Digitech Pro (Pty) Ltd Security Awareness and Training Manual

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. Introduction

Welcome to Digitech Pro (Pty) Ltd. As a new employee or contractor, you play a critical role in maintaining our company's security. This manual provides essential guidelines and practices to protect our company's information, assets, and reputation. During your one-month onboarding, you will learn about our security policies and how to apply them in your daily activities.

2. Company Security Policies

- **Confidentiality:** Ensure all company information is kept confidential and shared only with authorized personnel.
- **Integrity:** Maintain the accuracy and completeness of company data.
- **Availability:** Ensure that information and systems are available to authorized users when needed.

3. Access Control

- **User Accounts:** Use unique user accounts and do not share login credentials.
- **Passwords:** Create strong passwords (at least 12 characters with a mix of letters, numbers, and symbols) and change them regularly.
- **Two-Factor Authentication (2FA):** Use 2FA for accessing sensitive systems and data.

4. Data Protection

- **Data Classification:** Understand the different levels of data classification (e.g., public, internal, confidential) and handle data accordingly.
- **Encryption:** Use encryption to protect sensitive data both in transit and at rest.
- **Data Disposal:** Properly dispose of data and hardware that is no longer needed, ensuring that sensitive information is irrecoverable.

5. Email and Internet Usage

- **Email Security:** Be cautious of suspicious emails and avoid clicking on unknown links or downloading attachments from untrusted sources.
- **Internet Usage:** Use the internet responsibly and avoid accessing inappropriate or malicious websites.

6. Social Engineering and Phishing

- **Awareness:** Be aware of social engineering tactics and phishing attempts designed to steal information or compromise systems.

Database & Software As A Service I Cloud Computing I Geospatial Database Solutions

Email: info@digitechpro.co.za I Tel: +27 (0) 11 880 3196 I Website: www.digitechpro.co.za
Address: 35 First Avenue, Illovo, Johannesburg, 2196, South Africa
Co. Reg: 201909927807

- **Verification:** Always verify the identity of individuals requesting sensitive information or access.

7. Incident Reporting

- **Incident Types:** Understand different types of security incidents (e.g., data breaches, malware infections) and their potential impact.
- **Reporting Procedure:** Immediately report any suspected or actual security incidents to the IT security team through the designated communication channels.

8. Physical Security

- **Access Control:** Ensure that physical access to company premises and sensitive areas is restricted to authorized personnel only.
- **Equipment Security:** Secure laptops, mobile devices, and other equipment when not in use to prevent theft or unauthorized access.

9. Mobile Device Security

- **Device Management:** Use company-approved devices for work purposes and ensure they are regularly updated and patched.
- **App Usage:** Only install and use applications from trusted sources.

10. Remote Work Security

- **Secure Connections:** Use VPNs and other secure methods to connect to company networks remotely.
- **Home Office Setup:** Ensure your home office is secure and follows company guidelines for remote work security.

11. Regular Assessments and Continuing Education

- **Training Sessions:** Participate in regular security training sessions and assessments to stay updated on the latest security practices.
- **Self-Education:** Take advantage of available resources to continually improve your security knowledge and skills.

12. Conclusion

Security is a shared responsibility. By following the guidelines in this manual, you contribute to the overall security of Digitech Pro (Pty) Ltd. If you have any questions or need further clarification on any security matters, please do not hesitate to contact the IT security team.

Database & Software As A Service **I** Cloud Computing **I** Geospatial Database Solutions

Email: info@digitechpro.co.za **I** Tel: +27 (0) 11 880 3196 **I** Website: www.digitechpro.co.za
Address: 35 First Avenue, Illovo, Johannesburg, 2196, South Africa
Co. Reg: 201909927807

Acknowledgment: I, _____, acknowledge that I have read and understood the Security Awareness and Training Manual. I commit to following the guidelines and policies outlined within.

Signature:

Date:

Welcome to Digitech Pro (Pty) Ltd! Your commitment to security helps protect our company and our clients.

-