Email Policy

1. Purpose

This Email Policy aims to provide guidelines for the appropriate use of email within DevEngineer, ensuring communication is efficient, secure, and compliant with company standards and legal requirements.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who are granted access to [Company Name]’s email system. It covers proper email usage, security practices, monitoring, compliance, and incident response related to email communication.

3. Definitions

- **Confidential Information**: Data that is classified as sensitive and is protected from unauthorized disclosure.
- **Phishing**: A cyberattack that uses deceptive emails to trick users into providing sensitive information.
- **Spam**: Unsolicited and irrelevant emails sent in bulk to multiple recipients.
- **Ransomware**: Malicious software that encrypts a user's data and demands payment to restore access.
- **MFA (Multi-Factor Authentication)**: A security process requiring two or more verification methods to gain access to a system.

4. Policy

4.1 Acceptable Use

- Company-provided email systems are intended for business purposes. Personal use should be kept to a minimum and must not interfere with work duties.
- Emails should reflect professionalism, as they are an official form of business communication.

4.2 Prohibited Use

- The transmission of offensive, obscene, or discriminatory content is strictly prohibited.
- Sharing confidential or proprietary information without authorization is forbidden.
- Employees must not use third-party email services for conducting company business.

4.3 Email Security

- All emails containing sensitive information must be encrypted.
- Do not open suspicious email attachments or click on unknown links, as they may contain phishing or ransomware threats.

- Email accounts should be protected by strong, regularly updated passwords and multi-factor authentication (MFA).

4.4 Email Attachments

- Only approved file types, such as .pdf, .docx, and .xlsx, may be sent or received through the company's email system.
- Executable files (.exe), scripts, and certain compressed files (.zip, .rar) are prohibited to prevent the spread of malware.

4.5 Phishing and Spam

- All employees must complete mandatory training on identifying and reporting phishing attacks.
- Suspicious emails should be reported to the IT department immediately, using the "Report Phishing" feature in the email system.
- IT will implement and maintain email filtering to detect and block spam and phishing attempts.

4.6 Monitoring and Privacy

- The company reserves the right to monitor employee emails to ensure compliance with this policy and protect company interests.
- Employees should not expect personal email communications to remain private when using company systems.

4.7 Data Breaches and Incident Response

- In the event of a data breach resulting from email misuse or compromise, the incident must be reported to the IT department within 30 minutes of discovery.
- The IT and Security teams will immediately initiate an incident response plan, including isolating affected accounts, assessing the impact, and notifying relevant stakeholders.
- A full report will be submitted within 48 hours detailing the breach and corrective measures.

4.8 Retention and Archiving

- Emails will be retained for 7 years in compliance with company policy and legal obligations.
- Archiving procedures will be in place to securely store and retrieve emails when needed for audits, investigations, or legal proceedings.

4.9 Compliance

- All employees must comply with this policy, company standards, and relevant laws..
- Non-compliance may result in disciplinary action, up to and including termination.

5. Training and Awareness

- Employees will undergo annual email security training to stay updated on evolving threats like phishing, spear-phishing, and ransomware.
- Security awareness campaigns will regularly remind employees of best practices for email use.

6. Enforcement

- Violations of this policy may lead to disciplinary actions, including suspension of email access, termination, or legal action, depending on the severity of the violation.

Revision History

Version	Date	Changes	Approved By
1.0	25th of August,2024	Initial policy creation	Chief Security Officer.