STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 1 of 17

Reason for selection key B = Business or Contractual Requirements, R = Risk assessment requirement, L = Legal/Regulatory requirement

Control Ref	Control Title	Control Description	Implemented/ Applied?	Reason for selection			Justification for exclusion or Reference document
				B	R	L	
5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Y		X		DOC A5
5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Y		X		ISMS Manual section 9
6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Y	X	X		DOC A6.1
6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Y	X	X		DOC A6.1
6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Y		X		DOC A6.1
6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Y		X		DOC A6.1
6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	Y		X		DOC A6.1

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 2 of 17

6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Y	X	X		DOC A6.2
6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Y		X		DOC A6.2
7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Y	X	X	X	DOC A7
7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Y	X	X	X	DOC A7
7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Y		X		DOC A7
7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Y		X		DOC A7
7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Y	X	X	X	Employee handbook

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 3 of 17

7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Y		X			DOC A7
8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Y		X			DOC A8.1
8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Y		X			DOC A8.1
8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Y	X	X			Employee handbook
8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Y	X	X			DOC A7
8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Y		X			DOC A8.2
8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Y		X			DOC A8.2
8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Y		X			DOC A8.2

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 4 of 17

8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Y		X		DOC A8.2
8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Y		X		DOC A8.2
8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Y		X		DOC A8.2
9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Y		X		DOC A9.1
9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Y		X		DOC A9.1
9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Y	X	X		DOC A9.2
9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Y	X	X		DOC A9.2
9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Y	X	X		DOC A9.2

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 5 of 17

9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	Y		X		DOC A9.2
9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Y		X		DOC A9.2
9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Y		X		DOC A9.2
9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Y		X		DOC A9.2
9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Y		X		DOC A9.2
9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Y		X		DOC A9.2
9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Y		X		DOC A9.2
9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Y		X		DOC A9.2

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 6 of 17

9.4.5	Access control to program source code	Access to program source code shall be restricted.	Y	X	X		DOC A9.2
10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Y		X		DOC A10
10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Y		X		DOC A10
11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Y	X	X		DOC A11
11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Y	X	X		DOC A11
11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Y	X	X		DOC A11
11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Y		X		DOC A11
11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Y		X		DOC A11

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 7 of 17

11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Y		X		DOC A11
11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Y		X		DOC A11
11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Y		X		DOC A11
11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Y		X		DOC A11
11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Y		X		DOC A11
11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	Y		X		DOC A11
11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Y		X		DOC A11
11.2.7	Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has	Y		X		DOC A11

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 8 of 17

		been removed or securely overwritten prior to disposal or re-use.					
11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Y		X		DOC A11
11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Y		X		DOC A11
12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Y		X		DOC A12
12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Y		X		DOC A12
12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Y	X	X		DOC A12
12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Y	X	X		DOC A12
12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Y	X	X		DOC A12
12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Y	X	X		DOC A12

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 9 of 17

12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Y	X	X		DOC A12
12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Y	X	X		DOC A12
12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Y	X	X		DOC A12
12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Y	X	X		DOC A12
12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Y	X	X		DOC A12
12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Y	X	X		DOC A12
12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Y	X	X		DOC A12

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 10 of 17

12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Y		X		DOC A12
13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Y		X		DOC A13
13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Y		X		DOC A13
13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Y		X		DOC A13
13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Y		X		DOC A13
13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	Y		X		DOC A13
13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Y		X		DOC A13
13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of	Y		X		DOC A13

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 11 of 17

		information shall be identified, regularly reviewed and documented.					
14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Y		X		DOC A14
14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Y		X		DOC A14
14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Y		X		DOC A14
14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	Y		X		DOC A14
14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Y		X		DOC A14
14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Y		X		DOC A14
14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Y		X		DOC A14

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 12 of 17

14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Y		X		DOC A14
14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Y		X		DOC A14
14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	N				There is no outsourced development
14.2.8	System security testing	Testing of security functionality shall be carried out during development.	Y		X		DOC A14
14.2.9	System acceptance criteria	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Y		X		DOC A14
14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	Y		X		DOC A14
15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Y		X		DOC A15
15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure	Y		X		DOC A15

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 13 of 17

			components for, the organization's information.					
15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Y		X		DOC A15
15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	Y		X		DOC A15
15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Y		X		DOC A15
16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Y		X		DOC A16
16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Y		X		DOC A16
16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Y		X		DOC A16

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 14 of 17

16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Y		X		DOC A16
16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Y		X		DOC A16
16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Y		X		DOC A16
16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Y		X		DOC A16
17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Y		X		DOC A17
17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Y		X		DOC A17
17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Y		X		DOC A17

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 15 of 17

17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Y		X		DOC A18
18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Y		X	X	DOC A18
18.1.2	Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Y		X	X	DOC A18
18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Y	X	X	X	DOC A18
18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Y		X	X	DOC A18
18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Y		X	X	DOC A10
18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at	Y		X		DOC A18

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 16 of 17

			planned intervals or when significant changes occur.					
18.2.2	Compliance with security policies and standards		Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Y		X		DOC A18
18.2.3	Technical compliance review		Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards	Y		X		DOC A18

STATEMENT OF APPLICABILITY (SOA)

Document Control
Reference: DOC SOA
Issue No: 1.0
Issue Date: 2019-05-01
Page: 17 of 17

1   Document Owner and Approval

The Information Security Manager is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the MS.

A current version of this document is available to all members of staff on the company network and is published.

This procedure was approved by the CEO and is issued on a version controlled basis

Signature: *David Bonnstetter*_____

Date: 2019/05/03_____

TITLE	ISO 27001 Manual and SOA
FILE NAME	Information Security Manual and 1 other
DOCUMENT ID	cf6c976552517480caf98a0ed08818de0f3440cc
STATUS	● Completed

Document History

SENT

2019/05/01
09:35:24 UTC-7

Sent for signature to Dave Bonnstetter
(dave.bonnstetter@ttiltd.com) from john.kloian@ttiltd.com
IP: 208.186.1.4

VIEWED

2019/05/03
07:50:43 UTC-7

Viewed by Dave Bonnstetter (dave.bonnstetter@ttiltd.com)
IP: 72.195.221.199

SIGNED

2019/05/03
07:51:11 UTC-7

Signed by Dave Bonnstetter (dave.bonnstetter@ttiltd.com)
IP: 72.195.221.199

COMPLETED

2019/05/03
07:51:11 UTC-7

The document has been completed.