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 hosted services, managed devices, and identity access. 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 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.
• MDM: Mobile Device Management

• BYOD: "Bring Your Own Device" – personally owned devices approved for limited business access through app-level controls.

12.3 INTRODUCTION AND CONSEQUENCES OF POLICY VIOLATIONS

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.

Violations of this policy may result in disciplinary actions, up to and including termination of employment, 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 applicable law or other Commission policies. All users must access and use systems in accordance with the organization's Respectful Workplace, Acceptable Use, and other policies, as amended. Users must not access any system or information that they do not have a need to access for their work duties.

12.4.2 NO EXPECTATION OF 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 have an express or implied privacy right in any matter created, sent, received, accessed, or stored with any system, whether or not the user has a password. 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 MDM prior to accessing corporate data. Corporate-owned devices are fully managed, while BYOD access is limited to protected apps (e.g., email). 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 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 regularly deleting nonessential emails to improve system performance.

12.4.7 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.

12.4.8 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.

12.4.9 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. 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 with system password requirements and are responsible for protecting their passwords to access the computer system. Passwords should not be accessible to others 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. 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 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. Users are strictly prohibited from granting access to any files, applications, or systems on the organization's network to external individuals or third parties without prior authorization and oversight from the IS Department or the applicable Department Manager.

In circumstances where third-party vendors or contractors require recurring access to organizational system for maintenance, support, or other approved business purposes, such access must be formally authorized by the IS Department in advance.

Authorized third-party users will be provided with secure access, including uniquely assigned usernames, passwords, and role-based permissions, as determined and administered by the IS Department.

12.5.4 VIRUS DETECTION

Real-time threat detection is provided with 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 work duties or violate applicable law or other Commission 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, sexist, racist, profane, obscene, or violent 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 non-work downloads, including software, music, video clips, or any other files from the Internet must be approved by the IS Department.

The IS Department will handle all work-related downloads and program updates 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 PRIVACY AND 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 for any legitimate business reason.

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 inappropriate content while using the Internet, they must immediately disconnect from the site, regardless of whether the site was blocked by the system, and report to their supervisor.

12.7 E-MAIL

12.7.1 USE

Email is provided and must be used primarily for business communication. Limited personal use is permitted if it does not interfere with work duties or violate applicable law or other Commission policies. External email platforms must not be used for Commission communications.

12.7.2 GENERAL GUIDELINES

Emails should be composed with the same level of care and professionalism as other business communications. 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.

12.7.3 PROHIBITED ACTIVITIES

Users are prohibited from sending, receiving, or creating material that is harassing, sexually explicit, discriminatory, sexist, racist, profane, obscene, or violent 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 Commission accounts.

12.7.4 SENSITIVE COMMUNICATIONS

In general, email should not be used to transmit sensitive material 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 there is no expectation of personal privacy when using the Commission's email system. The Commission reserves the right to monitor email use for any legitimate business reason, regardless of security measures like passwords or deletion functions.

12.8 MOBILE DEVICE MANAGEMENT (MDM)

12.8.1 Purpose

The purpose of this policy is to establish a framework for the secure use and management of mobile devices within the organization, including Commission-issued and employee-owned devices. Access to email and other Commission software will not be allowed unless the device is registered into the company MDM. The policy ensures protection of data, mitigates risks related to data loss, and enforces compliance with security standards.

All employees must acknowledge this policy prior to enrolling any device. The policy is available on the intranet (Toolbox) and provided during onboarding.

12.8.2 Security Risks Addressed

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

Application management software 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 MDM with App Protection Policies
        - Monthly stipend available, requires enrollment and policy acceptance
        - Access is limited to work-related apps (email, intranet, etc.)
        - IS Department may remove Commission data; but ***does not access personal content***
    - Option B
        - Used for phone calls only
        - Monthly stipend available, requires policy acceptance
        - Use of work-related apps cannot be done on device and must be done on a different Commission-issued device
- Commission-issued Personal Phone

    - Managed via MDM with App Protection Policies
    - Access limited to work-related apps (email, intranet, etc.)
    - IS Department may remove Commission data; ***does not access personal content***
- Commission-issued Phones
    - Managed via MDM
    - Personal use allowed within reason
    - Subject to remote wipe, monitoring, and cost reviews
- Commission-issued Laptops & Tablets
    - Managed via MDM
    - Updates, configurations, encryption, and compliance handled by IS Department
    - No local admin rights unless authorized
    - Loss or policy violations result in remote wipe
- Commissioner Tablets
    - Managed via MDM
    - Updates, configurations, encryption, and compliance handled by IS Department
    - No local admin rights unless authorized
    - Loss or policy violations result in remote wipe
    - Limited to Adobe Reader and web browser
- Kiosk Tablets
    - Managed via MDM
    - Updates, configurations, encryption, and compliance handled by IS Department
    - No local admin rights unless authorized
    - Loss or policy violations result in remote wipe
    - Limited to web browser and customer related apps

12.8.4 User Responsibilities

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

- New registration of device in MDM

12.8.5 Policy Violations

Violations may lead to loss of access or remote Commission data wipe. And, like any other IS or other policy violation, disciplinary action, up to and including termination of employment.

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 the IS Department at [isadmin@grpuc.org] for questions or concerns.

Related Forms:

Information Systems Usage Acknowledgement Form

MDM Acknowledgement Form