DELL Technologies

Global ISO27001 - SoA

Dell Technologies Security & Resiliency Organization • Version 4.1 • Last Updated 02-03-2025

Statement of Applicability

ISO/IEC 27001:2022

Categories (4)	Controls Ref (93)	Controls Tiltle	Requirement Title	Purpose
5. Organizational Controls				
	5.1	Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur	To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.
	5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.	To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization.
	5.3	Separation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated	To reduce the risk of fraud, error and bypassing of information security controls.
	5.4	Management responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.

	5.5	Contact with authorities	The organization should establish and maintain contact with relevant authorities.	To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.
	5.6	Contact with special interest groups	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	To ensure appropriate flow of information takes place with respect to information security
	5.7	Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence.	To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.
	5.8	Information security in project management	Information security should be integrated into project management.	To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle
	5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained	To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.
	5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	To ensure information and other associated assets are appropriately protected, used and handled.
	5.11	Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment,	To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement.
	5.12	Classification of information	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party	To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.
	5.13	Labelling of information	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the	To facilitate the communication of classification of information and support automation of information processing and management.

	5.14	Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties	To maintain the security of information transferred within an organization and with any external interested party.
	5.15	Access control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements	To ensure authorized access and to prevent unauthorized access to information and other associated assets.
	5.16	Identity management	The full life cycle of identities should be managed	To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights
	5.17	Authentication information	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	To ensure proper entity authentication and prevent failures of authentication processes.
	5.18	Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	To ensure access to information and other associated assets is defined and authorized according to the business requirements.

	5.19	Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	To maintain an agreed level of information security in supplier relationships.
	5.20	Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	To maintain an agreed level of information security in supplier relationships.
	5.21	Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain	To maintain an agreed level of information security in supplier relationships.
	5.22	Monitoring, review and change management of supplier services	The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery	To maintain an agreed level of information security and service delivery in line with supplier agreements.
	5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements	To specify and manage information security for the use of cloud services
	5.24	Information security incident management planning and preparation	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events.
	5.25	Assessment and decision on information security events	The organization should assess information security events and decide if they are to be categorized as information security incidents.	To ensure effective categorization and prioritization of information security events.
	5.26	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	To ensure efficient and effective response to information security incidents
	5.27	Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	To reduce the likelihood or consequences of future incidents

	5.28	Collection of evidence	The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions.
	5.29	Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	To protect information and other associated assets during disruption.
	5.30	ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	To ensure the availability of the organization's information and other associated assets during disruption.
	5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.	To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security
	5.32	Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights.	To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.
	5.33	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records.

	5.34	Privacy and protection of PII	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	To ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII.
	5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.
	5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards.
	5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	To ensure the correct and secure operation of information processing facilities.
6. People Controls				
	6.1	Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	To ensure all personnel are eligible and suitable for the roles for which they are considered and remaineligible and suitable during their employment.
	6.2	Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	To ensure personnel understand their information security responsibilities for the roles for which they are considered.

	6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.
	6.4	Disciplinary process	A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.
	6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	To protect the organization’s interests as part of the process of changing or terminating employment or contracts.
	6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	To maintain confidentiality of information accessible by personnel or external parties.
	6.7	Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises.	To ensure the security of information when personnel are working remotely.
	6.8	Information security event reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	To support timely, consistent and effective reporting of information security events that can be identified by personnel.
7. Physical Controls				
	7.1	Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	To prevent unauthorized physical access, damage and interference to the organization’s information and other associated assets.
	7.2	Physical entry	Secure areas should be protected by appropriate entry controls and access points.	To ensure only authorized physical access to the organization’s information and other associated assets occurs.
	7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented.	To prevent unauthorized physical access, damage and interference to the organization’s information and other associated assets in offices, rooms and facilities.

	7.4	Physical security monitoring	Premises should be continuously monitored for unauthorized physical access	To detect and deter unauthorized physical access
	7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional	To prevent or reduce the consequences of events originating from physical and environmental threats.
	7.6	Working in secure areas	Security measures for working in secure areas should be designed and implemented.	To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.
	7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.
	7.8	Equipment siting and protection	Equipment should be sited securely and protected.	To reduce the risks from physical and environmental threats, and from unauthorized access and damage.
	7.9	Security of assets off-premises	Off-site assets should be protected.	To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.
	7.10	Storage media	Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	To ensure only authorized disclosure, modification, removal or destruction of information on storage media.
	7.11	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.
	7.12	Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.
	7.13	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance.
	7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	To prevent leakage of information from equipment to be disposed or re-used.

8. Technological Controls				
	8.1	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	To protect information against the risks introduced by using user endpoint devices.
	8.2	Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.	To ensure only authorized users, software components and services are provided with privileged access rights.
	8.3	Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	To ensure only authorized access and to prevent unauthorized access to information and other associated assets.
	8.4	Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed.	To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.
	8.5	Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.
	8.6	Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	To ensure the required capacity of information processing facilities, human resources, offices and other facilities.
	8.7	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.	To ensure information and other associated assets are protected against malware.
	8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	To prevent exploitation of technical vulnerabilities.
	8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed	To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes
	8.10	Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion
	8.11	Data masking	Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.

	8.12	Data leakage prevention	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.
	8.13	Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	To enable recovery from loss of data or systems.
	8.14	Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	To ensure the continuous operation of information processing facilities.
	8.15	Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations.
	8.16	Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	To detect anomalous behaviour and potential information security incidents
	8.17	Clock synchronization	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents.
	8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	To ensure the use of utility programs does not harm system and application controls for information security.
	8.19	Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.
	8.20	Networks security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	To protect information in networks and its supporting information processing facilities from compromise via the network.
	8.21	Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	To ensure security in the use of network services.
	8.22	Segregation of networks	Groups of information services, users and information systems should be segregated in the organization’s networks.	To split the network in security boundaries and to control traffic between them based on business
	8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	To protect systems from being compromised by malware and to prevent access to unauthorized web resources
			Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or

	8.24	Use of cryptography		integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.
	8.25	Secure development life cycle	Rules for the secure development of software and systems should be established and applied.	To ensure information security is designed and implemented within the secure development life cycle of software and systems.
	8.26	Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	To ensure all information security requirements are identified and addressed when developing or acquiring applications.
	8.27	Secure system architecture and engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	To ensure information systems are securely designed, implemented and operated within the development life cycle.
	8.28	Secure coding	Secure coding principles should be applied to software development.	To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.
	8.29	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	To validate if information security requirements are met when applications or code are deployed to the production environment.
	8.30	Outsourced development	NA	NA
	8.31	Separation of development, test and production environments	Development, testing and production environments should be separated and secured.	To protect the production environment and data from compromise by development and test activities.
	8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	To preserve information security when executing changes.
	8.33	Test information	Test information should be appropriately selected, protected and managed.	To ensure relevance of testing and protection of operational information used for testing.
	8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	To minimize the impact of audit and other assurance activities on operational systems and business processes.