ISO 27001:2022 Statement of Applicability

Version	3
Author:	Jonathan Scutt – IT and Compliance Manager
When:	November 2023
Approved by:	Kate Wood – Head of Operations

ISO Clause	Information security control	Applicable	Implemented	Description of Controls
5	**Organizational controls**			
5.1	Policies for information security	Yes	Yes	Our set of policies are approved by management and referenced in this SOA. It is adopted by our Leadership and applies to all team members and contractors. Employees must complete onboarding training and regular refreshers throughout the year.
5.2	Information security roles and responsibilities	Yes	Yes	Responsibility and accountability for the management of our ISMS resides with ISMS team with individual responsibilities documented. Overall accountability is with the Managing Director.
5.3	Segregation of duties	Yes	Yes	Our Access Control Policy ensures that conflicting duties and areas of responsibility are segregated. Further individuals' responsibilities are documented.
5.4	Management responsibilities	Yes	Yes	Mobilityways ensures all personnel do not misuse the information made available to them for the purpose of operations. It is Part of roles and responsibilities, ISMS policies and Objectives and training of employees referenced in our People Policy.
5.5	Contact with authorities	Yes	Yes	Mobilityways maintain contact with relevant law enforcement and regulatory bodies both in the normal course of our business and in exceptional circumstance to report security incidents or to maintain continuity of our business.
5.6	Contact with special interest groups	Yes	Yes	It is the responsibility of the IT and CTO roles to collect information from special interest groups about existing and emerging security threats and vulnerabilities.
5.7	Threat Intelligence	Yes	Yes	It is the responsibility of the IT and CTO roles to collect information about existing and emerging threats and to investigate, design and propose mitigation actions.
5.8	Information security in project management	Yes	Yes	Mobilityways addresses information security in all projects, Information security implications are expected to be addressed and reviewed regularly in all projects. Our Secure Development and Change Management policy, specific roles and responsibilities support this.
5.9	Inventory of assets	Yes	Yes	Mobilityways maintains a register of information assets, ensuring all information assets are identified and security controls are applied.
5.1	Acceptable use of assets	Yes	Yes	Mobilityways Acceptable Use Policy, Information Transfer Policy, Data Handling & Document and Records process, defines appropriate handling of assets & information.
5.11	Return of assets	Yes	Yes	Procedures are in place to ensure that Information Security related assets that are assigned to employees or contractors are returned when the contract with the employee or contractor ends.
5.12	Classification of information	Yes	Yes	Information is classified and labelled as set out in our Data Handling Policy, Procedures for Document and Record control. They guide asset owners and employees on the appropriate labelling of information assets.
5.13	Labelling of information	Yes	Yes	Information is classified and labelled as set out in our Data Handling Policy, Procedures for Document and Record control. They guide asset owners and employees on the appropriate labelling of information assets.
5.14	Information transfer	Yes	Yes	Transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities. Security training re-enforces our policies
5.15	Access control	Yes	Yes	Mobilityways operates a formal starters, movers and leavers procedure for granting and revoking access to all information technology systems and services. Policies and process are in place for employees to formally request access and change of access. Regular access audits are performed.
5.16	Identity management	Yes	Yes	Mobilityways operates a formal starters, movers and leavers procedure for granting and revoking access to all information technology systems and services. Policies and process are in place for employees to formally request access and change of access. Regular access audits are performed.
5.17	Authentication information	Yes	Yes	Mobilityways protect sensitive authentication information by providing employees with secure services and training to manage passwords. Password and MFA policy, regular training and quarterly security rating reviews re-enforces this.
5.18	Access rights	Yes	Yes	Mobilityways operates a formal starters, movers and leavers procedure for granting and revoking access to all information technology systems and services. Access audits are performed annually and 6 monthly for privileged accounts.
5.19	Information security in supplier relationships	Yes	Yes	Supplier risk assessments and agreements with suppliers include requirements that address the information security risks associated with information and communication technology services and product supply chain. Annual audits and monitoring ensure compliance with business requirements.
5.20	Addressing security within supplier agreements	Yes	Yes	Supplier risk assessments and agreements with suppliers include requirements that address the information security risks associated with information and communication technology services and product supply chain. Annual audits and monitoring ensure compliance with business requirements.

5.21	Managing information security in the ICT supply chain	Yes	Yes	Supplier risk assessments and agreements with suppliers include requirements that address the information security risks associated with information and communication technology services and product supply chain. Annual audits and monitoring ensure compliance with business requirements.
5.22	Monitoring, review and change management of supplier services	Yes	Yes	Supplier risk assessments and agreements with suppliers include requirements that address the information security risks associated with information and communication technology services and product supply chain. Annual audits and monitoring ensure compliance with business requirements.
5.23	Information security for use of cloud services	Yes	Yes	Supplier risk assessments and agreements with suppliers include requirements that address the information security risks associated with information and communication technology services and product supply chain. Annual audits and monitoring ensure compliance with business requirements.
5.24	Information security incident management planning and preparation	Yes	Yes	Management responsibilities and procedures are established to ensure a quick, effective, and orderly response to information security incidents.
5.25	Assessment and decision on information security events	Yes	Yes	The assessment of incident security events and the decision to classify as an information security incident is defined in our policy and procedure.
5.26	Response to information security incidents	Yes	Yes	The response to information security incidents are defined in policy and process documents.
5.27	Learning from information security incidents	Yes	Yes	All employees, contractors and 3rd party users of information technology systems and services are required to report any observed or suspected weaknesses in information technology systems or services using the same mechanisms as for actual Security Events.
5.28	Collection of evidence	Yes	Yes	Policy and process set out the procedure for gathering and retaining evidence and the chain of custody.
5.29	Information security during disruption	Yes	Yes	Plans have been developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required timescales following interruption to, of failure of, critical business processes.
5.30	ICT readiness for business continuity	Yes	Yes	Mobilityways Business Continuity Plans are tested and updated periodically to ensure that they are up to date and effective.
5.31	Legal, statutory, regulatory and contractual requirements	Yes	Yes	Registers are maintained to capture relevant ISMS related statutory, regulatory, and contractual obligations.
5.32	Intellectual property rights	Yes	Yes	Appropriate procedures are implemented to ensure compliance with statutory, regulatory, and other legal obligation requirements on the user of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
5.33	Protection of records	Yes	Yes	Policies are in place to ensure records are protected from loss, destruction, and falsification, in accordance with statutory and regulatory and other legal obligation and business requirements.
5.34	Privacy and protection of PII	Yes	Yes	Mobilityways Data protection and privacy policies, procedures, and training support relevant statutory and regulatory and (if applicable) in other legal requirements.
5.35	Independent review of information security	Yes	Yes	Audits are conducted internally by persons independent of the function of management being audited. Some audits may be performed by external 3rd parties.
5.36	Compliance with policies, rules and standards for information security	Yes	Yes	Mobilityways Leaders are responsible for ensuring compliance within their areas of responsibility. Non-compliance, corrective action, and opportunities for improvement are also reviewed at Management Review Meetings.
5.37	Documented operating procedures	Yes	Yes	Mobilityways Procedures, policies (containing procedures), training materials and other instructions / information is provided to those that need them to effectively fulfil the information security aspects of their roles. Where appropriate these documents are included in this SOA under the appropriate controls
6	**People controls**			
6.1	Screening	Yes	Yes	Background verification checks in line with our policy and procedure are carried out for all candidates for employment. These include Right to Work, DBS and 2 x professional references. The policy takes account of relevant laws and regulations; and is proportional to the business requirements. We have contractual agreements with contractors to comply with our Information Security policies and procedures.
6.2	Terms and conditions of employment	Yes	Yes	The contractual obligations for employees and contractors engaged by Mobilityways are set out in the Contract of Employment which all employees and directly employed contractors are required to sign before commencing employment. These terms and conditions also set out the continuing responsibilities for Information Security after employment ends.
6.3	Information security awareness, education and training	Yes	Yes	A program of Cyber Security Awareness and Training exists for all employees. Where there are role specific information security requirements, training needs are assessed, and appropriate training arranged.

6.4	Disciplinary process	Yes	Yes	We have a clear Disciplinary Policy and Procedure (and Performance Improvement Policy where applicable) to handle circumstances where an employee who has committed an information security breach.
6.5	Termination or change of employment responsibilities	Yes	Yes	Processes exist to ensure employees are reminded of their obligations regarding information security and the consequences of not meeting those obligations when they leave. When employees change roles, the responsibility rests with the line manager to advise the employee of any role specific obligations.
6.6	Confidentiality or nondisclosure agreements	Yes	Yes	Confidentiality and non-disclosure agreements are established and used where appropriate to protect information. Confidentiality clause is included in Contract of Employment
6.7	Remote working	Yes	Yes	Our policies and training take into account the risks and associated controls required.
6.8	Information security event reporting	Yes	Yes	We have procedures in place to ensure security events are reported and recorded. These procedures are supported with training courses and policy. Clear communication is given to employees on how to report incidents.
7	**Physical controls**			
7.1	Physical security perimeter	Yes	Yes	Physical perimeter security is defined by and managed in accordance with our Physical and Environmental Security Policy. Additional documented information supports the execution of the policy.
7.2	Physical entry	Yes	Yes	Physical entry controls are set out in our Physical and Environmental Security Policy. There is a visitor access procedure to support this policy.
7.3	Securing offices, rooms and facilities	Yes	Yes	Physical entry controls are set out in our Physical and Environmental Security Policy. There is a visitor access procedure to support this policy.
7.4	Physical security monitoring	Yes	Yes	Physical entry controls are set out in our Physical and Environmental Security Policy. There is a visitor access procedure to support this policy.
7.5	Protecting against external and environmental threats	Yes	Yes	Physical entry controls are set out in our Physical and Environmental Security Policy. There is a visitor access procedure to support this policy.
7.6	Working in secure areas	No		This is not applicable to Mobilityways has no secure working areas.
7.7	Clear desk and clear screen	Yes	Yes	Mobilityways Clear Desk and Screen Policy and training are in place to ensure that users clear their desk, devices are locked and no information is left exposed or unattended.
7.8	Equipment siting and protection	Yes	Yes	Equipment is sited or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.
7.9	Security of assets off-premises	Yes	Yes	Security is applied to assets and equipment off-site, taking into account the different risks that arise. Policies and training support this.
7.10	Storage media	Yes	Yes	The use, management and destruction of media is controlled by our Acceptable Use, Physical and Environmental Security and User endpoint device policy
7.11	Supporting utilities	No		This is not applicable to Mobilityways our business functions are entirely cloud based.
7.12	Cabling security	No		This is not applicable to Mobilityways our business functions are entirely cloud based.
7.13	Equipment maintenance	Yes	Yes	Equipment is correctly maintained to ensure its continued availability and integrity
7.14	Secure disposal or reuse of equipment	Yes	Yes	Policy, process and procedures exist that ensure that all equipment reuse is managed and is disposed of securely
8	**Technological controls**			
8.1	User endpoint devices	Yes	Yes	The requirements for both company provided devices and employee owned devices are set out in our policies. Cloud based Mobile device management is used along with, training to reinforce understanding and compliance.
8.2	Management of privileged access rights	Yes	Yes	Allocation and use of privileges are restricted and controlled in line with our policy and procedure.
8.3	Information access restriction	Yes	Yes	Access to information and application system functions by users and contractors is restricted in accordance with the defined Access Control Policy.
8.4	Access to source code	Yes	Yes	Access to source code is restricted to only those roles that require it.
8.5	Secure authentication	Yes	Yes	Access to all systems is controlled by a Password and MFA and Access Control Policy.
8.6	Capacity management	Yes	Yes	Use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance
8.7	Protection against malware	Yes	Yes	All devices have active anti-malware software that is configured in compliance with our policies.
8.8	Management of technical vulnerabilities	Yes	Yes	Technical vulnerabilities are identified and managed in line with our policies and processes. Information technology systems are checked for compliance with security implementation standards.
8.9	Configuration management	Yes	Yes	Configurations are managed in line with our policies and processes. Information technology systems are checked for compliance with security configuration standards and best practise.

8.10	Information deletion	Yes	Yes	The deletion of information is controlled by our Data Handling policies and procedures.
8.11	Data masking	Yes	Yes	Data masking and sanitization methods are controlled by our policies to ensure sensitive information is unrecognizable but still usable for development or statistical purposes.
8.12	Data leakage prevention	Yes	Yes	Data leakage prevention controls are in place to control data in transit.
8.13	Information backup	Yes	Yes	Back-up of information are taken and tested regularly in accordance with the Information Backup and Restore Policy.
8.14	Redundancy of information processing facilities	Yes	Yes	A managed process has been developed and maintained to ensure the required level of continuity for information security during an adverse, unplanned or emergency situation.
8.15	Logging	Yes	Yes	Audit logs recording user activities, exceptions and information security incidents are produced and kept for an agreed time period for investigations and access control monitoring.
8.16	Monitoring activities	Yes	Yes	Mobilityways monitoring efforts are optimised by employing specialised monitoring tools provided by our cloud service partners. These provide real-time notifications and advanced automated threat protection.
8.17	Clock synchronisation	Yes	Yes	Mobilityways devices are configured to a base standard to ensure accountability and non-repudiation.
8.18	Use of privileged utility programs	Yes	Yes	The use of utility programs that might be capable of overriding system and application controls is restricted and tightly controlled
8.19	Installation of software on operational systems	Yes	Yes	Mobilityways have policies and procedures in place to ensure the installation of software on production systems is appropriately controlled.
8.20	Network controls	Yes	Yes	Mobilityways maintain appropriate controls and procedures to ensure the consistent and secure operations of the network and related components.
8.21	Security of network services	Yes	Yes	Mobilityways ensure security is considered and addressed in all network service agreements
8.22	Segregation of networks	Yes	Yes	Networks are segregated as much as practical to prevent access overlap and to minimise impact of any incident to a network.
8.23	Web filtering	Yes	Yes	Web filtering is configured to prevent access to malicious or inappropriate website on the internal network.
8.24	Use of cryptography	Yes	Yes	Mobilityways operates formal policies, standards, and procedures on the use of cryptography controls for the protection of its information.
8.25	Secure development policy	Yes	Yes	Development of software within the organisation is set out in our policy for secure systems engineering principles.
8.26	Application security requirements	Yes	Yes	Information involved in application interactions is protected to ensure that its confidentiality, availability, and integrity is, by design and overall architecture is protected
8.27	Secure system engineering principles	Yes	Yes	Software security standards are in place to ensure that systems are designed, developed, implemented, maintained, and documented consistently in accordance with security requirements.
8.28	Secure coding	Yes	Yes	Software security standards are in place to ensure that systems are designed, developed, implemented, maintained, and documented consistently in accordance with security requirements.
8.29	Security testing in development and acceptance	Yes	Yes	Systems security requirements and functionality are integrated into software test plans
8.30	Outsourced development	Yes	Yes	Mobilityways shall supervise and monitor the activity of outsourced system development
8.31	Separation of development, testing and operational environments	Yes	Yes	Development, test and operational environments are separated by controlled access to reduce the risks of unauthorized access or changes to the operational system.
8.32	Change management	Yes	Yes	Policies and processes are documented to ensure that changes likely to impact information security are controlled.
8.33	Test information	Yes	Yes	Data used for testing systems are stored and processed in a manner that ensures appropriate security controls and compliance with all applicable privacy requirements and where production environment sensitive data is used in a test environment it shall be redacted or otherwise obfuscated.
8.34	Protection of information systems during audit testing	Yes	Yes	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes. Any number of scanning activities may be performed on systems, e.g., vulnerability scanning, compliance scanning, static code analysis, dynamic URL scanning, penetration testing as well as monitoring on end point systems.