|  |  |
| --- | --- |
| Policy No: 3.14 | Policy Name: **Cyber Security Reporting to DCJ** |

|  |  |
| --- | --- |
| Applies to: | Version: |
| Specific responsibility: | Date Approved: |
|  | Review Date: |

# Purpose

The purpose of this policy is to provide clarity in relation to how [Service Name] will respond if an information security incident occurs that impacts the privacy rights of clients accessing [Service Name].

This policy applies to all [Service name] staff members, students, volunteers and Board members. This policy has been developed based on information provided by the Department of Communities and Justice (DCJ).

# Policy statement

[Service Name] holds private information about clients and families who access our services. Information security incidents could be the result of hacking of [Service Name] ICT system or data theft, or the result of human or technical error or misadventure.

If a data breach occurs, [Service Name] is required to notify DCJ and keep them informed of progress until its resolution.

This policy should be reviewed along with the Notifiable Data Breach policy.

# References

Office of the Australian Information Commissioner

Privacy and personal Information Protection Act 1998

Health Records and Information Privacy Act 2002 (NSW)

Privacy Act 1988

Government Information (Public Access) Act 2009

Information Security Policy Department of Communities and Justice (15 February 2021)

# Definitions

Nil

# Procedure

## What is an information security incident?

Information security incidents could be the result of hacking of [Service Name] ICT system or data theft, or the result of human or technical error or misadventure. Some examples of information security incidents are:

* Deliberate interference with, or unauthorised accessing or electronic or physical records
* Loss of electronic and/or physical records as a result of a fire or flood
* Theft or loss of mobile storage devices such as a USB or laptop
* An email involving client information sent to the wrong person
* Unauthorised staff accidently or deliberately accessing restricted documents
* Someone from [Service Name] improperly sharing, or providing access to, sensitive information with a third party.

As soon as [Service Name] becomes aware of an information security incident, you are expected to:

* Notify DCJ and other relevant state and Commonwealth agencies
* Correct, contain or mitigate any loss of data
* Manage any media response required
* Inform and support any individuals or organisations directly affected
* Seek support and guidance from DCJ if required
* Cooperate with any direction provided by DCJ
* Implement remedial actions recommended by DCJ and any other state or Commonwealth agency you may have informed of the incident

If a requirement stated in this policy conflicts with a provision specified in your contract with DCJ, then the contract provision overrides that requirement.

## Step 1: Notify DCJ of an actual or suspected information security incident

The nature of the incident and the potential impact on DCJ clients and systems determines who and when to contact DCJ.

For malicious cyber-attacks on your ICT systems involving personal client information

If your organisation identifies a cyber-attack is in progress, or has occurred in your ICT systems:

* **Immediately** notify DCJ by completing the online notification form <https://www.onlineforms.dcj.nsw.gov.au/ics/Pages/Cyber-Security-Incident-Form.aspx> . This point of contact is monitored 24/7 by the DCJ Information Security Team.
* **Follow up on the online notification** with an email or letter to your DCJ contract manager **no later than the next business day**. If your organisation holds multiple contracts with DCJ, notify your lead DCJ contract manager.

A representative of the DCJ Information Security Team will contact your organisation to ascertain details of the incident.

For other incidents involving loss of client data or confidential program information

When your organisation detects any of these types of incident, **call and email your DCJ contract manager by the next business day.** If your organisation holds multiple contracts with DCJ, notify your lead DCJ contract manager.

## Step 2: investigate the information security incident and notify DCJ of early findings

**Within 48 hours** of notifying DCJ, you are required to undertake an early investigation of the information security incident and notify your lead DCJ contact manager of the findings in writing. You can use the DCJ Information Security Incident Report <https://www.facs.nsw.gov.au/download?file=800660> to satisfy this requirement, or to help guide your organisation’s own version of the report.

Your report of the early investigation and its findings must include:

* A description of the incident and its potential consequences
* Details of lost or potentially compromised client information / data
* Actions you have taken or planned to manage or remedy the information lost or compromised
* Any actions required to ensure any disruption to ongoing service is minimised.

## What happens after you notify DCJ?

Your lead DCJ contract manager will inform DCJ internal stakeholders about the information security incident, so that DCJ can manage any issues and risks in consultation with your organisation’s stakeholders. What you need to do and the actions we take will depend on the nature and seriousness of the incident.

If the incident is serious and involves a cyber attack or breach of your organisation’s ICT systems, DCJ may have to temporarily restrict your access to DCJ’s electronic systems.

In serious cases, DCJ may actively work with you to manage the incident. This is likely if the incident involves cyber attack or loss of client records due to theft, fire or flood. If other DCJ stakeholders need to contact you to obtain further information or to provide assistance, it will be done in consultation with your lead DCJ contract manager.

If client data is involved, your lead DCJ contract manager will work with your organisation to decide on the appropriate action to be taken to inform the clients affected.

For serious incidents, DCJ may documents the remedial actions required in a formal improvement plan which DCJ will work on with you to develop. In less serious cases, DCJ may agree to an informal plan of improvements to your information security and monitor your progress at regular contract meetings.

# Related documents

Notifiable Data Breaches Policy

# Review

|  |  |  |
| --- | --- | --- |
| **Reviewing and approving this policy** | | |
| Frequency | Person responsible | Approval |
| [How often will this policy be reviewed] | [Position of person responsible for reviewing policy] | [position of person/group who approves this policy] |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy review and version tracking** | | | |
| Review | Date approved | Approved by | Next review date |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |