manyother ltd

Information Security Policy

(V2.0 - Last updated January 2020)

1. Introduction

This document describes the policy approach the Company takes towards information security across the organisation. We take a systemic and holistic approach to information security, regarding it as an iterative process of continuous review and refinement.

2. Purpose

Information that is collected, analyzed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption.

Information may be put at risk by poor education and training, and the breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements being made against the Company.

This high-level Information Security Policy sits alongside the Data Protection Policy to provide the high-level outline of and justification for the Companies risk-based information security controls.

2.1. Objectives

The Companies security objectives are:

1. Information risks are identified, managed and treated according to an agreed risk tolerance
2. Authorized users can securely access and share information in order to perform their roles
3. Physical, procedural and technical controls balance user experience and security
4. Contractual and legal obligations relating to information security are met
5. Individuals accessing our information are aware of their information security responsibilities
6. Incidents affecting our information assets are resolved and learnt from to improve our controls in a timely manner.

2.2. Scope

The Information Security Policy and its supporting controls, processes and procedures apply to all information used within the Company, in all formats. This includes information processed by other organizations in their dealings with the Company.

The Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to Company information and technologies, including external parties that provide services to the Company.

2.3. Compliance

Compliance with the controls in this policy will be monitored by the Company.

2.4. Review

A review of this policy will be undertaken by the company annually or more frequently as required and will be approved by the Company

2.5. Policy Statement

It is the Company's policy to ensure that information is protected from a loss of:

- Confidentiality – information will be accessible only to authorized individuals
- Integrity – the accuracy and completeness of information will be maintained
- Availability – information will be accessible to authorized users and processes when required

The Company will implement an Information Security Management System based on the ISO 27001 International Standard for Information Security. The Company will also reference other standards as required, mindful of the approaches adopted by its Customers.

The Company will adopt a risk-based approach to the application of controls:

3. Information Security Policies

A set of lower level controls, processes and procedures for information security will be defined, in support of the high-level Information Security Policy and its stated objectives. This suite of supporting documentation will be approved by the Company and communicated to Company employees' and relevant external parties.

3.1. Organization of Information Security

The Company will define and implement suitable governance arrangements for the management of information security.

3.2. Human Resources Security

The Company's security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security education and training will be made available to all staff and associates and poor and inappropriate behavior will be addressed.

Where practical, security responsibilities will be included in role descriptions, person specifications and personal development plans including Independent Contractors.

3.3. Asset Management

All assets (information, software, electronic information processing equipment, service utilities and people) will be documented and accounted for. Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.

3.4. Access Control

Access to all information will be controlled and will be driven by business requirements. Access will be granted, or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented, where practical.

3.5. Cryptography (Passwords)

The Company will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems.

3.6. Physical and Environmental Security

The Company will keep all paper and physical information and documentation in a secure manor, documents will be disposed of in a controlled procedure and the building will remain locked when not in use.

3.7. Operations Security

The Company will ensure the correct and secure operations of information processing systems.

This will include:

1) Documented operating procedures
2) The use of formal change and capacity management
3) Controls against malware, viruses and phishing attacks
4) Vulnerability management

3.8. Communications Security

The Company will maintain network security controls to ensure the protection of information within its networks and provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities, in line with the classification and handling requirements associated with that information.

3.9. System Acquisition, Development and Maintenance

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

1) Controls to mitigate any risks identified will be implemented where appropriate.

2) Systems development will be subject to change control and separation of test, development and operational environments.

3.10. Supplier Relationships

The Company information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected. Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

3.11. Information Security Incident Management

Guidance will be available on what constitutes an Information Security incident and how this should be reported.

1) Actual or suspected breaches of information security must be reported and will be investigated.

2) Appropriate corrective action will be taken, and any learning built into controls.

3.12. Information Security Aspects of Business Continuity Management

The Company will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely recovery in line with documented business needs.

1) This will include appropriate backup routines and built-in resilience.

2) Business continuity plans must be maintained and tested in support of this policy.

3) Business impact analysis will be undertaken of the consequences of disasters, security failures, loss of service, and lack of service availability.

3.13. Compliance

The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements.

The Company will use a combination of internal and external audits to demonstrate compliance against chosen standards and best practice, including internal policies and procedures.

This will include IT Health Checks, gap analyses against documented standards, internal checks on staff compliance, and returns from Information Asset Owners.

End of Document