GREATER MIAMI EXPRESSWAY

INFORMATION TECHNOLOGY POLICY

Purpose

This Information Technology (IT) Policy establishes guidelines for the use, management, and protection of information technology (IT) resources at the Greater Miami Expressway Agency (GMX). The policy ensures the secure, efficient, and effective use of IT resources in alignment with GMX's mission.

Scope

This policy applies to all GMX employees, contractors, consultants, vendors, and any other individuals who access or use GMX IT resources, including but not limited to computers, mobile devices, networks, software, and data.

Acceptable Use of IT Resources

- **General Use:** IT resources are provided for official GMX business.
- **Unauthorized Activities:** Users must not engage in illegal, unethical, or GMX policy-violating activities. This includes, but is not limited to, unauthorized access to systems, distribution of malicious software, and viewing or distributing inappropriate content.
- **Data Protection:** Users are responsible for safeguarding sensitive information. Confidential data must be securely stored, transmitted, and disposed of. All information stored within a system will be protected to ensure confidentiality, integrity, and availability.

Security and Access Control

- **Passwords:** Users must create strong passwords that meet specified length and complexity requirements and change them regularly. Password sharing is prohibited.
- **User Access:** Access to GMX systems and data is granted based on job roles and responsibilities. Users should only access the information necessary to perform their duties.
- **Incident Reporting:** Any security incidents, such as data breaches or suspicious activity, must be reported immediately to the IT department.

Data Management

- **Secure Data Transmission**
    - **Encryption:** Use encrypted tunnels for electronic data transmission to third parties.

  - **Direct Encryption:** If tunnels are unavailable, encrypt data directly before transmission.
  - **Message Digests:** Create and supply message digest hashes for electronic data transmissions if necessary.
- **Backup and Recovery:** Regular backups of critical data must be performed and securely stored. Offsite encrypted backups are required to prevent loss in the event of a regional disaster. Recovery plans should be in place to restore data if needed.
- **Data Retention:** GMX will retain data according to applicable legal and regulatory requirements. Data no longer needed should be securely disposed of.

Network and System Management

- **Network Security:** The IT department is responsible for securing GMX's network infrastructure, including firewalls, intrusion detection systems, endpoint protection, and secure configurations.
- **Software Management:** Only authorized software may be installed on GMX systems. Users must not download or install software without prior approval from the IT department.
- **System Updates:** All systems must be regularly updated with the latest security patches and software updates to protect against vulnerabilities.

Mobile Device and Remote Access

- **Mobile Devices:** GMX mobile devices must be managed by GMX's Mobile Device Management system and secured with strong passwords.
- **Remote Access:** Remote access to GMX systems is only permitted through secure methods, such as Virtual Private Networks (VPNs), and must comply with GMX security standards, including multi-factor authentication (MFA).

Wi-Fi Policy

- **Users Responsibilities:** All users connecting to the GMX Wi-Fi network must comply with the GMX Acceptable Computer and Internet Use Policy.
- **Meeting Arrangements:** GMX staff organizing a meeting are responsible for providing their guests with the wireless key and captive portal guest credentials.

Compliance and Auditing

- **Regulatory Compliance:** GMX must comply with all applicable federal, state, and local laws, regulations, and policies related to IT and data security.

- **Audits:** Annual audits of IT systems and processes will be conducted to ensure compliance with this policy and identify any areas for improvement.

Training and Awareness

- **User Training:** All users must complete mandatory IT security training upon hire and annually thereafter. This training will cover best practices for data protection, password management, phishing, and other relevant topics.
- **Awareness Programs:** GMX will regularly conduct awareness programs to keep users informed about emerging threats and new security practices.

Consequences of Non-Compliance

Any violation of these policies or procedures will be considered a security breach. Depending on the severity of the violation, it may be referred to the Information Technology Manager, your direct supervisor, or the Executive Director for appropriate action, which could include termination of employment.

Policy Review and Updates

This policy will be regularly reviewed by the IT department and updated as necessary to reflect changes in technology, regulatory requirements, or GMX's operational needs.

GMX will continuously evaluate and enhance its IT systems through regular review, assessment of performance, and incorporation of industry best practices and technological advancements.

Adopted by the Governing Board on the 1st of October, 2024.