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 Micrsoft 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 Micrsoft 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)