Incident report process – Administering Institutions

National Health and Medical Research Council (NHMRC)
Version: 1.0

Document information

Issue Date	Version	Author	Organisation	Comments
17/06/2026	1.0	ITSA	NHMRC	

Contents

Introduction

Purpose

Protective Security Policy Framework (PSPF) requires Australian agencies to report cyber incidents to Australian Signal Directorate (ASD). Administering Institutions have cyber security incident (cyber incident) and data breach reporting requirements under the NHMRC Funding Agreement.

Under the Funding Agreement clause 4.7 and 4.8, it is stated that the Administering Institution must advise NHMRC of any cyber security incident or data breach (types of incidents to be reported are provided in the Data Spill Management Guide of the Information Security Manual from the Australian Cyber Security Centre (ACSC)) as soon as possible after they occur or as the Administering Institution is made aware of the incident or data breach where the incident involves NHMRC funded Research Activities or management of Research Activities.

Administering Institutions that experience a cyber incident, should report the incident to NHMRC. This document outlines the incident response process for reporting and notifying NHMRC and Administering Institutions in the event of a cyber incident.

Scope

This document defines the process of reporting, actions and escalation paths for institutions and NHMRC, in the event of a cyber incident.

Incident response playbook, operational, workplace, technical and internal incident activities are out of scope of this document.

Incident reporting process

Definition

An incident is defined as an unplanned event that disrupts, or has the potential to disrupt normal operations, services, or security within an organisation. It may affect systems, people, processes, or information and typically triggers investigation, management, or mitigation actions. In cyber security, an incident refers to a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices.

Cyber security incidents

Events that threaten confidentiality, integrity, or availability of information and systems including but not limited to:

- malware and ransomware
- phishing or credential compromise
- unauthorised access

- data breach or leak
- Denial-of-Service (DoS/DDoS) attacks
- loss of sensitive data
- improper data handling or data storage
- unauthorised disclosure
- supply chain cyber incidents.

Incident classification

Incidents are classified by impact and urgency. All cyber incidents must be classified across the following dimensions:

1. Impact: Extent of business or organisational effect
2. Urgency: Time sensitivity of response
3. Priority: determined based on impact and urgency.

Impact levels

Impact reflects the severity of business or organisational consequences.

Level	Description
Critical	Organisation-wide impact, major service outage, significant security or safety risk, or high legal/reputational exposure.
High	Multiple business areas affected, serious service degradation, or credible external impact.
Medium	Limited to a team or system, manageable impact, workaround available.
Low	Minimal disruption, isolated issue, no significant business impact.

Urgency levels

Urgency reflects the required speed of response or escalation.

Level	Description
Immediate	Requires immediate action to prevent severe impact or escalation.
High	Requires prompt action within hours.
Medium	Action required within the same business day.
Low	Action can be scheduled within normal business timeframes.

Priority matrix

Priority is determined using the following matrix.

Impact \ Urgency	Immediate	High	Medium	Low
Critical	P1 – Major	P1 – Major	P2 – High	P2 – High
High	P1 – Major	P2 – High	P2 – High	P3 – Medium
Medium	P2 – High	P3 – Medium	P3 – Medium	P4 – Low
Low	P3 – Medium	P4 – Low	P4 – Low	P4 – Low

Response expectations for priority levels

Priority	Description	Response expectations
P1 – Major Incident	Critical impact or high-risk event affecting core services, security, or safety	Immediate escalation, coordinated response,
P2 – High	Significant impact requiring urgent management	Rapid triage and escalation to appropriate teams
P3 – Medium	Moderate impact with controlled scope	Managed through standard incident processes
P4 – Low	Minor or isolated issue	Managed through routine operational support

Reporting process

Administering Institutions are required to notify NHMRC of all cyber incidents that affect digital assets. NHMRC's Cyber team will assess the incident and engage with the institution as required.

Any cyber incident reported to an NHMRC team, must be promptly escalated to the Cyber or IT Security Advisor (ITSA) teams, ensuring that all information is shared.

Incident information shared between agencies must be treated as classified and handled on a need-to-know basis. It must not be disclosed or discussed in a way that could adversely affect any agency's operation or reputation. Disclosure should be limited to NHMRC, the affected Administering Institution, ASD, AFP, and any other approved escalation points with formal approval of the accountable authority (the agency's Chief Security Officer (CSO) or CEO).

Escalation principles

The following principles apply to all cyber incidents under this process:

- Incidents must be reported as soon as practicable once actual or potential impact is identified.
- Escalation must not be delayed pending full technical investigation where there is a reasonable likelihood of impact.
- All parties must provide timely updates as new information becomes available.
- If severity increases, the incident must be reclassified and escalated further as required.

Reporting pathways

Notification submissions can be completed through the following pathways:

1. Contact the Cyber team directly: cybersecurity@nhmrc.gov.au
2. Contact NHMRC's Research Help Centre: help@nhmrc.gov.au

The initial notification should include, where available:

- incident title or short description
- date and time detected
- affected system, service, process, or dataset
- known or suspected impact
- whether the incident is ongoing
- whether sensitive, personal, or research-related data is involved
- Administering Institution contact officer and escalation contact.

Reporting timeframes

All Administering Institution Incidents should be reported as soon as practicable prior to public announcement from the Administering Institution and, where feasible, within 48 hours to 7 calendar days of incident identification.

Roles and responsibilities

Administering Institutions are responsible for:

- identifying and reporting cyber incidents
- undertaking initial triage and containment within their own environment
- assessing the incident's impact

- reporting incidents to NHMRC as soon as practicable
- nominating appropriate operational and technical contacts
- continuing to provide updates until the incident is resolved.

Administering Institutions remain responsible for managing incidents within their own environment unless and until the matter requires coordinated cross-party response.

NHMRC's Research Administration team is responsible for:

- Receiving incident notifications from Administering Institutions; supporting incident triage and escalate to ITSA/Cyber and CSO/Chief Information Security Officer (CISO)
- Ensuring NHMRC's Research Administration team is engaged where communication with other agencies is required
- Ensuring the Cyber team is engaged where the incident has actual or potential information security, cyber security, privacy, or data protection implications

The Cyber team is responsible for:

- Assessing the reported incident and advising on follow up actions as required based on incident impact, severity, containment actions, evidence preservation, and escalation requirements
- Providing specialist triage, investigation, containment, and response for cyber security and information security incidents
- Supporting NHMRC's CISO and CSO in communication with other Administrative Institutions as required
- Recommend escalation, containment measures, and additional notification actions where a cyber security risk is identified.