



GRAND RAPIDS PUBLIC UTILITIES COMMISSION REGULAR WORK SESSION MEETING AGENDA

Wednesday, August 13, 2025

8:00 AM

CALL TO ORDER: Pursuant to due notice and call thereof, a Work Session Meeting of the Grand Rapids Public Utilities Commission will be held on Wednesday, August 13, 2025 at 8:00 AM in the conference room of the Public Works/Public Utilities Service Center at 500 SE 4th Street, Grand Rapids, Minnesota.

CALL OF ROLL:

BUSINESS:

1. Consider a motion to ratify \$2,272,687.71 in verified claims for July and August 2025.
2. Operations & Capital Updates
3. Strategic Plan Annual Review

ADJOURNMENT:

The next Regular Meeting of the Commission is scheduled for Wednesday, August 27, 2025 at 4:00 PM in the conference room of the Public Works/Public Utilities Service Center at 500 SE 4th Street.

The next Special meeting/Work Session is scheduled for Wednesday, September 10, 2025 at 8:00 AM in the conference room of the Public Works/Public Utilities Service Center at 500 SE 4th Street.

The GRPUC has adopted a Meeting Protocol Policy, which informs attendees of the GRPUC's desire to conduct meetings in an orderly manner which welcomes all civil input from interested parties. If you are unaware of the policy, please contact our office at 218-326-7024 and we will provide you with a copy of the policy.



GRAND RAPIDS PUBLIC UTILITIES COMMISSION AGENDA ITEM

AGENDA DATE: August 13, 2025

AGENDA ITEM: Consider a motion to ratify \$2,272,687.71 in verified claims for July and August 2025.

PREPARED BY: Jean Lane, Business Services Manager

BACKGROUND:

See attached check registers:

Computer check register \$1,458,566.83
Manual check register \$814,120.88

Total \$2,272,687.71

RECOMMENDATION:

Consider a motion to ratify \$2,272,687.71 in verified claims for July and August 2025.

Grand Rapids Public Utilities
Accounts Payable
July/August 2025
(Meeting Date: 8/8/25)

Item 1.

NAME	AMOUNT	NAME	AMOUNT
APG Media	3,610.00	OPG-3	8,350.00
Bolton & Menk	64,937.50	Paul Bunyan	6,985.15
Border States	5,859.96	Personnel Dynamics	3,730.33
Burggrafs Ace	848.23	Pioneer Critical Power	10,585.17
Busy Bees Cleaning	2,324.00	Pitney Bowes	605.85
Central McGowan	2,182.67	Public Utilities	2,988.18
City of Grand Rapids	637.50	Quality Flow Systems	11,245.49
Cole Hardware	785.72	Rapid Crane & Rigging	7,200.00
Compass Minerals	4,870.21	Rapids Radio	955.50
Cooperative Response Center	2,262.60	RMB	2,300.80
Core & Main	15,953.17	Sandstrom	696.90
Davis Oil	2,236.31	SpencerFane	352.00
Duncan Co	3,780.92	SpryPoint	29,400.00
Emergent Software	8,287.50	Stuart Irby	1,975.00
Enterprise Fleet Management	6,060.55	TNT Construction	24,534.45
Fastenal	1,810.72	USA Bluebook	426.23
Gopher State One	267.30	UtilityLogic	2,695.00
Grainger	80.97	Vestis	139.78
Graybar	1,043.70	Viking Electric	242.06
Hach	317.44	Wesco	3,864.96
Hawkins	13,815.62	Xerox	367.99
Innovative	303.81	Ziegler	36.65
Idexx	1,483.89		
Itasca County	1,632.58	Energy Efficiency Rebate:	
League of MN Cities	15,034.00	Christianson, Ryan & Katie	1,000.00
Lanyk Electric	5,973.58	Healing Hands Chiropractic	1,800.00
Locators & Supplies	1,324.65	Mattson, Susan	140.00
MN Department of Labor & Industry	100.00	Mlinar, Matthew	30.00
MN Energy	18.00	My Place Hotel	3,175.29
MN Power	1,157,788.84	Niemi, Sally	20.00
Mpower	675.00	Russell, Carole	1,000.00
Northeast Service Cooperative	200.00	Thomas, Cindy Lee	20.00
Northeast Technical Services	1,595.00	Ward, Michael	20.00
Northwest Gas	882.11		
Nos Automation	2,700.00		
		Total	1,458,566.83

July 2025 Check Register

Document Date	Check #	Vendor Name	Document Amount	
7/1/2025	5413	Northeast Service Cooperative	4,844.00	7/31/2025
7/1/2025	5414	Northeast Service Cooperative	64,355.48	7/31/2025
7/1/2025	5415	WEX Health	1,168.16	7/31/2025
7/1/2025	5416	UNUM Life Insurance Company of America	4,341.71	7/31/2025
7/11/2025	5417	Public Employees Retirement Association	20,115.75	7/11/2025
7/11/2025	5418	MN Department of Revenue	5,964.14	7/11/2025
7/11/2025	5419	Wells Fargo Bank	34,324.48	7/11/2025
7/11/2025	5420	Voya Institutional Trust Company	11,378.59	7/11/2025
	5421-5424	Used in June and Feb		
7/8/2025	5425	Invoice Cloud	3,479.20	7/31/2025
7/15/2025	5426	WEX Health	1,168.16	7/31/2025
7/25/2025	5427	Public Employees Retirement Association	18,695.21	7/25/2025
7/25/2025	5428	MN Department of Revenue	5,389.27	7/25/2025
7/25/2025	5429	Wells Fargo Bank	31,340.16	7/25/2025
7/25/2025	5430	Voya Institutional Trust Company	10,532.42	7/25/2025
7/28/2025	5431	WEX Health	1,208.16	7/31/2025
7/8/2025	5432	Wells Fargo PCard	9,000.15	7/8/2025
7/11/2025	5433	Public Employees Retirement Association	0.00	7/11/2025
7/20/2025	5434	MN Department of Revenue	203.00	7/31/2025
7/20/2025	5435	MN Department of Revenue	85,469.00	7/31/2025
7/8/2025	84758	Postage By Phone System	5,000.00	7/8/2025
7/8/2025	84759	First Net AT & T Mobility	476.95	7/8/2025
7/8/2025	84760	Verizon Wireless	966.15	7/8/2025
7/8/2025	84761	Mattson Steve	27.30	7/8/2025
7/10/2025	84762	City of LaPrairie	19,486.00	7/31/2025
7/11/2025	84763	MN Child Support Payment Center	427.31	7/11/2025
7/11/2025	84764	NCPERS Group Life Insurance	80.00	7/11/2025
7/22/2025	84765	MN Pollution Control Agency	14,350.00	7/22/2025
7/22/2025	84766	Postage By Phone System	5,000.00	7/22/2025
7/22/2025	84767	Paul Bunyan Communications	11,131.70	7/22/2025
7/22/2025	84768	US Bank Equipment Finance	243.11	7/22/2025
7/22/2025	84769	Customer Refunds Utility Accounts	70.84	7/31/2025
7/22/2025	84770	Customer Refunds Utility Accounts	15.85	7/31/2025
7/22/2025	84771	Customer Refunds Utility Accounts	48.39	7/31/2025
7/22/2025	84772	Customer Refunds Utility Accounts	160.18	7/31/2025
7/22/2025	84773	Customer Refunds Utility Accounts	115.18	7/31/2025
7/22/2025	84774	Customer Refunds Utility Accounts	13.49	7/31/2025
7/22/2025	84775	Customer Refunds Utility Accounts	98.98	7/31/2025
7/22/2025	84776	Customer Refunds Utility Accounts	3.70	7/31/2025
7/22/2025	84777	Customer Refunds Utility Accounts	10.52	7/31/2025
7/22/2025	84778	Customer Refunds Utility Accounts	246.82	7/31/2025
7/22/2025	84779	Customer Refunds Utility Accounts	79.36	7/31/2025
7/22/2025	84780	Customer Refunds Utility Accounts	121.15	7/31/2025
7/22/2025	84781	Customer Refunds Utility Accounts	120.30	7/31/2025
7/22/2025	84782	Customer Refunds Utility Accounts	117.94	7/31/2025
7/22/2025	84783	Customer Refunds Utility Accounts	93.62	7/31/2025
7/22/2025	84784	Customer Refunds Utility Accounts	34.92	7/31/2025

7/22/2025 84785	Customer Refunds Utility Accounts	487.18	7/31/2025
7/22/2025 84786	Customer Refunds Utility Accounts	66.29	7/31/2025
7/22/2025 84787	Customer Refunds Utility Accounts	122.34	7/31/2025
7/22/2025 84788	Customer Refunds Utility Accounts	90.86	7/31/2025
7/22/2025 84789	Customer Refunds Utility Accounts	384.34	7/31/2025
7/22/2025 84790	Customer Refunds Utility Accounts	95.16	7/31/2025
7/22/2025 84791	Customer Refunds Utility Accounts	224.86	7/31/2025
7/25/2025 84792	MN Child Support Payment Center	427.31	7/25/2025
7/25/2025 84793	MN Council 65	1,855.80	7/25/2025
7/25/2025 84855	MN Unemployment Insurance Fund	764.55	7/25/2025
7/30/2025 84856	City of Grand Rapids	72,333.33	7/31/2025
7/31/2025 84857	City of Grand Rapids	136.50	7/31/2025
7/31/2025 84858	City of Grand Rapids	78,749.22	7/31/2025
7/31/2025 84859	Border States Electric	4,776.68	7/31/2025 *
7/8/2025 EFT000000000006	UPS	212.96	7/8/2025
7/22/2025 EFT000000000006	UPS	111.88	7/22/2025
7/25/2025 EFT000000000006	US Bank NA	116,993.75	7/25/2025
7/25/2025 EFT000000000006	Hansen Mark	40.00	7/25/2025
7/25/2025 EFT000000000006	Stoltz Gary	40.00	7/25/2025
7/25/2025 EFT000000000007	Blanchard Jason	40.00	7/25/2025
7/25/2025 EFT000000000007	LeClaire Mike	40.00	7/25/2025
7/25/2025 EFT000000000007	American Eagle Security Systems Incorporated	33,495.00	7/25/2025
7/25/2025 EFT000000000007	Riley Joseph	40.00	7/25/2025
7/25/2025 EFT000000000007	Dimich Corey	40.00	7/25/2025
7/25/2025 EFT000000000007	Stanley Tom	716.20	7/25/2025
7/25/2025 EFT000000000007	Trboyevich Doug	40.00	7/25/2025
7/25/2025 EFT000000000007	Rundell Eric	40.00	7/25/2025
7/25/2025 EFT000000000007	Langer Stephen A	40.00	7/25/2025
7/25/2025 EFT000000000007	Lane Jean	40.00	7/25/2025
7/25/2025 EFT000000000008	Computershare	134,816.55	7/25/2025
7/25/2025 EFT000000000008	Troumbly, Chad M	40.00	7/25/2025
7/25/2025 EFT000000000008	Sjostrand, Megan	40.00	7/25/2025
7/25/2025 EFT000000000008	Veith, Jaime	40.00	7/25/2025
7/11/2025 REMIT0000000000	Public Employees Retirement Association	0.00	7/11/2025

Checks Previously Approved **

4,776.68

Manual Checks/EFT to be approved

814,120.88

Total Manual Checks

818,897.56

Item 1.



GRAND RAPIDS PUBLIC UTILITIES COMMISSION AGENDA ITEM

AGENDA DATE: August 13, 2025

AGENDA ITEM: Operations & Capital Updates

PREPARED BY: GRPU Staff

BACKGROUND:

GRPU Operating & Capital Updates

RECOMMENDATION:

None. Review Only.

Grand Rapids Public Utilities

August 13, 2025

Operational and Capital Updates

GRPU Management Team





MISSION VISION VALUES

Item 2.

WHO WE ARE

Grand Rapids Public Utilities (GRPU) is a statutory municipal utility established by the city of Grand Rapids, Minnesota. The Grand Rapids Public Utilities Commission (GRPUC) provides full control, operation and management of the GRPU electric power distribution system, the water production, treatment and distribution systems, and the wastewater collection and treatment systems.



Our Vision

Our vision is to be a dynamic public asset for the thriving community of Grand Rapids, enhancing lives and fostering growth through excellence in the provision of essential utility services.



Our Mission

Our mission is to empower GRPU team members to deliver safe, reliable, affordable, sustainable, and customer-focused utility services for our community.



Our Values

Safety

We hold paramount the well-being of our employees and the public in all operations.

Integrity

We uphold ethical standards and foster trust with all stakeholders.

Customer Focus

We prioritize customer needs and satisfaction in all our decisions and actions.

Efficiency

We maximize resources to provide cost-effective services without compromising quality.

Reliability

We consistently deliver high-quality utility services and strive for uninterrupted access.

Sustainability

We employ environmentally responsible practices in our operations and services.

Transparency

We openly share information and decision-making processes, promoting informed community involvement.



Strategic and Sustainable Fiscal Management (FM)

Item 2.

Operations: Draft Fraud Prevention Policy by Jean Lane

Purpose:

Prevent fraudulent payments and protect public funds.

Scope:

Applies to all GRPU departments and employees involved in disbursement activities.

Background:

Fraud tactics like impersonation and fake invoices target public entities. GRPU must adapt with modern controls.

Key Controls:

•Accounts Payable:

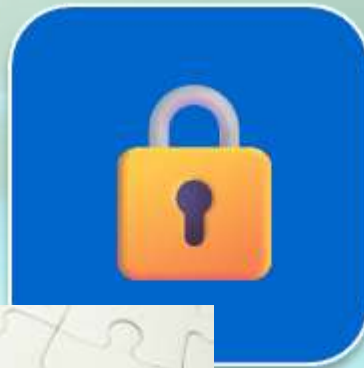
- Dual approvals, vendor file reviews, verbal confirmation of vendor changes
- ACH blocks/filters, positive pay, secure vendor info handling

•Payroll:

- Written + verbal confirmation for banking changes
- Secure storage of sensitive data

•Wire Transfers:

- Two-tier approval (e.g., \$250K / \$500K thresholds)
- Independent vendor verification outside of email





Engaging and Educating the Community (EC)

Item 2.

Operations: New SpryPoint Utility Bill Template by Julie Kennedy

- SpryPoint go-live is Sept 2-6
- Multi-channel awareness campaign begins next week
- Requesting Commissioner review of bill template
- Requesting Commissioner testimonials and voices

Coming Soon!

New Utility Customer Service Portal

Your one-stop destination for managing all your utility needs!

Grand Rapids Public Utilities is thrilled to announce the launch of its brand-new Utility Customer Service Portal, designed with you, the customer, in mind. Managing your utility services has never been easier or more convenient.

Easy account management

- 24/7 access
- User friendly

Streamlined billing and payments

- View bills
- Multiple payment options
- Set up auto-pay
- Go paperless


















Payments will not process after August 28 for any scheduled payments or auto pay until your new online account is created. This may affect bill pay through your bank. Customers will not be able to make a one-time payment after August 28 until the new online portal goes live.

All online customers must create a new online account.
All auto-pay customers must re-enroll.

Watch our website for more information: www.grpuc.org

Customer Outreach > SpryEngage

	Name ▾
	Commercial Customer Meetings
	Direct Mail
	Facebook
	Graphics
	Graphics for SpryPoint
	Group Housing Visits
	Herald Review & Manneys
	ICTV
	Open House at GRPU
	Radio
	SpryPoint Resources
	WDIO Digital Marketing
	Website
	SpryPoint Engagement Budget.xlsx



Operations: Family Medical Leave Act vs Paid Family Medical Leave by Megan Sjostrand

Feature	FMLA (Federal)	Minnesota PFML
Launch Date	Established in 1993, ongoing	Effective Jan 1, 2026
Eligible Employers	50+ employees within 75-mile radius. In spirit of the law, GRPU honors FMLA	Applies to nearly all employers regardless of size
Employee Eligibility	≥12 months employment; ≥1,250 hours in past 12 mo	Begins after 90 consecutive days on job (90 calendar days from date of hire) ; covers full- and part-time workers
Leave Type	FMLA (Federal)	Minnesota PFML
Medical (self)	Up to 12 workweeks unpaid per 12-mo	Up to 12 weeks paid per year (52-week period from first day of a qualifying leave)
Family / Bonding	Up to 12 weeks unpaid	Up to 12 weeks paid for bonding, caregiving, military,
Combined Maximum	12 weeks (or 26 weeks for military caregiver)	20-week annual cap; e.g. 12-week medical + 8-week family



Operational Excellence (OE)

Item 2.

Operations: FMLA vs PFML by Megan Sjostrand

Job Protection: Both guarantee reinstatement to same or equivalent job and continuation of benefits (e.g. healthcare) during leave.

Wage Replacement:

- **FMLA:** Leave is **unpaid**, though employees may substitute accrued PTO.
- **Minnesota PFML:** Partial paid benefit:
 - For weekly wages between \$0 and \$711.50 (half of the current state average), you get paid 90% .
 - For weekly wages between \$711.50 and \$1,423 (the current state average), you get paid 66%.
 - For weekly wages above \$1,423, you get paid 55%.

Weekly payments cannot exceed the state average weekly wage, \$1,423. To receive payments, you must have earned at least 5.3% of the state's average annual wage (about \$3,900) in the past year.





Operational Excellence (OE)

Item 2.

Operations: PFML Example by Megan Sjostrand

Mom Going on Leave for Childbirth (No Complications)

Facts:

- Employee gives birth (normal delivery, no complications)
- Pre-leave weekly gross income: \$1,700
- Using 2026 Average Weekly Wage (AWW) = \$1,423
- Leave type: First Medical Leave (for recovery), then Family Leave (bonding)
- For medical leave under Minnesota's Paid Family & Medical Leave (PFML) program, a certification form must be completed by a qualified health care provider. For bonding leave, documentation is required to confirm the birth or placement of a child in your home.



Operations: PFML Example by Megan Sjostrand

PFML Leave Duration Breakdown

Medical Leave (Own Serious Health Condition):

- Standard post-partum recovery is generally considered to be **6 weeks** or **8 weeks**
- In this case, let's assume **6 weeks** of Medical Leave

Family Leave (Bonding):

- Eligible for **up to 12 weeks** of Family Leave to bond with the newborn
- This bonding leave must be taken within **12 months** of the child's birth
- Can be taken **consecutively or intermittently**, but must be completed within that 12-month window

Total Time Off:

- **6 weeks Medical Leave + 12 weeks Family Leave = 18 weeks total leave**
- This is well within the 20-week PFML annual maximum





Operational Excellence (OE)

Item 2.

Operations: PFML Example by Megan Sjostrand

Step-by-Step Benefit Calculation for \$1,700/week

1. **First \$711.50** → 90% = **\$640.35**
2. **Next \$711.50** (up to AWW) → 66% = **\$469.59**
3. **Remaining \$277.00** (amount over AWW) → 55% = **\$152.35**

Total Weekly PFML Benefit =

\$640.35 + \$469.59 + \$152.35 = \$1,262.29

Estimated total PFML payout

18 weeks × \$1,262.29 = \$22,721.22 (gross)

Note: PFML benefits **are taxable** income, so actual take-home may be lower depending on withholdings.





Operational Excellence (OE)

Item 2.

Operations: State PFML vs Private PFML by Megan Sjostrand

Feature	Private Plan (Unum)	Minnesota State Plan
Annual Cost to Employer & Employee <i>*Employer is required to pay 50% of premium</i>	\$23,476.32 annual cost (.65% premium)	\$31,783.32 (.88% premium)
Claims Experience	Decades of experience	No claims processed to date
Billing & Admin	Consolidated with our other Unum benefits	Separate, state-run system
Turnaround Time	Proven, efficient processing	Unproven infrastructure
Employee Continuity	Integrated with STD & LTD	Standalone program
High Earner Support	Supplemental STD fills PFML gaps	PFML Based on (AWW) currently set at \$1,423.00/week for 2026
Employer Reimbursement	<ul style="list-style-type: none">• Employer reimbursement is allowed.• Employer can deduct taxes and benefit premiums.• Employer issues payment directly to the employee	<ul style="list-style-type: none">• No employer reimbursement available• Taxes are not automatically withheld• Employee is responsible for managing taxes and benefit premiums upon returning from leave

Short Term Disability Rate Credit: Unum has applied a PFML offset to the STD policy, reducing the monthly STD premium from \$991.61 to \$350.88 — an immediate savings of \$640.74/month = \$7,688.88 annual savings

Operational Excellence (OE)

Item 2.

Operations: PFML upcoming decisions by Julie Kennedy

GRPU decisions to be considered:

- Cover both employer and employee portion for PFML for 2026?
- Include PFML in compensation negotiations in 2026 for 2027-2029 labor contract
- Eliminate STD in lieu of PFML after 2027
- Continue to improve 3-deep concept



Strategic Planning: 3-Deep Concept

Julie Kennedy
General Manager

The Importance of a 3-Deep Concept in SOPs for Business Continuity and Succession Planning

GRPU will implement a "3-deep" concept in our Standard Operating Procedures (SOPs) as a proactive strategy to strengthen our organizational resilience, ensure business continuity, and support effective succession planning. The 3-deep model means that for every critical role and task, at least three individuals are trained and capable of performing it: the primary, a backup, and a second backup.

This approach reduces operational risk by ensuring that knowledge and responsibilities are not siloed with one person. Unexpected absences, turnover, or retirements won't halt operations if others are prepared to step in. It also promotes cross-training, enhances collaboration, and fosters a culture of shared accountability and continuous learning.

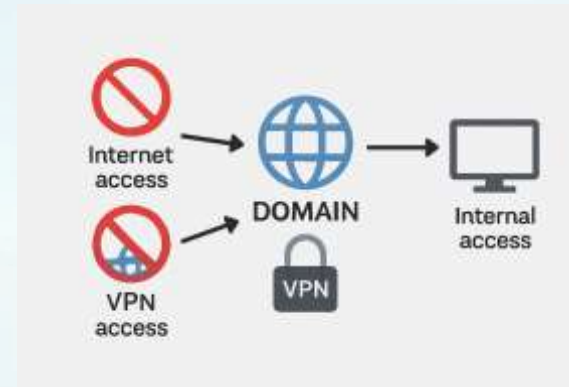
From a succession planning standpoint, the 3-deep model builds a pipeline of internal talent ready to move into higher-level roles. It provides opportunities for employees to grow their skillsets, increases organizational agility, and supports smoother transitions during staff changes.

Operational Excellence (OE)

Item 2.

Capital: Firewall Update by Mike LeClaire

- Existing Firewall Vulnerability Notification
- Shutdown External Domain and SSL
- Impact to customer access and online payments
- We are not the only ones – all TZ series SonicWalls
- Setback in configuration of NEW Firewall and backup



Operational Excellence (OE)

Item 2.

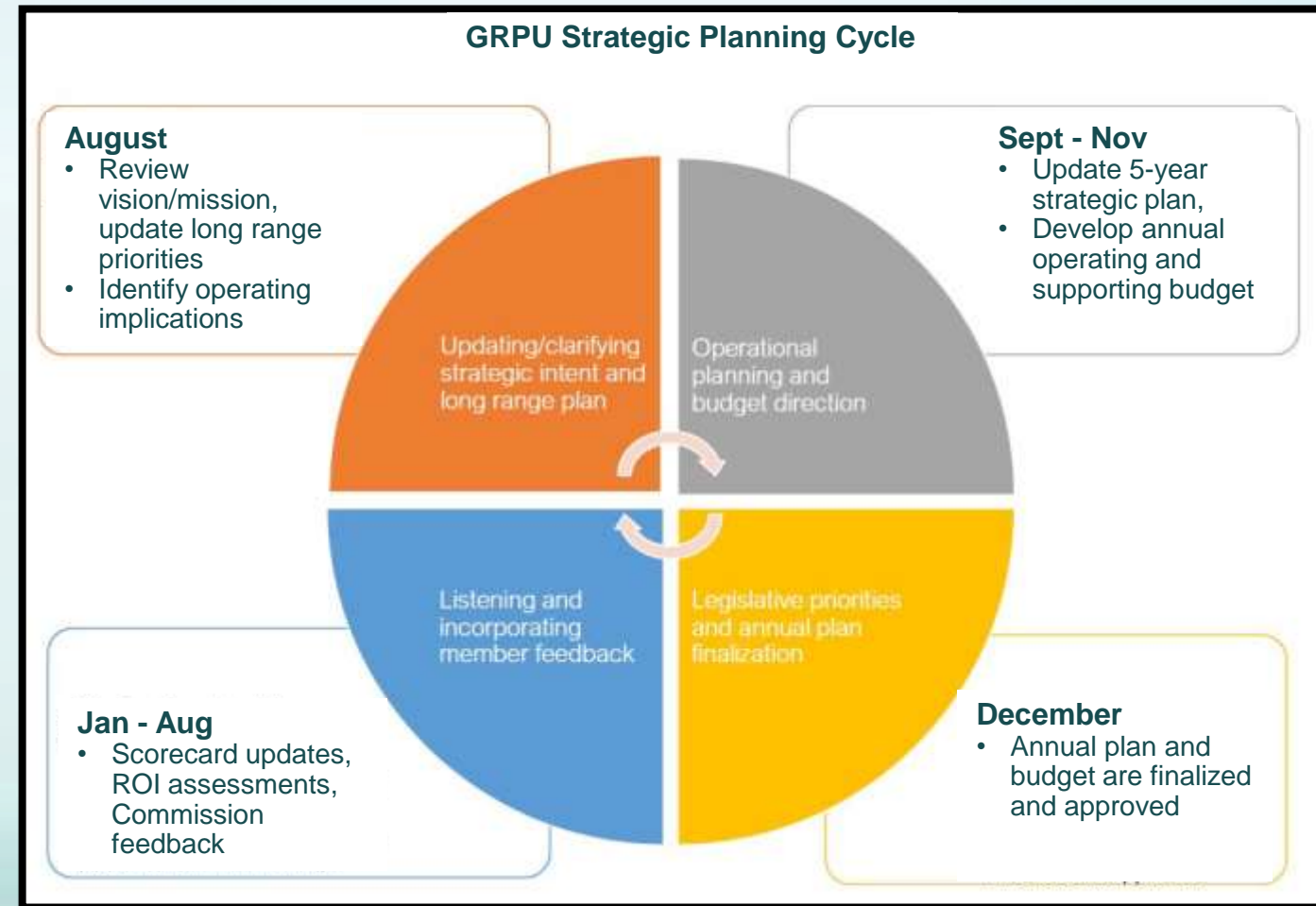
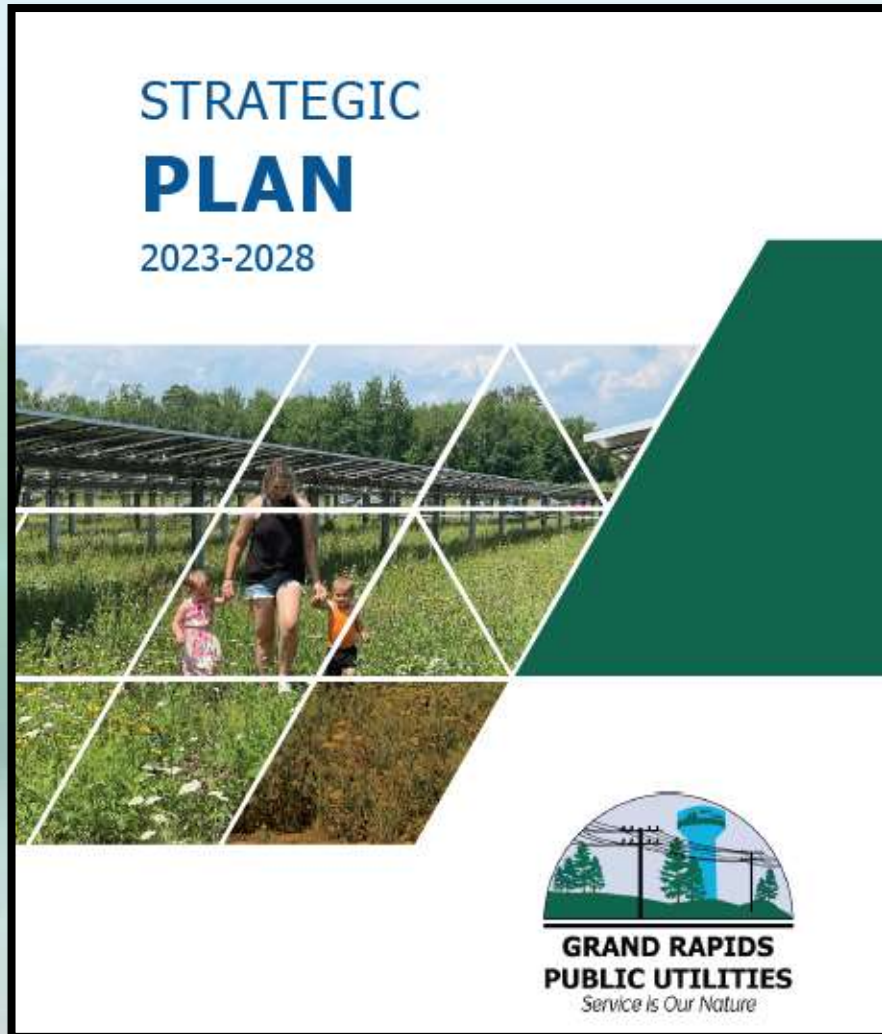
Capital: Information Systems Policy Modernization by Mike LeClaire

- Workstation Guidelines
- Remote Work Configuration
- Storage and Backups
- General Security
- Email
- NEW – Mobile Device Management
 - BYOD, Corporate Personal Phone, Corporate Phone (Shared), Corporate Laptops & Tablets, Kiosk tablets, Commission tablets
- Future updates to include unregistered device access to Microsoft Tenant – Currently not developed



Strategic Plan – Annual Review

Item 2.



Strategic Plan – Annual Review

Item 2.

GRPU Commission Strategic Planning Review

Please return to Julie by September 2, 2025

1. Take a minute to think about the needs and challenges our utility will be facing five years from now. What do you picture GRPU doing to respond?
2. Please review the planning assumptions that currently underpin GRPU's strategic plan (pages 6-7 of the plan). Are they still relevant? Have we missed anything?
3. Please review the strengths and weaknesses listed on pages 7-8 of the strategic plan. These are inwardly focused things that GRPU's leadership has identified in the past as important factors in our planning.
 - a. Which of them is no longer true and should be removed?
 - b. Which of them need to be updated?
 - c. Are there any strengths or weaknesses that should be added?
4. Please review the opportunities and threats listed on pages 8-9 of the strategic plan. These are outwardly focused forces that GRPU's leadership has identified in the past as important factors in our planning.
 - a. Which of them is no longer true and should be removed?
 - b. Which of them needs to be updated?

5. Previously, GRPUC developed the vision to be a dynamic public asset for the thriving community of Grand Rapids. Is that still a worthy goal? Why or why not?
6. If you believe GRPU should strive to be a public asset for Grand Rapids, what does that look like in the next five years and what do we need to do to grow in a manner consistent with that vision?
7. Please review our five strategic pillars as discussed on pages 12-14 of the strategic plan. Please write down the top 1-3 strategic things on which GRPU should be focused in each area, and the operational implications.

Pillar	Strategic Areas of Focus	Operational Implications
Uninterrupted, High-Quality Utility Services (US)	1.	1.
	2.	2.
	3.	3.

Grand Rapids Public Utilities

Upcoming Commission Meetings

Regular Meeting: August 27, 2025

Work Session: September 10, 2025





COMMISSION POLICY

Fraud Prevention

Category: Business Services	Subcategory:	Policy Number:
---------------------------------------	--------------	----------------

1.0 – Purpose

The purpose of this policy is to establish procedures to prevent fraudulent payments or transfers to employees, vendors, and contractors. Protecting public funds is a high priority for Grand Rapids Public Utilities Commission (GRPUC).

2.0 – Scope

This policy applies to all Grand Rapids Public Utilities (GRPU) departments and employees that have control over GRPU disbursement transactions and govern the actions of all GRPU employees.

3.0 – Background

Governments are becoming more transparent with information on the internet and electronic banking is becoming widely accepted. Effective internal control policies and procedures need to be adopted to protect municipal utility funds from fraudulently being disbursed.

Advances in technology have reduced the effectiveness of traditional fraud prevention techniques and have even enabled new forms of fraud. Fraudsters are using techniques like social engineering tactics, such as impersonation and manipulation, to deceive employees with legitimate-looking correspondence or phone calls to obtain personal information such as bank accounts or address changes that will re-direct payments intended for an employee or vendor. Often a fraudster will follow government news to learn of newly contracted vendors and use the information and proper timing to contact the municipal utility as the vendor impostor and request the first down payment. Municipal utilities should avoid listing dollar/percentage down payment details in commission public meeting information. Commonly used software allows fraudsters to copy or create legitimate-looking vendor invoices that include slight changes to the name and address.

4.0 – Policy

Processes to prevent fraud

Employee portals and municipal utility intranets should utilize multiple authentications when available. Following are processes to prevent the fraudulent disbursement of public funds.

Item 2.

Accounts payable

1. Vendor payment approvals
 - a. Require at least two approvals within the GRPU for all disbursements of funds.
 - b. Require municipal utility general manager or designee approval on large payments exceeding amounts set in GRPU policy.
2. Update and review vendor files annually
 - a. Review and correct duplicate vendors in system with minor differences, i.e., LLC or Inc.
 - b. Annually review list of vendors and close or inactivate vendors not currently used by GRPU.
 - c. Review for unusual activities such as fluctuation in payment amounts, activity for closed vendors, etc.
 - d. Compare vendor information such as phone numbers, address, and bank account information to employee records for other than employee expense reimbursements.
 - e. Develop vendor change form for critical information such as electronic banking information, addresses, or billing practices. These forms should not be provided online but requested from GRPU accounts payable.
 - f. Receive verbal communication using trusted information on files regarding all vendor changes on critical information.
3. Do not provide copies of contracts within commission packets that are posted on the GRPU website unless payment terms are hidden.
4. Do not provide copies of vendor invoices within commission packets that are posted on the utility website.
5. Always require a signed Form W-9 from every new payee in advance of making any payments or change in a mailing address. This can be confirmed online or directly with the IRS.
6. GRPU is required to use ACH blocks and filters as a fraud prevention tool. This requires wire transfers process to have two tier approval process. Above the first-tier specific dollar amount for a single approval, electronic or verbal authentication, with the banking institution and a higher second-tier specific dollar amount with dual approval, and verbal authentication with banking institution. For example, first-tier \$250,000 and second-tier \$500,000.
7. Required first-tier and second-tier specific dollar amount wire transfers to have a verification of the vendor payment with a representative of the vendor directly independent of email.
8. GRPU is required to use positive pay as a fraud prevention tool.

Payroll

1. Receive both written and verbal communication from the employee, confirming any requested changes to direct deposit banking information.
2. Develop employee change forms for critical information such as direct deposit banking information. These forms should not be provided online but requested from finance/human resources or kept on a secure employee intranet. All payroll and records containing data covered by Minnesota Government Data Practices Act must be stored and transmitted securely.

Review and Maintenance of Policy

The GRPU finance department is responsible for maintaining and reviewing this Fraud Prevention Policy.

GRPU Commissioner

GRPU Commissioner

POLICY HISTORY:

Adopted:

Revised:

12.0 INFORMATION SYSTEMS POLICY	2
12.1 PURPOSE	2
12.2 DEFINITIONS	2
12.3 INTRODUCTION	2
12.4 GENERAL	3
12.4.1 USE	3
12.4.2 PRIVACY	3
12.4.3 DEVICE MANAGEMENT	3
12.4.4 USER WORKSTATION GUIDELINES	3
12.4.5 REMOTE WORK CONFIGURATION	3
12.4.6 STORAGE & BACKUPS	4
12.4.5 TRANSPORTING FILES	4
12.4.7 WORK PRODUCT OWNERSHIP	4
12.4.7 SOFTWARE USE	4
12.5 SECURITY	5
12.5.1 PASSWORDS	5
12.5.2 ENCRYPTION	5
12.5.3 ACCESS	5
12.5.4 VIRUS DETECTION	6
12.6 INTERNET	6
12.6.1 USE	6
12.6.2 PROHIBITED ACTIVITIES	6
12.6.3 DOWNLOADS	6
12.6.4 MONITORING	6
12.6.5 INTERNET ACCESS CONTROL	7
12.7 E-MAIL	7
12.7.1 USE	7
12.7.2 GENERAL GUIDELINES	7
12.7.3 PROHIBITED ACTIVITIES	7
12.7.4 SENSITIVE COMMUNICATIONS	8
12.7.5 PRIVACY AND MONITORING	8
12.7.6 COMPLIANCE WITH APPLICABLE LAWS	8
12.7.7 OTHER POLICIES	8

12.8 MOBILE DEVICE MANAGEMENT (MDM)	9
12.8.1 Purpose.....	9
12.8.2 Security Risks Addressed.....	9
12.8.3 Device Categories & Management Policies.....	9
12.8.4 User Responsibilities	10
12.8.5 Policy Violations	10
12.8.6 Review and Updates.....	11

12.0 INFORMATION SYSTEMS POLICY

12.1 PURPOSE

The purpose of this policy is to govern the secure, responsible, and compliant use of the organization's cloud-based information systems and digital infrastructure. This includes all Microsoft Azure-hosted services, devices managed via Microsoft Intune, and identity access controlled by Microsoft Entra ID. The policy ensures the protection of data, user accountability, and consistent standards for all technology resources.

12.2 DEFINITIONS

The following definitions apply to this policy:

- **Information System:** All organizational computing resources including Azure-hosted services, virtual machines, cloud storage, corporate applications, endpoints, and associated networks.
- **Users:** All employees, contractors, consultants, temporary workers, and third parties authorized to access the organization's digital systems.
- **Microsoft Intune:** The mobile device and endpoint management platform used for enforcing compliance, security, and configuration policies.
- **Microsoft Entra ID:** The cloud-based identity and access management service (formerly Azure AD) for securing authentication and conditional access.
- **BYOD:** "Bring Your Own Device" – personally owned devices approved for limited business access through app-level controls.

12.3 INTRODUCTION

This policy governs the access to and use of the organization's information systems, including cloud-hosted services, on-premise devices, and remote access solutions. It also establishes procedures for data protection, authorized device use, identity access management, and system monitoring within Microsoft Azure and Microsoft 365

environments. Violations of this policy may result in disciplinary actions, contract termination, or legal consequences.

12.4 GENERAL

12.4.1 USE

Information systems are provided to support official organizational duties. Limited personal use is allowed if it does not interfere with work performance, incur additional cost, or violate other policies. All users must access systems in accordance with the organization's Respectful Workplace and Acceptable Use policies.

12.4.2 PRIVACY

All digital assets and communications transmitted through the organization's cloud and network systems are the property of the organization. While individual accounts are protected by passwords, users should not expect privacy. Microsoft Entra and security systems enable system administrators to access, monitor, or audit any activities within organizational systems.

12.4.3 DEVICE MANAGEMENT

All endpoints (laptops, tablets, smartphones) must be enrolled in Microsoft Intune prior to accessing corporate data. Corporate-owned devices are fully managed, while BYOD access is limited to protected apps (e.g., Outlook, Teams). Users may not alter configurations, disable compliance controls, or remove MDM tools. Personal data on BYOD devices remains private, but company data may be remotely wiped as needed. (For additional reference See Section 12.8)

12.4.4 USER WORKSTATION GUIDELINES

User workstations are set up to function within a sophisticated, networked environment. Users are not permitted to alter their system's configuration or delete/modify any files they did not create. If users encounter configuration issues, they should reach out to the IS Support team for help. All hardware and software changes or upgrades must be approved by the IS Manager. Installation of personal software on workstations or the network is prohibited unless explicitly authorized by the IS Manager. Users are encouraged to use the screen savers provided with the operating system. If you wish to use a different screen saver, please ensure it is appropriate for the workplace and get approval from the Department Manager. The marquee screen saver may only display the approved Mission Statement of the organization.

12.4.5 REMOTE WORK CONFIGURATION

Remote workstations must adhere to the same security and configuration standards as on-site workstations. Users are responsible for ensuring their remote work environment is secure and that their devices are configured correctly.

- **Security:** Remote workstations must have up-to-date antivirus software and use a secure, encrypted connection (VPN) to access the company network.

- **Configuration:** Users should not alter the configuration of their remote workstations without approval from the IS Manager. Any issues with configuration should be reported to IS Support.
- **Software:** Only authorized software may be installed on remote workstations. Personal software is prohibited unless explicitly approved by the IS Manager.
- **Data Protection:** Users must ensure that all company data is stored securely and that sensitive information is not accessible to unauthorized individuals.
- **Support:** IS Support is available to assist with any technical issues related to remote workstations. Users should contact IS Support for help with configuration, software, or security concerns.

12.4.6 STORAGE & BACKUPS

All workstations are backed up through Azure-based services with the following schedule:

- Daily incremental backups
- Weekly full backups
- Monthly offsite backups

Email systems automatically archive messages older than 60 days. Users are responsible for deleting nonessential emails to improve system performance. *(Need Clarification on how many days we want to set auto archive of messages. Also, should we develop an rule for auto deletion of nonessentials emails in the inbox, sent, deleted folders? Anything placed somewhere other than these folders would be saved after xxxx days?)*

12.4.5 TRANSPORTING FILES

To facilitate off-site work, employees may copy appropriate files to and from external storage devices or jump drives. “Appropriate files” include word processing documents, electronic spreadsheets, sanitary video files, and presentation graphic files. Any external storage devices or jump drives that are used in computers outside of the Commission must be scanned for viruses before being used in a Commission computer. No other files or information may be copied to or from Commission computers.

12.4.7 WORK PRODUCT OWNERSHIP

All digital files, content, and work products created, accessed, or stored on organizational systems are the exclusive property of the organization, regardless of the device used.. No user may withhold work products from the organization.

12.4.7 SOFTWARE USE

According to U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as \$100,000 per work copied, and criminal penalties, including fines and imprisonment. The Commission does not condone the illegal duplication of software or any other form of criminal activity. Employees who engage in such activity are also subject to discipline under the Commission’s disciplinary policies. The Commission complies with all software copyrights and terms of all software licenses. Commission employees may not

duplicate licensed software or related documentation. Any such duplication may result in liability for civil or criminal penalties. Software owned by the Commission may not be copied to external systems unless the license agreement allows such use and the IS Manager has approved the installation. Users may not modify or otherwise alter any software owned by the Commission.

12.5 SECURITY

Information security is essential to protect organizational assets and comply with legal, regulatory, and contractual obligations.

12.5.1 PASSWORDS

Users must comply system password requirements and are responsible for protecting their passwords to access the computer system. Passwords should not be written down or stored online and must be changed regularly to maintain system security. Users are accountable for all actions performed with their user account access. Accessing the system using another user's access is prohibited without management authorization.

While users may have confidential passwords, this does not guarantee privacy for anything viewed, created, stored, sent, or received on the computer system. Management retains access to all data on the system, regardless of password protection. Users are not allowed to add extra security measures or passwords to their workstations or files without documented approval from the IS Manager.

12.5.2 ENCRYPTION

Data in transit and at rest must be encrypted using approved protocols such as TLS and BitLocker. Unauthorized encryption tools may not be used without IS approval.

12.5.3 ACCESS

Access to systems is granted based on Role-Based Access Control (RBAC). Users must not access files or systems without proper authorization. All cloud access is governed by Conditional Access policies in Microsoft Entra ID to enhance security. Users are required to lock or sign off from their devices when unattended to prevent unauthorized access.

Remote Access Guidelines:

Secure Connections: Remote access to the company network must be conducted through secure, encrypted connections (e.g., VPN).

Multi-Factor Authentication (MFA): Users must use Multi-Factor Authentication for remote access to ensure an additional layer of security.

Device Security: Remote devices must have up-to-date antivirus software and security patches installed.

Access Control: Remote access is subject to the same RBAC policies as on-site access. Users should only access systems and files necessary for their role.

Monitoring and Logging: All remote access activities are monitored and logged to detect and respond to potential security incidents.

User Responsibility: Users must ensure their remote work environment is secure and that unauthorized individuals do not have access to company systems or data.

12.5.4 VIRUS DETECTION

Microsoft Defender is used to provide real-time threat detection and automated remediation. External files or media must be scanned before use. Suspicious emails and attachments must not be opened. Users are expected to report potential threats immediately.

12.6 INTERNET

12.6.1 USE

Internet use is allowed primarily for work-related tasks. Limited personal use is acceptable if it does not interfere with duties or violate other policies. Internet access must occur through secure, organization-approved firewalls or VPNs.

12.6.2 PROHIBITED ACTIVITIES

Users must not display, store, or download material that is harassing, sexually explicit, discriminatory, profane, obscene, or intimidating on the computer system or from the Internet. The use of the computer system for entertainment purposes, such as downloading or playing games, is strictly prohibited.

12.6.3 DOWNLOADS

All downloads, including software, music, video clips, virus definitions, program updates, or any other files from the Internet, must be managed by the Information Systems (IS) department. Users are not permitted to download files directly to their workstations without prior authorization from the IS Manager. This ensures that all downloads are vetted for security and compliance with company policies.

The IS department will handle all downloads through the network server and distribute them to individual users as needed. This policy helps maintain system integrity and protects against potential security threats. Any attempt to bypass these restrictions may result in disciplinary action.

12.6.4 MONITORING

Employees should be aware that there is no expectation of personal privacy when using the Commission's Internet system. While the Commission does not routinely monitor Internet usage, it reserves the right to do so to ensure system integrity and efficiency, prevent unauthorized access and misuse, retrieve business-related information, or investigate reports of misconduct.

The presence of passwords does not limit the Commission's right to monitor Internet activity. Information obtained through monitoring may be disclosed to third parties if necessary, without prior notification to users.

12.6.5 INTERNET ACCESS CONTROL

The Commission may utilize software to block access to websites deemed inappropriate for business use. If a user encounters sexually explicit or other inappropriate content while using the Internet, they must immediately disconnect from the site, regardless of whether the site was blocked by the system.

12.7 E-MAIL

12.7.1 USE

Email provided through Microsoft Exchange Online must be used for business communication. Limited personal use is permitted but must not impact business operations. External email platforms must not be used for corporate communications.

12.7.2 GENERAL GUIDELINES

Emails should be composed with the same level of care and professionalism as other business communications. Ensure content is accurate and free of spelling and grammatical errors. Avoid typing emails in all uppercase letters, as this is hard to read and can be perceived as shouting.

Emails may be stored indefinitely across multiple systems and should not be considered private or secure. Many individuals, beyond the intended recipient, may have access to email content.

The email system is configured to automatically include the following confidentiality notice on every email:

This email and any files transmitted with it are privileged and confidential and are intended only for the use of the individual or entity to whom they are addressed. If you are not the intended recipient, please be advised that you have received this email in error and that any use, dissemination, distribution, printing, or copying of this email is strictly prohibited. If you have received this email in error, please immediately contact Grand Rapids Public Utilities at 218-326-7024. We will reimburse your reasonable expenses incurred in notifying us. ***(We do not currently utilize this. Is this something we should use, modify the language or eliminate entirely?)***

12.7.3 PROHIBITED ACTIVITIES

Users are prohibited from sending material that is harassing, sexually explicit, discriminatory, profane, obscene, or intimidating via email or any other form of communication. If users encounter inappropriate emails, they should report the incident to their supervisor immediately. Additionally, users are not allowed to send anonymous email messages from corporate email accounts.

12.7.4 SENSITIVE COMMUNICATIONS

In general, email should not be used to transmit sensitive material such as employee reprimands or other confidential information. When it is necessary to send sensitive information via email, the following guidelines should be followed:

Attorney-Client Privilege: Emails sent to attorneys should be marked as confidential.

Encryption: Consider encrypting sensitive communications to ensure they are not disclosed to unintended parties. This is especially important for confidential or legally sensitive information.

Recipient Verification: Double-check that emails containing sensitive information are addressed to the correct recipient(s) to avoid accidental disclosure.

Confidentiality Notice: Include a confidentiality notice in the email to remind recipients of the sensitive nature of the information.

Secure Channels: Whenever possible, use secure communication channels for transmitting sensitive information.

By following these guidelines, users can help protect sensitive information and maintain confidentiality.

12.7.5 PRIVACY AND MONITORING

Employees should understand that personal privacy is not guaranteed for any email content using the Commission's email system. The Commission may monitor email to ensure proper use and system performance, it reserves the right to do so to:

- Maintain system integrity and efficiency
- Prevent and discourage unauthorized access and misuse
- Retrieve business-related information
- Investigate reports of misconduct or misuse
- Reroute or dispose of undeliverable email
- Respond to lawful requests for information, including those from law enforcement agencies

The Commission retains the right to access all email content, regardless of security measures like passwords or deletion functions.

12.7.6 COMPLIANCE WITH APPLICABLE LAWS

Users must comply with all applicable data protection, copyright, and cybersecurity laws when using organizational email.

12.7.7 OTHER POLICIES

All email usage must align with the organization's Code of Conduct, Acceptable Use, and Respectful Workplace policies.

12.8 MOBILE DEVICE MANAGEMENT (MDM)

12.8.1 Purpose

The purpose of this Mobile Device Management (MDM) Policy is to establish a framework for the secure use and management of mobile devices within the organization, including corporate-issued and employee-owned devices. Access to Microsoft Teams and Corporate email will not be allowed unless the device is registered into the company MDM. The policy ensures protection of company data, mitigates risks related to data loss, and enforces compliance with security standards using Microsoft Intune.

All employees must acknowledge this policy prior to enrolling any device. The policy is available on the intranet and provided during onboarding. ***(Acknowledgement Form Created may need revision based on any rework to section 12.8)***

12.8.2 Security Risks Addressed

- Loss or Theft
- Malware and Phishing
- Unauthorized Access
- Data Leakage
- Jailbroken or Rooted Devices

Microsoft Intune is used to detect non-compliance, enforce policies, and allow remote data wipes if necessary.

12.8.3 Device Categories & Management Policies

- BYOD Phones
 - *Option A*
 - Managed via Microsoft Intune with App Protection Policies
 - Access limited to company apps (Outlook, Teams, SharePoint, etc.)
 - \$40/month stipend requires enrollment and policy acceptance
 - Company may remove corporate data; ***does not access personal content***
 - *Option B*
 - Position required for calls only
 - \$40/month stipend and policy acceptance
 - Use of company apps on corporate-issued devices for work-related tasks.
- Corporate Personal Phone
 - Managed via Microsoft Intune with App Protection Policies
 - Access limited to company apps (Outlook, Teams, SharePoint, etc.)
 - Company may remove corporate data; ***does not access personal content***
- Corporate Phones
 - Fully managed by Intune
 - Personal use allowed within reason

- Subject to remote wipe, monitoring, and cost reviews
- Data on device is company property
- Corporate Laptops & Tablets
 - Full Intune management required
 - Updates, configurations, encryption, and compliance handled by IS
 - No local admin rights unless authorized
 - Loss or policy violations result in remote wipe
- Commission Tablets
 - Full Intune management required
 - Updates, configurations, encryption, and compliance handled by IS
 - No local admin rights unless authorized
 - Loss or policy violations result in remote wipe
 - Limited to Adobe Reader and Microsoft Edge
- Kiosk Tablets
 - Full Intune management required
 - Updates, configurations, encryption, and compliance handled by IS
 - No local admin rights unless authorized
 - Loss or policy violations result in remote wipe
 - Limited to Microsoft Edge and customer related apps

12.8.4 User Responsibilities

- Comply with MDM policy
- Report lost/stolen devices immediately
- Do not bypass Intune or security settings
- Complete mobile security training annually
- Provide proof of service within 72 hours if requested
- IS support will monitor security compliance frequently, upon notification of non-compliance user will have 5 business days to work with IS support to rectify non-compliance. If the device is not compliant possible results:
 - All corporate applications will be removed from device
 - New registration of device in Intune

12.8.5 Policy Violations

Violations may lead to:

- Loss of access
- Remote corporate data wipe
- Disciplinary action, up to termination

Appeals must be filed with Human Resources within 5 business days. ***(Do we want to list this and further develop an appeals process?)***

12.8.6 Review and Updates

This policy is reviewed annually and updated as necessary to reflect changes in technology, laws, or business needs.

Feedback & Questions

Contact IS Support at [isadmin@grpuc.org] for questions or concerns regarding MDM.

(Acknowledgement Form Created may need revision based on any rework to sections 12.1 to 12.8)

DRAFT



GRAND RAPIDS PUBLIC UTILITIES COMMISSION AGENDA ITEM

AGENDA DATE: August 13, 2025

AGENDA ITEM: Strategic Plan Annual Review

PREPARED BY: Julie Kennedy, General Manager

BACKGROUND:

Each year, the Commission and management staff review the organization's SWOT, strategic and operational progress. We will be introducing this year's annual review process at Wednesday's Work Session.

RECOMMENDATION:

None - review only.