Telstra Statement of Applicability – ISO/IEC 27001:2022 Annex A Controls

Telstra Group Limited holds certificate number IS 764456 and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2022 for the following scope in accordance with this statement of applicability:

Telstra's information security management system encompassing people, process, technology, and facilities, supporting the development, management, delivery and assurance of products and services to enterprise, business and government customers of Telstra Limited (including Telstra Purple), Telstra Corporation Limited (trading as Telstra InfraCo) and Telstra International entities in core countries.

Ref#	Control Title	Control Description	Justification for Inclusion	Applicable	Justification for exclusion
A.5 Organisational Controls					
A.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 enable compliance to information security requirements.	Yes	N/A
A.5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organisation needs	To enable compliance to information security requirements.	Yes	N/A
A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated	To enable compliance to information security requirements.	Yes	N/A
A.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 organisation	To ensure that all employees and contractors comply with company information security policies.	Yes	N/A
A.5.5	Contact with authorities	The organisation should establish and maintain contact with relevant authorities	To ensure compliance with legal and regulatory requirements and ensure appropriate visibility of external threats.	Yes	N/A
A.5.6	Contact with special interest groups	The organisation should establish and maintain contact with special interest groups or other specialist security forums and professional associations	To ensure compliance with legal and regulatory requirements and ensure appropriate visibility of external threats	Yes	N/A
A.5.7	Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence	To ensure compliance with legal and regulatory requirements and ensure appropriate visibility of external threats	Yes	N/A
A.5.8	Information security in project management	Information security should be integrated in project management	To reduce the risk of new/updated systems and services being introduced with security weaknesses	Yes	N/A

Ref#	Control Title	Control Description	Justification for Inclusion	Applicable	Justification for exclusion
A.5.9	Inventory of information and other associated assets	An inventory of information and other assets, including owners, should be developed and maintained	To ensure all assets are appropriately documented and securely managed in line with policies.	Yes	N/A
A.5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented	To ensure all assets are securely managed.	Yes	N/A
A.5.11	Return of assets	Personnel and other interested parties as appropriate should return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement	To ensure all assets are securely managed.	Yes	N/A
A.5.12	Classification of information	Information should be classified according to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements	To ensure that information is classified and handled securely.	Yes	N/A
A.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 organisation	To ensure that information is classified and handled securely.	Yes	N/A
A.5.14	Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organisation and between the organisation and other parties	To ensure that information is transferred securely within the organisation and between other parties. .	Yes	N/A
A.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	To ensure all access to information is managed	Yes	N/A
A.5.16	Identity management	The full lifecycle of identities should be managed	To ensure all access to information is managed	Yes	N/A
A.5.17	Authentication management	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 all access to information is managed	Yes	N/A

Ref#	Control Title	Control Description	Justification for Inclusion	Applicable	Justification for exclusion
A.5.18	Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on rules for access control	To ensure all access to information is managed	Yes	N/A
A.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 and services	To ensure the security of information shared with third parties	Yes	N/A
A.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 ensure the security of information shared with third parties	Yes	N/A
A.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 ensure the security of information shared with third parties	Yes	N/A
A.5.22	Monitoring, review and change management of supplier services	The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery	To ensure the security of information shared with third parties	Yes	N/A
A.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 organisation's information security requirements	To ensure the security of information shared with third parties	Yes	N/A
A.5.24	Information security incident management planning and preparation	The organisation should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities	To ensure that the impact of information security incidents is minimised	Yes	N/A
A.5.25	Assessment and decision on information security events	The organisation should assess information security events and decide if they are to be categorised as information security incidents	To ensure that the impact of information security incidents is minimised	Yes	N/A
A.5.26	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures	To ensure that the impact of information security incidents is minimised	Yes	N/A
A.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 risk of information security incidents being repeated	Yes	N/A

Ref#	Control Title	Control Description	Justification for Inclusion	Applicable	Justification for exclusion
A.5.28	Collection of evidence	The organisation should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events	To ensure that information security incident evidence is collected in a compliant manner.	Yes	N/A
A.5.29	Information security during disruption	The organisation should plan how to maintain information security at an appropriate level during disruption	To ensure the security of information (company, employee and customer) during a disruption	Yes	N/A
A.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 security of information (company, employee and customer) during a disruption	Yes	N/A
A.5.31	Identification of legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meet these requirements should be identified, documented and kept up to date	To reduce the risk of legal or regulatory action	Yes	N/A
A.5.32	Intellectual property rights	The organisation should implement appropriate procedures to protect intellectual property rights	To ensure software licencing requirements are complied with.	Yes	N/A
A.5.33	Protection of records	Records should be protected from loss, destruction, falsification, unauthorised access and unauthorised release	To reduce the risk of record loss or compromise	Yes	N/A
A.5.34	Privacy and protection of PII	The organisation 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 the risk of compromise of personally identifiable information is minimised.	Yes	N/A
A.5.35	Independent review of information security	The organisation'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 policy compliance and control objectives are being met and documented processes and procedures are being followed.	Yes	N/A
A.5.36	Compliance with policies and standards for information security	Compliance with the organisation's information security policy, topic-specific policies, rules and standards should be reviewed regularly	To ensure policy compliance and control objectives are being met and documented processes and procedures are being followed.	Yes	N/A

Ref#	Control Title	Control Description	Justification for Inclusion	Applicable	Justification for exclusion
A.5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them	To reduce the risk of information security incidents	Yes	N/A
A.6 People Controls					
A.6.1	Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organisation 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 staff are recruited in line with legal and regulatory requirements. To reduce the likelihood of employee-based security incidents	Yes	N/A
A.6.2	Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organisation's responsibilities for information security.	To reduce the likelihood of employee-based security incidents.	Yes	N/A
A.6.3	Information security awareness, education and training	Personnel of the organisation and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, top-specific policies and procedures, as relevant for their job function.	To ensure all staff understand the importance of information security and their role to ensure it.	Yes	N/A
A.6.4	Disciplinary process	A disciplinary process should be formalised and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation	To ensure appropriate processes are in place to deal with information security breaches by internal staff	Yes	N/A
A.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 ensure business information security requirements continue to be met by staff and contractors after their employment has terminated or their role has changed.	Yes	N/A
A.6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties	To ensure the security of information shared with personnel and other relevant interested parties.	Yes	N/A

Ref#	Control Title	Control Description	Justification for Inclusion	Applicable	Justification for exclusion
A.6.7	Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.	To ensure security of information while people are working away from the organisation's premises	Yes	N/A
A.6.8	Information security event reporting	The organisation should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner	To ensure that the impact of information security incidents is minimised	Yes	N/A
A.7 Physical Controls					
A.7.1	Physical security perimeter	Security perimeters should be defined and used to protect areas that contain information and other associated assets	To reduce the risk of unauthorised access to sites	Yes	N/A
A.7.2	Physical entry controls	Secure areas should be protected by appropriate entry controls and access points	To reduce the risk of unauthorised access to secure areas	Yes	N/A
A.7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented	To reduce the risk of unauthorised access to offices, rooms, and facilities	Yes	N/A
A.7.4	Physical security monitoring	Premises should be continuously monitored for unauthorised physical access	To reduce the risk of unauthorised access to sites	Yes	N/A
A.7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented	To ensure the risk of external and environmental risks is minimised	Yes	N/A
A.7.6	Working in secure areas	Security measures for working in secure areas should be designed and implemented	To minimise the risk of secure areas being compromised	Yes	N/A
A.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 designed and appropriately enforced	To ensure the security of company, employee, and customer information.	Yes	N/A
A.7.8	Equipment siting and protection	Equipment should be sited securely and protected	To reduce the risk of external and environmental threats to equipment	Yes	N/A
A.7.9	Security of assets off-premises	Off-site assets should be protected	To reduce the risk of asset security being compromised	Yes	N/A

Ref#	Control Title	Control Description	Justification for Inclusion	Applicable	Justification for exclusion
A.7.10	Storage media	Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements	To reduce the risk of asset security being compromised	Yes	N/A
A.7.11	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities	To reduce the risk of system or service availability or integrity incidents	Yes	N/A
A.7.12	Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage	To reduce the risk of system or service security incidents due to cabling security breaches	Yes	N/A
A.7.13	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information	To reduce the risk of system or service availability or integrity incidents	Yes	N/A
A.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 reduce the risk of asset security being compromised	Yes	N/A
A.8 Technological Controls					
A.8.1	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected	To reduce the risk of the use of endpoint devices negatively impacting the security of information	Yes	N/A
A.8.2	Privileged access rights	The allocation and use of privileged access rights should be restricted and managed	To ensure that privileged access to systems and services is managed	Yes	N/A
A.8.3	Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy or access control	To ensure that access to systems and services is managed securely	Yes	N/A
A.8.4	Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed	To ensure that program source code is managed securely	Yes	N/A
A.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 that access authentication information is securely managed.	Yes	N/A
A.8.6	Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements	To reduce the risk of critical systems being unavailable	Yes	N/A

Ref#	Control Title	Control Description	Justification for Inclusion	Applicable	Justification for exclusion
A.8.7	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness	To reduce the risk of malware impacting systems and services	Yes	N/A
A.8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organisation's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken	To reduce the risk of systems and services being impacted by security incidents	Yes	N/A
A.8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed	To reduce the risk of systems and services being impacted by security incidents	Yes	N/A
A.8.10	Information deletion	Information stored in information systems, devices or in other storage media should be deleted when no longer required	To reduce the risk of asset security being compromised	Yes	N/A
A.8.11	Data masking	Data masking should be used in accordance with the organisation's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration	To reduce the risk of asset security being compromised	Yes	N/A
A.8.12	Data leakage prevention	Data leakage prevention should be applied to systems, networks and any other devices that process, store or transmit sensitive information	To reduce the risk of asset security being compromised	Yes	N/A
A.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 minimise the impact of system or service availability or integrity incidents	Yes	N/A
A.8.14	Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements	To reduce the risk of non-availability of systems and services	Yes	N/A
A.8.15	Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed	To provide evidence for information security incident investigation. To assist in the prevention of information security incidents.	Yes	N/A

Ref#	Control Title	Control Description	Justification for Inclusion	Applicable	Justification for exclusion
A.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 provide evidence for information security incident investigation. To assist in the prevention of information security incidents.	Yes	N/A
A.8.17	Clock synchronisation	The clocks of information processing systems used by the organisation should be synchronised to approved time sources	To provide evidence for information security incident investigation.	Yes	N/A
A.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 that the capability to override system and application controls is managed securely	Yes	N/A
A.8.19	Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems	To reduce the risk of information security incidents	Yes	N/A
A.8.20	Network controls	Networks and network devices should be secured, managed and controlled to protect information in systems and applications	To reduce the risk of network security breaches	Yes	N/A
A.8.21	Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored	To reduce the risk of network security breaches	Yes	N/A
A.8.22	Segregation in networks	Groups of information services, users and information systems should be segregated in the organisation's networks	To reduce the risk of network security breaches	Yes	N/A
A.8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content	To reduce the risk of information security incidents	Yes	N/A
A.8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented	To ensure that cryptography is applied appropriately	Yes	N/A
A.8.25	Secure development lifecycle	Rules for the secure development of software and systems should be established and applied	To reduce the risk of new/updated systems having security weaknesses	Yes	N/A
A.8.26	Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications	To reduce the risk of new/updated systems having security weaknesses	Yes	N/A
A.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 reduce the risk of new/updated systems having security weaknesses	Yes	N/A

Ref#	Control Title	Control Description	Justification for Inclusion	Applicable	Justification for exclusion
A.8.28	Secure coding	Secure coding principles should be applied to software development	To reduce the risk of new/updated systems having security weaknesses	Yes	N/A
A.8.29	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle	To reduce the risk of new/updated systems having security weaknesses	Yes	N/A
A.8.30	Outsourced development	The organisation should direct, monitor and review the activities related to outsourced system development	To reduce the risk of new/updated systems having security weaknesses	Yes	N/A
A.8.31	Separation of development, test and production environments	Development, testing and production environments should be separated and secured	To reduce the risk to the operational environment from development and testing activities	Yes	N/A
A.8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures	To reduce the risk of information security incidents	Yes	N/A
A.8.33	Test information	Test information should be appropriately selected, protected and managed	To reduce the risk of new/updated systems having security weaknesses	Yes	N/A
A.8.34	Protection of information systems during audit and testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management	To ensure that business processes are not disrupted by system audits.	Yes	N/A