YourIT!
Your Logo Goes Here

GDPR Assessment

ISO 27001 Policy and Procedures

Scan Date: 1/18/2018

Prepared for:
My Client Company
Prepared by:
YourIT Company

1/18/2018

TABLE OF CONTENTS

INFORMATION SECURITY POLICIES AND PROCEDURES

A.1 - EXECUTIVE SUMMARY

The purpose of this document is to detail the information security policies of the organisation.

This document details the policies, procedures, controls, and monitoring requirements defined to protect information confidentiality and integrity.

A.2 - INTRODUCTION

This document enumerates the information security policies and procedures adopted by our organisation to secure the organisation's information processing system and protect sensitive and/or confidential information. The policies are intended to ensure the confidentiality, integrity and availability of data residing on the organisation's information processing system networks and computers and the transmission of data outside of the organisation's information processing system when appropriate. These policies and procedures do not cover every condition, requirement, stipulation, stipulation, or facet of the ISO 27001 security standard or the European Union (EU) and/or EU Member State regulatory requirements defined in the appendix or appendices attached to this information security policy nor were they intended to do so.

The processes adopted by our organisation herein are designed to automate the documentation and reporting of technological requirements and not, for example, tasks that involve administrative attention such as employee background checks, disciplinary and sanction warnings, or third-party supplier contract management. The following policies and procedures support the administrative, physical, and technical safeguards of ISO 27001 whether required or addressable, to the extent described below and identified by the ISO 27001 Appendix A section as follows:

A.3 - SCOPE OF COVERAGE BY POLICIES AND AUTHORITY

[3.1] - SCOPE OF COVERAGE BY SECURITY POLICIES

The scope of coverage by the security policies and procedures is intended to include assets owned, leased, managed by, or operated on behalf of the organisation by employees and third parties.

The security policies and procedures are intended to protect:

a) All information, data, documents, databases, or other information stored on the organisation's information processing systems and network.

b) All desktop computers, server computers, data storage systems and devices, communications networks, firewalls, hubs, switches, routers, mobile devices, and any other devices used to transmit, store, or process information operating within the organisations information processing system and network infrastructure.

c) All computing platforms, operating system software, middleware, and/or application software under the control of third parties that connect in any way to the organisation's information processing system.

Security policies and procedures apply to all users of the information processing system including of employees, third parties, contractors, and vendors that access the system on site or through remote

computing connections. Vendors include, but are not limited to, information technology (IT) and cloud service providers that store, process, or transmit the organisation's information.

[3.2] - AUTHORITY TO ENFORCE SECURITY POLICIES

The organisation's Information Security Officer (ISO) and Data Protection Officer (DPO) are authorised to implement and enforce the information security policies and procedures detailed throughout this document pertaining to their respective roles in information security and data protection.

A.4 - RISK ANALYSIS AND MANAGEMENT

[4.1] RISK ANALYSIS

Implement a Generic reference to Regulatory requirements as referenced in the Appendices to this policy.

Policy: A comprehensive risk analysis process, known as a Data Protection Impact Assessment, will be performed upon all of the organisation's assets including Information Processing Systems will be conducted periodically and involves identifying risk and vulnerabilities in the organisation's information processing systems.

To do this, the organisation will conduct an accurate and thorough assessment of the potential threats and vulnerabilities to the confidentiality, integrity and availability of confidential, sensitive, or personally identifiable information at the organisation's sites. Then the organisation will reduce the risks and vulnerabilities to an appropriate and reasonable level or to the greatest extent possible though ongoing management. The risk analysis will be performed following industry best practice standards. A Data Protection Impact Assessment will be completed no less than one time a year or after successful implementation of any major system change. Major system change would include an office relocation, replacement of system component containing confidential, sensitive, and personally identifiable information, etc.

Procedure: The objective of the Data Protection Impact Assessment is to complete comprehensive, periodic and independent review of the organisation's security vulnerabilities. The organisation will start a risk assessment with a current inventory of all known devices and applications on the network and the organisation will "map" or diagram their interdependencies so the organisation can better understand the complex relationships between applications and devices. The organisation will also identify frequency and format of the assessment process (self-risk assessment versus third-party, independent data protection impact assessment), and document it. The Data Protection Impact Assessment process will include review of administrative, physical and technical safeguards, and also take into consideration criticality, impact and creation of recommendations identifying mitigation strategies.

The Risk Assessment will include a risk score for measurement and ongoing change analysis and an executive level summary report in narrative form. A more comprehensive Data Protection Impact Assessment involving more manual input through on-site surveys as well as using automated data collection routines will be performed, at least, annually or in the event of a significant change (office move, changing the organisation's information processing system, moving servers to the cloud, etc.) or conducted at the direction and authorisation of the Information Security Officer (ISO) and the Data Protection Officer (DPO).

[4.2] RISK MANAGEMENT

Policy: Once the organisation has completed the risk analysis process, the next step is risk management. Risk management, required by ISO 27001 and the European Union General Data

Protection Regulation (EU GDPR), includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of confidential, sensitive, and personally identifiable information and protect against any reasonably anticipated threats, hazards, or disclosures of sensitive data confidential, sensitive, or personally identifiable information not permitted by local, state, and federal statutory guidelines or regulations including EU GDPR.

The first step in the risk management process should be to develop and implement a Risk Treatment Plan. The purpose of a Risk Treatment Plan is to provide structure for the evaluation, prioritization, and implementation of risk-reducing measures and controls. The risk prioritization and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their risk score.

An important component of the Risk Treatment Plan is the plan for implementation of the selected security measures and controls. The implementation component of the plan should address:

- Risk score (threat and vulnerability combinations) assigned to a particular issue being addressed;
- Recommendation of measures and controls selected to reduce the risk of an issue;
- Implementation project priorities, such as required resources; assigned responsibilities; start and completion dates; and maintenance requirements.

The implementation component of the risk management plan may vary based on the circumstance. Compliance with the EU GRPR requires financial resources, management commitment, and the workforce involvement. Cost is one of the factors the organisation must consider when determining measures and controls to fix an issue. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate. The output of this step is a Risk Treatment Plan that contains prioritized risks, options for mitigation of those risks, and a plan for implementation. The plan will guide the organisation's actual implementation of security measures to reduce risks to confidential, sensitive, and personally identifiable information data to reasonable and appropriate levels.

The final step in the risk management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk analysis and risk management are not one-time activities. Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Procedure: The objective of risk management is to create and document a planned risk management approach as follows:

a) The most recent Data Protection Impact Assessment shall be used to develop or modify the Risk Treatment Plan.

b) The Risk Treatment Plan shall include implementation specifics and prioritized timelines for selected risk mitigation strategies identified in ongoing Data Protection Impact Assessments, or the Data Protection Impact Assessment report.

c) The Information Security Officer (ISO), the Data Protection Officer (DPO), or designated third party will execute the Risk Treatment Plan by reviewing and addressing issues identified therein and will be responsible for implementation of the IT security, network and system recommendations.

The organisation will implement automated tools and use other means to continually review and evaluate systems and devices that might store or have access to confidential, sensitive, or personally

identifiable information. The organisation will conduct a regular inventory of the information processing systems containing confidential, sensitive, or personally identifiable information and the security measures used to protect those systems. The organisation will give highest priority to fixing issues associated with unacceptably high risk rankings and will then work to minimize or eliminate the risk based upon feasibility and effectiveness of specific method. The organisation's Information Security Officer (ISO), the Data Protection Officer (DPO), or designated third party will oversee the implementation of solutions to better secure systems that store, process or transmit confidential, sensitive, or personally identifiable information

Automated tools will be used to validate that remediation has occurred and reports will be archived for at least TBD years. The tool activities will focus on collecting data through open protocols across the network or operating systems and producing reports and analysis on antivirus, patch and reliability, for example. The organisation will complement the automated reporting with walk through audits, device inspections and user list reviews.

A.5 - INFORMATION SECURITY POLICIES OVERVIEW

[5.1] - MANAGEMENT DIRECTION FOR INFORMATION SECURITY

The main purpose of document is "to provide management direction and support for information security in accordance with the business requirements and relevant laws and regulations" (ISO 27002-2013 Requirement 5.1).

The organisation's policies reflect its commitment to address concerns around information security. Information security relates to protection and treatment all data stored or transmitted by the organisation, especially those related to personal data.

[5.1.1] - POLICIES FOR INFORMATION SECURITY

The organisation will define a set of information security policies that will be:

a) approved by management

b) published for use by employees and relevant third parties that have access to or provide services for the processing of information within the organisation

c) communicated to employees and relevant third parties

[5.1.2] - REVIEW OF POLICIES FOR INFORMATION SECURITY

This document will be reviewed on an annual basis, or if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness.

A.6 - ORGANIZATION OF INFORMATION SECURITY

[6.1] - INTERNAL ORGANISATION OF INFORMATION SECURITY POLICIES AND PROCEDURES

Policy: The organisation will formulate and implement a framework to manage, initiate, and control the implementation of information security within the organisation.

Truncated Sample Report