

A1 Group IT Security Infrastructure

1. Introduction

The A1 Group of companies recognises the critical importance of securing its IT infrastructure to safeguard sensitive information and maintain operational continuity. This document serves as a comprehensive guide to the measures and practices implemented to achieve these objectives.

2. Managed IT Services Provider: Cybit

Cybit, a trusted IT solutions provider established in 1991, plays a pivotal role in fortifying our digital landscape. They ensure the security of our servers, backup systems, and local data, establishing a robust and consistent infrastructure. With ISO27001 accreditation, Cybit's 30 years of industry experience instils confidence in their ability to deliver efficient, flexible, and secure IT solutions. Our digital contingency plans are reinforced by regular backups, solidifying the foundation of our operational resilience.

3. Security Applications and Measures

Microsoft Office 365 Defender for Business:

This comprehensive security suite is deployed to all users, offering advanced threat protection and intelligence across the Office 365 software suite.

Broadcom Email Filtration:

Safeguards email communications through a multi-layered approach, utilizing advanced threat-protection methods to secure sensitive data.

Endpoint Protection:

Microsoft Endpoint is deployed for servers, allowing real-time monitoring of system health and providing detailed information about system and user activities.

Multi-Factor Authentication (MFA):

MFA is implemented for both local and remote access, requiring users to provide a second form of authentication, such as a fingerprint or security token, in addition to their username and password.

4. System Access Control

- Access to computer systems is tightly controlled through a combination of unique usernames and passwords, ensuring that only authorised individuals can access sensitive data.
- Remote users enhance security through the use of Multi-Factor Authentication (MFA), requiring an additional layer of authentication for remote access.

5. Anti-Virus and Malicious Code Protection

- Office 365 Defender for Business is continuously updated and deployed to all users, providing real-time protection against a spectrum of malicious codes and viruses.

6. System Auditing and Monitoring

- Regular monitoring of system logs, network traffic, and user activities is conducted to identify any suspicious or abnormal behaviour promptly.

- Microsoft Endpoint facilitates real-time monitoring, offering detailed insights into system and user activities, enabling swift detection and response to potential security threats.

7. Segregation of Duties

- Defined roles and responsibilities limit access to specific levels within the organization, ensuring that only authorised personnel can access sensitive information.
- Change control and administration are centrally managed by Cybit, ensuring security controls are maintained and changes adhere to policies and procedures.

8. Remote Access Policy

- Secure MS Proxy and Multi-Factor Authentication (MFA) are employed to fortify remote access, ensuring encrypted data transmission between the employee's device and the internal network.
- Access to systems and data remotely is carefully assigned based on job responsibilities, providing only authorised individuals with remote access.

9. Removable Media Strategy

- Removable media, such as USB drives, are assigned to managers only, who are responsible for providing such media to employees as needed.
- Guidelines for handling removable media are in place to protect data from unauthorised access or misuse.

10. Physical and Electronic Security Measures

- Computer equipment is stored in locked environments to prevent unauthorised access and theft.
- CCTV surveillance is deployed to monitor the physical environment and detect any suspicious activity, enhancing the overall security posture.

11. Data Deletion Capabilities

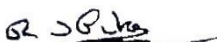
- Robust data deletion capabilities are in place to comply with the Data Protection Act 1998 and specific data retention policies.
- Regular backups stored securely provide resilience against accidental data deletion, ensuring data recovery capability.

12. Cyber Awareness Training

- Monthly organised phishing emails are part of ongoing cyber awareness and security training, ensuring staff remains vigilant and informed about potential threats and best practices

Revision

The Company will make all employees aware of this Company Policy.

Signed: 

Date: 1/1/24

Russell Pike - **Managing Director A1 Group**

Next Review date 1st January 2025