SESLHD POLICY COVER SHEET

NAME OF DOCUMENT	ICT Vendor Compliance
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/318
DATE OF PUBLICATION	February 2025
RISK RATING	Low
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standards: Standard 1 – Clinical Governance ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems.
REVIEW DATE	February 2030
FORMER REFERENCE(S)	N/A
EXECUTIVE SPONSOR	Director, Digital Health, SESLHD
AUTHOR	Shane Feeney
POSITION RESPONSIBLE FOR THE DOCUMENT	Head of ICT Risk & Cyber Security Digital Health Directorate Awais.Vaseer@health.nsw.gov.au
FUNCTIONAL GROUP(S)	Information Management and Data
KEY TERMS	Information security, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance, Vendor Management, contract.
SUMMARY	This document provides the overarching policy under which information systems should have security and system patches and service packs applied in the South Eastern Sydney Local Health District.

1. POLICY STATEMENT

Many departments within the LHD engage vendors directly to supply a solution or a service which interacts with the LHD staff and the digital infrastructure. To ensure that appropriate information security measures are taken and that both the department (client) and the vendor are in the best possible position regarding information security, this policy outlines the principles that need to be applied prior to the commencement of the service or implementation of the solution.

The best position for the department and the vendor is to apply this policy at the commencement of the engagement well before a services or solution is developed.

The following principles are to be applied to vendors' (Service Providers) who supply solutions and/or services to ensure that the solutions and services meet the minimum information security requirements.

2. AIMS

The purpose of the ICT Vendor Management policy is to describe the principles used to manage and protect assets that are managed by vendors from deliberate or inadvertent unauthorised acquisition, damage, disclosure, manipulation, modification, loss, or use.

The policy ensures that system performance and relating Service Levels Agreements (SLAs), Key Performance Indicators (KPIs) meet minimum information security requirements.

Appendix A: outlines who is Accountable, Responsible, Consulted and Informed in relation to each of the ISO/IEC 27001:2013 controls.

3. TARGET AUDIENCE

This Policy applies to all parties including permanent, temporary and casual staff of South Eastern Sydney Local Health District, staff seconded from other organisations and contingent workers including labour hire, service providers, professional services contractors and consultants, who are managing digital assets that have vendors supporting the digital asset and for vendors/ Service providers who supply a digital service to the LHD.

4. VENDOR COMPLIANCE POLICY SCOPE

The scope of the ICT Vendor Compliance policy applies to all vendors that supply digital systems, servers, applications, cloud services, Platforms as a Service (PaaS), Applications as a Service (AaaS), Infrastructure as a Service (IaaS).

Departments within the LHD are to ensure that vendors meet the requirements prior to implementing the contracted service or solution.

4.1 Attachment to the SESLHD Infrastructure

Prior to attaching a vendor managed system to the SESLHD infrastructure, System Architectural and Information Security reviews must be conducted by engaging Digital Health by lodging a request via the eHealth State Wide Service Desk (SWSD). The outcome of which a reviews must be produced using the Digital Health Risk Framework for Digital Systems.

For “As a Service” services, the service must undergo System Architectural and Information Security reviews to ensure that the service meets;

- The Australian Federal Government information security and privacy legislation.
- The NSW Government information security and privacy legislation.
- SESLHD Information Security Policy and it’s supporting technical policies requirements; and
- Australian Signals Directorate (ASD) Essential Eight.

4.2 Service Principles

A key specific factor when engaging a vendor/ Service Provider is to determine the degree of co-management and contract monitoring operations prior to implementation. To be compliant to the NSW Cyber Security Policy, the compliance principles outlined in Appendix A, must be addressed either through the service contract or an addendum to the contract.

The key service principles are;

- Key performance indicators (KPIs) required to meet the business requirements must be documented prior to commencement of the contract.
- Service Level Agreements (SLAs) required to meet the business requirements must be documented.
- Service and security patch update regimes, implementation windows and lifecycle must follow LHD change management processes.
- Monthly Service performance reports of the system or service under management.
- Evidence (data) of SLAs, KPIs and performance levels being met must be auditable.
- A support and maintenance RACI (Responsible, Accountable, Consulted, and Informed) must be documented and given to the LHD vendor manager and Digital Health.
- Roles, responsibilities, and access in the RACI must be in alignment with the following;
    - Roles and responsibilities of staff supporting and managing the service must be defined.
    - Where duties and areas of responsibility conflict, they must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisations assets.

  - Appropriate contact with relevant authorities/ key departmental stakeholders must be maintained.
- Service provider's adherence to the NSW policy on data handling and classification policy. See Section 4.4 Service Provision and Privacy.
- Information security must be addressed in project management of the design, build, deployment, and handover to operations.
- Service providers must perform background checks for personal who have access to the supported systems and confirmation of the checks must be given to the LHD application owner and vendor manager.
- Service providers must ensure that their personnel who have access to the supported systems have been formally made aware of the LHD Information Security policies.
- Service providers must ensure that their personnel have been formally made aware of the continuance of the LHD Information Security policies after employment termination.
- Service providers must adhere to ISO/IEC 27001:2013 Control A.8.3 regarding media handling and disposal where applicable in relation to the supported system(s) and services.
- Service providers must ensure that ISO/IEC 27001 Control A.9.1 & A.9.2 regarding access control is enforced.
- Service providers password and account management practices must follow the SESLHD User Access Management Procedure, in particular;
  - Access reviews must be conducted at least every 12 months and non-active accounts must be suspended and end dated. Evidence of the account review must be provided to the application owner and vendor manager.
- Service providers and application owners must implement system and application access control as specified in ISO/IEC 27001 Control A.9.4.
  - Information access restriction: Access to information and application systems functions must be restricted in accordance with the access control policy.
  - Secure log-on procedures: Access control policy must be enforced, access to the systems and applications must be controlled by a secure logon procedure.
  - Password management system or utilise the LHD active directory (Stafflink) domain.
  - Password management be interactive and must ensure quality passwords.
  - Use of privileged utility programs that might be capable of overriding systems and application controls must be restricted and tightly controlled.
- Service providers and application owners must implement cryptography control as specified in ISO/IEC 27001 Control A.10.0 where applicable.
- Service providers must ensure that ISO/IEC 27001 Control A.12.2 Malware mitigation is applied and that the Anti-Virus is updated as virus

signatures are released.

- Service providers and application managers/owners must execute an Information Backup regime to protect against data loss. Ref: ISO/IEC 27001 Control A.12.3 Backup.
- Service providers must ensure that ISO/IEC 27001 Control A.12.4 logging and monitoring is applied as per the following;
    - Event logging (A.12.4.1): Event logs recording user activities, exceptions, faults, and information security events must be produced, kept, and regularly reviewed.
    - Protection of log information (A.12.4.2): Logging facilities and log information must be protected against tampering, unauthorised access and deletion.
    - Administrator and operator logs (A.12.4.3): System admin and system operator activities must be logged, and the logs protected and regularly reviewed.
    - Clock synchronisation (A.12.4.4): The clocks of all relevant information processing systems must be synchronised to a single reference time source.
- Service providers and application managers may utilise the monitoring systems that are deployed and managed by Digital Health.
- Prior to systems being connected to the LHD digital infrastructure, service providers must adhere to the LHD systems accreditation procedure and ensure that the systems patching (Operating System and application) is up to date and malware control is in place. Systems/ Services must be certified by the Digital Health prior to connection.
- Service providers must apply ISO/IEC 27001:2013 Control A.12.6 Technical vulnerability management to the systems and;
    - Information about technical vulnerabilities of information systems being used must be passed on to the application and vendor manager in a timely fashion, the LHD's exposure to such vulnerabilities are to be evaluated and appropriate measures taken to address the associated risk.
    - Users must not be able to install non-purpose (additional) software.
- Where service providers have installed a network, the network must be certified compliant to Digital Health standards and meets the LHD Network Security policy PD313. The vendor is to implement;
    - Network controls which must be managed and controlled to protect information in systems and applications.
    - Security mechanisms, service levels and management requirements of all networks service must be identified and included in network service agreements, whether these services are provided in-house or outsourced.
    - Groups of information services, users and information systems must be segregated on networks.
- Service providers must adhere to the NSW Government Data Handling policy ensure that ISO/IEC 27001 Control A.13.2 is applied to the service as per the following;

- Formal transfer policies, procedures and controls must be in place to protect the transfer of information through the use of all types of communication.
- Agreements must address the secure transfer of business information between the LHD and external parties and meet the LHD Data protection requirements.

4.3 Implicit Controls

Section 2.3 Service Principles calls out security principles that must be explicitly adhered to. There are several principles that are not explicitly called out as they are covered under the LHD Information Security policies and are designated in the Appendix A as "implicit" principles.

Department Managers and Specialist ICT should familiarise themselves with the LHD Information Security and associated policies.

A full assignment of Responsibility, Accountability, Consulted and Informed (RACI) actions are outlined in the Appendix A and reflect "Explicit" and "Implicit" principles.

4.4 Service Provision and Privacy

As part of the service, the Service providers must demonstrate that they will be complying with the privacy principles for corporate and patient data in line with the tenets of the NSW Government Privacy and Personal Information Protection Act 1998 (PPIP), the Health Records and Information Privacy Act 2002 (HRIP) and the Australian Federal Government Privacy Act 1988 in particular;

Service Provision and Privacy

- Appropriate technical and organisational measures must be taken to safeguard the security of the service and data handling where data is exported outside the LHD domain to other organisations.
- Patient data must not be exported for systems development and testing. Service providers must use their own self-generated data.
- For remediation of a system issue and patient data is required, authorisation must be sought from the department director for the use of the data for a fixed period and service provider's staff must adhere to both the NSW Government Privacy acts, PPIP & HRIP. The data must be deleted from the test system after the issue has been remedied.
- Vendors must implement a procedure for risk notification to the client of pending threats or newly identified vulnerabilities for their systems.
- An appropriate procedure in managing data breaches and notification of a breach as per the Australian Federal Government Mandatory Data breach notification scheme and the NSW Privacy and Personal Information Protection Act (Part 6A)
- The highest privacy settings must be the default configuration for a system.
- External facing systems and/or services must undergo a penetration test with identified issues resolved prior to commissioning.

Data

- That data segmentation and classification occurs in line with SESLHD Information Security policy.
- That securing of virtualised environments and classification occurs in line with Digital Health requirements and eHealth policies.
- The service provider/ vendor must indicate the purpose of the use of any data that has been collected or received as part of the course of supporting the system.
- Written authorisation must be obtained if the service provider is to use the data other than that for which it is intended.
- Data minimisation occurs is only to collect, obtain, derive, and process data to the extent necessary (need-to-know principle).
- Opt-out of data transmission option for data transfers and monitoring is available.
- Data ownership is always retained with the Local Health District and must not be subverted.
- All systems data is isolated from other vendor clients if in a mixed service environment.
- That data context is employed to affirm data source incontestability and authenticity where data is transferred externally.
- The systems/application owners must take steps to establish disaster recovery management and implement continuity controls which are assessed at regular intervals to ensure that they are valid and effective during adverse situation. The test is to be conducted at least annually.

Encryption

Appropriate Cryptography (Encryption) principles must be applied only if there is a requirement determined by a risk assessment.

- Encryption should be the default position and applied at all stages of handling data, including in communication (local and internet), storage of data at rest, storage of keys, identification, access, as well as a secure boot process.
- Data should be encrypted at the application layer using end-to-end security, cryptographic principles, and key management should be documented with the documents submitted to Digital Health for acceptance.

Compliance and Risk

- Service providers are accountable for meeting the Australian Federal and NSW state government's legislative and mandated requirements for privacy, handling of data, contractual and ethical compliance, as well as for any misuse of collected personal data. If the data is compromised, disclosed, inappropriately accessed or lost, the vendors must formally notify their client of the compromise and the impact as soon as possible.
- The service provider must conduct an assessment of the risk of data

being compromised, disclosed, inappropriately accessed, or lost. Likewise, an assessment of the consequences from regulatory, contractual, and ethical perspective should be conducted.

Risk assessment must be conducted using the NSW risk management methodology and AS/NZS ISO31000:2018.

- Service providers must have a Security Management Plan for the service provided.

Secure Design and Updates

- **Security by default:** The service provider should ensure that the most secure, proven, well understood and securely updateable settings are applied before starting operations and during the life time of the service.
- **Secure updates:** Trusted and transparent updates should only be provided by authorised parties and that the subscriber must be notified of the updates.
- **Implementation of Updates and Patches:** Application of Updates and Patches must be implemented using the LHD Change Management procedure. No patch or update is to be applied without prior approval.
- **Time to Patch:** Critical systems patches must be applied as soon as practicable after a risk assessment has been conducted and an Emergency Change Request approved. Non-critical patches must be tested and applied within an agreed time frame after the release of the patch. The agreed timeframes for patching are prescribed by the ACSC Essential Eight Maturity Model (refer to Patch Operating Systems and Patch Application mitigation strategies).Furthermore, the timeframes must correspond to the business criticality of service and the target Essential 8 maturity level (1,2 or 3)
- **High-level secure baseline:** A high-level secure baseline should be applied when safety is at stake or safety can be materially impacted.
- **Safe and secure interactions:** The Service provider must implement and validate safety principles, separately from security principles and provide documentation of the validation to the client.
- **Authentication of identities:** Only Digital Health approved authentication mechanism of identities are to be applied. Where possible, the system must use the eHealth Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) for account authentication.

Monitoring and Functions

- **Assurance:** The Service Provider must have a maintenance plan for the entire life cycle for the systems and the Service Provider must provide end of life guarantees for vulnerabilities notifications, updates, patches, and support.
- **Defined functions:** The Service provider must ensure that the systems are only able to perform documented functions, particular for the service.
- **Secure interface points:** The Service provider must document secure and non- secure interface points to reduce the risk of security breach.
- **Authentication of identities among themselves:** System

communications and authentication should use common technologies and applications.

4.5 Compliance Reporting and Monitoring

Systems/Services must where possible be monitored to ensure that the patches and firmware upgrades have been applied.

A system that cannot be actively monitored must have a scheduled frequency of the checks which is determined by the risk posture.

Security patching status must be reported to the SESLHD Information Security Governance Council (ISGC) bi-annually.

4.6 Fit for Purpose

The NSW consumer law covers systems and services provided by service providers (vendors). The Consumer Act states that services or systems supplied must be “Fit for Purpose”.

If a system is not providing the business outcomes as stated at the commencement of the service, then it is regarded as being Not Fit for Purpose and opens an avenue for recourse with the vendor.

This particularly applies to digital systems when the system is affected by malware that impedes its function. Remediation may require anti-virus (AV), systems security patches to be installed or an alternative approach to restoring integrity and availability.

Systems which have a clinical application that have been certified by the US FDA, European EMDA or Australia’s TGA or elsewhere and the certification applies to a specific build or combination of software or hardware, where adding AV or security patches may affect the certification in which case external information security measures must be implemented to provide integrity and availability.

It should be noted that the Fit for Purpose can only be applied if at the commencement of the service if the required outcomes were stated in sufficient detail such as having Functional and Non-Functional specifications stipulated.

5. SYSTEMS INFORMATION SECURITY DOCUMENTATION

To mitigate risk and ensure that the system/ service is set up correctly, the system/ service must be accompanied by information security documentation as described below. The documentation is required in the event of the system/service failing and needs to be rebuilt or it is hacked, and an investigation needs to occur to determine the source of the issue.

5.1 Security Documentation Purpose

To maintain the system securely, documents must be maintained in relation to the system’s information security so that it provides;

- Assurance that the device is or can be secured;
- How to secure the system;
- Allowing a risk assessment to be conducted in the changing threat environment to allow for mitigation actions to occur if required;

Service/solution providers must supply the relevant security documentation prior to the commencement of the service.

5.2 Security Document Contents

For each new and existing system, the security documents or contents relating to security must specify but not limited to;

- Administration defaults and how to change the defaults including passwords and access portals;
- Communications protocol ports that are open or closed and authentication information;
- Past patches list and bugs that were fixed;
- Current version and patch status;
- Forums and community groups where the client can go for information;
- Information Security best practice;
- Any Security standards the system complies with
- Critical processes that may require monitoring;

5.3 Default Security KPIs and metrics. Security Management Plan

All systems must have a Security Management plan accompanying the security information documentation that governs the integrity, privacy, security, and confidentiality of information, especially highly sensitive information, and the responsibilities of departments and individuals for such information.

The level of complexity and coverage is dependent upon the system criticality which will be determined through conducting a risk assessment.

5.4 Security Document Exemptions

Any exemptions to the ICT Vendor Compliance Policy must be approved by the Chief Information Officer (CIO) or SISO after undergoing a risk assessment. Written approval for exemption must be completed through a SESLHD Brief and must be recorded within the Document Management System (i.e., Content Manager) as per the SESLHD Records Management Standard.

6. DOCUMENTS

The associated documents that relate to Vendor systems assessment are located on the Digital Health intranet.

- External System Security Assessment Procedure
- Information Classification Procedure
- Information Transfer Procedure
- Password Management Procedure
- Risk Management Procedure

7. REFERENCE DOCUMENTS

The following documents are referenced in this policy:

Legislation, Policies and Guidelines

- Health Records and Information Privacy Act 2002 (NSW) (HRIP Act)
- Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)
- NSW Government Cyber Security Policy
- NSW Health Policy Directive PD2020_046 - Electronic Information Security
- NSW Government Information Classification Labelling and Handling Guidelines
- ACSC (ASD) Cloud Security Guidance
- Australian Signals Directorate (ASD) Essential Eight
- MICTA/ICTA Contracts (ICT Purchasing Framework)
- SESLHDPD/310 - Information Security

7.1 Standards

- ISO 27001:2013 Information technology - Security Techniques - Information security management systems
- ISO/IEC 27002:2013. Information Technology - Security Techniques - Code of Practice for Information Security Management
- ISO 31000 Risk management - Principles and guidelines
- IEC 62443 Security for operational technology - Automation and Control System

8. DEFINITIONS

AV: antivirus software is a type of utility used for scanning and removing viruses from your computer. While many types of antivirus (or "anti-virus") programs exist, their primary purpose is to protect computers from viruses and remove any viruses that are found.

ISO/IEC 27001:2013: ISO/IEC 27001 is an information security standard, part of the ISO/IEC 27000 family of standards

LDAP: the Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network. Directory services play a significant role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.

Malware: is any software intentionally designed to cause damage to a computer, server, client, or computer network. Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software.

Subscriber or Client: the Subscriber is the department of person who has purchased a service, application, or systems to deliver a business outcomes.

System(s): a system(s) can be either a standalone or combination of either hardware, software or end point machine that delivers a specific related service such as controlling a MRI machine and recording the images for review and forwarding.

Vendor or Service Provider: a vendor is a person or organisation that vends or sells contingent labour, digital services as a service. Specifically, a vendor can be an independent consultant, a consulting company, or staffing company.

Vendor Managed System: is a system that is;

- Operationally maintained by the vendor who supplied the machine/application or contracted via a third party.
- Perform a single service;
    - Either through connecting to a machine and to the network with custom controlling software, in which Machine-to-Machine-to-Human (M2M2H) communications is enabled, or
    - Supplying a service such as an application configured for the LHD's needs.
- Vendor managed systems produce an output or artefact and act on it or send it to other systems for further analysis or output.
- An application which collects and analyses this data for further consolidation and presentation,
- Has a Human machine interface (HMI) for the manipulation and packaging of the data, typically a terminal or Windows interface.
- The ability to transmit data either by email or file transfer,
- Has the ability to send diagnostic data to the vendor and/or allow the vendor to login remotely for updates and diagnosis.

9. VERSION AND APPROVAL HISTORY

Date	Version	Author	Approval
March 2019	DRAFT	Initial draft Shane Feeney, Program Manager ICT Security & Strategy	Flora Karanfilovski Director, Health ICT
May 2019	DRAFT	Draft for comment period. No feedback received. Final version approved by Executive Sponsor. Formatted by Executive Services prior to tabling at June 2019 Executive Council meeting.	Flora Karanfilovski Director, Health ICT
June 2019	1	Endorsed at June 2019 Executive Council meeting.	
6 February 2025	1.1	Minor review by Awais Vaseer, Head of ICT Risk & Cyber Security. Updated reference documents and Vendor Acknowledgement Sheet included.	Clarence Yap Director, Digital Health

ICT Vendor Acknowledgement

10. Vendor Sign Off

As representative of ,I hereby acknowledge the receipt of SESLHD ICT Vendor Compliance policy. I understand and agree to comply with all the terms, conditions and controls outlined in this policy. I understand that adherence to this policy is a mandatory requirement for procurement of ICT solutions and services.

ICT Vendor Representative name
ICT Vendor Representative position
Signature
Date

APPENDIX A

	Compliance Assessment Area				RACI		
Clause	**Section**	**Objective/ Control**	**Definitions**	**Implicit/ Explicit**	**Owner**	**Vendor**	**Health ICT**
A.6	**Organisation of Information Security**						
A.6.1	**Internal Organisation**	To establish a management framework to initiate & control the implementation & operation of information security within the organisation					
A.6.1.1	Information Security roles and responsibilities	All information security responsibilities MUST be defined and allocated.	The responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly identified, defined, communicated to the relevant parties and stakeholders.	Explicit	AR	R	C
A.6.1.2	Segregation of Duties	Conflicting duties & areas of responsibility MUST be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	Duties and areas of responsibility must be documented and separated in order to reduce opportunities for unauthorised modification or misuse of information or services.	Explicit	AR	R	C
A.6.1.3	Contact with Authorities	Appropriate contact with relevant authorities MUST be maintained.	A procedure/process documenting when and by whom contact with relevant authorities must be available when a breach occurs.	Explicit	AR	R	C
			There must be a process for routine contact and intelligence sharing with stakeholders and other supporting groups.		AR	R	C
A.6.1.4	Contact with special Interest groups	Appropriate contact with special interest groups or other specialist security forums & professional associations MUST be maintained.	Revenant individuals that maintain the serviced systems within the organisation must have appropriate contacts with special interest groups or other specialist security forums and professional associations.	Implicit	R	AR	C

A.6.1.5	Information security in project management	Information security MUST be addressed in project management regardless of the type of the project.	All relevant projects associated to the supported system must go through Information security reviews, regardless of the type of the project.	Explicit	A	R	C
A.7	**Human Resource Security**						
A.7.1	**Prior to employment**	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.					
A.7.1.1	Screening	Background verification checks on ALL candidates for employments MUST be carried out in accordance with relevant laws, regulations & ethics and MUST be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	1. Are background verification checks carried out on all new candidates for employment?	Explicit	R	AR	I
			2. Are these checks approved by appropriate management?		R	AR	I
			3. Are the checks compliant with relevant laws, regulations and ethics?		R	AR	I
			4. Are the level of checks required supported by business risk assessments?		R	AR	I
A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors **MUST** state their and the organisation's responsibilities for information security.	1. Are all employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements?	Explicit	R	AR	I
			2. Do employment / service contracts specifically cover the need to protect business information?		R	AR	I
A.7.2	**During employment**	To ensure that the employees and contractors are aware of and fulfil their information security responsibilities.					
A.7.2.1	Management responsibilities	Management **MUST** require all employees & contractors to apply information security in accordance with established policies and procedures of the organisation.	1. Are managers (of all levels) engaged in driving security within the business?	Explicit	AR	R	C
			2. Does management behaviour and policy drive, and encourage, all employees, contractors and 3rd party users to apply security in accordance with established policies and procedures?		AR	R	C

A.7.2.2	Information security awareness, education, and training	All employees of the organisation and where relevant, contractors **MUST** receive appropriate awareness education & training and regular updates in organisational policies and procedures, as relevant for their job function.	Do all employees, contractors and third party users undergo regular security awareness training appropriate to their role and function within the organisation?	Explicit	AR	R	C
A.7.2.3	Disciplinary process	There **MUST** be a formal and communicated disciplinary process in place to take action against employees who have committed and information security breach.	1. Is there a formal disciplinary process which allows the organisation to take action against employees who have committed an information security breach?	Implicit	AR	R	C
			2. Is this communicated to all employees?		AR	R	C
A.7.3	**Termination and change of employment**	To protect the organisation's interest as part of the process of changing or terminating employment.					
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment **MUST** be defined, communicated to the employee or contractor and enforced.	1. Is there a documented process for terminating or changing employment duties?	Explicit	R	AR	C
			2. Are any information security duties which survive employment communicated to the employee or contractor?		R	AR	C
			3. Is the organisation able to enforce compliance with any duties that survive employment?		R	AR	C
A.8	**Asset management**						
A.8.1	**Responsibility for assets**	To identify organisational assets and define appropriate protection responsibilities.					
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities **MUST** be identified and an inventory of these assets **MUST** be drawn up and maintained.	1. Is there an inventory of all assets associated with information and information processing facilities?	Implicit	AR	I	CI
			2. Is the inventory accurate and kept up to date?		AR	I	CI
A.8.1.2	Ownership of assets	Assets maintained in the inventory **MUST** be owned.	All information assets must have a clearly defined owner who is aware of their responsibilities.	Implicit	AR	I	CI

A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information and information processing facilities **MUST** be identified, documented, and implemented.	1. Is there an acceptable use policy for each class / type of information asset?	Implicit	AR	I	C
			2. Are users made aware of this policy prior to use?		AR	I	C
A.8.1.4	Return of assets	All employees and external party users **MUST** return all the organisational assets in their possession upon termination of their employment, contract, or agreement.	Is there a process in place to ensure all employees and external users return the organisation's assets on termination of their employment, contract, or agreement?	Implicit	AR	R	C
A.8.2	**Information classification**						
A.8.2.1	Classification of information	Information MUST be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	1. Is there a policy governing information classification?	Implicit	R	I	A
			2. Is there a process by which all information can be appropriately classified?		AR	I	C
A.8.2.2	Labelling of information	An appropriate set of procedures for information labelling MUST be developed and implemented in accordance with the information classification scheme adopted by the organisation.	Is there a process or procedure for ensuring information classification s appropriately marked on each asset?	Implicit	AR	R	CI
A.8.2.3	Handling of assets	Procedures for handling assets **MUST** be developed and implemented in accordance with the information classification scheme adopted by the organisation.	1. Is there a procedure for handling each information classification?	Implicit	R	AR	CI
			2. Are users of information assets made aware of this procedure?		R	AR	CI

A.8.3	**Media handling**	To prevent unauthorised disclosure, modification, removal, or destruction of information stored on media.					
A.8.3.1	Management of removable media	Procedures **MUST** be implemented for the management of removal media in accordance with the classification scheme adopted by the organisation.	1. Is there a policy governing removable media?	Explicit	R	I	A
			2. Is there a process covering how removable media is managed?	Explicit	AR	R	C
			3. Are the policy and process(es) communicated to all employees using removable media?		R	AR	C
A.8.3.2	Disposal of media	Media **MUST** be disposed of securely when no longer required using formal procedures.	Is there a formal procedure governing how removable media is disposed?		AR	R	C
A.8.3.3	Physical media transfer	Media containing information **MUST** be protected against unauthorised access, misuse, or corruption during transportation.	1. Is there a documented policy and process detailing how physical media should be transported?	Explicit	R	I	A
			2. Is media in transport protected against unauthorised access, misuse, or corruption?		R	AR	C
A.9	**Access control**						
A.9.1	**Business requirements for access control**	To limit access to information and information processing facilities.					
A.9.1.1	Access control policy	An access control policy **MUST** be established, documented, and reviewed based upon business & information security requirements.	1. Is there a documented access control policy?	Explicit	R	R	A
			2. Is the policy based on business requirements?		AR	R	C
			3. Is the policy communicated appropriately?		AR	R	C
A.9.1.2	Access to networks and network services	Users **MUST** only be provided with access to the network and network services that they have been specifically authorised to use.	Are controls in place to ensure users only have access to the network resources they have been specially authorised to use and are required for their duties?	Explicit	AR	R	C

A.9.2	**User access management**	To ensure authorised user access and prevent unauthorised access to systems and services.					
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process **MUST** be implemented to enable assignment of access rights.	Is there a formal user access registration process in place?	Explicit	AR	R	C
A.9.2.2	User access provisioning	A formal user access provisioning process **MUST** be implemented to assign or revoke access rights for all user types to all systems and services.	Is there a formal user access provisioning process in place to assign access rights for all user types and services?	Explicit	AR	R	C
A.9.2.3	Management of privileged access rights	The allocation and use of privileged rights **MUST** be restricted and controlled.	Are privileged access accounts separately managed and controlled?	Explicit	AR	R	C
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information **MUST** be controlled through formal management process.	Is there a formal management process in place to control allocation of secret authentication information?	Explicit	AR	R	C
A.9.2.5	Review of user access rights	Asset owners **MUST** review users' access rights at regular intervals.	1. Is there a process for asset owners to review access rights to their assets on a regular basis?	Explicit	AR	R	C
			2. Is this review process verified?		AR	R	C
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities **MUST** be removed upon termination of their employment, contract, or agreement, or adjusted upon change.	Is there a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role?	Explicit	AR	R	C
A.9.3	**User responsibilities**	To make users accountable for safeguarding their authentication information.					
A.9.3.1	Use of secret authentication information	Users **MUST** be required to follow the organisation's practices in the use of secret authentication information.	1. Is there a policy document covering the organisations practices in how secret authentication information must be handled?	Explicit	AR	R	C
			2. Is this communicated to all users?		AR	R	C

A.9.4	**System and application access control**	To prevent unauthorised access to systems and applications.					
A.9.4.1	Information access restriction	Access to information and application systems functions **MUST** be restricted in accordance with the access control policy.	Is access to information and application system functions restricted in line with the access control policy?	Explicit	AR	R	C
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to the systems and applications **MUST** be controlled by a secure logon procedure.	Where the access control policy requires it, is access controlled by a secure log-on procedure?	Explicit	AR	R	C
A.9.4.3	Password management system	Password management systems MUST be interactive and **MUST** ensure quality passwords.	1. Are password systems interactive?	Explicit	AR	R	C
			2. Are complex passwords required?		AR	R	C
A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding systems and application controls **MUST** be restricted and tightly controlled.	Are privilege utility programs restricted and monitored?	Explicit	AR	R	C
A.9.4.5	Access control to program source code	Access to source code **MUST** be restricted.	Is access to the source code of the Access Control System protected?	Implicit	AR	R	C
A.10	**Cryptography**						
A.10.1	**Cryptographic controls**	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information.		Explicit			
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for the protection of information **MUST** be developed and implemented.	Is there a policy on the use of cryptographic controls?	Explicit	R	R	A

A.10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys **MUST** be developed and implemented through their whole life cycle.	Is there a policy governing the whole lifecycle of cryptographic keys?	Explicit	R	R	A
A.11	**Physical and environmental security**						
A.11.1	**Secure areas**	To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.		Implicit			
A.11.1.1	Physical security perimeter	Security perimeters **MUST** be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	1. Is there a designated security perimeter?	Implicit	AR	I	C
			2. Are sensitive or critical information areas segregated and appropriately controlled?		AR	I	C
A.11.1.2	Physical entry controls	Secure areas **MUST** be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	Do secure areas have suitable entry control systems to ensure only authorised personnel have access?	Implicit	AR	I	C
A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities **MUST** be designed and applied.	1. Have offices, rooms and facilities been designed and configured with security in mind?	Implicit	AR	I	C
			2. Do processes for maintaining the security (e.g., Locking up, clear desks etc.) exist?		AR	I	C
A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents **MUST** be designed and applied.	Have physical protection measures to prevent natural disasters, malicious attack or accidents been designed in?	Implicit	AR	I	C
A.11.1.5	Working in secure areas	Procedures for working in a secure area **MUST** be designed and applied.	1. Do secure areas exist?	Implicit	AR	I	C
			2. Where they do exist, do secure areas have suitable policies and processes?		AR	I	C
			3. Are the policies and processes enforced and monitored?		AR	I	C

A.11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises **MUST** be controlled and if possible isolated from information processing facilities to avoid unauthorised access.	1. Are there separate delivery / loading areas?	Implicit	AR	I	C
			2. Is access to these areas' controls?	Implicit	AR	I	C
			3. Is access from loading areas isolated from information processing facilities?		AR	I	C
A.11.2	**Equipment**	To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.		Implicit			
A.11.2.1	Equipment siting and protection	Equipment **MUST** be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.	1. Are environmental hazards identified and considered when equipment locations are selected?	Implicit	AR	I	C
			2. Are the risks from unauthorised access / passers-by considered when siting equipment?	Implicit	AR	I	C
A.11.2.2	Supporting utilities	Equipment **MUST** be protected from power failures and other disruptions caused by failures in supporting utilities.	1. Is there a UPS system or backup generator?	Implicit	AR	I	C
			2. Have these been tested within an appropriate timescale?		AR	I	C
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services **MUST** be protected from interception, interference, or damage.	1. Have risk assessments been conducted over the location of power and telecommunications cables?	Implicit	AR	I	C
			2. Are they located to protect from interference, interception, or damage?		AR	I	C
A.11.2.4	Equipment maintenance	Equipment **MUST** be correctly maintained to ensure its continued availability and integrity.	Is there a rigorous equipment maintenance schedule?	Implicit	AR	I	C
A.11.2.5	Removal of assets	Equipment, information, or software **MUST not** be taken off-site without prior authorisation.	1. Is there a process controlling how assets are removed from site?	Implicit	AR	I	C
			2. Is this process enforced?		AR	I	C
			3. Are spot checks carried out?		AR	I	C
A.11.2.6	Security of equipment and		1. Is there a policy covering security of assets off-site?	Implicit	AR	I	C

	assets off-premises	Security **MUST** be applied to off-site assets taking into account the different risks of working outside the organisation's premises.	2. Is this policy widely communicated?		AR	I	C
A.11.2.7	Secure disposal or reuse of equipment	All items of equipment containing storage media MUST be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	1. Is there a policy covering how information assets may be reused?	Implicit	AR	I	C
			2. Where data is wiped, is this properly verified before reuse/disposal?		AR	I	C
A.11.2.8	Unattended user equipment	Users **MUST** ensure that unattended equipment has appropriate protection.	1. Does the organisation have a policy around how unattended equipment should be protected?	Implicit	AR	I	C
			2. Are technical controls in place to secure equipment that has been inadvertently left unattended?		AR	I	C
A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removal storage media and a clear screen policy for information processing facilities **MUST** be adopted.	1. Is there a clear desk / clear screen policy? 2. Is this well enforced?	Implicit	AR	I	C
A.12	**Operations security**						
A.12.1	**Operational procedures and responsibilities**	To ensure correct and secure operations of information processing facilities.		Implicit			
A.12.1.1	Documented operating procedures	Operating procedures **MUST** be documents and made available to all users who need them.	1. Are operating procedures well documented?	Implicit	A	R	CI
			2. Are the procedures made available to all users who need them?		A	R	CI
A.12.1.2	Change management	Changes to the organisation, business process, information processing facilities and systems that affect information security **MUST** be controlled.	Is there a controlled change management process in place?	Implicit	A	R	CI

A.12.1.3	Capacity management	The use of resources **MUST** be monitored, tuned and projections made of future capacity requirements to ensure the required systems performance.	Is there a capacity management process in place?	Implicit	I	AR	CI
A.12.1.4	Separation of development, testing and operational environments	Development, testing and operational environments **MUST** be segregated to reduce the risks of unauthorised access of changes to the operational environment.	Does the organisation enforce segregation of development, test, and operational environments?	Implicit	I	AR	CI
A.12.2	Protection from malware	To ensure that information and information processing facilities are protected against malware.		Implicit			
A.12.2.1	Controls against malware	Detection, prevention, and recovery controls to protect against malware **MUST** be implemented, combined with appropriate user awareness.	1. Are processes to detect malware in place?	Implicit	A	R	CI
			2. Are processes to prevent malware spreading in place?		A	R	CI
			3. Does the organisation have a process and capacity to recover from a malware infection?		A	R	CI
A.12.3	Backup	To protect against data loss		Implicit			
A.12.3.1	Information backup	Backup copies of information, software and systems images **MUST** be taken and tested regularly in accordance with an agreed backup policy.	1. Is there an agreed backup policy?	Implicit	AR	R	I
			2. Does the organisation's backup policy comply with relevant legal frameworks?		AR	R	I
			3. Are backups made in accordance with the policy?		AR	R	I
			4. Are backups tested?		AR	R	I
A.12.4	**Logging and monitoring**	To record events and generate evidence.		Implicit			
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults, and information security events **MUST** be produced, kept and regularly reviewed.	Are appropriate event logs maintained and regularly reviewed?	Implicit	A	R	CI

A.12.4.2	Protection of log information	Logging facilities and log information **MUST** be protected against tampering and unauthorised access.	Are logging facilities protected against tampering and unauthorised access?	Implicit	A	R	CI
A.12.4.3	Administrator and operator logs	System admin and system operator activities **MUST** be logged, and the logs protected and regularly reviewed.	Are sysadmin / sysop logs maintained, protected, and regularly reviewed?	Implicit	A	R	CI
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organisation or security domain **MUST** be synchronised to a single reference time source.	Are all clocks within the organisation	Implicit	A	R	CI
A.12.5	Control of operational software	To ensure the integrity of operational systems		Explicit			
A.12.5.1	Installation of software on operational systems	Procedures **MUST** be implemented to control the installation of software on operational systems	Is there a process in place to control the installation of software onto operational systems?	Explicit	A	R	CI
A.12.6	Technical vulnerability management	To prevent exploitation of technical vulnerabilities.		Explicit			
A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used **MUST** be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	1. Does the organisation have access to updated and timely information on technical vulnerabilities?	Explicit	A	R	CI
			2. Is there a process to risk assess and react to any new vulnerabilities as they are discovered?	Explicit	A	R	CI
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users **MUST** be established and implemented.	Are there processes in place to restrict how users install software?	Explicit	A	R	CI

A.12.7	**Information systems audit considerations**	To minimise the impact of audit activities on operational systems.		Implicit			
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems **MUST** be carefully planned and agreed to minimise disruptions to business processes.	1. Are IS Systems subject to audit?	Implicit	AR	I	CI
			2. Does the audit process ensure business disruption is minimised?		AR	I	CI
A.13	**Communications security**						
A.13.1	Network security management	To ensure the protection of information in networks and it's supporting processing facilities.		Explicit			
A.13.1.1	Network controls	Networks **MUST** be managed and controlled to protect information in systems and applications	Is there a network management process in place?	Explicit	AR	R	CI
A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all networks service **MUST** be identified and included in network service agreements, whether these services are provided in-house or outsourced.	1. Does the organisation implement a risk management approach which identifies all network services and service agreements?	Explicit	AR	R	CI
			2. Is security mandated in agreements and contracts with service providers (in house and outsourced).		AR	R	CI
			3. Are security related SLAs mandated?		AR	R	CI
A.13.1.3	Segregation in networks	Groups of information services, users and information systems **MUST** be segregated on networks.	Does the network topology enforce segregation of networks for different tasks?	Explicit	AR	R	CI

A.13.2	**Information transfer**	To maintain the security of information transferred within an organisation and with any external entity.					
A.13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls **MUST** be in place to protect the transfer of information using all types of communication.	1. Do organisational policies govern how information is transferred?	Explicit	A	R	CI
			2. Are procedures for how data should be transferred made available to all employees?		A	R	CI
			3. Are relevant technical controls in place to prevent non-authorised forms of data transfer?		A	R	CI
A.13.2.2	Agreements on information transfer	Agreements **MUST** address the secure transfer of business information between the organisation and external parties.	Do contracts with external parties and agreements within the organisation detail the requirements for securing business information in transfer?	Explicit	A	R	CI
A.13.2.3	Electronic messaging	Information involved in electronic messaging **MUST** be appropriately protected.	Do security policies cover the use of information transfer while using electronic messaging systems?	Explicit	A	R	CI
A.13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information **MUST** be identified, regularly reviewed, and documented.	1. Do employees, contractors and agents sign confidentiality or non-disclosure agreements?	Explicit	A	R	CI
			2. Are these agreements subject to regular review?		A	R	CI
			3. Are records of the agreements maintained?		A	R	CI
A.14	**System acquisition, development and maintenance**						
A.14.1	Security requirements of information systems	To ensure that the information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provides services over public networks.		Implicit			
A.14.1.1	Information security	The information security related requirements **MUST** be included in the requirements for new	1. Are information security requirements specified when new systems are introduced?	Implicit	A	R	CI

	requirements analysis and specification	information systems or enhancements to existing information systems.	2. When systems are being enhanced or upgraded, are security requirements specified and addressed?		A	R	CI
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks **MUST** be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.	Do applications which send information over public networks appropriately protect the information against fraudulent activity, contract dispute, unauthorised discloser, and unauthorised modification?	Implicit	A	R	CI
A.14.1.3	Protecting application services transactions	Information involved in application services transactions **MUST** be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.	Are controls in place to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay attacks?	Implicit	A	R	CI
A.14.2	Security in development and support processes	To ensure that information security is designed and implemented within the development lifecycle of information systems.		Implicit			
A.14.2.1	Secure development policy	Rules for the development of software and systems MUST be established and applied to developments within the organisation.	1. Does the organisation develop software or systems?	Implicit	AR	R	CI
			2. If so, are there policies mandating the implementation and assessment of security controls?		AR	R	CI
A.14.2.2	System changes control procedures	Changes to the systems within the development lifecycle MUST be controlled using formal managed Controls procedures.	Is there a formal change control process?	Implicit	AR	R	CI
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications MUST be reviewed and tested to ensure there is no adverse impact on the organisation operations or security.	Is there a process to ensure a technical review is carried out when operating platforms are changed?	Implicit	AR	R	CI

A.14.2.4	Restrictions on changes to software packages	Modifications to software packages MUST be discouraged, limited to necessary changes and all changes SAHLL be strictly controlled.	Is there a policy in place which mandates when and how software packages can be changed or modified?	Implicit	AR	R	CI
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems **MUST** be established, documented, maintained and applied to any information systems implementation efforts	Does the organisation have documented principles on how systems must be engineered to ensure security?	Implicit	AR	R	CI
A.14.2.6	Secure development environment	Organisations **MUST** establish and appropriately protect secure development environments for system development and integration efforts that cover the entire systems development lifecycle.	1. Has a secure development environment been established?	Implicit	AR	R	CI
			2. Do all projects utilise the secure development environment appropriately during the system development lifecycle?		AR	R	CI
A.14.2.7	Outsourced development	The organisation **MUST** supervise and monitor the activity of outsourced systems development.	1. Where development has been outsourced is this supervised?	Implicit	AR	R	CI
			2. Is externally developed code subject to a security review before deployment?		AR	R	CI
A.14.2.8	System security testing	Testing security functionality **MUST** be carried out during development	Where systems or applications are developed, are they security tested as part of the development process?	Implicit	AR	R	CI
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria **MUST** be established for new information systems, upgrades, and new versions.	Is there an established process to accept new systems / applications, or upgrades, into production use?	Implicit	AR	R	CI
A.14.3	Test data	To ensure the protection of data used for testing.		Implicit			
A.14.3.1	Protection of test data	Test data MUST be selected carefully, protected, and controlled.	1. Is there a process for selecting test data?	Implicit	AR	R	CI
			2. Is test data suitably protected?		AR	R	CI

A.15	**Supplier relationships**						
A.15.1	Information security in supplier relationships	To ensure protection of the organisations assets that is accessible by suppliers.		Explicit			
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets **MUST** be agreed with the supplier and documented.	1. Is information security included in contracts established with suppliers and service providers?	Implicit	R	I	A
			2. Is there an organisation-wide risk management approach to supplier relationships?		AR	I	CI
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements **MUST** be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the organisation's information.	1. Are suppliers provided with documented security requirements?	Implicit	AR	I	CI
			2. Is supplier access to information assets & infrastructure controlled and monitored?		AR	I	CI
A.15.1.3	Information and communication technology supply chain	Agreements with the suppliers **MUST** include requirements to address the information security risks associated with the information and communications technology services and product supply chain.	Do supplier agreements include requirements to address information security within the service & product supply chain?	Implicit	AR	I	CI
A.15.2	Supplier service delivery management			Implicit			
A.15.2.1	Monitoring and review of supplier services	Organisations **MUST** regularly monitor, review and audit supplier service delivery.	Are suppliers subject to regular review and audit?	Implicit	AR	I	CI
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls **MUST** be managed, taking account of the criticality of the business information, systems and process involved and re-assessment checks.	Are changes to the provision of services subject to a management process which includes security & risk assessment?	Implicit	AR	I	CI
A.16	**Information security incident management**						

A.16.1	Management of information security incidents and improvements	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weakness.		Implicit			
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures MUST be established to ensure a quick, effective, and orderly response to information security incidents.	Are management responsibilities clearly identified and documented in the incident management processes?	Implicit	AR	I	CI
A.16.1.2	Reporting information security events	Information security events MUST be reported through appropriate management's channels as quickly as possible.	1. Is there a process for timely reporting of information security events?	Implicit	AR	I	CI
			2. Is there a process for reviewing and acting on reported information security events?		AR	I	CI
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organisation's information systems and services **MUST** be required to note and report any observed or suspected information security weakness in systems or services.	1. Is there a process for reporting of identified information security weaknesses?	Implicit	AR	I	CI
			2. Is this process widely communicated?		AR	I	CI
			3. Is there a process for reviewing and addressing reports in a timely manner?		AR	I	CI
A.16.1.4	Assessment of and decision on information security events	Information security incidents **MUST** be assessed and it be decided if they are to be classified as information security incidents.	Is there a process to ensure information security events are properly assessed and classified?	Implicit	AR	I	CI
A.16.1.5	Response to information security incidents	Information security incidents **MUST** be responded to in accordance with the documented procedures.	Is there an incident response process which reflects the classification and severity of information security incidents?	Implicit	AR	I	CI
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents **MUST** be used to reduce the likelihood or impact of future incidents.	Is there a process or framework which allows the organisation to learn from information security incidents and reduce the impact / probability of future events?	Implicit	AR	I	CI
A.16.1.7			1. Is there a forensic readiness policy?	Implicit	AR	I	CI

	Collection of evidence	The organisation **MUST** define and apply procedure for the identification, collection, acquisition, and preservation of information which can serve as evidence.	2. In the event of an information security incident is relevant data collected in a manner which allows it to be used as evidence?		AR	I	CI
A.17	**Information security aspects of business continuity management**						
A.17.1	Information security continuity	Information security continuity MUST be embedded in the organisation's business continuity management systems.		Implicit			
A.17.1.1	Planning information security continuity	The organisation **MUST** determine its requirements for information security and continuity of information security management in adverse situations, e.g., during a crisis or disaster.	Is information security included in the organisation's continuity plans?	Implicit	AR	I	CI
A.17.1.2	Implementing information security continuity	The organisation **MUST** establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for information security during adverse situations.	Does the organisation's information security function have documented, implemented, and maintained processes to maintain continuity of service during an adverse situation?	Implicit	AR	I	CI
A.17.1.3	Verify, review, and evaluate information security continuity	The organisation MUST verify the established and implemented information security continuity controls at regular intervals to ensure that they are valid and effective during adverse situations.	Are continuity plans validated and verified at regular intervals?	Implicit	AR	I	CI
			Is there a DR plan?		AR	I	CI
			Does the organisation's information security function have documented, implemented, and maintained processes to maintain continuity of service during a DR situation?		AR	I	CI
			Are there defined DR parameters, MOT, RTO, RTM?		AR	I	CI
			Is there a risk measurement against the DR?		AR	I	CI
			Have the Risk profiles been approved by management?		AR	I	CI
			Is there a DR run sheet?		AR	I	CI
A.17.2	Redundancies	To ensure availability of information processing facilities.		Implicit			

A.17.2.1	Availability of information processing facilities	Information processing facilities MUST be implemented with redundancy sufficient to meet availability requirements.	Do information processing facilities have sufficient redundancy to meet the organisations availability requirements?	Implicit	AR	I	CI
A.18	**Compliance**						
A.18.1	Compliance with legal and contractual requirements	To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements.		Implicit			
A.18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements **MUST** be explicitly identified, documents and kept up to date for each information systems and the organisation.	1. Has the organisation identified and documented all relevant legislative, regulatory, or contractual requirements related to security?	Implicit	AR	I	CI
			2. Is compliance documented?		AR	I	CI
A.18.1.2	Intellectual property rights	Appropriate procedures **MUST** be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.	1. Does the organisation keep a record of all intellectual property rights and use of proprietary software products?	Implicit	AR	I	CI
			2. Does the organisation monitor for the use of unlicensed software?		AR	I	CI
A.18.1.3	Protection of records	Records **MUST** be protected from loss, destruction, falsification, unauthorised access, and unauthorised release, in accordance with legislative, regulatory, contractual, and business requirements.	Are records protected from loss, destruction, falsification and unauthorised access or release in accordance with legislative, regulatory, contractual, and business requirements?	Implicit	AR	I	CI
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information **MUST** be ensured as required in relevant legislation and regulation where applicable.	1. Is personal data identified and appropriately classified?	Explicit	AR	I	CI
			2. Is personal data protected in accordance with relevant legislation?		AR	I	CI
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls **MUST** be compliant with all relevant agreements, legislation, and regulations.	Are cryptographic controls protected in accordance with all relevant agreements, legislation, and regulations?	Implicit	AR	I	CI

A.18.2	Information security reviews	To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.		Implicit			
A.18.2.1	Independent review of information security	The organisation's approach to managing information security and its implementation (i.e., control objectives, controls, objectives, policies, processes, and procedures for information security) **MUST** be reviewed independently at planned intervals or when significant changes occur.	1. Is the organisations approach to managing information security subject to regular independent review?	Implicit	AR	I	CI
			2. Is the implementation of security controls subject to regular independent review?		AR	I	CI
A.18.2.2	Compliance with security policies and standards	Managers **MUST** regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.	1. Does the organisation instruct managers to regularly review compliance with policy and procedures within their area of responsibility?	Implicit	AR	I	CI
			2. Are records of these reviews maintained?		AR	I	CI
A.18.2.3	Technical compliance review	Information systems **MUST** be regularly reviewed for compliance with the organisation's information security policies and standards.	Does the organisation regularly conduct technical compliance reviews of its information systems?	Implicit	AR	I	CI

APPENDIX B

Essential Eight Explained			
Mitigation Strategies to Prevent Malware Delivery and Execution		**Mitigation Strategies to Limit the Extent of Cyber Security Incidents**	
Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g., Windows Script Host, PowerShell and HTA) and installers.	**Patch applications** e.g., Flash, web browsers, Microsoft Office, Java, and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.	**Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Do not use privileged accounts for reading email and web browsing.	**Patch operating systems.** Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Do not use unsupported versions.
Why: All non-approved applications (including malicious code) are prevented from executing.	**Why:** Security vulnerabilities in applications can be used to execute malicious code on systems.	**Why:** Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.	**Why:** Security vulnerabilities in operating systems can be used to further the compromise of systems.
Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	**User application hardening**. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g., OLE), web browsers and PDF viewers.	**Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high availability) data repository.	
Why: Microsoft Office macros can be used to deliver and execute malicious code on systems.	**Why:** Flash, ads and Java are popular ways to deliver and execute malicious code on systems.	**Why:** Stronger user authentication makes it harder for adversaries to access sensitive information and systems.	

Mitigation Strategies to Recover Data and System Availability			
Daily backups of important new/changed data, software, and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually, and when IT infrastructure changes.			
Why: To ensure information can be accessed following a cyber security incident (e.g., a ransomware incident).			