WA Cyber Security Policy Clauses and SRC Standards Table

The first column of the table lists the clauses from the 2024 WA Cyber Security Policy (the Policy) that are relevant to information management. The other columns provide actions (A) or recommendations (R) drawn from the State Records Commission (SRC) standards, State Records Office (SRO) Records Management Advice or other whole-of-government policies and guidance. The last column identifies roles and responsibilities.

Policy Clause	Information Management Actions (A) / Recommendations (R)	Source	Roles and Responsibilities
1.Governance **1.4 Cyber Security Governance** Each entity must establish governance of cyber security for their entity.	**A:** Establish policies and procedures to oversee and maintain electronic and physical security and protection of the organisation's information. **A:** Document these policies and procedures in your organisation's record keeping plan (RKP). **A:** Ensure that security and authentication mechanisms do not make digital information inaccessible in the long term.	*SRC Standard 2: Record Keeping Plans*, Principle 2 Policies and Procedures *SRC Standard 8: Managing Digital Information*, Principle 3 Security of Digital Information	CEO (the Accountable Authority of an organisation – CEO, Director General or chief employee) Cyber Security Executive Chief Information Officer Corporate Information Coordinator Information Communication and Technology (ICT) staff
	A: Establish and maintain a business continuity plan (BCP) and Records Disaster Management Plan (RDMP), including • information assets and the systems in which they are stored in • ability to provide backups • a flow diagram of information lifecycle • the frequency of system backups (accuracy of backup in the event of an incident) based on business operation needs. **A:** Include the plan(s) as Attachment 4 of your organisation RKP.	*SRC Standard 2: Record Keeping Plans*, Principle 4 Preservation. SRO Records Management Advice: Records Disaster Management Plans	CEO Cyber Security Executive Risk and Governance staff Corporate Information Coordinator Chief Information Officer Information Communication and Technology (ICT) staff Directors / Managers

WA Cyber Security Policy Clauses and SRC Standards Table

Policy Clause	Information Management Actions (A) / Recommendations (R)	Source	Roles and Responsibilities
	R: Consider a cyber security incident response in the BCP or RDMP that outline information recovery strategies during an emergency		
1.4 Cyber Security Governance Each entity must establish governance of cyber security for their entity.	**A:** Establish and maintain a records disposal program with appropriate procedures in accordance with approved retention and disposal authority/ies, relevant SRC Standards and the *SRO Guideline – Records Retention, Disposal and Destruction*. **A:** Evidence the disposal program in the organisation RKP. This ensures that information that are not State archives are not kept unnecessarily meaning they are not at risk during cyber security incidents.	*SRC Standard 2: Record Keeping Plans*, Principle 5 Retention and Disposal.	Corporate Information Coordinator Information Management staff CEO or authorised delegate(s)
	R: Consider risks involved in keeping details of, or copies of, personal information when collecting and handling personal information for business purposes. **A:** Establish policies and procedures to appropriately manage personal information that is retained which are consistent with the Australian Privacy Principles set out in Schedule 1 to the Privacy Act 1988 (Cth).	SRO Records Management Advice: Retention of Personal Information *Privacy and Responsible Information Sharing Act 2024*	Directors / Managers / Coordinators All employees
	R: Design record keeping requirements into systems across their life cycle to factor the need to retain information for longer than the life cycle of a system which impact decommissioning plans, migration plans etc. This allows for appropriate management and identification of impacts based on its life cycle and archival status.	SRO Records Management Advice: Business Information Systems	Chief Information Officer Information Communication and Technology (ICT) staff Corporate Information Coordinator

WA Cyber Security Policy Clauses and SRC Standards Table

Policy Clause	Information Management Actions (A) / Recommendations (R)	Source	Roles and Responsibilities
1.5 Data Offshoring Governance Each entity must define and understand its risks associated with data offshoring.	**A:** Undertake a risk assessment before storing information or application systems offsite or offshore. **A:** Identify the physical location of the data centre of the cloud services used by the organisation to store the organisation's information. Tier 1 Risk Information, held on a cloud, must have its data centre located in Australia (in other words, information must not be offshored). **A:** Document the above in the organisation RKP.	*SRC Standard 2: Record Keeping Plans*, Principle 4 Preservation. *SRC Standard 8: Managing Digital Information*, Principle 3 – Security of Digital Information WA Government Offshoring Position and Guidance, Risk Information Assessment Table	Cyber Security Executive Chief Information Officer Information Communication and Technology (ICT) staff Corporate Information Coordinator
1.6 Secure Device Disposal Governance Each entity must maintain oversight of the secure disposal of devices, computers or media that hold digital information	**A:** Establish policies and procedures regarding the secure disposal of devices and digital information of temporary value. Disposal must occur in accordance with an approved disposal authority and in such a way it cannot be reconstructed.	*SRC Standard 8: Managing Digital Information*, Principle 2 – Appraisal, Retention and Disposal of Digital Information State Records Office Guideline Management of Digital Records Records Retention, Disposal and Destruction	Chief Information Officer Information Communication and Technology (ICT) staff Corporate Information Coordinator Information Management Staff

WA Cyber Security Policy Clauses and SRC Standards Table

Policy Clause	Information Management Actions (A) / Recommendations (R)	Source	Roles and Responsibilities
2. Identify **2.1 Cyber Security Context** To understand its cyber security context and as a basis for sound cyber security decision-making, each entity must maintain an inventory of their ICT environment including 2.1.a devices, servers and other ICT equipment 2.1.c critical databases and information assets.	**R:** Establish and maintain an Information Asset Register that outlines the organisation's networks, technology, information, and systems as recommended by the WA Information Classification Policy; and Privacy and Responsible Sharing (PRIS) Readiness Guidance activities. This should be an accurate list of the organisation's information and information holdings. **A:** Establish and maintain a listing of vital records and how they may be obtained if systems and infrastructure were unavailable in a cyberattack **A:** Document the vital records program in the organisation RKP. **A:** System integrations of business information systems with record keeping systems are known and managed appropriately. **R:** Maintain a log of information shared with third parties (data transfer logs are used to record all data imports and exports from systems). **R:** Develop and maintain data transfer processes and supporting data transfer procedures for the organisation.	PRIS Readiness Guidance 8 Information Survey and Information Asset Register WA Information Classification Policy *SRC Standard 2: Record Keeping Plans*, Principle 2 Policies and Procedures Principle 4 Preservation. SRO Records Management Advice Records Disaster Management Plans Vital Records	Chief Information Officer Corporate Information Coordinator Directors / Managers / Coordinators

WA Cyber Security Policy Clauses and SRC Standards Table

Policy Clause	Information Management Actions (A) / Recommendations (R)	Source	Roles and Responsibilities
2.2 Cyber Security Risk Management Each entity is required to assess and manage information security risks to the entity, taking account of various factors including: 2.2.d critical information managed by the entity.	**A:** Undertake a risk assessment of on site, off site, data centres and cloud storage, archives, and backups of the organisation information. **A:** Document the risk assessments in the organisation RKP.	*SRC Standard 2: Record Keeping Plans*, Principle 4 Preservation.	Cyber Security Executive Risk and Governance staff Chief Information Officer Corporate Information Coordinator
3. Protect **3.1 Australian Cyber Security Centre (ACSC) Controls** Each entity is required to implement ACSC Cyber Security Centre controls,	**R:** WA government staff and any contractors with access to government Information should hold a national police clearance. See also **3.6 Identity and Access Management** on how relevant access to information should be managed. **A:** Ensure the security of information at rest (when it is stored) and during transfer (when it is being transmitted from one place to another). This includes control and management of the safe disposal or transfer of information upon termination of contract, sharing or engagement with third parties. Recommended controls include:	WA Cyber Security Policy Additional and more detailed information around personnel management to protect from specific information security risks can be found in guidance developed by the State Security and Defence Policy directorate of the Department of the Premier and Cabinet. This	Directors / Managers / Coordinators Human Resources Cyber Security Executive Chief Information Officer Corporate Information Coordinator Information Communication and Technology (ICT) staff Information Management staff

WA Cyber Security Policy Clauses and SRC Standards Table

Policy Clause	Information Management Actions (A) / Recommendations (R)	Source	Roles and Responsibilities
including 3.1.2.5 Personnel Management.	• managing media sanitisation levels used by government suppliers to ensure that they are adequate to sensitive information level requirements. Sensitive information media sanitisation methods include multiple overwrites, encryption with key destruction, degaussing and physical destruction. (see Guidelines for Media Sanitization (nist.gov) for further guidance) • handling information stored on removable or decommissioned hardware appropriately based on NIST SP 800-88 or equivalent • ensuring that ICT equipment is destroyed prior to disposal, and that media disposal processes, and supporting media disposal procedures, are developed, implemented and maintained • maintaining physical security of information systems, data storage and records. See also **3.5 Physical Security of Assets** • ensuring Tier 1 Risk information is hosted in Australia and encrypted at rest and in transit (refer to the WA Offshoring Position for definition of risk tiers and further information) • implementing multi-factor authentication for access to Tier 1 Risk information • managing access to information according to their information classification. Refer to the WA Information Classification Policy • placing appropriate controls and managing high value high risk information assets identified in the organisation's vital records register • cleansing of hidden document metadata or XML prior to publishing or distribution.	can be requested from ossem@dpc.wa.gov.au *SRC Standard 2: Record Keeping Plans*, Principle 4 Preservation *SRC Standard 8: Managing Digital Information*, Principle 2 – Appraisal, Retention and Disposal of Digital Information State Records Office Guideline Management of Digital Records Records Retention, Disposal and Destruction WA Government Offshoring Position and Guidance, Risk Information Assessment Table WA Information Classification Policy	

WA Cyber Security Policy Clauses and SRC Standards Table

Policy Clause	Information Management Actions (A) / Recommendations (R)	Source	Roles and Responsibilities
	A: Dispose of information of temporary value securely in accordance with an approved disposal authority and in such a way it cannot be reconstructed.		
3.5 Physical Security of Assets Each entity must ensure that physical access to information technology and cyber security assets is managed to prevent unauthorised use and physical damage.	**A:** Implement security measures to prevent unauthorised access to information, systems, and storage including: • physical security of physical (non-digital) information • physical security of on-premise servers holding digital information • physical security of all ICT assets holding digital records i.e. physical security of the building (see also **3.6 Identity and Access Management**). **A:** Document these measures in the organisation's RKP	*SRC Standard 2: Record Keeping Plans*, Principle 4 Preservation. Local Government Physical Security of Server Assets - Office of the Auditor General (This better practice guide for local government can be applied to state Government)	Cyber Security Executive Chief Information Officer Corporate Information Coordinator
3.6 Identity and Access Management Each entity must implement appropriate management, monitoring and review of its user, customer and system accounts to	**A:** Manage, monitor and review user and system accounts to prevent unauthorised access or alteration to the organisation's information. Recommended controls include: • maintaining personnel security of staff, contractors, volunteers and suppliers according to the information classification, confidentiality, availability and integrity of systems of the information accessed in the course of performance of duties. • ensuring all employees are aware of their responsibilities regarding capture and	WA Cyber Security Policy WA Information Classification Policy *SRC Standard 8: Managing Digital Information*, Principle 3 Security of Digital Information	Chief Information Officer Corporate Information Coordinator Information Communication and Technology (ICT) staff Information Management staff All employees

WA Cyber Security Policy Clauses and SRC Standards Table

Policy Clause	Information Management Actions (A) / Recommendations (R)	Source	Roles and Responsibilities
prevent unauthorised access.	management of information; and remote access of the organisation's system • ensuring that unprivileged accounts are prevented from modifying and deleting backups. • ensuring that privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups. • ensuring backup administrator accounts are prevented from modifying and deleting backups during their retention period. • ensuring that users transferring data to and from systems are held accountable for data transfers they perform.		
6. Recover **6.1 Capability to Restore Services and Information** Each entity must have the capability to restore their services and information within the timeframes as defined by the entity's Business Continuity Plan or Incident Management Plans.	**A:** Back up systems regularly so information can be restored from a cyber security incident. Note: The frequency of system backups (and frequency is important because it determines the accuracy of backups in the event of an incident) should be pre-determined by the CEO in collaboration with the Cyber Security Executive, based on business operation needs of the organisation, and recorded in the organisation's cyber security governance document / disaster recovery governance document. See **1.4 Cyber Security Governance**. **A:** Submit a report to the State Records Commission via sro@sro.wa.gov.au if a cyber security incident causes the loss of State records and archives.	*SRC Standard 8: Managing Digital Information*, Principle 4 Storing Digital Information *State Records Act 2000* sections 60, 68 and 78	Chief Information Officer Corporate Information Coordinator Information Communication and Technology (ICT) staff Information Management staff