Forestry Corporation

Policy

Title	Data Breach Policy	**Version**	1
Policy No.	P 2026/08	**Effective date**	25/08/2026

Acknowledgment of Country

Forestry Corporation of NSW acknowledges the traditional custodians of the land on which we live and work, and pay our respects to Elders past, present and future.

1. PURPOSE

This policy outlines how Forestry Corporation (FCNSW) will manage and report eligible data breaches involving personal information or health information and is prepared to support compliance with the Mandatory Notification of Data Breach Scheme (MNDB Scheme) established under Part 6A of the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

2. BACKGROUND

FCNSW has established a full set of privacy and data breach policies, procedures and plans to support staff in understanding their responsibilities in managing personal and health information. Under the MNDB scheme FCNSW is required to prepare and publish a Data Breach Policy for managing breaches under the PPIP Act.

3. SCOPE

This Policy applies to all employees, contractors and service providers of FCNSW who handle personal information or health information.

This policy applies to eligible data breaches involving personal information or health information held by, or on behalf of, FCNSW, including eligible data breaches that occur:

- Within FCNSW
- Between FCNSW and another public sector agency; or
- Through unauthorised access to information by an external person or entity.

The policy does not apply to data breaches that:

- Do not involve personal or health information; or
- Are not likely to result in serious harm to an individual.

4. DEFINITIONS

Term	Meaning
Eligible Data breach (EDB)	An incident in which there has been unauthorised access to, unauthorised disclosure of, or loss of, personal or health information held by (or on behalf of) FCNSW and the data breach is likely to result in serious harm to an affected individual. This may include financial loss, fraud, physical or emotional harm or reputational damage.

Personal information	Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
Health information	Information or an opinion about an individual's health, disability, health services or other matters protected under applicable health privacy legislation.
Affected individual	An individual to whom the personal information or health information involved in a data breach relates.

5. ROLES AND RESPONSIBILITIES

Role	Responsibility
CEO	▪ Carrying out all responsibilities to meet the obligations imposed on the organisation under the Mandatory Notification of Data Breach Scheme.
Data Breach Response Team (DBRT)	▪ Support the CEO in responding to, assessing and containing a suspected data breach.
Privacy Officer	▪ Implementing this DBP. ▪ Coordinates the DBRT on the assessment and management of suspected data breaches and notification decisions
Managers	▪ Ensuring staff report suspected data breaches promptly to the Privacy Officer and supports the containment, assessment and mitigation activities.
All staff, contactors or third party providers	▪ Handle personal information and health information in accordance with relevant Acts and FCNSW Privacy Policy. ▪ Immediately report suspected or actual data breaches to their Manager or direct to FCNSW Privacy Officer.

6. WHAT IS A DATA BREACH

Unauthorised access to, unauthorised disclosure of, or loss of, personal or health information held by (or on behalf of) FCNSW or any accidental or unlawful destruction or alteration of personal or health information held by (or on behalf of) FCNSW. A suspected data breach will be classified as an 'eligible data breach' if the unauthorised access to, or unauthorised disclosure is likely to cause or likely to result in serious harm to an individual.

Data breaches may be deliberate or due to human error or accident and can include data put at risk by cyberattacks, ransomware, spear phishing, malware, system and process failure, employee mistakes, deliberate misconduct, lost or stolen devices and other risks.

7. REPORTING AND RESPONDING TO A DATA BREACH

FCNSW will undertake five key steps in responding to a data breach:

- Initial report
- Contain the breach
- Assess the breach to determine if the breach is an Eligible Data Breach
- Mitigate
- Notify and communicate
- Review to prevent future breaches

FCNSW Data Breach Response Plan details how each of these steps is managed.

8. ASSESSMENT OF SUSPECTED ELIGIBLE DATA BREACHES

Where there are reasonable grounds to suspect that an eligible data breach may have occurred, the agency will conduct an assessment as soon as practicable and, where required, within the timeframe set by the Privacy and Personal Information Protection Act 1998 (NSW). The assessment will consider the type and sensitivity of information involved, the circumstances of the breach, whether the information is protected by security measures, the likelihood of unauthorised access or disclosure, the persons who may have obtained the information, and the nature and seriousness of potential harm to affected individuals.

The assessment of a suspected or actual data breach including any reasonable steps that can be implemented to mitigate any harm will be undertaken by FCNSW DBRT within 30 days of the date FCNSW became aware of a suspected data breach.

9. NOTIFICATION OF ELIGIBLE DATA BREACH

If it is determined that an eligible data breach has occurred, FCNSW will notify the Privacy Commissioner and affected individuals as soon as practicable, unless an exemption applies (under Part 6A, Division 4 of the PPIP Act). The notification will include the information required by the MNDB Scheme, including:

- a description of the breach
- recommended steps affected individuals should consider taking
- information about making a privacy complaint to the Privacy Commissioner

10. TRAINING AND CONTROLS

All employees are provided with privacy awareness and cyber security training and are required to complete code of conduct training.

FCNSW has in place a Cyber Security Portal which provides employees with easy access to IT security policies, security awareness training, current alerts, advice on how to protect information and report a cyber incident. The portal also links to other relevant sites, including FCNSW Privacy site.

11. RECORD KEEPING

FCNSW will keep a record of data breaches including a data breach register which will contain all information required by law and the MNDB Scheme. The register will be maintained securely and reviewed to identify trends, risks and opportunities to improve privacy and information security practices.

A record of the Data Breach Response Report completed by the Data Breach Response Team for each suspected EDB will also be maintained in FCNSW records management system. The Data Breach Response Report is an important tool to identify potential areas for improved data and privacy management.

12. LEGISLATION AND COMPLIANCE OBLIGATIONS

- *Privacy and Personal Information Protection Act 1998 (NSW)*
- *Government Information (Public Access) Act 2009 (NSW)*
- *Health Records and Information Privacy Act 2002 (NSW)*

13. RELATED FCNSW POLICIES AND DOCUMENTS

- Privacy Policy
- Code of Conduct Policy
- Records & Information Management Policy
- Information Security Policy
- User Access Management Control Policy

- Privacy Management Plan
- Privacy Manual
- Data Breach Response Plan

14. REVISION HISTORY

Version	Author	Summary of changes	Approver	Approval date
1	Privacy Officer	New policy	Executive Leadership Team	25/8/2026

Anshul Chaudhary
Chief Executive Officer