Digitech Pro

Digitech Pro (Pty) Ltd Information Security Policy

May 2024

Document Title		Security Awareness Policy	
Authors/s		Llewellyn Holtshausen/Ntiyiso Mbhalati/ Credo Unamaca	
Effective Date	**Review Cycle**	**Last Review Date**	**Next Review Date**
27 May 2024	Quarterly		September 2024

Table of Contents

1. Purpose

The purpose of this Information Security Policy is to establish a framework for protecting Digitech Pro (Pty) Ltd's information assets. This policy outlines the standards and practices necessary to ensure the confidentiality, integrity, and availability of our information systems.

2. Scope

This policy applies to all employees, contractors, vendors, and other parties who have access to Digitech Pro's information systems and data. It covers all forms of information, including but not limited to electronic data, physical documents, and verbal communications.

3. Definitions

- **Information Assets:** Data, information systems, hardware, software, and other resources related to information processing.
- **Confidentiality:** Ensuring that information is accessible only to those authorized to have access.
- **Integrity:** Safeguarding the accuracy and completeness of information and processing methods.
- **Availability:** Ensuring that authorized users have access to information and associated assets when required.

4. Information Security Objectives

- Protect against unauthorized access to, alteration, disclosure, or destruction of data.
- Ensure the integrity and availability of information systems.
- Comply with relevant legal, regulatory, and contractual obligations.
- Educate and train employees on information security best practices.

5. Responsibilities

- **Management:** Responsible for the implementation and enforcement of this policy, ensuring adequate resources are available.
- **IT Department:** Responsible for the technical implementation of security measures and monitoring compliance.
- **Employees and Contractors:** Responsible for adhering to the information security policies and procedures.

6. Information Classification

Information must be classified based on its sensitivity and criticality:

- **Public:** Information intended for public dissemination.
- **Internal:** Non-sensitive information intended for internal use.
- **Confidential:** Sensitive information requiring protection against unauthorized disclosure.
- **Restricted:** Highly sensitive information requiring stringent protection measures.

7. Access Control

- **User Accounts:** Unique user accounts must be created for each individual, with access rights based on job responsibilities.
- **Authentication:** Strong passwords and multi-factor authentication must be used to secure access to systems.
- **Authorization:** Access to information and systems must be granted based on the principle of least privilege.

8. Data Protection

- **Encryption:** Sensitive data must be encrypted both in transit and at rest.
- **Data Backup:** Regular backups must be performed, and backup data must be securely stored and tested periodically.
- **Data Disposal:** Sensitive data must be securely disposed of when no longer needed, using methods that ensure it is irrecoverable.

9. Network Security

- **Firewalls:** Firewalls must be deployed to protect network boundaries.
- **Intrusion Detection:** Intrusion detection and prevention systems must be implemented to monitor and respond to potential threats.
- **Secure Configuration:** All network devices must be securely configured and regularly updated with security patches.

10. Incident Management

- **Reporting:** All employees must report any suspected security incidents to the IT security team immediately.
- **Response:** The IT security team must have an incident response plan to address and mitigate security incidents promptly.
- **Recovery:** Post-incident reviews must be conducted to improve security measures and prevent future occurrences.

11. Physical Security

- **Access Control:** Physical access to company premises and sensitive areas must be restricted to authorized personnel.
- **Secure Areas:** Servers and other critical infrastructure must be housed in secure areas with appropriate physical security controls.
- **Device Security:** All devices must be secured when not in use to prevent theft or unauthorized access.

12. Employee and Contractor Responsibilities

- **Training:** All employees and contractors must undergo regular information security training.
- **Compliance:** Employees and contractors must comply with all information security policies and procedures.
- **Reporting:** Any security concerns or breaches must be reported to the IT security team immediately.

13. Compliance and Monitoring

- **Audits:** Regular audits must be conducted to ensure compliance with this policy.
- **Monitoring:** Continuous monitoring of information systems must be performed to detect and respond to security threats.
- **Penalties:** Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

14. Policy Review and Updates

This policy must be reviewed and updated at least annually or whenever significant changes occur to ensure its continued effectiveness and relevance.

15. Acknowledgment

All employees and contractors must acknowledge their understanding and acceptance of this Information Security Policy.

Acknowledgment: I, _______________________, acknowledge that I have read and understood the Digitech Pro (Pty) Ltd Information Security Policy. I commit to following the guidelines and policies outlined within.

Signature:

Date: