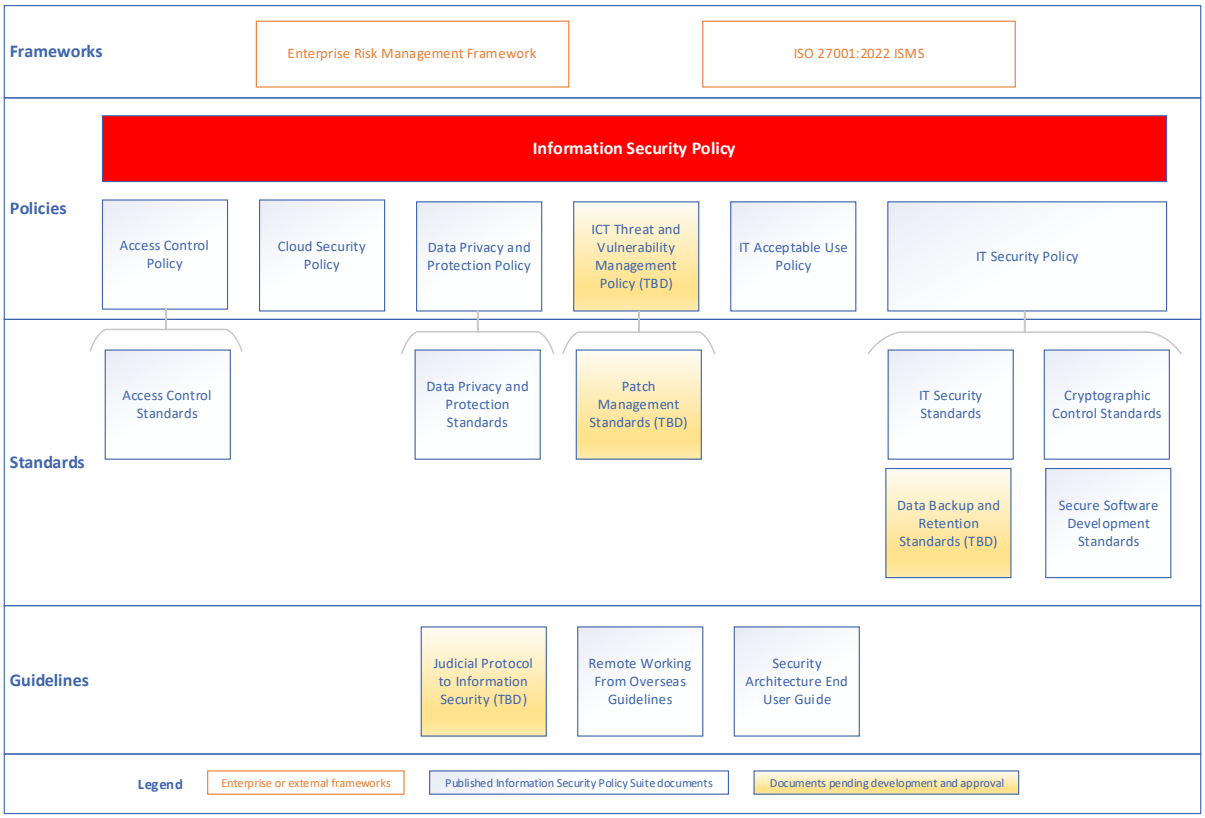
Information Security Policy

Table of contents



The red highlighted box shows where this document sits within the Information Security Policy Suite.

1 Purpose

This policy provides all Department of Communities and Justice (DCJ) employees and approved users with direction and support and establishes an implementation framework for security. The purpose of this policy is to clearly articulate the information security behaviours and practices that DCJ requires its employees and approved users to comply with.

Information security is fundamental to the successful operations of DCJ. As the custodians of information that is politically, commercially or personally sensitive, DCJ has a 'duty of care' to protect information from accidental or malicious modification, unauthorised access, loss or release.

DCJ is committed to ensuring the integrity of its information systems.

This policy and supporting documents contain information relating to the responsibilities of all users to appropriately protect the information they use and manage as part of their daily roles.

This policy is written in line with the NSW Cyber Security Policy and ISO/IEC 27000 suite of standards for managing information security.

Definition of DCJ information security:

"The protection of DCJ information assets against unauthorised access, modification or non-availability, whether in storage, processing, or transit. Information security includes identification of measures necessary to detect and protect DCJ information assets from such risks."

1.1 Related policies

This document is related to the following policies:

- IT Security Policy
- Data Privacy and Protection Policy
- IT Acceptable Use Policy
- Access Control Policy
- Cloud Security Policy
- End User Computing Policy
- Code of Ethical Conduct
- Enterprise Risk Management Policy
- NSW Cyber Security Policy 2020 v3.0

2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information
CCSO	NSW Chief Cyber Security Officer
CDIO	Chief Digital Information Officer
CISO	Chief Information Security Officer
CITO	Chief Information Technology Officer
DCJ	Department of Communities and Justice
IACS	Industrial automation and control systems
ICT	Information and communication technologies
IDS	Information and Digital Services
Information asset	Any information (both physical and digital in any format, including audio and visual);

	Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
ISMS	Information security management system
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory. Any request for deviation from a "must" must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a "must not" must follow the procedures for requesting exceptions.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met.

3 Scope

The requirements and expectations outlined in this policy applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information.
- any other body authorised to administer, develop, manage and support DCJ information systems and assets.

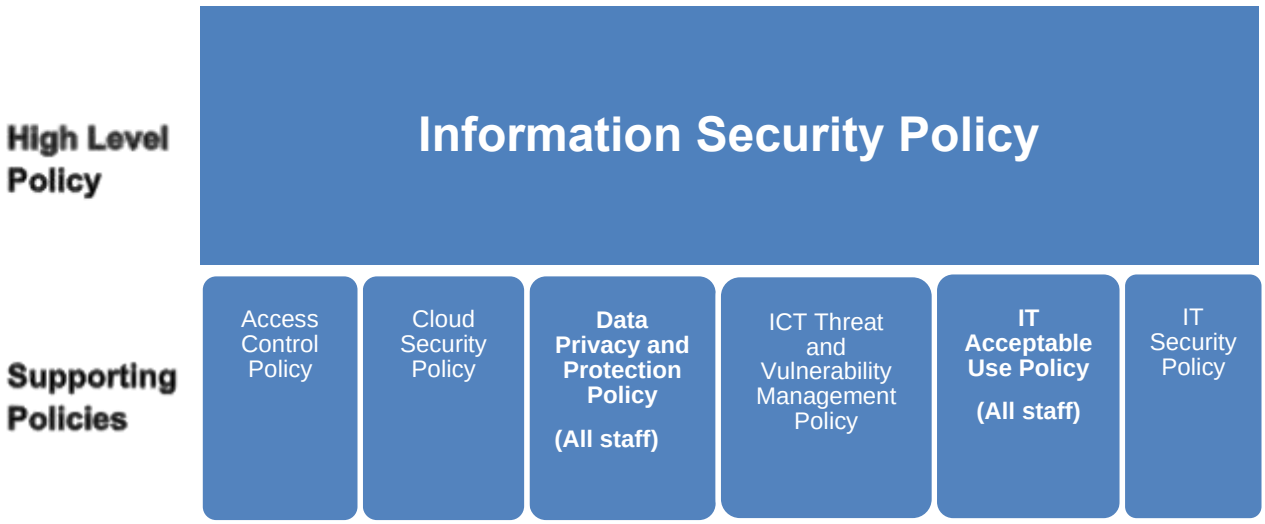
This policy does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges' tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

4 Information security policy schema

DCJ has developed a hierarchical approach to deploying the Information Security Policy. A suite of policy documents has been designed which segments the policy content into sections which are refined and tailored to a target audience. This approach allows for policies to be targeted at staff to ensure the content is applicable and the reader is not overburdened with information they cannot apply or relate to.

The diagram below depicts this schema and identifies the applicability of the documents to staff.



Documents in bold need to be read by all staff, the remaining documents, however, must be read by staff involved in the procurement, management and design of services and information systems.

5 Policy statement

DCJ is committed to ensuring the confidentiality, integrity and availability of its clients' information and the information of the organisation as a whole. The Information Security Policy articulates the standards DCJ must operate to, within a security context. DCJ's security strategy, security improvements register and information security management system (ISMS) enable this standard to be achieved.

DCJ is committed to maintaining and improving an ISMS to meet our obligations to protect its information assets under international industry standards, and where appropriate specified areas of DCJ will be certified to the standard to ensure the effective integration and integrity of this management system.

6 ISMS objectives

1. **Executive engagement** – Executive management are engaged by, aware of and support information security within DCJ.

2. **Assess threats and vulnerabilities** – The identification and assessment of security threats and vulnerabilities to key assets is undertaken regularly and tracked over time.
3. **Manage information security risks** – Develop and maintain effective security management processes to address identified risks.
4. **Learn from security incidents** – Record, analyse and investigate all reported security incidents and policy breaches to develop improvements to prevent their reoccurrence.
5. **Cyber vulnerability trend** – Continuous improvement of security of all externally facing systems through a risk based vulnerability management program.
6. **Project engagement** – Ensure all projects engage Information security during the planning phase at a minimum.
7. **Awareness** – Deliver continual security awareness to staff.
8. **Procurement** – Purchasing decisions consider information security.
9. **ISMS Calendar** – An ISMS calendar is maintained which specifies when key actions must occur.
10. **Induction** – Newly hired staff complete an induction program that identifies their responsibilities for Information security and confidentiality.
11. **Compliance** – With legislative and regulatory obligations.

7 Policy

7.1 Hardware and software acquisition

CITO/CDIO endorsement must be obtained for all acquisitions (Capex and Opex) of:

- Computer Hardware
- Software
- Maintenance renewal
- Any mobile applications (apps) in excess of $50, or any app that holds client or staff sensitive information

7.2 Risk management process

Risk management is an essential part of an effective approach to information security. The DCJ approach to risk management is documented within the Enterprise Risk Management Policy. DCJ's enterprise risk team is actively involved in assisting DCJ cyber security with ensuring the risk framework is

applied in assessing cyber security risks, analysing cyber security risks, and addressing cyber security risks across DCJ.

Staff must consider cyber security risk in all of their activities including decision making. Should staff identify a risk they should raise it with their management and process it as per the Enterprise Risk Management Policy.

7.3 Non-compliance

The Information Security Management team is to be informed as soon as possible of any actual or suspected breach of this policy. Non-compliance or breaches of this policy, without an appropriate exception, will be investigated and misconduct escalated with Corporate Governance and Performance, which may result in disciplinary action in accordance with the DCJ Code of Ethical Conduct and NSW Government Personnel Handbook. Non-compliance or breaches may be reported to the IDS Service Desk on 02 9765 3999 (ex-FACS) or 02 8688 1111 (ex-Justice).

Alternatively, you may send an email to the Cyber Risk Audit and Compliance team (CRAC) via information.security@justice.nsw.gov.au

7.4 Procedures for requesting exceptions

Requests for exceptions must articulate an appropriate business case to justify deviation from a policy or standard. The business case should include relevant information such as the reason for the exception, a designated owner, a scope and a timeframe for the exception, mitigating or compensating controls to manage risk and a remediation plan to realign with the breached policy or standard.

Requests for exceptions are effected by completing a Security Policy Exception Request form. Exceptions must be approved by the information asset owner and the Chief Digital Information Officer and must be recorded in the exceptions register. Exceptions will be reviewed at the cessation of the exception period and will require re-approval should they need to be extended.

7.5 Management commitment to information security

Background verification checks on all candidates for employment, contractors, and third-party users must be carried out in accordance with relevant laws, regulations and proportional to the individual's proposed organisational role.

Newly hired staff are required to complete an induction program that identifies their responsibilities for Information security and confidentiality.

All staff are accountable and required to comply with the Information Security Policy and must ensure DCJ facilities, information or information processes will not be knowingly exposed to unacceptable levels of risk.

DCJ takes a top-down approach to information security by which the most senior executive layers of the organisation contribute to, review and approve the Information Security Policy. Updates are communicated to all staff to ensure they act in accordance with the policy. Staff awareness is maintained through appropriate training and communication.

The following information security groups provide DCJ staff with direction and support on information security matters:

- ICT Steering Committee – provides advice and guidance to the DCJ Senior Executive Committee on matters regarding ICT and information management.
- Audit and Risk Committee – supports the CISO and DCJ more broadly by considering cyber security, providing oversight and management of risks and audits, and ensuring DCJ meets its responsibilities. The risk registers inform internal audit planning.

7.6 Allocation of information security responsibilities

Responsibilities outlined below may be delegated but remain the responsible party remains accountable for them.

7.6.1 DCJ Executive Board

- Ensuring DCJ complies with the requirements of the NSW Cyber Security Policy and timely reporting on compliance with the Policy
- Assign overall responsibility for information asset protection and ownership.
- Approves policies as appropriate.
- Ensures DCJ develops, implements and maintains an effective information and cyber security plan.
- Determines DCJ's tolerance for security risks using the approved whole-of-government Enterprise Risk Management Policy.
- Appropriately resources and supports DCJ cyber security initiatives including training and awareness and continual improvement initiatives to support this policy.
- Ensures that staff are aware of and adequately comply with information security policies.

7.6.2 Chief Digital Information Officer (CDIO) / Chief Information Technology Officer (CITO)

- Works with DCJ's CISO to implement this policy.
- Supports the development of a cyber-security plan.

- Ensures that all staff, including consultants, contractors and outsourced service providers understand the cyber security requirements of their roles.
- Clarifies the scope of their responsibilities for cyber security relating to assets such as information, building management systems and IACS.
- Ensures a secure-by-design approach for new initiatives and upgrades to existing systems to ensure compliance with the organisations cyber risk tolerance.
- Ensures all their staff and providers understand their role in building and maintaining secure systems.

7.6.3 Chief Information Security Officer (CISO)

- Ensures that the Secretary of the department and information asset owners are informed of any significant information security issues and the status of the department's information security.
- Defines and implements a cyber-security plan for the protection of the DCJ's information and systems.
- Attends DCJ or cluster risk committee meetings as an advisor or member.
- Implements policies, procedures, practices and tools to ensure compliance with this policy.
- Represents DCJ on whole-of-government collaboration, advisory or steering groups established by the NSW Chief Cyber Security Officer (CCSO).
- Establishes training and awareness programs to increase staff's cyber security capability.
- Builds cyber incident response capability that links to DCJ's incident management and whole of government cyber response plan.
- Collaborates with privacy, audit, information management and risk officers to protect DCJ's information and systems.
- Provides independent assurance to the Chief Digital Information Officer and DCJ Executive on the appropriateness of security objectives and Information Security Policies, standards, processes, procedures, baselines and guidelines to effectively comply with the security objectives.
- Advises, coordinates and promotes security.
- Provides information security advice on new projects and initiatives.
- Establishes and provides security training and awareness programs, including guidance on but not limited to:

  - Classifying information and applying DLMs in accordance with the PSPF and NSW Guidelines;
  - Overclassification to mitigate risk of classification not being implemented or ignored;
  - Carriage, transfer, sharing or disposal of information in line with its security classification and management requirements;
  - Use of information within DCJ premises, away from DCJ premises, and when travelling overseas by applying appropriate security controls;
  - Levels of ongoing access permitted to security classified information for each level or security clearance;
  - Ensuring DCJ personnel are cognizant of the need-to-know principle; and
  - How DCJ personnel can report emergencies, breaches, or disclosures of sensitive or security classified information.
- Ensures compliance with government and regulatory information security related requirements.
- Produces technical security risk assessments and recommendations.
- Maintains an executive level information security forum to ensure the ISMS meets the expectations of the organisation.
- Assists to ensure that the risk framework is applied in assessing cyber security risks and assist with setting of risk appetite.

7.6.4 Manager, Risk Audit and Compliance

- Reports to the Chief Information Security Officer.
- Operational effectiveness of information security controls.
- Risk, Audit and Compliance team responsibilities.
- Coordination of the department's ISMS.
- Development of information security policies, procedures and controls.
- Manage, maintain and measure Information Security Policy standard and process compliance.
- Measure the effectiveness and maturity of information security controls.
- Identify and manage information security improvements.
- Maintains a management level information security forum to ensure the ISMS meets the expectations of the organisation.

7.6.5 Manager, Cyber Security

- Reports to the Chief Information Security Officer.
- Operational effectiveness of cyber security controls.
- Cyber team responsibilities.
- Management of information security incidents and investigations

7.6.6 Information asset owners (service owners and information owners)

An information asset's owner is responsible for applying the relevant sensitive or security classification to systems under their control. To do this they must assess the Business Impact Level (BIL) based on the likely damage if the information's confidentiality was compromised. The owner remains responsible for controlling the sanitisation, reclassification or declassification of that information.

- Ensure that appropriate security, consistent with the policy, is implemented.
- Appropriately classify official information assets and apply the lowest level of sensitivity or security classification practicable[1].
- Appropriately sanitise, reclassify, or declassify information assets in line with the classification requirements as prescribed by the *State Records Act 1998*.
- Determine access privileges, and ensure they have the appropriate security clearance required to access the information.
- Apply appropriate DLMs through text-based or colour-based protective markings.
- Appropriately use information within DCJ premises, away from DCJ premises and when travelling overseas by applying appropriate security controls.
- Facilitate regular risk reviews of their information assets with a view to identify any potential risks and assess the controls in place to protect assets. This should be done with the assistance of RAC.
- Regularly review risks and threats which impact their information assets and ensure they are mitigated or escalated appropriately.

[1] *Information asset owners should balance the needs and expectations of DCJ, the wider government and community to protect information and ensure appropriate access. Over classification of information can result in access to information being unnecessarily limited or delayed, increased administrative time and costs, and classifications being devalued or ignored. Security classifications must also not be applied as an effort to restrain competition, hide violations or inefficiencies of legal or administrative processes, or prevent or delay the release of information that does not need protection.

- Ensure security breaches or near misses affecting their information assets are reported to CRAC for investigation, including any inadvertent disclosures or compromises of sensitive and security classified information.
- Maintain business continuity plans and disaster recovery plans.
- Engage CRAC and participate in identifying the information security requirements of their information assets.
- Update auditable registers with holdings for SECRET and TOP SECRET information.
- Ensure that security requirements are incorporated into the design, operation and management of information systems. Appropriately store, carry, transfers, share or dispose of information in line with its security classification and management requirements.
- Ensure that any OFFICIAL: Sensitive information created is managed in accordance with the Information Protection Principles.
- Participate in activities that monitor the effectiveness of cyber security for their systems as needed, including internal and external audits, KPI and SLA reporting, and ISMS management activities.

7.6.7 Custodians

A custodian is a person/s that is delegated responsibility over information by the information asset owner. Custodians are users required to maintain, operate, and implement technology solutions.

- Have responsibility of maintaining and operating the information asset on behalf of the business/information owner.
- Have ‘custody’ of assets, not necessarily belonging to them, for limited time (e.g. network administrators and operators).
- Implement access requirements as requested by the information asset owners.
- Detect and report on security violation attempts (review and monitoring).
- Approve, reject, remove and review system privileges on a timely basis, to reflect user movements, absences, terminations and investigations.
- Maintain a proactive approach to ensuring the security of the system for which they are responsible is kept at the highest possible security level.
- Ensure that changes to system(s) are appropriately tested.

7.6.8 Business Centre Managers

- Ensure that new employees receive appropriate instruction regarding their information security responsibilities during induction.
- Ensure that verification checks on employees (including contract employees) are completed prior to commencement, particularly where the role being filled involves handling highly classified information or exercises significant authority.
- Ensure that contract employees sign an appropriate confidentiality agreement prior to commencement of their employment.
- Advise the relevant system administrators of any access changes that are required as a result of employee terminations, transfers or role changes.
- Recovery of all access cards, keys and tokens from terminated employees (including contract employees).
- Appropriate escalation of security incidents, breaches, and weakness of which they are notified.
- Authorise and issue guidance on the use of removable media within their business centre.

7.6.9 Users

- A user is any staff or other authorised person who uses information in the course of daily business activities.
- Use and preserve assets' security by adhering to security policies.
- Are aware of their responsibilities.
- Comply with the requirements of these policies, standards and guidelines.
- Report violations or suspected violations of these policies in a timely manner.
- Maintain confidentiality of operating system and application passwords.
- Use information and information resources for responsible and authorised purposes.
- Must not disclose information publicly or to unauthorised parties without the approval of a Director or above.
- Contract employees (staff) must sign a formal undertaking concerning the need to protect the confidentiality of the department's information, both during and after contractual employment with the department.

7.6.10 Security operations

- Implement security to meet operational business needs.
- Operate/administer IT security and adhere to the security policy.
- Maintain a functional information security forum to co-ordinate information security practice and reporting.
- Respond to security incidents.
- Maintain and manage vulnerability management and penetration testing programs.
- Securely managing the provision of user access to the department's information systems as approved by the business centre manager (or delegate).
- Monitor system/security logs for evidence of unauthorised activity.
- Report potential, suspected and actual security breaches to the Manager, Cyber Security.
- Assisting the Manager, Cyber Security in investigation of potential, suspected and actual security breaches.

7.7 Segregation of duties

Where practicable, approval and execution duties should be separated to prevent unauthorised access or misuse of information assets. Where this delineation is not controlled or the opportunity for collusion is high, auditing and alerting should be implemented in order to monitor these scenarios.

7.8 Contact with authorities

Every contact involving authorities about an information security incident or problem, where possible, should be initiated by a member of the Cyber Security team, legal team, or a DCJ executive.

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers, information security providers and telecommunications operators must be maintained.

7.9 Awareness

All staff are required to complete the appropriate level of information security awareness training. The training is targeted at three categories of employees:

- All DCJ employees and contractors who are directly employed by DCJ

- DCJ employees who either manage and/or support DCJ ICT infrastructure and systems, or are responsible for identifying and/or managing risks for their business area
- DCJ executives (Band 1 and higher)

Management are responsible for ensuring that their staff complete all mandatory information security training.

From time-to-time security management may post security advisories. These advisories will be communicated to staff who should remain aware of the information security changes, consider the advice provided and apply it where practical.

7.10 Identification of applicable legislation and contractual requirements

All applicable legal, statutory, contractual, or regulatory requirements must be documented and defined. Specific requirements and responsibilities for controls or other activities related to these legal regulations must then be delegated to the appropriate business unit.

7.11 Independent review of information security

External independent auditors will be engaged by DCJ on an annual basis or more frequently as required to validate security controls in line with the Audit Management Standard.

Findings of these reviews must be tabled in an audit register with an owner, a remediation plan and management commitment.

7.12 Technical compliance review

At regular intervals technical compliance reviews should be conducted to ensure services are compliant with Information Security Policy and standards. Technical findings must be recorded in the DCJ audit register, an owner identified, a remediation plan constructed and management commitment defined.

8 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

9 Related legislation, regulation and other documents

This policy aligns with the NSW Cyber Security Policy.

Compliance to the above supports the intentions of:

9.1 Commonwealth

- *Electronic Transactions Act 1999*
- *Electronic Transactions Amendment Act 2011*
- *Copyright Act 1968*
- *Cybercrime Act 2001*
- *Telecommunications (Interception and Access) Act 1979*
- *SPAM Act 2003*
- *Privacy Act 1988*
- *Crimes Act 1914*

9.2 NSW

- *Crimes Act 1900*
- *Government Sector Employment Act 2013*
- *Independent Commission Against Corruption Act 1988*
- *Privacy Amendment (Enhancing Privacy Protection) Act 2012*
- *Public Finance and Audit Act 1983*
- *Privacy and Personal Information Protection Act 1998*
- *Health Records Information Privacy Act 2002*
- *Government Information (Public Access) Act 2009*
- *State Records Act 1998*
- *Workplace Surveillance Act 2005*

10 Document information

Document name	Information Security Policy
Document reference	D22/1832018
Replaces	Information Security Policy V2.2
Applies to	All of DCJ with the exception of Judiciary and NCAT Board members
Policy administrator	Chief Information Security Officer
Approval	Deputy Secretary, Corporate Services
Approved date	28/09/2023

11 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance Information and Digital Services Corporate Services
Email	SecurityPolicy@facs.nsw.gov.au

If you need assistance identifying when you need to engage information security, please see **Appendix – Engaging information security.**

12 Version and review details

Version	Effective date	Reason for amendment	Due for review
2.2	29/06/2022	Annual review due	29/06/2023
3.0	28/09/2023	Annual review	28/09/2024

13 Appendix – Engaging information security

The following questionnaire can be used to help you determine when you need to engage Cyber Risk Audit and Compliance team.

- Do you believe your password has become known to another party?
- Do you believe your computer has been infected with Malware?
- Have you just received a scam email?
- Have you seen something that breaches the Information Security Policy and need to report it?
- Do you need a security investigation carried out?

If you answer yes to any of the above, please use the following contact points:

- For urgent security incidents outside the business hours 8:30am – 4:30pm, please call 1300 325 29237 (1300 DCJ CYBER)
- For urgent security incidents, please email security.incident@justice.nsw.gov.au
- For all other security inquiries please email information.security@justice.nsw.gov.au

- Are you running or involved with a project which is implementing, updating or removing an ICT component?
- Are you running or involved with a project which has the potential to impact the confidentiality, integrity or availability of DCJ information, services or assets?
- Are you procuring a service from a third party which sees DCJ information being stored, used, created or processed by the third party?
- Are you sharing DCJ information with a non-DCJ party?

If you answer yes to any of the above or related legal advice, please email:

- **CRAC:** Securityarchitecture@facs.nsw.gov.au
- **Legal:** infoandprivacy@justice.nsw.gov.au