Globe Technologies Ltd.
Remote.
Nairobi, Kenya.
globeheadquarters@gmail.com

Internet and Email Security Policy

Last Update: 31/08/2024

NOTE:

The purpose of this policy is to minimize risks associated with the use of internet and email services within Globe Technologies Ltd. ("the Company", "Us", "We" or "Our". It establishes controls to protect against unauthorized access, theft of information, malicious disruption of services and the misuse of Our assets.

Scope

This policy applies to all users of information systems within the Company, including employees, contractors, vendors, business partners and functional units regardless of geographic location. It covers all digital environments operated by Us or contracted third-party services.

All users must comply with this policy, as well as other applicable security policies and standards set by the Company. If any user does not fully understand this document in whole or part, he/she should contact Us on *globeheadquarters@gmail.com.*

The Information Security Department shall resolve any conflicts arising from this Policy accordingly.

Responsibilities

- Information Security Manager: Oversees the implementation and maintenance of this policy.
- Security Department: Responsible for policy accuracy and enforcement.
- Users: Responsible for understanding and adhering to this policy.

Definitions

- Accountability: Ensuring actions can be linked to an identified user, who is held responsible for those actions.
- Authentication: Process of verifying the identity of a user accessing the Company's systems.
- Confidentiality: Ensuring that sensitive information is only accessible to authorized individuals.
- Privacy: Information provided by employees, customers and others is protected such that it is used solely for the stated purposes of the Company's Privacy Policy; where the provider has authorized such use, and its use is in compliance with all the privacy regulations set by the local government.
- Private Information: Information classification that relates to their "privacy" type. This could be either customer related information or private information related to staff (such as medical records).
- Sensitive: concerned with highly classified information or involving discretionary authority over important official matters.
- Sensitive Information: Data that requires protection, such as proprietary code, customer data or financial information.

Policy Statement

Since We operate and maintain innovative digital Products and Services, it is crucial to establish security measures for internet and email usage to prevent unauthorized access and protect corporate assets.

Our Products, Services, interconnectivity and general resources available on the Internet introduce new opportunities and new risks. In response to the risks, this Policy describes the Company's official practices regarding Internet and Email security.

Internet Security Policies

1. Reliance on Information Downloaded from the Internet

Information from external sources on the internet should be verified by separate sources before use. We prohibit the overreliance on unverified information that could compromise the integrity of Our systems.

Due to the lack of quality control processes on the Internet, and a considerable amount of information is outdated or inaccurate. Unless tools and solutions such as Privacy Enhanced Mail (PEM), Pretty Good Privacy (PGP) and Public Key Infrastructure (PKI – certificate authority based solutions) are used, it is also relatively easy to spoof other users on the Internet.

2. Release of Company Information

No proprietary information (e.g., code, internal documents) should be shared over the internet unless explicitly authorized. All sensitive data must be encrypted before being sent via email or other internet-based services. Further, users must not place Our material (software, documents, internal memos, etc.) on any publicly accessible platform.

3. Information Protection

All sensitive information, including customer data, intellectual property and financial information, must be encrypted using approved methods before being transmitted over the internet. Credit card numbers, passwords and other sensitive credentials that can be used to gain access to goods or services, must not be sent over the Internet in readable form.

Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

4. Reporting Security Problems

Users have the responsibility to notify Us immediately of any evidence of any security violation involving Our Products and Services with regard to: potential security breaches, including unauthorized access, malware transmission or data tampering.

User Expectations and Privacy

Users should not send private or confidential information over the internet unless properly encrypted. We reserve the right, at any time and without prior notice, to monitor internet activity, emails and file directories to ensure compliance with Our policies, supports performance, prevents unauthorized access and assists with the management of Our information systems.

The use of Our Internet Resources

Internet resources are strictly for business-related activities. Personal use of the company's network for non-work-related activities is prohibited and punishable.

Public Representations

Only authorized employees of Globe Technologies Ltd. may speak on behalf of the company in public forums or through official Our channels. Employees and contractors are prohibited from sharing company-sensitive information in public internet spaces (e.g., forums, blogs, social media platforms etc.,).

Only authorized personnel or third party contractors may establish Internet or other external network connections. These connections include the establishment of multi- computer file systems. Other users wishing to establish a trusted connection with Us must authenticate themselves at the firewall before gaining access to Our internal network.

Configuration Management

All configuration details of the network architecture, including firewall settings and security protocols, must be documented and regularly reviewed to ensure they meet current security standards.

Regular Review of User Accounts

We regularly review user accounts and access permissions to ensure that they are up to date and only granted to authorized personnel. The period between reviews is usually not more than six months.

Audit and Accountability of Internet Connections

Our Security Audit Team reviews Internet connection audit reports created on the firewall for any suspicious activities against two or more connections. The period between reviews is one month. Reports of the findings are forwarded to the Information Security Manager..

Internet Usage

1. Password Access Requirements

Passwords must meet the Company's password requirements and users must comply with the most restrictive password formats specified.

2. User Authorization & Verification

Every user with log-in access to the Our Products and Services must have a unique User ID assigned to him/her.

3. Requesting and Granting User Authorization

Each personnel requesting a User ID must provide a written authorization from the head of his/her department.

Requests for an Internet connection must be accompanied by a justification for such access. The request must be authorized by head of his/her department.

An associate that requires only the inclusion of an electronic mail alias entry must establish authorization in the same manner as that described for a login user.

4. Confidentiality

Users are prohibited from downloading or executing programs from untrusted sources without approval from the Information Security Department. All downloaded files must undergo a security scan before being moved to production environments.

Email Usage

Emails must be used for legitimate business purposes only. Any form of inappropriate, offensive or harassing communication via email is strictly prohibited. Confidential information must not be sent through email unless it is encrypted and authorized for transmission.

- Monitoring: We reserve the right to monitor email communication to ensure compliance with this policy.
- Attachments: Email attachments are scanned for viruses and attachments above 3MB compressed.

Firewall and Network Security

All network traffic through Our firewalls adhere to the company's firewall policies. Unauthorized access attempts and network anomalies are reported to the Security Department.

Legal Compliance

We comply with all relevant local, national and international laws regarding internet and electronic communications.

Compliance and Enforcement

Compliance with this policy is mandatory for all the users of Our Products and Services. Violations may result in disciplinary action, including the loss of network access privileges or termination of employment.

Contact Us

If you have any questions about this Internet Security Policy, You may contact us on: *globeheadquarters@gmail.com*