has made organization chart changes with job titles, responsibility and personnel changes occurring. These titles and roles need to be updated and reflected in a new policy.

More importantly, SPU has added the following infrastructure:

- Pump House 15 and Wells 15, 16 and 17 at the 17th Avenue Sports Complex
- Pump House 20 and Wells 20 and 21 near the Shakopee High School
- Pump House 23 and Well 23 at Windermere along Zumbro Ave
- Booster Stations at River Valley, Valley Creek and Windermere
- Ground Storage Tank 7 at Wood Duck Trail, elevated Storage Tank 8 at Windermere and elevated Storage Tank 9 is under construction at Wood Duck Trail.

The infrastructure supporting Pump Houses 15 and 20, and the higher quality water pumped from Wells 15, 16, 17, 20 and 21, which meets or exceeds all MCL levels established by SDWA without treatment, have allowed staff to continue to operate in accordance with the current nitrate policy.

During the recent construction of Well and Pump House 23, water quality samples were taken from a test well before construction that showed desirable water quality test results, with nitrates measured at 1.86 mg/L. However, after development of Well 23, slightly elevated nitrate levels have remained during well production and initial testing. The average nitrate levels of all tests to date from Well 23 is 6.45 mg/L.

Well 23 is currently the only well connected directly to Pump House 23 and not able to be blended with other wells at the well head to get below the 5.0 mg/L nitrate level.

This scenario is not covered in the previously adopted nitrate policy, thus requiring a review and update of the Nitrate Testing and Operations Policy, including the creation of a new and temporary policy for Well 23.

DISCUSSION

Nitrate Testing and Operations Policy dated 8/4/2025 (See Attachment B)

Staff has revised and updated the proposed Nitrate Testing and Operations Policy for all SPU wells. The previously adopted policy was used as the basis of this update with the following changes:

- New job titles and roles were updated to include the General Manager, Director of Field Operations and the Water Operations Supervisors.
- Operation Protocol was modified. Of importance, the first Action Level was increased from a nitrate level of 4.99 mg/L and below to 5.99 mg/L and below. This allows additional operational flexibility for the operators. This change is desired so the operators aren't required to take additional actions or reprogram SCADA steps/routines for a single test over the 5.0 mg/L nitrate threshold. Nitrate test results can fluctuate. In general, nitrate test results for SPU wells have decreased over time and the previous 2-year average nitrate level for all wells in the Normal HES Zone is 3.67 mg/L. The previous 2-year average nitrate level for all wells in the 1st HES Zone is 1.69 mg/L.
- New language was created for when sharp increases in nitrate test results occur at a well. A nitrate level increase of 2.0 mg/L or greater will require additional testing and fall into Emergency Operations scenario if the well isn't able to be blended below the target 5.0 mg/L level.
- Lastly, the document was reformatted and tables for the testing schedule and internal operations protocol were improved.

Nitrate Testing and Operations Policy (Well 23 Only) dated 8/4/2025

SPU engaged an engineering consultant, SEH Inc., to update SPU's water system model and develop a nitrate distribution model to understand how using Well 23 and the Windermere Booster Station concurrently would impact the nitrate levels of the water blended and subsequently distributed from Tank 8. The findings of the modeling were presented before the Commission at the June 16, 2025 Workshop with availability for questions and additional discussion.

The model intentionally used conservative nitrate levels* of 2.58 mg/L from the Windermere Booster station with 7.80 mg/L from Well 23. It was demonstrated that if Well 23 is operated at 600 gpm concurrently with the Windermere Booster station at 1000 gpm, the resulting sustained nitrate level exiting Tank 8 for distribution was approximated to be 6.4 mg/L.

*Note: For the nitrate levels used in the modeling, the 2.58 mg/L nitrate level used for the Windermere Booster station is the average results of Wells 20 and 21 closest to the booster station. The 2-year average nitrate level for all wells in the 1st HES Zone is 1.69 mg/L. The 7.80 mg/L nitrate level from Well 23 is the highest test result received from Well 23 since construction. The average nitrate level for Well 23 (excluding the test well result) is 6.45 mg/L. It is anticipated that the sustained 6.4 mg/L nitrate level from Well 23 and Windermere Booster Station blended water at Tank 8 is a worst case scenario based on the conservative modeling effort.

Staff has developed a proposed Nitrate Testing and Operations Policy for Well 23 Only (See Attachment C). This policy was created from the guidance of the SEH model and Commission feedback.

This policy is intended to be a temporary policy, and should be updated or replaced when an additional well is constructed and connected to Pump House 23. SPU has two additional well sites secured near PH23 and is seeking an additional well site in the vicinity.

All conditions and requirements of the proposed SPU Nitrate Testing and Operations Policy shall apply to Well 23, with the exceptions of the testing schedule and internal operation procedures listed below:

- The Testing Schedule requires weekly testing for first three months of operation to better monitor and establish a baseline nitrate level for the well.
 - It is anticipated that a monthly testing protocol will be required after the first three months of operation are completed.
- Operational Protocol

The Action Levels proposed in the Well 23 Only policy allows SPU staff to operate Well 23 at the same time as the Windermere Booster Station to fill Tank 8 as long as the Well 23 nitrate test results do not exceed 6.99 mg/L.

 - Shortage or Emergency conditions would be required to operate Well 23 above the 1st action level nitrate level, with more frequent testing required.

SPU staff will continue to provide water quality testing results to the Commission as required by policy. Any significant changes to the water quality from Well 23 will be brought back to the Commission for discussion.



PO Box 470 • 255 Sarazin Street
Shakopee, Minnesota 55379
Main 952.445-1988 • Fax 952.445-7767
www.shakopeeutilities.com

REQUESTED ACTION

Staff is requesting that the Commission approve the Nitrate Testing and Operation Policy, and the temporary Nitrate Testing and Operation Policy (Well 23 Only), both dated 8/4/2025 by motion.

SHAKOPEE PUBLIC UTILITIES – WATER DEPARTMENT TESTING AND OPERATIONAL PROCEDURES – NITRATES

Adopted by SPU Commission 5/2/2005

TESTING SCHEDULE FOR ALL WELLS:

NITRATE LEVEL:

2.5 mg/l and below
2.5 mg/l and above
8.5 mg/l and above

TESTING FREQUENCY:

Quarterly testing
Monthly testing
72 hours of pumping

This monitoring frequency is much more stringent than required by the MN Department of Health (MDH). According to Minnesota Safe Drinking Water Rules, quarterly sampling is required only when NO₃ levels are above 5.4 mg/l (50% of the Maximum Contaminant Level of 10 mg/l).

The prior 13-months of NO₃ results will be provided to Commission every month.

OPERATIONAL PROCEDURES – NORMAL, SHORTAGE, EMERGENCY

NORMAL CONDITIONS -

Regular pumping from a well will be immediately suspended upon receiving test result above 10.0 mg/l.

Wells taken out of service for nitrate levels will be tested before being put back in service. Regular pumping will not resume until test results are below 10.0 mg/l for two consecutive weeks.

SHORTAGE CONDITIONS -

A "shortage" is defined as a condition where water pressures or storage tanks are below levels desired, but not so extreme as to constitute an emergency. Examples would be a prolonged drought, pump failure, or storage tank being out of service.

Under shortage conditions the preferred action is the imposition of restrictions on water usage by sprinkling restrictions or similar conservation measures. As an alternative response, wells previously taken out of service due to elevated nitrate levels may be placed in operation in conjunction with other wells to blend water. Blended water will be monitored to determine that the nitrate level of water supplied to the public is 10.0 mg/l or below.

If blended water of 10.0 mg/l is not exceeded, public notification is not required by the MN Department of Health.

Utility Commissioners will be advised of the event.

EMERGENCY CONDITIONS –

An “emergency” is defined as an extreme condition where a threat to life and safety is reasonably seen. Examples would be a shortage of water pressure due to fire-fighting use, or to low water storage levels giving inadequate fire protection.

Under emergency conditions, wells taken out of service due to elevated nitrate levels may be placed in operation at the discretion of the appropriate utilities staff personnel, normally the Water Superintendent, or as directed by the Utilities Manager.

In the event that wells with high nitrate levels are run under the emergency conditions, public notification is required by the MN Department of Health and SPUC emergency procedures will be followed. SPUC will take appropriate action to assure suitable water is available as required by various customers.

Utilities Commissioners will be advised of an emergency event.

This policy is set to assure public safety when nitrates levels begin to approach upper limits. This is the ultimate priority of the Utilities. The public must be confident safeguards are in place as to not allow nitrates above the MCL to enter the water supply.

General Notes to the Testing Schedule and Operational Procedures:

1. When four consecutive repeat samples that are reliably and consistently below a given schedule threshold, the testing frequency will revert to the average of the four latest tests.
2. SPUC testing schedule will meet or exceed state and federal requirements.
3. Water quality standard and public notification procedures will comply with state and federal SDWA requirements.
4. Water pumped to waste (not for public consumption) is not subject to the testing schedule or the operational procedures.

INTERNAL OPERATIONAL PROCEDURES FOR ALL WELLS

ACTION LEVEL (mg/l)	STANDARD OPERATING RESTRICTIONS	
	<u>INITIAL RESPONSE</u> by Water Operations	<u>CONFERRED RESPONSE</u> taken by Water Supt
9.00 and over	EMERGENCY condition only hand operation by Supt. immediate resampling	EMERGENCY condition only hand operation by Supt. follow-up sampling
7.50 to 8.99	EMERGENCY condition only hand operation by Supt. immediate resampling	blend to <7.50 - run in Auto set Well in last stage only follow-up sampling
5.00 to 7.49	blend to <5.00 - run in Auto set Well in last stage only	blend to <5.00 - run in Auto set Well in any stage
4.99 and below	no restrictions run in any stage	no restrictions run in any stage

TESTING PROTOCOL

WELL	FREQUENCY	REASON
2	1/quarter	FIG well
3	1/quarter	MTS/FIG well
4	1/month	Jordan well
5	1/month	Jordan well
6	1/month	Jordan well
7	1/month	Jordan well
8	1/month	Jordan well
9	1/month	Jordan well
10	1/quarter	MTS well
11	1/month	Jordan well
12	1/month	Jordan well
13	1/month	Jordan well
14	1/quarter	FIG well

SHAKOPEE PUBLIC UTILITIES – WATER DEPARTMENT INTERNAL OPERATING PROTOCOL – NITRATES

The "Standard Testing and Operational Procedures - Nitrates Levels", as adopted by the Commission November 1998, requires compliance with all health regulations and restricts the operations of wells between 10 mg/l and 5 mg/l. With the wealth of data collected since 1998 it has been determined an update is required and is contained within this document. This internal operating protocol will be as stringent where water demand allows.

TESTING PROTOCOL

Testing protocol has been slightly modified from current SPUC policy "Testing and Operational Procedures – Nitrate Levels". These changes reflect the additions of wells (10 through 14) to the system and also Well 2 being sealed off from the MTS/H formation. This testing is the minimum baseline for all wells and is listed in the following table labeled Testing Protocol. Additional testing may be required as indicated in the Internal Operational Procedures chart.

This monitoring frequency is much more stringent than required by the MN Department of Health (MDH). According to Minnesota Safe Drinking Water Rules, quarterly sampling is required only when NO₃ levels are above 5.4 mg/l (50% of the Maximum Contaminant Level of 10 mg/l).

OPERATIONAL PROTOCOL

Operational protocol is based on the latest test results received from the MDH and/or the private laboratory being used by SPUC for nitrate analysis. No restrictions are placed upon wells having NO₃ levels below 5 mg/l, which is 50% of the Maximum Contaminant Level (MCL) of 10 mg/l. Nitrate MCL violation criteria states there is a violation when the MDH confirmation average exceeds 10.4 mg/l. SPUC Operating restrictions begin to take place when lab results show a well's nitrate level over 5 mg/l. This protocol can be seen in the chart labeled Internal Operational Procedures For All Wells. Operating restrictions are identified for wells with NO₃ levels between 5 mg/l and 7.5 mg/l (50% to 75% of the MCL). Further restrictions are given for levels over 7.5 mg/l and again at levels over 9.0 mg/l.

This protocol is set to assure public safety when nitrates levels begin to approach upper limits. This is the ultimate priority of the Utilities. The public must be confident safeguards are in place as to not allow nitrates above the MCL to enter the water supply.

ACTION LEVELS

A change in action level to a more restrictive operation will be made as soon as possible after a report of a nitrate level calling for a more restrictive Action Level.

A change in action level to a less restrictive operation will not be made until 2 consecutive follow -up test results are at a lower Action Level.

Sharp increases in nitrate levels may call for changes in action levels. If a test result calls for an increase of more than one step in Action Level, the Action Level will be designated as 1 additional Action Level above the test result.

For example: for Well 5, operating at an action level of "below 5.00" a test of 7.56 mg/l would be two action levels steps – but add one additional step to designate the Action Level in the "9.00 and over" range.

TIMING OF REPORTING AND CONFERRED RESPONSE

When the conditions call for the need to confer, the Water Superintendent and Utilities Manager will make every effort to meet the following timelines:

Before - changing to a less restrictive operation

ASAP - upon receiving test report showing water pumped into the system exceeding 10 mg/l

ASAP – if a well had to be run on "hand" operation for an emergency condition, regardless of nitrate levels

Within 1 day – after an emergency condition, if a well was not run for some reason

Within 1 day – of a test result calling for a more restrictive Action Level

Each workday – when operating under an exemption to Internal Operating Protocol

As needed – for routine review of current Action Levels on various wells

RETESTING SAMPLES and INVESTIGATIONS OF RESULTS

Certain samples tested by our private laboratory will be retested to verify the reliability of our results. Retests will be routinely done when test results exceed the following levels contained on the following table. A resample of the well will also be required in conjunction with the retest.

The Superintendent will order retests without waiting to discuss with the Utilities Manager, but will advise that a retest has been requested. The Superintendent may order other retests whenever needed.

In specific instances when results indicate a significant change the Water Superintendent will meet with the Utilities Manager to discuss an investigations to determine the possible cause of the nitrate increase. It may be determined the best course of action will fall outside the scope of specified procedure. In this case the course of action will be approved by the Utilities Manager.

EXEMPTIONS

Operations will be as described under this Internal Operating Protocol unless specific exemption is directed by the Utilities Manager.

ATTACHMENT B**NITRATE TESTING AND OPERATIONS POLICY***8/4/2025***1 Testing Schedule for All Wells**

This monitoring frequency is much more stringent than required by the MN Department of Health (MDH). According to Minnesota Safe Drinking Water Rules, quarterly sampling is required only when N03 levels are above 5.4 mg/L (~50% of the Maximum Contaminant Level of 10.0 mg/L).

Nitrate Level (mg/L)	Testing Frequency
2.5 mg/L and below	Quarterly testing
2.5 mg/L and above	Monthly testing
8.5 mg/L and above	Every 72 hours of pumping

Table 1: Testing Schedule for Nitrate Levels

The prior 12-months of N03 results will be provided to Commission on a quarterly basis.

2 Operating Conditions**2.1 Normal Condition**

Normal is defined as a condition where pumps, water pressures and storage tanks are operating at desired levels.

- Regular pumping from a well will be immediately suspended upon receiving test result above 10.0 mg/L.
- Wells taken out of service for nitrate levels will be tested before being put back in service. Regular pumping will not resume until test results are below 10.0 mg/L for two consecutive weeks.

2.2 Shortage Conditions

Shortage is defined as a condition where pumps, water pressures or storage tanks are below levels desired, but not so extreme as to constitute an emergency. Examples would be a prolonged drought, pump failure, or storage tank being out of service.

- Under shortage conditions the preferred action is the imposition of restrictions on water usage by sprinkling restrictions or similar conservation measures.
- As an alternative response, wells previously taken out of service due to elevated nitrate levels may be placed in operation in conjunction with other wells to blend water. Blended water will be monitored to determine that the nitrate level of water supplied to the public is 10.0 mg/L or below.
- If blended water of 10.0 mg/L is not exceeded, public notification is not required by the MN Department of Health. Utility Commissioners will be advised of the shortage event.

2.3 Emergency Conditions

Emergency is defined as an extreme condition where a threat to life and safety is reasonably seen. Examples would be a shortage of water pressure due to fire-fighting use, or to low water storage levels giving inadequate fire protection.

- Under emergency conditions, wells taken out of service due to elevated nitrate levels may be placed in operation at the discretion and concurrence of the Water Operations Supervisor(s), Director of Field Operations, and General Manager.
- In the event that wells with high nitrate levels are run under emergency conditions, public notification is required by the MN Department of Health and SPUC emergency procedures will be followed. SPUC will take appropriate action to assure that suitable water is available as required by various customers. Utilities Commissioners will be advised of an emergency event.
- This policy is set to ensure public safety when nitrates levels begin to approach upper limits. This is the ultimate priority of the Utilities. The public must be confident safeguards are in place as to not allow nitrates above the MCL to enter the water supply.

3 General Notes

- When four consecutive repeat samples are reliably and consistently below a given schedule threshold, the testing frequency will revert to the average of the four latest tests.
- SPUC testing schedule will meet or exceed state and federal requirements.
- Water quality standard and public notification procedures will comply with state and federal SDWA requirements.
- Water pumped to waste (not for public consumption) is not subject to the testing schedule or the operational procedures.

4 Operational Protocol

This internal operating protocol is intended to be as stringent as possible, where water demand allows.

4.1 Testing Protocol

The testing schedule for nitrates in Table 1: Testing Schedule for Nitrate Levels, as shown in section 1 above, is the minimum baseline for all wells. Additional testing may be required as indicated in the Internal Operational Procedures chart.

This monitoring frequency is more stringent than required by the MN Department of Health (MDH). According to Minnesota Safe Drinking Water Rules, quarterly sampling is required only when N03 levels are above 5.4 mg/L (~50% of the Maximum Contaminant Level of 10.0 mg/L).

This protocol is set to assure public safety when nitrates levels begin to approach upper limits. This is the ultimate priority of the Utilities. The public must be confident safeguards are in place as to not allow nitrates above the MCL to enter the water supply.

4.2 Operational Protocol

Operational protocol is based on the latest test results received from the MDH and/or the private laboratory being used by SPUC for nitrate analysis. No restrictions are placed upon wells having N03 levels below 6.0 mg/L, which is 60% of the Maximum Contaminant Level (MCL) of 10.0 mg/L.

Nitrate MCL violation criteria states there is a violation when the MDH confirmation average exceeds 10.4 mg/L. SPU Operating restrictions begin to take place when lab results show a well's nitrate level exceeding 6.00 mg/L. This protocol can be seen in the chart below labeled Table 2: Internal Operational Procedures For All Wells.

Action Level (mg/L)	Initial Response Water Operations Supervisor(s)	Conferred Response Taken in concurrence of Water Operations Supervisor(s), Director of Field Operations and General Manager
5.99 mg/L and below	No restrictions, run in any stage	No restrictions, run in any stage
6.00 mg/L to 7.49 mg/L	Blend to < 5.00mg/L and run in Auto with other wells	Blend to < 5.00mg/L and run in Auto with other wells
7.50 mg/L to 8.99 mg/L	Shortage Condition, run in Auto At lowest SCADA step based on system demands	Blend to < 7.50mg/L and run in Auto at lowest SCADA step
9.00 mg/L and above	Emergency Condition, run in Hand operation only	Emergency Condition, run in Hand operation only

Table 2: Internal Operational Procedures for All Wells

4.3 Action Levels

- A change in Action Level to a more restrictive operation will be made as soon as possible after a report of two consecutive nitrate level results calling for a more restrictive Action Level.
- A change in Action Level to a less restrictive operation will not be made until two consecutive follow-up test results are at a lower Action Level.
- Sharp increases in nitrate levels may call for additional operating protocol. If a test result shows an N03 increase of increase of 2.0 mg/L or more; and can't be blended below 5.0 mg/L, the well shall immediately fall into Emergency Operations. Two additional nitrate tests, with 72 hours between tests, shall be taken and the results shall determine the appropriate continued operating Action Level.

4.4 Reporting and Conferred Response

When the conditions call for the need to confer, the Director of Field Operations, General Manager and Water Operation Supervisor(s) will make every effort to meet the following timelines:

- **Before:** Changing a well running in Emergency Condition to a less restrictive Action Level
- **Immediately:** Upon receiving test report showing water pumped into the system exceeding 10 mg/L; or if a well had to be run on "hand" operation for an Emergency Condition, regardless of nitrate levels
- **Within 1 day:** After an emergency condition, if a well was not run for some reason; or when a test result calls for a more restrictive Action Level
- **Each workday:** When operating under an exemption to Internal Operating Protocol
- **As needed:** For routine review of current Action Levels on various wells

4.5 Retesting Samples and Investigations

Certain samples tested by our private laboratory will be retested to verify the reliability of our results. Retests will be routinely done when test results exceed the following levels contained on the following table. A resample of the well will also be required in conjunction with the retest.

The Water Operations Supervisor(s) will order retests without waiting to discuss with the Director of Field Operations or General Manager, but will advise that a retest has been requested.

In specific instances when results indicate a significant change the Water Operations Supervisor(s) and Director of Field Operations will meet with the General Manager to discuss an investigation to determine the possible cause of the nitrate increase. It may be determined the best course of action will fall outside the scope of specified procedure. In this case the course of action will be approved by the General Manager

4.6 Exemptions

Operations will be as described under this Internal Operating Protocol unless specific exemption is directed in writing by the General Manager.

NITRATE TESTING AND OPERATIONS POLICY

(Well 23 Only)

8/4/2025

This is a temporary nitrate testing and operations policy for Well 23 only. Well 23 is not able to be blended per MDH requirements at the well head at this time. Due to elevated nitrate levels during well production and initial testing, Well 23 is proposed to be mixed with water from the Windermere Booster Station in Tank 8.

This policy is a temporary policy and is intended to be updated or replaced when an additional well is constructed and connected to Pump House 23 to allow for blending at the well head.

All conditions and requirements of the SPU Nitrate blending policy shall apply to Well 23, with the exceptions of the testing schedule and internal operation procedures listed below.

1 Testing Schedule (Well 23 Only)

Well 23 shall be operated and tested on a weekly basis from August 1, 2025 until October 31, 2025 to establish a baseline of nitrate testing results. Starting November 1, 2025, The average of all previous test results shall be used to establish an initial testing frequency. Additional testing shall be at the following intervals:

Nitrate Level (mg/L)	Testing Frequency
2.5 mg/L and below	Quarterly testing
2.5 mg/L to 6.99 mg/L	Monthly testing
7.0 mg/L to 8.99 mg/L	Weekly testing
9.0 mg/L and above	Every 72 hours of pumping

Table 1: Testing Schedule for Nitrate Levels

4.2 Operational Protocol (Well 23 Only)

Action Level (mg/l)	Initial Response Water Operations Supervisor(s)	Conferred Response Taken in concurrence of Water Operations Supervisor(s), Director of Field Operations and General Manager
6.99 mg/L and below	Run well 23 with Windermere Booster Station to < 7.00 mg/L Can run in Auto	Run well 23 without Windermere Booster Station to < 7.00 mg/L Can run in Auto
7.00 mg/L to 8.99 mg/L	Shortage Condition, hand Operation concurrently with Windermere Booster Station	Emergency Condition, hand operation only if Windermere Booster Station is offline
9.00 mg/L and above	Emergency Condition, run in Hand operation only	Emergency Condition, run in Hand operation only

Table 2: Internal Operational Procedures for All Wells

July 30, 2025

TO: Greg Drent, General Manager 
FROM: Sharon Walsh, Director of Marketing, Key Accounts and Special Projects 
SUBJECT: Crisis Communication Plan

Overview

At the June Workshop, a walk-thru of a preliminary Crisis Communication Plan was done. The commissioners shared feedback with me. This included:

- A smaller team for the Crisis Management Team
 - o General Manager
 - o Director of Communications
 - o Legal Advisor
 - o Commission President, as a backup to the General Manager
 - o Leadership Representative (as needed based on crisis)
- If the GM is to be the primary spokesperson, a backup is needed in the event he is not available and/or he is busy solving the crisis.
- More frequent CMT meetings are needed at the onset of a crisis (4 hours or daily is not responsive enough at the onset of a crisis)
- Having legal input on all external communications is advised/preferred
- Incorporate the SME and Legal when speaking to the authorities
- Streamline the document so it is user-friendly during a crisis situation
- Make communication protocols and the approval process clear to users.

Changes noted above have been incorporated into this document. Because this is a public document, cell phone numbers and key account information was not included. This information is in the internal document.

Action Requested

Staff is requesting approval of the design of the SPU Crisis Communication Plan as presented. NOTE: This plan is a dynamic document in that contacts will continually need to be updated, communication platforms may change, and following a crisis, changes should be included to improve the plan for future applications.

SPU Crisis Communication Plan

1. Introduction

1.1 Purpose

The purpose of this Crisis Communication Plan is to have a dynamic document readily available in the event of a crisis that warrants public communications. This plan helps ensure the Crisis Management and Leadership Teams can quickly and accurately communicate to our customers, the media, our employees and/or government entities impacted by the crisis, sharing critical information, setting expectations and building trust with our audiences.

This plan includes guidelines and defined procedures for both communications and limited emergency response plans among responsible parties.

1.2 Objectives

1. **Deliver timely and accurate information to relevant stakeholders:** Have prepared responses readily available; ensure staff awareness of process; and have applicable, critical audiences identified.
2. **Protect and manage the organizations' reputation:** limit the number of individuals speaking to the media/public for consistent messaging; share only known facts (no speculations); provide public acknowledgement of the situation; and expressed empathy.
3. **Coordinate communication efforts across departments:** **SPU Crisis Mgmt Team** group text (Leadership Team) and **Emergency Operations** email (Leadership team and supervisors).
4. **Manage public perception by engaging with the media and public:** provide concise and consistent messaging. Use SPU social media platform to get messaging out quickly and widespread.
5. **Ensuring compliance with legal and regulatory requirements:** Individual department head tasked to execute protocol as required and applicable to each situation.

1.3 Scope

This Crisis Communication Plan covers the procedures and protocols necessary for the effective management of communication during a broad range of potential crises that may impact SPU's organization. The scope of this plan includes, but is not limited to, the following types of crises:

1. **Natural Disasters:** Events such as high winds, tornadoes, flooding, flash floods, severe droughts, excessive heat, fires or lightning strikes that could disrupt operations and affect the safety of employees and stakeholders.
2. **Technological Incidents:** Cyber-attacks, data breaches (customer info, internal or financial), and other technological failures that comprise information security and disrupt digital operations.
3. **Operational Failures or Crises:** Significant disruptions in the supply chain; product recalls; infrastructure failures; project delays or halts; major system outages (including load shedding) damages or contamination; or any operational issues that impede the organization's ability to function effectively.
4. **Public and SPU Safety:** Severe workplace accidents that may affect public safety (i.e., chemical exposure, electrocution, contamination, equipment accident, etc.); terroristic threats or violent acts against SPU; active shooters; aggressive customer threats or altercations; or any incidents that pose a risk to the health and safety of employees and other stakeholders.
5. **Staffing and Employee Emergencies:** Staffing emergencies to include the sudden loss of SPU General Manager or mass loss of employees (i.e., vehicle accident, plane crash, attack at industry event, team accidents, etc.). Negligent or illegal employee behaviors including financial theft/embezzlement; inappropriate/scandalous behavior affecting SPU's public image; breach of regulatory requirements, legal violations or any compliance-related problems that could result in legal penalties or loss of licenses.

This plan applies to all employees, contractors, and any third parties acting on behalf of our organization. It outlines the roles and responsibilities of the Crisis Management Team (CMT), provides guidelines for internal and external communications, and specifies the processes for crisis identification, assessment, response, and recovery.

The Crisis Communication Plan is intended to be a dynamic document that will be reviewed and updated regularly to address emerging risks and incorporate best practices in crisis management. It serves as a critical tool to ensure our organization can respond promptly and effectively to crises, mitigate negative impacts, and maintain trust with our stakeholders.

1.4 Definitions

To ensure clarity and common understanding, the following key terms used in this Crisis Communication Plan are defined as follows:

Activation Criteria	Predefined conditions or thresholds that trigger the activation of the Crisis Management Team and the implementation of the Crisis Communication Plan.
Communication Channel	The medium or platform used to convey messages to stakeholders during a crisis. Examples include press releases, social media, email, and the organization's website.
Crisis	A <i>significant</i> event or situation that poses a threat to the organization's operations, reputation, financial stability, or stakeholder safety. Crises require immediate attention and coordinated response efforts.
Crisis Assessment	The process of evaluating the severity, potential impact, and scope of a crisis to determine the appropriate response measures.
Crisis Management Team (CMT)	A designated group of individuals responsible for managing the organization's response to a crisis. The CMT includes roles such as Crisis Manager, Communications Lead, and Legal Lead. Commission President as needed.
Emergency Response Plan	A plan that outlines procedures for ensuring the safety and security of individuals during an immediate crisis, such as evacuation protocols and emergency contact information.
External Communication	The process of disseminating information to external stakeholders during a crisis. This includes communication with the media, customers, suppliers, community partners, regulatory bodies, and the general public.

Incident Reporting	The process of documenting and reporting the details of a crisis incident, including the nature of the crisis, actions taken, and outcomes achieved as required by regulatory guidelines.
Internal Communication	The process of disseminating information within the organization during a crisis. This includes communication with employees, management, and internal departments.
Leadership Team (LT)	Current members of the SPU Leadership Team, which are Directors.
Message Development	The process of creating, approving, and disseminating communication messages during a crisis. This includes initial statements, updates, and responses to stakeholder inquiries.
Post-Crisis Review	An evaluation conducted after a crisis has been resolved to assess the effectiveness of the response, identify lessons learned, and recommend improvements to the crisis communication plan.
Reputation Management	Strategies and actions taken to protect and restore the organization's reputation during and after a crisis. This includes managing public perception and addressing negative publicity.
Simulation Exercise	A training activity designed to test and evaluate the organization's crisis communication plan and response capabilities. Simulation exercises help identify strengths and areas for improvement.
Spokesperson	An individual authorized to represent and speak on behalf of the organization during a crisis. The spokesperson is responsible for delivering official statements and responding to media inquiries.

Stakeholders	Individuals or groups who have an interest in or are affected by the organization's actions, including employees, customers, suppliers, community leaders, regulators, and the general public.
---------------------	--

2. Crisis Management Team

2.1 Team Composition

1. Crisis Manager
2. Communications Lead
3. Legal Lead
4. Commission President (as needed)
5. Leadership Team Member (as needed)

2.2 Responsibilities

Role	Name	Responsibilities	Contact Information
Crisis Manager	General Manager – Greg Drent	<p>Oversee the overall crisis response and decision-making process. Coordinate the activities of the CMT.</p> <p>Ensure that all aspects of the crisis are being addressed effectively.</p> <p>Serves as the primary spokesperson for the organization.</p>	<p>Office: 952-233-1511</p> <p>Cell: xxx-xxx-xxxx</p> <p>Email: gdrent@shakopeeutilities.com</p>
Communications Lead	Director of Communications – Sharon Walsh	<p>Develop all internal and external communications.</p> <p>Disseminate all external communications.</p>	<p>Office: 952-233-1531</p> <p>Cell: xxx-xxx-xxxx</p> <p>Email: swalsh@shakopeeutilities.com</p>

Legal Lead	Utility Council – Spencer Fane LLP	Provide guidance and legal direction for messaging and external communication content.	Office: 612-268-7000 Cell: xxx-xxx-xxxx Email:
Commission Representative	Commission President – B.J. Letourneau	In the absence of the Crisis Manager, take over the leadership of the CMT and serve as the primary spokesperson for the organization. Based on the crisis, public speaking responsibilities may be delegated to appropriate department lead.	Cell: xxx-xxx-xxxx Email: bletourneau@shakopeeutilities.com
Leadership Team Member	Department Director	Provide critical Operations, Technical, Financial or Administrative insight to help build accurate communication content. Be a resource for the Communications Lead.	TBD – Event specific

3. Crisis Identification and Risk Assessment

3.1 Crisis Identification

Methods for Identifying Crises

1. Incident Reporting System:
 - An internal incident reporting system is in place to allow employees and stakeholders to report potential crises promptly.
 - Reports can be submitted via the website, phone, email or in-person
 - Incident Reporting Contact Information:
 - Report an Emergency – shakopeeutilities.com
 - Email – customerservice@shakopeeutilities.com
 - Phone: (952) 445-1988
 - Greg Drent (in person)
2. Monitoring and Surveillance:
 - Continuous monitoring of various channels, including social media, news outlets, industry reports, and regulatory updates, to detect early signs of a crisis.
3. Internal Communication Channels:
 - Regular communication with employees, management, and other internal stakeholders to gather information on potential issues.
 - Encouragement of a culture of openness where employees feel comfortable reporting concerns without fear of retaliation.
4. Customer Feedback:
 - Analysis of customer feedback received through support channels, surveys, and social media to identify emerging issues that could escalate into a crisis.
 - Establishment of a process for frontline customer service representatives to escalate potential crisis indicators to management.
5. Regulatory and Compliance Audits:
 - Regular audits and reviews of compliance with industry regulations and internal policies to identify vulnerabilities and areas of concern.
 - Collaboration with legal and regulatory teams to stay informed about new regulations and potential risks.

All incidents are given to the General Manager for immediate review.

3.2 Crisis Risk Assessment

Assessment Process

- Gather Initial Information:
 - GM to include appropriate department lead(s) to assist in the assessment process and provide valuable insight.
 - Collect all available information regarding the crisis from initial reports, monitoring tools, and stakeholder communications.
 - Ensure that information is accurate, verified, and comprehensive.
- Establish Assessment Criteria:
 - Use predefined criteria to evaluate the crisis. Key criteria include:
 - **Impact on Operations:** The extent to which the crisis affects the organization's ability to continue its operations.
 - **Reputation Damage:** The potential for the crisis to harm the organization's public image and stakeholder trust.
 - **Financial Implications:** The estimated financial loss or cost associated with the crisis.
 - **Safety and Legal Issues:** The risk to the health and safety of employees and stakeholders, and any legal ramifications.
- Severity Categorization:
 - Based on the assessment criteria, categorize the crisis into one of the following levels:
 - **Minor:** Limited impact on operations, minimal reputational damage, no significant financial loss, and low safety/legal risks.
 - **Moderate:** Noticeable impact on operations, moderate reputational damage, manageable financial loss, and moderate safety/legal risks.
 - **Severe:** Major disruption to operations, severe reputational damage, significant financial loss, and high safety/legal risks.

Example Assessment

1. *Crisis Description:*
 - *A data breach affecting customer information has been identified.*
2. *Impact on Operations:*
 - *Medium: Some disruption to IT systems, but core operations continue.*
3. *Reputation Damage:*
 - *High: Significant risk to customer trust and potential negative media coverage.*
4. *Financial Implications:*
 - *High: Potential fines, compensation costs, and loss of business.*
5. *Safety and Legal Risks:*
 - *Medium: Legal implications due to breach of data protection regulations.*
6. *Stakeholder Analysis:*
 - *Affected stakeholders include customers, employees, regulators, and the media.*
7. *Scenario Planning:*
 - *Best-case: Quick containment and transparent communication limit damage.*
 - *Worst-case: Extensive media coverage and legal action lead to severe reputational and financial loss.*
 - *Most likely: Moderate media coverage, some customer criticism, and regulatory scrutiny.*
8. *Communication Strategy:*
 - *Develop key messages tailored to each stakeholder group, ensuring transparency and consistency.*
 - *Immediate notification to affected customers, transparent media statements, and regular updates to regulators and internal stakeholders.*

3.3 Activation

Following a preliminary risk assessment, a Crisis Communication Plan may or may not be activated.

1. CMT Activation Decision:

- Based on the preliminary assessment, the Crisis Manager decides if an activation of the Crisis Communication Plan and CMT is necessary.
 - Situations that are deemed to be Minor in the severity categories may not require an activation.
- If activation is required, the Crisis Manager issues an activation notice to all CMT and LT members via group text “SPU Crisis Mgmt Team”, and an email to “Emergency Operations” to ensure critical staff are aware of the crisis and are prepared to assist.
- The SPU Commission is also advised of the crisis via email.
 - Commissioners are only actively involved should the General Manager not be able to lead the team and/or address the public.
- Initial CMT Meeting:
 - The Crisis Manager convenes an initial CMT meeting as soon as possible, either in person or via a virtual meeting platform.
 - This meeting will include the appropriate LT members as determined by the type of crisis.
 - During the initial meeting, the CMT reviews the situation, confirms roles and responsibilities, and establishes immediate action steps.
 - Leadership Team (LT) Members may have various levels of involvement after the initial activation notice depending on the situation.
 - Only critical Leadership Team members will be on the CMT beyond the initial activation notice.
- Post CMT Meeting:
 - Assigned staff members execute instructions as communicated in the initial CMT meeting.
 - During the initial crisis situation, follow up meetings are scheduled every 1-2 hours for situation updates, staff involvement and communication messaging.
 - As crisis is stabilized, meetings may drop to every 4 hours (twice per day), eventually reaching once per day when crisis is nearing resolution.

4. Communication Protocols

4.1 Communication Channels

The following channels will be used to communicate with internal and external audiences involved with the crisis:

- Social Media
- Website
- Email
- Texts
- Phone calls
- Intranet/NISC iVue
- Instant Messaging (TEAMS Chat)
- Townhall Meetings (in-person or virtual)
- Employee Meetings
- Press Releases/Media Responses

4.2 Communication Protocols

1. Initial Statement:
 - An initial statement will be issued within the first few hours of the crisis being identified.
 - Content: Brief description of the crisis, confirmation that the CMT is addressing the situation, and commitment to provide updates.
2. Regular Updates:
 - Regular updates will be issued to provide new information, actions taken and next steps.
 - Frequency: Every two hours, or more frequently, if significant developments occur. Every 4 hours once response plans are enacted and then daily after crisis is under control.
3. Consistency and Accuracy:
 - Ensure all communications are consistent, accurate, and aligned with the organization's messaging.
 - Approval Process: All external communications must be approved by the Communication Lead and Legal Lead before release. Include the CM's approval, if available, but do not delay communications.
4. Transparency and Accountability:
 - Communicate transparently about the situation and the organization's response efforts.
 - Content: Acknowledge any mistakes or shortcomings, provide explanations, and outline corrective measures.

5. Monitoring and Feedback:

- Monitor media coverage, social media conversations, and public sentiment to gauge the effectiveness of communication efforts.
- Responsible Person: Communications Director and support staff
- Action: Adjust communication strategies based on feedback and emerging issues.

4.3 Internal Communication

Communication Method	Description	Responsible Person	Frequency	Content
Email Updates	Regular email updates will be sent to all employees to provide information on the crisis, response actions, and any changes to operations.	Communication Lead	As needed, with a minimum of daily updates during an active crisis.	Detailed crisis updates, and critical response plans.
Intranet Portal (NISC iVue)	A dedicated section on the company intranet will be used to post updates, FAQs, and resources related to the crisis.	Finance/Admin Lead	Daily, if critical information changes	Crisis updates, response plans, contact information, support resources.

All Employee Meetings	Virtual or in-person town hall meetings will be held to provide updates, address employee concerns, and answer questions. (Microsoft Teams or in-person)	Crisis Manager	As needed, typically, at key stages of the crisis response.	High level overviews, key information. Supportive and constructive content.
Instant Messaging	Use of internal messaging platforms (e.g., TEAMS Chat) for real-time updates and communications.	Communication Lead	As needed, as updates are available	Short, quick and concise messages or edits

4.4 External Communication

Communication Method	Description	Responsible Person	Frequency	Content
Social Media (Facebook)	Provide real-time updates and engage with the public.	Communications Lead	Initial release as soon as possible after the crisis is confirmed by GM, followed by regular updates as warranted by crisis and/or developments – every 2 hours or more frequently if urgent actions are required.	Crisis updates, safety instructions, and critical response plans.

Website	A dedicated crisis update section on the SPU website will be maintained to provide comprehensive information and resources.	Communications Lead	Throughout the day (24 hours) until crisis is under control, then daily until resolved.	Official statements, FAQ's, impact on services, contact information
Email Updates	Mass email notifications from NISC.	Communication Lead (content) and Finance/Admin (delivery)	An initial release as soon as possible after the crisis is identified, with instructions to follow the situation on SM and website.	Information on how the crisis affects products/services, critical response plans, and what to expect and where to go as the crisis evolves.
Phone Calls or SMS Messaging	Critical accounts and Key Accounts will be notified with a phone call or text in addition to email to create a faster notification.	Communication Lead and staff	An initial release as soon as possible after the crisis is identified, with instructions to follow the situation on SM and website. Future notifications as needed to those affected.	Detailed crisis updates and critical response plans. What to expect and where to go as the crisis evolves.

Town Hall Meetings	Virtual or in-person town hall meetings will be held to provide updates, address stakeholder concerns, and answer questions. (Microsoft Teams or in-person). Recordings posted on website.	Crisis Manager	As needed, Typically, at key stages of the crisis response.	High level overviews, key information, and response plans. Q&A Resource contacts.
--------------------	--	----------------	---	---

4.5 Message Development

Message Development Process

1. Information Gathering:
 - Collect accurate and comprehensive information about the crisis from all relevant sources, including the Crisis Management Team, incident reports, and monitoring tools.
 - Responsible Person: Communication Lead
 - Sources: Internal meetings/reports, media coverage, social media, official statements.
2. Message Drafting:
 - Draft initial messages that address the key aspects of the crisis, including what happened, who is affected, what actions are being taken, and what stakeholders need to do.
 - Responsible Person: Communication Lead
 - Content: Clear, concise, and factual information.
3. Review and Approval:
 - All messages must be approved by the Communications Lead and Legal Lead. Include the CM's approval, if available, but do not delay communications.
 - Utilize other relevant CMT members to ensure accuracy, compliance, and consistency.
 - Responsible Person: Communications Lead and Legal Lead, and CM when applicable.
 - Approval Timeframe: Within 1 hour for urgent messages, 4 hours for less time-sensitive updates.
4. Key Message Components:
 - Introduction: Acknowledge the crisis and express concern for those affected.
 - Details of the Crisis: Provide a brief, factual summary of what happened.

- **Impact:** Explain how the crisis affects stakeholders and the organization.
- **Actions Taken:** Outline the steps being taken to address the crisis.
- **Call to Action:** Provide clear instructions or recommendations for stakeholders.
- **Contact Information:** Offer channels for stakeholders to get more information or assistance.

4.5 Spokesperson Identification

Spokesperson	Contact Info
Primary	Greg Drent, General Manager 952-233-1511 xxx-xxx-xxxx (cell) gdrent@shakopeeutilities.com
Secondary	BJ Letourneau, Commission President xxx-xxx-xxxx (cell) Email: bletourneau@shakopeeutilities.com

Spokesperson Guidelines

1. **Training and Preparation:**
 - Spokespersons must undergo regular media training to develop effective communication skills and crisis response techniques.
 - Training includes mock interviews, message delivery practice, and review of past crisis communications.
2. **Message Consistency:**
 - Ensure that all communications are aligned with the key messages developed by the Crisis Management Team.
 - Avoid speculation and stick to verified facts to maintain credibility and trust.
3. **Calm and Professional Demeanor:**
 - Maintain a calm and professional demeanor during all interactions with the media and the public.
 - Show empathy and concern for those affected by the crisis.
4. **Transparency and Honesty:**
 - Communicate transparently about the situation and the organization's response efforts.
 - Acknowledge any limitations in the information available and commit to providing updates as more details become known.
5. **Media Interaction Protocol:**
 - Prepare key messages and talking points before any media interaction.
 - Listen carefully to questions and respond clearly and concisely.
 - Redirect any questions outside the spokesperson's scope to the appropriate team member or department.

5. Crisis Response

5.1 Ongoing Management

Regular CMT Meetings

1. Scheduled Meetings:

- The Crisis Management Team (CMT) will hold regular meetings to review the status of the crisis and adjust response strategies as needed.
- Frequency: Every 1-2 hours during the initial phase, then every 4 hours as the situation stabilizes. Daily meetings continue until the situation is resolved.
- Responsible Person: Crisis Manager
- Meeting Platform: In-person, video conference, or conference call
- Agenda:
 - Review current situation and updates
 - Assess the effectiveness of response actions
 - Identify new issues or challenges
 - Plan next steps and assign tasks

Continuous Assessment and Adjustment

2. Monitoring and Analysis:

- Continuously monitor the crisis situation through various channels, including news reports, social media, internal reports, and feedback from stakeholders.
- Analyze data to identify trends, potential risks, and areas needing attention.
- Responsible Person: IT Lead and Communication Lead
- Tools Used: Monitoring software, social media analytics, incident reports

3. Adjust Response Strategies:

- Based on the continuous assessment, adjust the response strategies to address new developments and emerging issues.
- Ensure that all adjustments are communicated to the CMT and relevant stakeholders promptly.

Responsible Person: Crisis Manager

Documentation: Update the crisis management plan and action logs

Ongoing Communication Updates

4. Internal Updates:

- Provide regular updates to employees about the status of the crisis and any changes to operations or safety protocols.
- Use multiple communication channels such as email, intranet, and internal messaging platforms.
- Responsible Person: Communications Lead (content) and Finance/Admin Lead (delivery)
- Frequency: At least once per shift or as significant updates occur

5. External Updates:

- Continue to communicate with external stakeholders, including customers, media, regulators, and the public.
- Issue regular social media posts and website updates to keep stakeholders informed.
- Responsible Person: Communication Lead
- Frequency: Every 2 hours initially or if urgent actions needed, down to every 4 hours once crisis is contained and then daily or as significant updates occur.

Coordination with External Agencies

6. Collaboration with Authorities:

- Maintain close communication with local authorities, emergency services, and regulatory bodies to ensure coordinated efforts.
- Provide necessary information and support to these agencies as required.
- Responsible Person: Legal Lead and Operations Lead
- Agencies Involved: Police, fire department, health agencies, regulatory bodies

7. Stakeholder Engagement:

- Engage with key stakeholders, including business customers, critical customers and community leaders, to provide updates and address concerns.
- Schedule regular briefings and Q&A sessions to maintain transparency and trust.
- Responsible Person: Crisis Manager, Communications Lead and Operations Lead
- Frequency: Semi-weekly or as significant updates occur

Resource Management

8. Allocation of Resources:

- Ensure that adequate resources (personnel, financial, technological) are allocated to manage the crisis effectively.
- Monitor resource usage and make adjustments as necessary to meet changing needs.
- Responsible Person: Operations Lead and Finance/Admin Lead

9. Support Services:

- Provide support services to employees and stakeholders affected by the crisis, such as counseling, medical assistance, and financial support.
- Responsible Person: Finance/Admin Lead

Documentation and Record-Keeping

10. Maintain Records:

- Keep detailed records of all actions taken, decisions made, and communications issued during the crisis.
- Ensure that all documentation is accurate, complete, and securely stored for future reference and review.
- Responsible Person: Legal Lead and IT Lead
- Documentation: Crisis management log, meeting minutes, communication records

5.3 Post-Crisis Review

Post-Crisis Review Steps

1. Conduct a Debriefing Meeting:

- Convene the Crisis Management Team (CMT) and Commissioners to conduct an initial **debriefing meeting within 72 hours after the crisis has been resolved.**
- Responsible Person: Crisis Manager
- Agenda:
 - Overview of the crisis and timeline of events
 - Review of actions taken and decisions made
 - Discussion of what went well and areas for improvement
- Meeting Platform: In-person or video conference

2. Collect Feedback:

- Gather feedback from all participants involved in the crisis response, including CMT members, employees, and external stakeholders.
- Use surveys, interviews, and feedback forms to collect comprehensive insights.
- Responsible Person: Communication Lead and Finance/Admin Lead
- Tools Used: Online surveys, feedback forms, one-on-one interviews

3. Analyze Response Effectiveness:

- Evaluate the effectiveness of the crisis response based on key performance indicators (KPIs) such as response time, communication clarity, stakeholder satisfaction, and resource allocation.
- Identify strengths and weaknesses in the crisis management process.
- Responsible Person: Crisis Manager, Communications Lead and designated Leadership Team member(s)
- Metrics: Response time, stakeholder feedback, financial impact, operational impact

4. Document Lessons Learned:

- Compile a detailed report documenting the lessons learned from the crisis.
- Highlight successful strategies and areas needing improvement
- Responsible Person: Crisis Manager
- Report Content:
 - Summary of the crisis and response actions
 - Key findings from feedback and analysis
 - Recommendations for future improvement

5. Update Crisis Communication Plan:

- Revise the Crisis Communication Plan based on the lessons learned and recommendations from the post-crisis review.
- Ensure that all changes are communicated to relevant personnel and integrated into training programs.
- Responsible Person: Crisis Manager and Communication Lead
- Documentation: Updated crisis communication plan, revised protocols, new training materials

6. Share Findings with Stakeholders:

- Communicate the findings and improvements from the post-crisis review to key stakeholders, including employees, customers, investors, and regulatory bodies.
- Ensure transparency and demonstrate the organization's commitment to continuous improvement.
- Responsible Person: Communication Lead and Customer Service Lead
- Communication Channels: Email updates, intranet announcements, stakeholder meetings

6. Training and Exercises

6.1 Training Programs

1. Crisis Management Team Training:

- Objective: To equip the CMT with the skills and knowledge required to manage crises effectively.
- Content:
 - Overview of the Crisis Communication Plan
 - Roles and responsibilities of CMT members
 - Crisis identification and assessment
 - Communication strategies and message development
 - Decision-making under pressure
 - Coordination with external agencies and stakeholders
- Format: In-person workshops, online modules, and role-playing exercises
- Frequency: Annually
- Duration: ½ day (2-4 hrs)
- Responsible Person: Crisis Manager

2. Employee Awareness Training:

- Objective: To ensure that all employees understand their roles during a crisis and know how to respond appropriately.
- Content:
 - Introduction to the Crisis Communication Plan
 - Reporting procedures for potential crises
 - Basic crisis response protocols
 - Internal communication channels during a crisis
 - Personal safety and evacuation procedures
- Format: Online training modules and interactive sessions
- Frequency: Annually, with refresher courses as needed
- Duration: 1-2 hours
- Responsible Person: Finance/Admin Lead and Communications Lead

3. Spokesperson Training:

- Objective: To prepare designated spokespersons to communicate effectively with the media and the public during a crisis.
- Content:
 - Media relations and handling press inquiries
 - Crafting and delivering key messages
 - Techniques for managing difficult questions
 - Maintaining composure under pressure
 - Simulated press conferences and interviews
 - Format: In-person workshops and mock interviews
 - Frequency: Bi-annually

- Duration: 1/2 day (2-4 hours)
 - Responsible Person: Communication Lead and External Consultant
4. Simulation Exercises:
- Objective: To test the effectiveness of the Crisis Communication Plan and the readiness of the Crisis Management Team and employees.
 - Content:
 - Full-scale crisis simulation based on realistic scenarios
 - Real-time decision-making and coordination
 - Post-exercise debrief and evaluation
 - Identifying gaps and areas for improvement
 - Format: Live drills and tabletop exercises
 - Frequency: Biannually
 - Duration: 1/2 day (2-4 hours)
 - Responsible Person: Crisis Manager and External Consultant

7. Appendices

7.1 Contact Lists

Crisis Management Team (CMT)

Name	Role	Phone	Email
Greg Drent	Crisis Manager	952-233-1511	gdrent@shakopeeutilities.com
Sharon Walsh	Communication Lead	952-233-1531	swalsh@shakopeeutilities.com
Spencer Fane LLC	Legal Lead	612-268-7000	
BJ Letourneau	Commissioner President	952-445-1988	bletourneau@shakopeeutilities.com

Leadership Team

Name	Role	Phone	Email
Brad Carlson	Director of Field Ops	952-345-2488	bcarlson@shakopeeutilities.com
Philip Dubbe	Director of IT	952-345-2470	pdubbe@shakopeeutilities.com
Kelley Willemssen	Director of Finance/ Administration	952-233-1516	kwillemssen@shakopeeutilities.com
Joe Adams	Director of Planning & Engineering	952-233-1501	jadams@shakopeeutilities.com

SPU Commission

Name	Role	Phone	Email
Kathi Mocol	Commissioner VP	952-445-1988	kmocol@shakopeeutilities.com
Jim Dulaney	Commissioner	952-445-1988	jdulaney@shakopeeutilities.com
Kayden Fox	Commissioner	952-445-1988	kfox@shakopeeutilities.com
Justin Krieg	Commissioner	952-445-1988	jkrieg@shakopeeutilities.com

Community/Partner Contacts

Name	Organization	Phone	Email
William Reynolds	City Administrator	952-233-9311	breyolds@shakopeeMN.gov
Chelsea Petersen	Asst City Administrator	952-233-9310	cpetersen@shakopeeMN.gov
Matt Lehman	Mayor	952-496-2069	
Tim Zunker	Chamber of Commerce	952-445-1660	tzunker@shakopee.org
Jeff Tate	Crisis Mgr - City	952-233-9400	jtate@shakopeemn.gov

Emergency Services

Service	Phone
Police	952-445-1411 or 911
Fire Department	952-233-9400 or 911
Ambulance	911
St. Francis Regional Medical Center	952-428-3000
Scott County Sheriff	952-496-8300 or 911
FEMA	1-800-621-3362

Regulatory Contacts

Name	Organization	Phone	Email or Website
	MN DOH - Main	651-201-5000	https://www.health.state.mn.us/about/phones.html
	MN DOH – Drinking Water	651-201-4700	https://www.health.state.mn.us/communities/environment/water/index.html
	OSHA –Emergency	800-321-6742	www.osha.gov
	CDC (Environmental Hazard)	800-232-4636	cdcinfo@cdc.gov

Utilities Contacts

Service	Organization	Phone
Electricity	Xcel Energy - Safety	800-895-2999
Gas	Centerpoint - Emergency	800-722-9326
Utility Association	MMUA	763-551-1230
Power Generation	MMPA-Oncu Er	312-349-6868

Key Suppliers

Name	Organization	Phone	Email
Ethan Sweet – Account Mgr	BSE	218-330-7625	esweet@borderstates.com
John Selsvold	Core & Main	952-937-9666	john.selsvold@coreandmain.com
Brad Bersch – Account Mgr	USS	262-328-7241	bradb@united-systems.com
Mark Bruss – Channel Field Sales Mgr	Ittron	314-406-4561	mark.bruss@itron.com

Key Customers/Clients

Name	Organization	Phone	Email

7.2 Communication Templates

Holding Statement Template

- Facebook

We are aware of an incident that occurred on [date] at [location]. We are currently investigating the situation and gathering all the relevant details. Our priority is to ensure the safety and well-being of our employees, customers, and the community.

We are working – or - *closely with [relevant authorities/agencies as applicable]* - to address the situation as quickly and efficiently as possible. We are committed to providing accurate and timely information as soon as it becomes available. Currently, we do not have all the facts.

Statement from Leadership:

"[Name, Title] stated, 'Our thoughts are with everyone affected by this incident. We are doing everything we can to support those impacted and to address the situation. We appreciate your patience and understanding as we work through this.'"

Please share this post with others and continue to follow us on Facebook for further updates.

We thank you for your understanding and cooperation during this time.

– Internal Email

We are aware of an incident that occurred on [date] at [location]. We are currently investigating the situation and gathering all the relevant details. Our priority is to ensure the safety and well-being of our employees, customers, and the community.

We are working – or - *closely with [relevant authorities/agencies as applicable]* - to address the situation as quickly and efficiently as possible. At this time, we do not have all the facts, but we are committed to providing accurate and timely information as soon as it becomes available.

We will provide updates and directions as soon as we have more information. Please monitor your email for future updates and instructions.

We thank you for your understanding and cooperation during this time.

Media Statement Template (followup)

- Facebook

SPU is currently responding to [brief description of the crisis]. As previously stated, our primary concern is the safety and well-being of our employees, customers, and the community. We are taking immediate steps to address the situation and provide support to those affected.

Incident Overview:

- When it happened: [Date and time of the incident]
- What happened: [Provide a factual description of the incident]
- Where it happened: [Location of the incident]
- Immediate actions taken: [List the steps taken to address the crisis]
- Support provided: [Describe any support being offered to those affected]
- Coordination with authorities: [Mention any collaboration with emergency services or authorities]
- Please click here for additional information regarding the impact of this situation and the next steps we are taking to contain and resolve the incident.

- Website (the above, plus the following)

Impact Assessment:

- Operational impact: [Briefly describe how operations are affected]
- Safety impact: [Mention any injuries or safety concerns]
- Reputation impact: [Address any potential impact on the organization's reputation]
- Stakeholder Communication:
 - Employees: [Summary of internal communication efforts]
 - Customers: [Summary of communication with customers]
 - Public and media: [Summary of public and media communication efforts]

Next Steps:

- Ongoing response efforts: [Describe any ongoing actions or investigations]
- Future updates: [Mention how and when the organization will provide further updates]
Please follow us on Facebook where updates will be provided. Links to our website will be provided with more detailed information, contacts and resources.
- Media requests can be directed to:
 - Name: Sharon Walsh
 - Title: Director of Communications
 - Phone: 952-233-1531
 - Email: swalsh@shakopeeutilities.com

Internal Memo Template (follow up)

Team,

As you are aware, [Brief description of the crisis/event] occurred on [date] at [location].

Here's what we know so far:

Incident Overview:

- What happened: [Brief, factual description of the incident]
- Impact: [Initial impact, such as injuries, service disruptions, data breaches, etc.]

Our Response:

Here are the immediate steps we have taken:

- [Action 1]
- [Action 2]
- [Action 3]

Support and Resources:

We understand that this situation may cause concern and uncertainty. We are committed to providing support and resources to our employees:

- Workplace Safety: [Any changes to workplace safety protocols or procedures]
- Operational Changes: [Information on any changes to work hours, remote work policies, etc.]
- Communication: Please check your email and iVue regularly for updates. We will provide updates as more is learned or the situation evolves. You can expect daily communications at a minimum. If urgent communication is needed, we will text you or speak to you in person. Please keep your cell phones near you.
- Be Supportive: Offer support to your colleagues and reach out if you need help.
- Follow Guidelines: Adhere to any new safety protocols or procedures.

Leadership Statement:

[Name, Title] shared, 'The entire leadership team is deeply concerned about this incident and we are taking all necessary steps to address the situation, keep everyone safe and support our team - our work family - anyway that we can. Please reach out to your supervisor if you need additional assistance.'

Closing: Thank you for your cooperation and assistance as we navigate these new waters. We will continue to provide updates as more information becomes available.

Press Release Template (if needed/requested)

[City, State] – [Date] – Shakopee Public Utilities (SPU)

Introduction:

On [Date], SPU experienced a [brief description of the crisis]. This incident occurred at [location] and resulted in [immediate impact, such as injuries, service disruptions, data breaches, etc.].

Body: (Detailed account of what, when and impact)

At approximately [time], [description of the events leading to the crisis]. The cause of the incident is currently under investigation, and we are working closely with [relevant authorities or agencies]."

Company's Response: (Actions taken – what we've done)

We have initiated our emergency response plan, which includes [specific actions taken]. Our priority is the safety and well-being of our employees, customers, and the community. We have [steps taken to mitigate the crisis].

Statements from Leadership: (Express empathy, commitment to resolution and future preventative measures)

"We are deeply concerned and troubled by this incident and are committed to taking all necessary steps to prevent it from happening again. Our thoughts are with those affected, and we are doing everything we can to support them during this challenging time."

Future Actions: (Outline the steps your company plans to take to prevent similar incidents in the future. Mention any policy changes, safety improvements, or additional training.)

We will be conducting a thorough review of our [relevant processes] and implementing additional safety measures, including [specific actions].

Contact Information:

For further information, please contact:

Sharon Walsh, Director of Communications

952-233-1531

swalsh@shakopeeutilities.com

Shakopee Public Utilities (SPU) is a local municipal utility providing electric and water services to the City of Shakopee and surrounding townships. SPU has approximately 21,000 residential, commercial and industrial electric customers, and approximately 12,000 water customers. Since 1950 we have diligently worked to provide quality services that are reliable and competitively priced, and to be a proud and supportive community member.

7.3 Forms

Crisis Assessment Template

1. Crisis Overview

Incident Report Date: _____ Time: _____ Reported By: _____

Crisis Description:

Type of Crisis: 1-5 (see page 2)

Brief Description:

Affected Areas/Departments:

2. Initial Impact Assessment – impact on each category

Operations: _____

Safety and Security: _____

Reputation: _____

Financial Implications: _____

Legal and Regulatory: _____

3. Stakeholder Analysis/Affected Stakeholders:

Employees: _____

Customers: _____

Suppliers: _____

Regulators: _____

Media/Public: _____

4. Severity and Risk Assessment Severity Levels:

Impact	Probability	Severity Level
Low	Low	Minor
Moderate	Moderate	Moderate
High	High	Severe

5. Response Actions

Immediate Actions Already Taken:

Additional Actions Required to Further Manage and Mitigate the Crisis:

Resource Allocation (personell, financial, technical):

6. Communication Plan Internal Communication:

Internal Audience

Communication Method:

External Customers

Communication Method:

Media/Public

Communication Method:

7. Monitoring and Review/Ongoing Monitoring:

Methods for monitoring the situation (e.g., regular updates, reporting systems):

Schedule for reviewing the status and effectiveness of the response actions:

Incident Report Template

1. Incident Overview

Date of Incident: _____

Time of Incident: _____

Location of Incident: _____

Reported By: _____

2. Brief Description of the Incident:

3. Incident Details

How was the incident detected?

Initial Actions Taken:

Were emergency services contacted?

- Yes
- No

If Yes, which services and response times:

Injuries or Fatalities:

- Yes
- No

If Yes, provide details:

4. Root Cause Analysis/Preliminary Investigation:

Possible Causes Identified:

Supporting Evidence:

Post-Crisis Review Template

Crisis Overview Crisis – Attach the completed Crisis Assessment Form

Crisis Management and Response Operational Impact:

Affected Departments/Areas: _____

Impact on Operations: _____

Safety and Security:

Injuries or Fatalities: _____

Safety Measures Implemented: _____

Financial Impact:

Estimated Costs: _____

Insurance Claims: _____

Stakeholder Impact:

Affected Stakeholders: _____

Stakeholder Communication: _____

Performance Evaluation Response Effectiveness:

Response Time: _____

Decision-Making: _____

Resource Allocation: _____

Communication Effectiveness:

Internal Communication: _____

External Communication: _____

Coordination with External Agencies:

Agencies Involved: _____

Effectiveness of Coordination: _____

Lessons Learned Strengths:

What Worked Well: _____

Areas for Improvement:

Challenges Faced: _____

Gaps Identified: _____

Recommendations Immediate Actions: _____

Actions to Address Identified Gaps: _____

Long-Term Improvements: _____

Policy Changes: _____

Training and Preparedness: _____

Resource Needs:

Additional Resources Required: _____

Plan Updates and Follow-Up Updates to Crisis Communication Plan:

Specific Changes to be Made: _____

Follow-Up Actions:

Assigned Responsibilities: _____

Follow-Up Review Date: _____

Review and Approval Prepared By:

Name: _____

Title: _____

Date: _____

Reviewed By:

Name: _____

Title: _____

Date: _____

Approved By:

Name: _____

Title: _____

Date: _____

Location: [Internal Document Management System Link]