EVERYTHING IT
Computer Systems

Information Security Policy

Contents

List of Tables

1 Introduction

As a modern, forward-looking business, Everything IT recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders, and other stakeholders.

Information security is an essential component of this requirement and the core of how operations are managed within the organisation.

Cybercrimes are also becoming increasingly more common across the world making cyber security one of the top priorities for everyone. Consequently, there has been a rapid increase in legislation and cybersecurity regulations.

In recent years there have been a number of hacking campaigns on-going against Irish Entities. Multiple Irish ISP's & State Agencies , and in 2021 the HSE, were targeted. These attacks consist of DDOS (Distributed Denial of Service) attacks and attempts to install Ransomware software onto Company Networks.

What this tells us, is that in order for us to protect our organisation from cyber-crime, a clear and organised Information Security Policy should be in place that not only addresses the technical security controls required for mitigation of risks but also by addressing the risks of user actions, behaviours, and decisions they make when faced with new emerging socially engineered threats.

2 Leadership Commitment

In order to provide a seamless level of continuous operation, Everything IT has invested in the implementation of an **Information Security Management System (ISMS)** in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally recognised best practice.

Everything IT has decided to attain certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB). In addition, the guidance contained in the codes of practice ISO/IEC 27017 and ISO/IEC 27018 has been adopted as these have relevance for Cloud Service Providers (CSPs).

Everything IT regularly submit themselves to internal and external audits against the ISO27001 standard by an accredited certification body in order to maintain and uphold current certification. A copy of our certification can be made available on requested to any stakeholder that require this.

3 Purpose

This document defines the information security policy of Everything IT and its purpose is to direct the information security activities within the organisation's ISMS.

. The operation of the ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

4 Scope

The policy is aligned to the scope of Everything IT's ISMS which is as follows:

The scope for this Information Security Management System (ISMS) includes security, privacy and governance controls that cover the operations of Everything IT and all services provided to Everything IT's Clients. These services include Helpdesk Activities, Consultancy, Network Design, Procurement & Maintenance Services. This is in accordance with the Statement of Applicability.

This policy should be widely shared and communicated to all relevant stakeholders, , including board members, directors, employees, suppliers and other third parties who have access to Everything IT systems.

This policy applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Everything IT systems.

The following supporting documents are relevant to this information security policy and provide additional information about how it is applied:

- *Risk Assessment and Treatment Process*
- *Statement of Applicability*
- *Supplier Information Security Evaluation Process*
- *Internet Acceptable Use Policy*
- *Cloud Computing Policy*
- *Mobile Device Policy*
- *Teleworking Policy*
- *Access Control Policy*
- *User Access Management Process*
- *Cryptographic Policy*
- *Physical Security Policy*
- *Anti-Malware Policy*
- *Backup Policy*
- *Logging and Monitoring Policy*
- *Software Policy*

- *Technical Vulnerability Management Policy*
- *Network Security Policy*
- *Electronic Messaging Policy*
- *Information Security Policy for Supplier Relationships*
- *Availability Management Policy*
- *IP and Copyright Compliance Policy*
- *Records Retention and Protection Policy*
- *Privacy and Personal Data Protection Policy*
- *Clear Desk and Clear Screen Policy*
- *Social Media Policy*

5 Information Security Policy

5.1 Information Security Requirements

A clear definition of the requirements for information security within Everything IT will be agreed and maintained with the internal business and cloud service customers so that all ISMS activity is focussed on the fulfilment of those requirements.

Statutory, regulatory, and contractual requirements will also be documented and input to the planning process. Specific requirements regarding the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the Everything IT Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings/briefings, policy communication and awareness training.

5.2 Framework for Setting Objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001 the reference controls detailed in Annex A of the standard will be adopted where appropriate by Everything IT. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans. For details of which Annex, A controls have been implemented and which have been excluded please see the *Statement of Applicability*.

In addition, enhanced and additional controls from the following codes of practice will be adopted and implemented where appropriate:

- *ISO/IEC 27002 – Code of practice for information security controls*
- *ISO/IEC 27017 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- *ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

The adoption of these codes of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

5.3 Continual Improvement of the ISMS

Everything IT policy, regarding continual improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) regarding information security
- Make information security processes and controls more measurable to provide a sound basis for informed decisions
- Review relevant metrics on a continual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties, including cloud service customers
- Review ideas for improvement at regular management meetings to prioritise and assess timescales and benefits

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

5.4 Information Security Policy Areas

Everything IT defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and once formally approved, is communicated to an appropriate audience, both within and external to, the organization.

The table below shows the individual policies within the documentation set and summarises each policy’s content and the target audience of interested parties.

Policy Title	Areas addressed
Internet Acceptable Use Policy	Business use of the Internet, personal use of the Internet, Internet account management, security and monitoring and prohibited uses of the Internet service.
Cloud Computing Policy	Due diligence, signup, setup, management, and removal of cloud computing services.
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets, and smartphones, whether provided by the organization or the individual for business use.
Teleworking Policy	Information security considerations in establishing and running a teleworking site and arrangement e.g., physical security, insurance, and equipment
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management
Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management.
Backup Policy	Backup cycles, cloud backups, off-site storage, documentation, recovery testing and protection of storage media
Logging and Monitoring Policy	Settings for event collection. protection and review
Software Policy	Purchasing software, software registration, installation and removal, in-house software development and use of software in the cloud.
Technical Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening and awareness training.

Policy Title	Areas addressed
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks, and remote access; network security management, including roles and responsibilities, logging and monitoring and changes.
Electronic Messaging Policy	Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.
Information Security Policy for Supplier Relationships	Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contract.
Availability Management Policy	Availability requirements and design, monitoring and reporting, non-availability, testing availability plans and managing changes.
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties, and software license compliance.
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction, and review.
Privacy and Personal Data Protection Policy	Applicable data protection legislation, definitions, and requirements.
Clear Desk and Clear Screen Policy	Security of information shown on screens, printed out and held on removable media.
Social Media Policy	Guidelines for how social media should be used when representing the organization and when discussing issues relevant to the organization.

Table 1 - Set of policy documents

5.5 Application of Information Security Policy

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the top management of Everything IT and must be complied with. Failure by an employee to comply with these policies may result in disciplinary action being taken in accordance with the organization’s *Employee Disciplinary Process*.

Questions regarding any Everything IT policy should be addressed in the first instance to the employee’s immediate line manager.