Statement of Applicability.

(version 120 – December 3rd 2021 – 11:53AM CET)

CHILI publish

All controls which are applicable (marked by "YES"), are also implemented.

ISO 27001 Required Control (version 115)	**Applicability and justification**
A.5 Information Security Policies	
A.5.1 Management direction for information security	
A. 5.1.1 Policies for information security	YES Policies are a best practice to distribute clear and concise agreements on how information must be handled. Information security objectives and principles to guide the activities relating to information security must be defined. Roles and responsibilities must be defined. Processes for handling deviations and exceptions must be defined. This can be described in policies or CHims components linked to these policies.
A. 5.1.2 Review of the policies for information security	YES Business strategy, regulations, legislations contracts and related security objectives, threat environment may change, as can the CHims environment be changed. This results in the need for policies to be reviewed at planned intervals or at any timeframe. This is best practice and reduces information security events in a fast evolving world.
A.6 Organization of information security	
A.6.1 Internal organization	
A. 6.1.1 Information security roles and responsibilities	YES Information security is a responsibility for every CHili publish staff member. But depending on the staff context (handled assets, authorization levels, training requirements for handling assets, connection with suppliers, customers, used tools, different roles in the organization, staff handling multiple roles), the responsibilities must be described in an explicit way to make sure: - All related responsibilities are explicitly described - Segregation of responsibilities is implemented where possible This best practice reduces risks on faulty information handling or escalation in case of an event.
A. 6.1.2 Segregation of duties	YES Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's asset.
A. 6.1.3 Contact with authorities	YES Organization under attack from the Internet may need authorities to take action against the attack source. Having contact with the authorities are also useful to anticipate and prepare for upcoming changes in laws an regulations which have to be implemented by the organization, enabling the organization to prepare for events and act more effective in case an event occurs. Contact with other authorities include utilities, emergency services, electricity suppliers health and safety, telecommunication providers.
A. 6.1.4 Contact with special interest groups	YES Control is included to reduce risks by being up to date by acquiring knowledge on best practices, understanding the current completeness of the information security environment, receiving early warnings of alerts, advisories and patches to prevent damage by attacks and exploits of vulnerabilities. Having contacts defined to gain faster specialist and information security advice. Also sharing and exchanging information about new technologies, products threats or vulnerabilities supports CIA of information.
A. 6.1.5 Information security in project management	YES Information security is integrated in the processes executing projects to reduce the risk of information security events during the execution of these projects.
A.6.2 Mobile devices and teleworking	

A. 6.2.1 Mobile device policy	YES Information of stakeholders is handled on mobile devices. This invokes a possible information security risk. This risk must be handled. To reduce these risks, a mobile device policy, agreed by the staff is in place..
A. 6.2.2 Teleworking	YES Information of stakeholders is handled during teleworking. This invokes a possible information security risk. these risks must be handled. To reduce these risks, a mobile device policy, agreed by the staff is in place..
A.7 Human resource security	
A.7.1 Prior to employment	
A. 7.1.1 Screening	YES Depending on the role of a staff member, the CIA of the handled information must be handled. To prevent abuse of handling information and reduce risks of hiring not trustworthy staff, a background verification check must be executed on potential new staff members.
A. 7.1.2 Terms and conditions of employment	YES To reduce risks in information security, new staff members must formally agree with the CHims procedures, responsibilities, use of assets and disciplinary actions in case information is not handled correctly.
A.7.2 During employment	
A. 7.2.1 Management responsibilities	YES To reduce risks in information security handling, management requires all staff to apply the applicable policies and procedures in the organization.
A. 7.2.2 Information security awareness, education and training	YES To reduce risk in information security handling, all staff receive regular and timely security awareness training.
A. 7.2.3 Disciplinary process	YES To further reduce risk in information security handling, communicate and enforce the (a policy) commitment for the staff, so a formal disciplinary process is in place.
A.7.3 Termination and change of employment	
A. 7.3.1 Termination or change of employment responsibilities	YES To reduce risks in information security handling, after termination or change of employment, the rule of having access and need to know and need to use basis must be established.
A.8 Asset management	
A.8.1 Responsibility for assets	
A. 8.1.1 Inventory of assets	YES Inventory of assets help to ensure effective protection of the assets take place and reduces risks on faulty information handling.
A. 8.1.2 Ownership of assets	YES It is a good practice to have an accountable person for each asset, so that the assets can be protected and managed.
A. 8.1.3 Acceptable use of assets	YES It is a good practice to have the acceptable use of each asset made explicit, so that each organization member knows how to handle the information asset in a secure way. Having acceptable use of assets clear and trained, reduce risk of faulty information handling.
A. 8.1.4 Return of assets	YES It is a good practice to formally manage return of assets where appropriate to reduce risk of abuse of confidentiality, integrity and availability of the involved information.

A.8.2 Information classification	
A. 8.2.1 Classification of information	YES It is a requirement and good practice to classify information, so it can be labelled and handled the correct way by the staff. When information can be classified clearly, the risk of abusing the information is reduced.
A. 8.2.2 Labelling of information	YES It is a requirement to label information, so it can be handled the correct way by the staff. When information is labelled, the risk of abusing the information is reduced.
A. 8.2.3 Handling of assets	YES Procedures and related training on handling labelling information is in place to reduce risk of faulty handled information.
A.8.3 Media handling	
A. 8.3.1 Management of removable media	YES A formal procedure is in place on how to handle removable media that might contain information. It is a good practice to train the staff on this, and have them formally agree to decrease risk of faulty information handling.
A. 8.3.2 Disposal of media	YES To reduce risk on leaked information, it is a good practice to have a formal procedure in place to dispose of the media.
A. 8.3.3 Physical media transfer	YES To reduce risk on leaked information, it is a good practice to have a formal procedure in place to dispose of the media.
A.9 Access control	
A.9.1 Business requirements of access control	
A. 9.1.1 Access control policy	YES An access control policy must be in place to e.g. guarantee confidentiality of information, to manage access to staff on need-to-know and need-to use basis, but make sure the information is available where required. This is a good practice.
A. 9.1.2 Access to networks and network services	YES Access to networks and network services must be managed to e.g. guarantee confidentiality of information, to manage access to staff on need-to-know and need-to-use basis, but make sure the information is available where required. This is a good practice.
A.9.2 User access management	
A. 9.2.1 User registration and de-registration	YES User registration and de-registration must be managed to e.g. guarantee confidentiality of information, to manage access to staff on need-to-know and need-to-use basis, but make sure the information is available where required. This is a good practice.
A. 9.2.2 User access provisioning	YES User access provisioning must be managed to e.g. guarantee confidentiality of information, to manage access to staff on need-to-know and need-to-use basis, but make sure the information is available where required. This is a good practice.
A. 9.2.3 Management of privileged access rights	YES Privileged access must be restricted and controlled to e.g. guarantee confidentiality of information, to manage access to staff on need-to-know and need-to-use basis, but make sure the information is available where required. Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems. Managing of privileged access is therefore a good practice.

A. 9.2.4 Management of secret authentication information of users	YES Allocation of secret authentication information must be controlled since this user specific information is directly linked to the information this user has access to, and should be on need-to-know and need-to-use basis. This is a good practice and reduces risks on information security breaches.
A. 9.2.5 Review of user access rights	YES To make sure user access needs to remain on need-to-know and need-to-use basis, and next to the user access management, an extra regular review of access controls reduces the risk of unallowed or blocked information access. This is a good practice and reduces risks on information security breaches.
A. 9.2.6 Removal or adjustment of access rights .	YES There is a formal procedure in place to make sure that in case staff leaves, access is revoked. This to reduce risk of leaking information.
A.9.3 User responsibilities	
A. 9.3.1 Use of secret authentication information of users	YES Staff signs an agreement, agreeing to the organization's practices on handling information, to reduce risk of faulty handling of information.
A.9.4 System and application access control	
A. 9.4.1 Information access restriction	YES It is a good practice to restrict user based information access on need-to-know and need-to-use basis.
A. 9.4.2 Secure log-on procedures	YES It is a good practice to have secure log-on procedures in place to give users access to information.
A. 9.4.3 Password management system	YES It is a good practice to have a password management system and related policy in place, including the necessary password requirements and login procedure, to reduce risk of unauthorized access to information.
A. 9.4.4 Use of privileged utility programs	YES In IT environments, it is a good practice to handle access to privileged utility accounts in a restricted and controlled way, to reduce risk of inappropriate information handling.
A. 9.4.5 Access control to program source code	YES CHILI publish develops source code, which is part of the IP of the company, and which must be protected. Hence access to this source code must be restricted. This is a good practice and reduces risk on leaking information.
A.10 Cryptography	
A.10.1 Cryptographic controls	
A.10.1.1 Policy on the use of cryptographic controls	YES A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use. Cryptographic controls are used in different locations throughout the organization. Managing these cryptographic controls is a good practice.

A.10.1.2 Key management	YES The management of cryptographic keys is essential to the effective use of cryptographic techniques and therefore a good practice to have a policy in place.
A.11 Physical and environmental security	
A.11.1 Secure areas	
A.11.1.1 Physical security perimeter	YES The logical and organizational split and availability of information might be linked to specific zones inside and outside the company. It is good practice to also have physical different security perimeters, which are linked to the confidentiality of the information located in the specific perimeters.
A.11.1.2 Physical entry controls	YES The logical and organizational split and availability of information might be linked to specific zones inside and outside the company. It is good practice to also have physical different security perimeters, which are linked to the confidentiality of the information located in the specific perimeters.
A.11.1.3 Securing offices, rooms and facilities	YES The logical and organizational split and availability of information might be linked to specific zones inside and outside the company. It is good practice to also have physical different security perimeters, which are linked to the confidentiality of the information located in the specific perimeters.
A.11.1.4 Protecting against external and environmental threats	YES It is good practice to assess the external and environmental threats to the locations where information is handled, assess the risk, and manage it.
A.11.1.5 Working in secure areas	YES The logical and organizational split and availability of information might be linked to specific zones inside and outside the company. It is good practice to also have physical different security perimeters, which are linked to the confidentiality of the information located in the specific perimeters.
A.11.1.6 Delivery and loading areas	YES It is good practice to make clear agreements on how packages, delivered to the company address, are handled. This to reduce risks of unauthorized access within specific perimeters and related information for unauthorized visitors.
A.11.2 Equipment	
A.11.2.1 Equipment siting and protection	YES It is good practice to protect the equipment where information is managed on to reduce risks from several threats and opportunities for unauthorized access.
A.11.2.2 Supporting utilities	YES It is good practice to support utilities against power failures and other disruptions to prevent undesired loss of information. CHILI publish has a server room for which this is applicable.

A.11.2.3 Cabling security	YES It is good practice to manage cables carrying data or supporting information services to prevent interception, interference or damage. This is applicable to CHILI publish.
A.11.2.4 Equipment maintenance	YES It is a good practice to have a maintenance policy in place for continuous availability and integrity of information.
A.11.2.5 Removal of assets	YES As part of asset management, to control access, and to prevent leaking of information on assets, it is good practice to have this control in place, and the formal agreement of the staff handling the information.
A.11.2.6 Security of equipment and assets off-premises	YES In times of remote working it is good practice to have a formally trained policy in place which is formally agreed upon by the staff, this to reduce the risk of leaking information.
A.11.2.7 Secure disposal or re-use of equipment	YES To prevent unauthorized access to information which is on need-to-know and need-to-use basis, a formal policy describes how equipment is either securely disposed or re-used. This is a good practice and reduces risk on faulty information sharing.
A.11.2.8 Unattended user equipment	YES To prevent unauthorized access to information, users are trained, and agree upon a way of working which ensures unattended equipment has appropriate protection. This is a good practice and reduces the risk on information breaches.
A.11.2.9 Clear desk and clear screen policy	YES To prevent unauthorized access to information, users are trained and formally agree upon the clear desk and clear screen policy. This is a good practice and reduces the risk on information breaches.
A.12 Operations security	
A.12.1 Operational procedures and responsibilities	
A.12.1.1 Documented operating procedures	YES Formally approved standard operating procedures reduce the risk of faulty information handling during operations.
A.12.1.2 Change management	YES Changes of systems can have impact on the CIA triad of information. A formal process to manage changes reduces risk of a negative impact of changes on information security handling.
A.12.1.3 Capacity management	YES Capacity management ensures availability of information by ensuring sufficient capacity.
A.12.1.4 Separation of development, testing and operational environments	YES Segregation of development, testing and operational environments reduces the risk for customers to have a environment in place where information security gaps are present.
A.12.2 Protection from malware	
A.12.2.1 Controls against malware	YES It is crystal clear that the control of malware reduces risks in confidentiality, availability and integrity of company and customer data. One of the best practices is also to give formal security awareness training where this topic is emphasized.
A.12.3 Backup	
A.12.3.1 Information backup	YES Secure back-ups, related procedure and testing these procedure is a way to mitigate risk of data loss in case of an event resulting in data loss on active systems.

A.12.4 Logging and monitoring	
A.12.4.1 Event logging	YES Event logging and review of logs is a means to trace-back anomalies, execute root cause and post-mortem analysis, helping to prevent information security breaches or act on them in case an event occurred..
A.12.4.2 Protection of log information	YES The integrity of logged events is a condition for the logged events to have value during the trace-back anomalies, execute root cause and post-mortem analysis, disciplinary cases and helping to prevent information security breaches or act on them in case an event occurred.
A.12.4.3 Administrator and operator logs	YES privileged users might be able to manipulate logs of other information security systems. As preventive action, and for root cause and post-mortem analysis and disciplinary cases, access for system administrators and operators are logged and regularly reviewed.
A.12.4.4 Clock synchronization	YES The correct setting of computer and system clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. This is a good practice.
A.12.5 Control of operational software	
A.12.5.1 Installation of software on operational systems	YES Faulty risk handling is prevented by having controlled standard operational procedures in place, reducing risks when installing new software.
A.12.6 Technical vulnerability management	
A.12.6.1 Management of technical vulnerabilities	YES To prevent exploits of vulnerabilities that impact information of security, the organization must remain knowledgeable about actual and future vulnerabilities to handle related information security risks in a timely fashion.
A.12.6.2 Restrictions on software installation	YES To reduce risks on information security breaches via software installed by users, rules about the installation of software and related risk handling are in scope of this ISMS.
A.12.7 Information systems audit considerations	
A.12.7.1 Information system audit controls	YES To reduce and avoid impact on operational information systems, audit requirements and activities are planned and agreed upon.
A.13 Communications security	
A.13.1 Network security management	
A.13.1.1 Network controls	YES To protect information sent over networks and prevent information breaches, the networks are managed and controlled to protect the transported information.
A.13.1.2 Security of network services	YES To reduce the risk of non-availability of information where required.
A.13.1.3 Segregation in networks	YES Where appropriate and practically possible, groups of information services, users and information systems are seggregated on networks, to reduce limit the impact when a security event takes place.

A.13.2 Information transfer	
A.13.2.1 Information transfer policies and procedures	YES Since company internal information or more strict classified information is transmitted via communication facilities, the mentioned procedures and controls must be in place to reduce the risk of information security breaches.
A.13.2.2 Agreements on information transfer	YES Since company internal information or more strict classified information is transmitted via communication facilities, the mentioned procedures and controls must be in place, also in the communication between the company and external parties, to reduce the risk of information security breaches.
A.13.2.3 Electronic messaging	YES Since company internal information or more strict classified information is transmitted via electronic messaging, the mentioned procedures and controls must be in place to prevent information security breaches.
A.13.2.4 Confidentiality or non-disclosure agreements	YES It is good practice, and for the sake of good information security to have this control in place.
A.14 System acquisition, development and maintenance	
A.14.1 Security requirements of information systems	
A.14.1.1 Security requirements of information systems	YES Used information systems must be qualified to protect the information used and handled by those tools, and to reduce risk of information breaches.
A.14.1.2 Securing application services on public networks	YES Information passing over public networks is protected to reduce risk of interception and abuse of information.
A.14.1.3 Protecting application services transactions	YES Information passing over public networks is protected to reduce risk of interception and abuse of information.
A.14.2 Security in development and support processes	
A.14.2.1 Secure development policy	YES To secure information handled by internally developed application, rules for development with attention to information security, are in place. This is a good practice and reduces the risk of developing vulnerable software and systems.
A.14.2.2 System change control procedures	YES To reduce risk of information breach, changes to the systems in the development lifecycle are formally managed.
A.14.2.3 Technical review of applications after operating platform changes	YES To reduce risk of information breach, changes to the systems in the development lifecycle are formally tested.
A.14.2.4 Restrictions on changes to software packages	YES To reduce the possibility of uncontrolled and unknown information security risks.
A.14.2.5 Secure system engineering principles	YES To secure information handled by internally developed application, and to reduce related information security breaches, rules for development with attention to information security, are in place.

A.14.2.6 Secure development environment	YES Development environments are appropriately protected, protecting company owned and hosted information, reducing the risk on information security breaches.
A.14.2.7 Outsourced development	YES To secure information handled by internally developed application, rules for development with attention to information security, are in place, also for outsourced development. This to reduce the risk on developing vulnerable software and/or systems.
A.14.2.8 System security testing	YES To reduce risk of information breach, changes to the systems in the development lifecycle are formally tested, including the security functionality.
A.14.2.9 System acceptance testing	YES To reduce risk of information breach, changes to the systems in the development lifecycle are formally tested.
A.14.3 Test data	
A.14.3.1 Protection of test data	YES Test data is carefully protected and controlled, to ensure fluent testing of a.o. the information security related functionality of the product. Test data is also part of the IP, and protection of the test data reduces the risk of loss of this IP.
A.15 Supplier relationships	
A.15.1 Information security in supplier relationships	
A.15.1.1 Information security policy for supplier relationships	YES To make sure information is handled securely by suppliers, and reduce the risk of information security breaches, agreements with suppliers on secure handling of information security must be handled depending on the access to the organization's assets.
A.15.1.2 Addressing security within supplier agreements	YES To make sure information is handled securely by suppliers, and reduce the risk of information security breaches, agreements with suppliers on secure handling of information security must be handled depending on the access to the organization's assets.
A.15.1.3 Information and communication technology supply chain	YES To make sure information is handled securely by suppliers, and reduce the risk of information security breaches, agreements with suppliers on secure handling of information security must be handled depending on the access to the organization's assets.
A.15.2 Supplier service delivery management	
A.15.2.1 Monitoring and review of supplier services	YES To reduce risk in faulty handling of information by a supplier, suppliers are monitored and regularly reviewed.
A.15.2.2 Managing changes to supplier services	YES When services by suppliers change, the scope of the information accessed by the supplier may change, hence the related risk may change. In that case, also the related risk must be managed.
A.16 Information security incident management	
A.16.1.1 Responsibilities and procedures	YES To handle information security incidents effective and efficient, a formalized procedure, including management responsibilities is in place. This is a good practice.
A.16.1.2 Reporting information security events	YES To handle information security incidents effective and efficient, a formalized procedure, including management responsibilities is in place. This includes communication through appropriate management. This is a good practice.

A.16.1.3 Reporting information security weaknesses	YES All staff is regularly trained to report information security weaknesses to be able to respond effectively and efficiently. This is a good practice.
A.16.1.4 Assessment of and decision on information security events	YES To have an inclusive effective and efficient response, all information security events are logged, and classified. This is a good practice and helps to prevent other future information security events.
A.16.1.5 Response to information security incidents	YES There is a formal procedure in place explaining on how to handle information security events and incidents. This is a good practice and enables the organizaztion to learn an prevent other future information security events.
A.16.1.6 Learning from information security incidents	YES For continuous improvement purposes, and detect if related information security incidents could occur, post-mortem analysis is done on information security incidents. This reduces the risk of future information security events.
A.16.1.7 Collection of evidence	YES Forensic gathering is part of the information security handling process. This reduces the risk of future information security events and enables the organizaztion to take appropriate actions. This is a good practice.
A.17.1.1 Planning information security continuity	YES To insure continuity of information security management during adverse situations, a formallized trained and tested policy is in place. This is a good practice.
A.17.1.2 Implementing information security continuity	YES To make sure an adverse situation is handled well, and continuous improvement purposes, formal processes are in place to warrant the required level of continuity for information security during such situations. This is a good practice.
A.17.1.3 Verify, review and evaluate information security continuity	YES To make sure an adverse situation is handled well, a formal information continuity exercise is regularly held, of which the outputs lead to verification, review and evaluation of the existing controls in place, and for continuous improvement purposes. This is a good practice.
A.17.2 Redundancies	
A.17.2.1 Availability of information processing facilities	YES To ensure availability of information, sufficient redundancy in information facilities must be provided. This reduces the risk of information being unavailable when required.
A.18 Compliance	
A.18.1 Compliance with legal and contractual requirement	
A.18.1.1 Identification of applicable legislation and contractual requirements	YES To remain in line with contractual, legal and regulatory obligations, the company must remain up-to-date and manage the applicable contractual, legal and regulatory obligations. This is a good practice.
A.18.1.2 Intellectual property rights	YES To remain in line with contractual, legal and regulatory obligations, and to keep IP as valuable asset in the company, IP rights and usage of proprietary software products are regulated. This is a good practice.

A.18.1.3 Protection of records	YES Records must be protected to be in line with needs and expectations of interested parties of the CHILI publish information security management system. This is a good practice, and required for the availability and integrity of the related records.
A.18.1.4 Privacy and protection of personally identifiable information	YES Relevant legislation and regulations related to PII must be followed, to protect confidentiality, integrity and availability of personal identifiable information. This is an obligation required by law.
A.18.1.5 Regulation of cryptographic controls	YES Relevant legislation, regulations and contractual obligations related to cryptographic controls must be followed, to reduce risks on not following legislations, regulations and contractual obligations and protect information as required. This is an obligation by law.
A.18.2 Information security reviews	
A.18.2.1 Independent review of information security	YES To avoid conflict of interested and obtain the ISO27001 certificate, internal and external audits are executed by parties not having responsibility on building and maintaining the ISMS. To reduce risks in unwanted interpretations and implementations of the standard.
A.18.2.2 Compliance with security policies and standards	YES To make sure the scope of the current ISMS keeps being up-to-date with the ever changing context of the world we live in, components of the ISMS must be reviewed regularly , to reduce information security risks.
A.18.2.3 Technical compliance review	YES Security demands and hacking technology evolves and security policies and standards are evolving. Information systems must be regularly reviewed for compliance with these evolutions to reduce risks and events.

– END OF DOCUMENT --