Section 2: Statement of Applicability for ISO 27001

2.1 Purpose and Scope

2.1.1 Purpose

The purpose of this document is to define which controls are appropriate to be implemented at Smooth Sailing Solutions, the objectives of these controls and how they are implemented, as well as to approve residual risks and formally approve the implementation of said controls.

This document includes all controls listed in Annex A of the ISO 27001 standard.

2.1.2 Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at Smooth Sailing Solutions and its subsidiaries.

Controls are applicable to the entire Information Security Management System (ISMS) scope.

2.2 Applicability of Controls

The following controls from ISO 27001 Annex A are applicable.

Justification for Selection / Non-selection is based on risk assessment results and/or contractual or legal obligations.

Control Objectives are defined for each of the controls and derived from Annex A. It is left blank if the control is marked as inapplicable.

Implementation Method specifies the document(s) relevant for each control. If there are no documents relevant for the control, a description of the process is given. It is left blank if the control is marked as inapplicable.

Status indicates the status of implementation:

- PL: “Planned”,
- IP: “In Process”, or
- IMP: “Implemented”.
- Left blank if the control is marked as inapplicable.

Table 2-1: Applicability of Controls

ID	ISO/IEC 27001 Controls	Appli cable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.5	Information Security Policies					
A.5.1	**Management direction for information security**					
A.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.	*Information Security Policy* and policies and standards referred to below in this column	
A.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.	Each policy, standard, and procedure has a designated owner who must review the document at planned intervals. These are recorded in each document.	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Appli cable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.6	Organization of Information Security					
A.6.1	**Internal organization**					
A.6.1.1	Information security roles and responsibilities			All information security responsibilities shall be defined and allocated.	Responsibilities for information security are listed in various policy and standards documents. If required, INFOSEC OVERLORD defines additional responsibilities.	
A.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.	Any activity that includes sensitive information is approved by one person and implemented by another.	
A.6.1.3	Contact with authorities			Appropriate contacts with relevant authorities shall be maintained.	*Business Continuity Policy* *Incident Response Standard*	
A.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.	[job title] is responsible for monitoring [list names of interest groups and security forums]	
A.6.1.5	Information security in project management			Information security shall be addressed in project management, regardless of the type of the project.	Project managers are required to include applicable information security rules in every project. *Change Management Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Appli cable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.6.2	**Mobile devices and teleworking**					
A.6.2.1	Mobile device policy			A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	? *Acceptable Use Standard*	
A.6.2.2	Teleworking			A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	*Acceptable Use Standard* *Remote Access Standard* *Remote Access Tools Standard*	
A.7	Human Resource Security					
A.7.1	**Prior to employment**					
A.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.	*Background Check Standard* *Vendor Selection Standard* *Vendor Security Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.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.	All employees sign the *Statement of Acceptance of ISMS Documents* and the *Employee Confidentiality Statement* *Vendor Security Standard* *Non-Disclosure Agreement*	
A.7.2	**During employment**					
A.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.	Management actively requires that all information security policies, standards, and procedures be implemented by all employees, suppliers, and outsourcing partners. *Vendor Security Standard*	
A.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.	*Information Security Policy* *Information Security and Privacy Training and Awareness Plan* *Vendor Security Standard*	
A.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.	*Statement of Acceptance of ISMS Documents* *[Employee Handbook]*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.7.3	**Termination and change of employment**					
A.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.	*Vendor Security Standard* requires that all agreements with vendors and partners contain clauses that remain valid after the termination of employment *Confidentiality Statements* are signed by all employees.	
A.8	Asset Management					
A.8.1	**Responsibility for assets**					
A.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.	[Inventory of Assets] *Data Classification Standard*	
A.8.1.2	Ownership of assets			Assets maintained in the inventory shall be owned.	[Inventory of Assets] *Acceptable Use Standard*	
A.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.	*Acceptable Use Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.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.	*Acceptable Use Standard* *Vendor Security Standard*	
A.8.2	**Information classification**					
A.8.2.1	Classification of information			Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	*Data Classification Standard*	
A.8.2.2	Labeling 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.	*Data Classification Standard*	
A.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.	*Data Classification Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Appli cable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.8.3	**Media handling**					
A.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.	*Data Classification Standard*	
A.8.3.2	Disposal of media			Media shall be disposed of securely when no longer required, using formal procedures.	*Media Destruction Standard*	
A.8.3.3	Physical media transfer			Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	*Data Classification Standard*	
A.9	Access Control					
A.9.1	**Business requirements of access control**					
A.9.1.1	Access control policy			An access control policy shall be established, documented and reviewed based on business and information security requirements.	*Minimum Access Standard*	
A.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.	*Minimum Access Standard* *Remote Access Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Appli cable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.9.2	**User access management**					
A.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.	*Minimum Access Standard*	
A.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.	*Minimum Access Standard*	
A.9.2.3	Management of privileged access rights			The allocation and use of privileged access rights shall be restricted and controlled.	*Minimum Access Standard*	
A.9.2.4	Management of secret authentication information of users			The allocation of secret authentication information shall be controlled through a formal management process.	*Minimum Access Standard* *Password Construction Standard* *Password Protection Standard*	
A.9.2.5	Review of user access rights			Asset owners shall review users' access rights at regular intervals.	*Minimum Access Standard*	
A.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.	*Minimum Access Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.9.3	**User responsibilities**					
A.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.	*Acceptable Use Standard* *Minimum Access Standard* *Password Protection Standard*	
A.9.4	**System and Application Access Control**					
A.9.4.1	Information access restriction			Access to information and application system functions shall be restricted in accordance with the access control policy.	*Minimum Access Standard* *Data Classification Standard*	
A.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.	A secure log-on process exists for all computers on the network	
A.9.4.3	Password management system			Password management systems shall be interactive and shall ensure quality passwords.	*Password Protection Standard*	
A.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.	*Server Security Standard* Only [job title] has the right to use privileged utility programs	
A.9.4.5	Access control to program source code			Access to program source code shall be restricted.	The program source code is stored [describe technical implementation] and only [job title] has access rights	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.10	Cryptography					
A.10.1	**Cryptographic controls**					
A.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.	*Acceptable Encryption Standard*	
A.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.	*Acceptable Encryption Standard* *Encryption End User Key Protection Standard*	
A.11	Physical and Environmental Security					
A.11.1	**Secure areas**					
A.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.	*Physical Access Security Standard*	
A.11.1.2	Physical entry controls			Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	*Physical Access Security Standard*	
A.11.1.3	Securing offices, rooms, and facilities			Physical security for offices, rooms and facilities shall be designed and applied.	*Physical Access Security Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Appli cable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.11.1.4	Protecting against external and environmental threats			Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	*Physical Access Security Standard*	
A.11.1.5	Working in secure areas			Procedures for working in secure areas shall be designed and applied.	*Physical Access Security Standard*	
A.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.	*Physical Access Security Standard*	
A.11.2	**Equipment**					
A.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.	*Environmental Security Standard*	
A.11.2.2	Supporting utilities			Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	*Environmental Security Standard*	
A.11.2.3	Cabling security			Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	*Environmental Security Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Appli cable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.11.2.4	Equipment maintenance			Equipment shall be correctly maintained to ensure its continued availability and integrity.	*Environmental Security Standard*	
A.11.2.5	Removal of assets			Equipment, information or software shall not be taken off-site without prior authorization.	*Acceptable Use Standard* *Physical Access Security Standard*	
A.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.	*Acceptable Use Standard* *Physical Access Security Standard* *Remote Access Standard* *Remote Access Tools Standard*	
A.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 been removed or securely overwritten prior to disposal or re-use.	*Media Destruction Standard*	
A.11.2.8	Unattended user equipment			Users shall ensure that unattended equipment has appropriate protection.	*Acceptable Use Standard* *Clean Desk Standard* *HIPAA Workstation Security Standard*	
A.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.	*Acceptable Use Standard* *Clean Desk Standard* *HIPAA Workstation Security Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.12	Operations Security					
A.12.1	**Operational procedures and responsibilities**					
A.12.1.1	Documented operating procedures			Operating procedures shall be documented and made available to all users who need them.	[Operating Procedures for Information and Communication Technology]	
A.12.1.2	Change management			Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	*Change Management Standard*	
A.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.	*Capacity Management Standard*	
A.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.	*Lab Security Standard* *Secure Development Standard*	
A.12.2	**Protection from malware**					
A.12.2.1	Controls against malware			Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	*Acceptable Use Standard* *Software Installation Standard* *Web Application Security Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.12.3	**Backup**					
A.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.	[Data Backup and Restoration Plan] *Acceptable Use Standard* *Records Retention Standard* *Disaster Recovery Standard* *Secure Development Standard*	
A.12.4	**Logging and monitoring**					
A.12.4.1	Event logging			Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	*Information Logging Standard*	
A.12.4.2	Protection of log information			Logging facilities and log information shall be protected against tampering and unauthorized access.	*Information Logging Standard*	
A.12.4.3	Administrator and operator logs			System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	*Information Logging Standard*	
A.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.	System clocks on all computers are synchronized [describe how they are synchronized and with which accurate time source]	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.12.5	**Control of operational software**					
A.12.5.1	Installation of software on operational systems			Procedures shall be implemented to control the installation of software on operational systems.	*Acceptable Use Standard* *Software Installation Standard*	
A.12.6	**Technical vulnerability management**					
A.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.	*Incident Response Standard* *Security Response Plan Standard*	
A.12.6.2	Restrictions on software installation			Rules governing the installation of software by users shall be established and implemented.	*Acceptable Use Standard* *Software Installation Standard*	
A.12.7	**Information systems audit considerations**					
A.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.	*Audit Standard* *Information Logging Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.13	Communications Security					
A.13.1	**Network security management**					
A.13.1.1	Network controls			Networks shall be managed and controlled to protect information in systems and applications.	*Acceptable Encryption Standard* *Bluetooth Baseline Requirements Standard* *DMZ Equipment Standard* *Encryption End User Key Protection Standard* *Lab Security Standard* *Network Connection Standard* *Remote Access Standard* *Remote Access Tools Standard* *Router and Switch Security Standard* *Server Security Standard* *Wireless Communication Standard*	
A.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.	*Network Connection Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.13.1.3	Segregation in networks			Groups of information services, users and information systems shall be segregated on networks.	*Network Connection Standard*	
A.13.2	**Information transfer**					
A.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.	*[Operating Procedures for Information and Communication Technology]* *Information Transfer Standard* *Acceptable Encryption Standard* *Remote Access Standard* *Remote Access Tools Standard* *Wireless Communication Standard*	
A.13.2.2	Agreements on information transfer			Agreements shall address the secure transfer of business information between the organization and external parties.	*[Operating Procedures for Information and Communication Technology]* *Information Transfer Standard*	
A.13.2.3	Electronic messaging			Information involved in electronic messaging shall be appropriately protected.	*Acceptable Use Standard* *Data Classification Standard* *Information Transfer Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Appli cable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.13.2.4	Confidentiality or nondisclosure agreements			Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	The form of the *Confidentiality Statement* is pre-defined	
A.14	System Acquisition, Development and Maintenance					
A.14.1	**Security requirements of information systems**					
A.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.	When acquiring new information systems or changing existing ones, [job title] must document security requirements in the [Security Requirements Specification]	
A.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.	*Secure Development Standard*	
A.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.	*Secure Development Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.14.2	**Security in development and support processes**					
A.14.2.1	Secure development policy			Rules for the development of software and systems shall be established and applied to developments within the organization.	*Secure Development Standard*	
A.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.	*Change Management Standard* and associated procedures	
A.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.	[job title] is responsible for reviewing and testing all applications after operating system changes, before they are put into production	
A.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.	*Change Management Standard* *Software Installation Standard*	
A.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.	*Secure Development Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.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.	*Secure Development Standard*	
A.14.2.7	Outsourced development			The organization shall supervise and monitor the activity of outsourced system development.	*Vendor Security Standard* *Secure Development Standard*	
A.14.2.8	System security testing			Testing of security functionality shall be carried out during development.	*Secure Development Standard*	
A.14.2.9	System acceptance testing			Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	*Secure Development Standard*	
A.14.3	**Test data**					
A.14.3.1	Protection of test data			Test data shall be selected carefully, protected and controlled.	*Lab Security Standard* *Secure Development Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Appli cable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.15	Supplier Relationships					
A.15.1	**Information security in supplier relationships**					
A.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.	*Vendor Security Standard*	
A.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 components for, the organization’s information.	*Vendor Security Standard*	
A.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.	*Vendor Security Standard*	
A.15.2	**Supplier service delivery management**					
A.15.2.1	Monitoring and review of supplier services			Organizations shall regularly monitor, review and audit supplier service delivery.	*Vendor Security Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.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.	*Vendor Security Standard*	
A.16	Information Security Incident Management					
A.16.1	**Management of information security incidents and improvements**					
A.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.	*Incident Response Standard*	
A.16.1.2	Reporting information security events			Information security events shall be reported through appropriate management channels as quickly as possible.	*Incident Response Standard*	
A.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.	*Incident Response Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.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.	*Incident Response Standard*	
A.16.1.5	Response to information security incidents			Information security incidents shall be responded to in accordance with the documented procedures.	*Incident Response Standard*	
A.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.	*Incident Response Standard*	
A.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.	*Incident Response Standard*	
A.17	Information Security Aspects of Business Continuity Management					
A.17.1	**Information security continuity**					
A.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.	[Procedure for Identification of Requirements] *Business Continuity Policy* [Business Impact Analysis Methodology]	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.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.	*Business Continuity Plan Standard* *Disaster Recovery Standard* *Security Response Plan Standard*	
A.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.	*Business Continuity Plan Standard* *Disaster Recovery Standard* *Security Response Plan Standard* [Post-incident Review Form]	
A.17.2	**Redundancies**					
A.17.2.1	Availability of information processing facilities			Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	[Recovery strategy for IT infrastructure]	
A.18	Compliance					
A.18.1	**Compliance with legal and contractual requirements**					
A.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.	[List of Legal, Regulatory, Contractual and Other Requirements]	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Appli cable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.18.1.2	Intellectual property rights			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.	*Acceptable Use Standard* ?	
A.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.	*Data Classification Standard* *Records Retention Standard* *Secure Development Standard* [Procedure for Document and Record Control]	
A.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.	*Privacy Standard*	
A.18.1.5	Regulation of cryptographic controls			Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	*Acceptable Encryption Standard* *Encryption End User Key Protection Standard*	

Table 2-1: Applicability of Controls (Continued)

ID	ISO/IEC 27001 Controls	Applicable (Y/N)	Justification for Selection / Non-selection	Control Objectives	Implementation Method	Status
A.18.2	**Information security reviews**					
A.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 planned intervals or when significant changes occur.	*Audit Standard* certification audit by [name of certification body]	
A.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.	*Audit Standard* All owners of information assets, INFOSEC, and management regularly review the implementation of security controls	
A.18.2.3	Technical compliance review			Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	*Audit Standard* INFOSEC OVERLORD is responsible for checking the technical compliance of information systems with security requirements.	

2.3 Acceptance of Residual Risks

Since not all risks could be reduced in the risk management process, all residual risks are hereby accepted:

1. all risks with the value 0, 1 or 2, and
2. risks which could not be reduced to the abovementioned levels after the application of controls, according to the following table:

[Complete the table with data on all individual risks which are not acceptable – use the Risk Treatment Table as the source.]

Table 2-2:

No.	Name of Asset	Threat	Vulnerability	New Impact	New Probability	Residual Risk

2.4 Compliance and Control

Section 2: *Statement of Applicability for ISO 27001* is a controlled document. While this document may be printed, the electronic version maintained on the Smooth Sailing Solutions POLICY DOCS LOCATION is the controlled copy. Any printed copies of this document are not controlled.

Document Section Classification: Internal Only

2.4.1 Reference Documents

- *ISO/IEC 27001 standard, clause 6.1.3 d*
- *Information Security Policy*
- *Risk Assessment and Risk Treatment Methodology*
- *Risk Assessment and Risk Treatment Report*

2.4.2 Change Control

Table 2-3: Amendment History

Version	Date	Person	Description of Change
0.1	June 21 2019	T. Ryng	Initialization per template.
0.2	June 24 2019	T. Ryng	Edits for Vendor Security.
0.3	June 25 2019	T. Ryng	Copy edits. Add Control Objectives.
0.4	June 28 2019	T. Ryng	Normalization of document titles as their drafts are published. Copy edits.

2.4.3 Review and Approval

This document is valid as of [date].

The owner of this document is indicated in Table 2-4. This person must review and, if necessary, update the document at least annually, and immediately after risk assessment review and updates to the *Risk Assessment Table* and *Risk Treatment Table*.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of nonconformities due to unclearly defined implementation method of individual controls,
- number of nonconformities due to unclearly defined control objectives, and
- number of controls for which the achievement of objectives cannot be measured.

Table 2-4: Approval

Name	Title	Signature	Date
	EXECUTIVE-TYPE PERSON		

◈◈◈