Cyber Security Incident Management Procedure

Section 1 - Introduction

Purpose

(1) This document describes the University's procedure for handling cyber security incidents.

(2) While cyber security incidents are managed by personnel in incident response roles, all users of the University's digital assets have a responsibility to:

a. minimise the risk of sensitive and important information being lost or falling into the hands of unauthorised persons;
b. protect digital assets on which sensitive and important information is stored, processed, or communicated; and
c. promptly report suspected or actual cyber security incidents to the Cyber Security team via dts-cybersecurity@newcastle.edu.au, or via Service Catalogue – DTS.

Scope

(3) This procedure addresses the four phases of cyber incident response which are preparation; detection and analysis; containment, eradication, and recovery; and post-event activity.

(4) This procedure sits within the University's incident management hierarchy, which includes the following documents:

a. Cyber Security Incident Management Procedure (this document);
b. Digital Technology Solutions (DTS) Incident Management Process;
c. DTS Critical Incident Management Guide; and
d. Business Continuity Management Policy and Business Continuity Management Framework.

Audience

(5) All University staff, students, volunteers, vendors, and members of advisory and governing bodies, in all campuses and locations of the University and at all times while engaged in University business or otherwise representing the University.

Definitions

(6) In the context of this document the following definitions apply:

a. Event means an identified exception to the normal operation of infrastructure, systems, or services. Not all events become incidents.
b. Cyber security incident means an adverse event that poses a risk to the confidentiality, integrity or availability of a digital asset, or is a violation of explicit or implied University policy, standard, or code of conduct.

c. Incident Lead means a member of the Cyber Security team who is assigned operational responsibility for the management of a cyber security incident.
d. Incident Communications Lead refers to the person responsible for communications during a major or significant incident.
e. Critical infrastructure means any asset or data identified as being subject to the requirements of the Security of Critical Infrastructure Act 2018.

Common Types of Cyber Security Incidents

(7) Common types of cyber security incidents are described in Table 1.

Table 1 – Common Types of Cyber Security Incidents

Incident Type	Description
Compromised credentials	A password used to login to University systems is reported in an online breach or suspected of compromise.
Unauthorised access	Any unauthorised access to the University's network, systems or services.
Denial of Service (DoS) and Distributed Denial of Service (DDoS)	A system or service is overwhelmed with traffic to the point where the system or service is unavailable. This can occur maliciously or due to inadequate capacity planning.
Phishing	Deceptive messages are received by staff or students, with the intent to elicit personal information or sensitive information about the University or send malware.
Ransomware	A type of malware used to lock or encrypt victims' files until a ransom is paid.
Malware	Installation of malicious software such as a virus, worm, Trojan horse, or other code-based malicious entity on a digital asset.
Data breach	Unauthorised access and disclosure of information.
Improper use of digital assets	Any actions that violate the Digital Technology Conditions of Use Policy including: - sharing corporate or sensitive information with unauthorised persons; - using University assets to undertake illegal activities; - downloading forbidden software such as crypto miners and network monitoring tools; - using unapproved virtual private networking (VPN) services or network anonymisers; and - making unauthorised changes to the configuration of digital assets.
Loss or theft of device with University data	A physical device used to undertake University work is lost or stolen, including personal devices used to access University email services.

Section 2 - Relationship with Digital Technology Solutions and Critical Incident Management

(8) The following clauses describe the relationship between cyber security incident management and Digital Technology Solutions (DTS) and critical incident management.

DTS Incident Management

(9) The DTS Incident Management team is responsible for incidents causing a significant deterioration, degradation, or disruption to a digital service or asset.

(10) The Cyber Security team is responsible for cyber security incident management, which runs in conjunction with the DTS incident management process.

(11) If, during a standard DTS incident investigation, DTS staff suspect that an outage or service disruption is cyber security-related, the Cyber Security Incident Management Procedure is triggered.

(12) If it is determined that an incident is not cyber security-related, the Cyber Security team will discontinue its participation in the DTS incident response process.

Critical Incident Management

(13) Major and significant incidents require immediate escalation to the Incident Communications Lead, who is responsible for the DTS Critical Incident Management process.

(14) The DTS Critical Incident Management process interfaces with the University's business continuity process should an incident require such escalation.

(15) Significant incidents impacting critical infrastructure as defined by the Security of Critical Infrastructure Act 2018, must be reported to the Australian Cyber Security Centre (ACSC) within 72 hours of detection by the Chief Information Security Officer via cyber.gov.au.

(16) Data breaches affecting privacy and personal information as defined by the NSW Privacy and Personal Information Protection Act 1998, must be reported by the Chief Information Security Officer or a staff member of the Privacy Team so that an assessment of harm, and where necessary, notification to affected individuals and the IPC/OAIC can occur.

Section 3 - Cyber Security Incident Management Process

(17) Cyber security incident response has four phases that comprise the following activities:

a. Preparation: ensuring policies, communications plans, and technologies required for incident response are available and accessible.
b. Detection: identifying and confirming that an incident has occurred, categorising the impact of the incident and prioritising response activities.
c. Containment, eradication and recovery: minimising the impact of the incident using a containment strategy and recovering systems and data.
d. Post-incident activity: assessing the response to the incident and preparing an incident closure report that contains lessons learnt, and the actions taken to prevent similar incidents from occurring in the future.

(18) The University's Information Classification and Protection Policy should be considered when communicating sensitive information during all phases of an incident.

(19) To assist with the technical aspects of an incident, the Incident Lead may seek advice from external organisations such as the Australian Cyber Security Centre (ACSC), Australian Signals Directorate (ASD), Australian Security and Intelligence Organisation (ASIO), AusCERT, CERT Australia, vendors, and service providers.

(20) If an Incident Lead communicates with external parties, the Traffic Light Protocol (TLP) should be used. The TLP is an industry standard for sharing sensitive information.

(21) The University's data classifications broadly align with the TLP, as shown in Table 2.

Table 2 – TLP Classifications and University Data Classifications

University Data Classification	TLP Classification
Highly Restricted	RED
Restricted	AMBER
X-in-Confidence	GREEN
Public	WHITE

Phase 1: Preparation

(22) The initial phase involves preparing personnel who hold incident response roles and making tools and resources available for use during an incident.

Preparing to handle an Incident

(23) Preparation activities that enable the Incident Lead to respond to an incident include:

a. Policies. The University's Digital Security Policy, Digital Technology Conditions of Use Policy, Business Continuity Management Policy, Business Continuity Management Framework, Privacy Management Framework and Risk Management Framework must be up-to-date and be readily available for use.
b. Stakeholder notification. If incidents are prioritised as major or significant, the Incident Lead must immediately send a notification to relevant stakeholders in accordance with the Information Technology Services Critical Incident Management Guide and the University's Business Continuity Management Framework.
c. Technology. Technology to support the cyber security incident management must be available during an incident. This may include a laptop, a mobile internet connection (if network access is impacted), and access to copies of software and documents, such as policies and guidelines.
d. Training. Annual training is provided to personnel in incident response roles on their responsibilities, duties, and protocols to follow during an incident.

Phase 2: Detection and Incident Analysis

(24) A cyber security incident begins when a cyber security-related event is reported. Events are reported through a range of channels including an automated system diagnostic, an incident ticket submitted to the DTS Service Desk, or an email sent to the Cyber Security team.

(25) The following steps are undertaken as part of incident detection and analysis:

a. The identified cyber security event is assigned to an Incident Lead.
b. The Incident Lead performs an analysis to determine if a cyber security incident has occurred and assigns a status to the incident (see Table 3).
c. The Incident Lead assesses the potential impact of the incident to the University using the University's Risk Management Framework.
d. Based on the risk assessment, the Incident Lead determines the Incident Category (see Table 4) and associated Incident Priority (see Table 5)
e. If an incident is of a 'Major' or 'Significant' category, the incident is assigned to the Incident Lead for management (as per the DTS Critical Incident Management Guide).
f. If an incident involves a breach of personally identifiable information (PII) or protected health information (PHI), the Incident Lead escalates the incident to the Chief Digital & Information Officer for referral to the University's Privacy and Rights to Information Manager.

Table 3 – Incident Status

Status	Description
Confirmed	Event/incident analysis activities confirm that an incident has occurred, and a response is underway.
Disposition	**Reason**
Unidentified	Event/incident analysis activities are unable to locate an incident. The incident is deemed Resolved-Unidentified.
Transferred	Event/incident analysis activities confirm that an incident occurred and the incident is transferred to another business unit for further investigation or action.
Deferred	Event/incident analysis activities confirm that an incident occurred however incident response activities are deferred due to the low impact of the incident or due to resource constraints. Critical and High priority cases cannot be deferred without approval from the Chief Digital & Information Officer.
False Indicator	Event/incident analysis activities show that the indicators of the incident were false positives.
Misconfiguration	Event/incident analysis activities show that the event was caused by system misconfiguration or malfunction.
Duplicate	Event/incident analysis activities show that the incident is a duplicate of another record in the Service Desk and is merged with the existing workflow.

Table 4 – Incident Category

Incident Category	Impact	Examples
Major	An incident affecting the entire University.	-Substantial, possibly wide-ranging, actual or potential damage to the confidentiality, integrity or availability of the University's digital assets. - An incident that impacts the availability of perimeter security infrastructure. - Bulk exposure of PII, PHI or intellectual property (IP) into the public domain, where such exposure results in compliance and/or reputational consequences.
Significant	An incident affecting multiple facilities, user groups or campuses.	- Contained actual or potential damage to the confidentiality, integrity or availability of the University's digital assets. - More than 10% of users are unable to access or use digital assets. - Exposure of a small amount of confidential or sensitive University information, PII, PHI or IP into the public domain or to an unauthorised individual.
Escalated	An incident affecting a facility or campus.	- Malware incident that does not fall into a higher severity. - Loss of data that does not include PII or PHI. - Phishing campaign that impacts more than 100 users.
Normal	Minor incident	- Incidents resulting in some localised inconvenience. No significant impact to the University.

(26) Each Incident Category has an associated priority level. The Incident Priority reflects the timeframe for communicating with relevant stakeholders and for containing the incident. Incident priority levels are described in Table 5.

Incident Category	Incident Priority	Notification Timeframe*	Containment / Remediation Timeframe	Stakeholders to notify
Major	1	Immediate notification	Within 8 hours	- Incident Cmmunications Lead - Chief Information Security Officer - Chief Digital & Information Officer.

Incident Category	Incident Priority	Notification Timeframe*	Containment / Remediation Timeframe	Stakeholders to notify
Significant	2	Within 1 hour	Within 24 hours	- Incident Communications Lead - Chief Information Security Officer - Chief Digital & Information Officer
Escalated	3	Within 8 hours	Within 3 business days	- Chief Information Security Officer - Chief Digital & Information Officer
Normal	4	Not applicable	Not applicable	- Not applicable
Any incident impacting PII or PHI	1	Immediate notification	24 hours	- Chief Information Security Officer - Chief Digital & Information Officer for referral to the Privacy and Rights to Information Manager.
*timeframe begins when a cyber security incident is confirmed through the detection and analysis.				

(27) The Incident Lead is responsible for ensuring incidents are managed in accordance with their priority level, and for escalating major and significant cyber security incidents to the Incident Communications Lead within the defined timeframes.

(28) Once notified the Incident Communications Lead is responsible for exercising the DTS Critical Incident Management Guide.

Phase 3: Containment, Eradication and Recovery

(29) Phase 3 begins once the suspected event is classified as a Confirmed Incident. The Incident Lead manages and coordinates this phase.

(30) The primary objective is to confine any adverse impact to the University's operations and assets, followed by eradication of the threat and the return of operations and assets to their normal state.

(31) Strategies to contain, eradicate and recover from the incident vary based on the type of the incident, and responsibilities may be shared by multiple teams who report to the Incident Lead.

(32) Incident Leads require investigation expertise to effectively identify the root cause and impact of an incident. Alternatively, Incident Leads can engage third parties with the appropriate skills to perform investigations.

(33) An appropriate combination of the following actions must be undertaken to complete this phase:

a. initial containment of the incident:
    i. acquire, preserve, secure and document evidence;
    ii. confirm containment of the incident;
    iii. further analyse the incident and determine if containment was successful; and
    iv. implement additional containment measures, if necessary.
b. eradicate the incident:
    i. identify and mitigate all vulnerabilities that were exploited;
    ii. the Incident Lead will undertake the necessary activities to resolve the problem and restore the affected services to their normal state. If external support has been requested, the external bodies will also be involved in resolving the problem; and
    iii. remove the components of the system(s) causing the incident.
c. recover from the incident:

i. return affected systems and services to a state that is ready for operation, and are not in a state prone to repeat compromise; and
ii. confirm that the affected systems and services are functioning normally.

Phase 4: Post-Incident Activity

(34) Post-incident activities commence once an incident is resolved or closed and include a post incident review and the development of an incident closure report.

(35) The Incident Lead conducts a post incident review workshop with relevant stakeholders and any external parties involved in the incident response. The review will reflect on the:

a. root cause of the incident;
b. incident response issues;
c. what worked well in the response to the incident;
d. whether the incident could have been prevented; and
e. how elements of incident response such as people, process, organisation, support, technology, and training can be improved.

(36) The Incident Lead documents the findings and actions from the post incident review within a closure report. The closure report must contain the following information:

a. summary of the incident;
b. incident actors;
c. Incident Leads;
d. detailed Incident Description;
e. relevant evidence;
f. technical details;
g. eradication actions;
h. conclusion; and
i. lessons learnt.

(37) The completed report is shared with the Chief Digital & Information Officer for review and approval.

(38) The Incident Lead delivers the incident closure report to appropriate stakeholders and communicates follow-up actions.

Continuous Improvement

(39) The Cyber Security team is responsible for reviewing the operational effectiveness of the incident response capability which includes the people, process, organisation, support, technology, and training for incident response.

(40) At a minimum, the incident response capability should be tested at least annually by engaging a third party or by running internal exercises.

(41) The Cyber Security team is responsible for coordinating the implementation of recommendations from incident response tests, incident closure reports and feedback from DTS.

Section 4 - Roles and Responsibilities

DTS Staff

(42) As managers of the University's digital environment, DTS staff are responsible for:

a. identifying cyber security incidents;
b. reporting cyber security incidents to the Cyber Security team;
c. working with the Cyber Security team to follow the Cyber Security Incident Management Procedure; and
d. protecting all incident-related information that is considered Restricted or Highly-Restricted.

Cyber Security Team

(43) The Cyber Security team sits within DTS and is responsible for the protecting the University from cyber security threats. The team’s responsibilities include:

a. reviewing and actioning incidents raised via the dts-cybersecurity@newcastle.edu.au mailbox, staff and other sources of information;
b. ensuring all relevant information necessary to analyse the incident is gathered;
c. initiating incident response procedures as per this document; and
d. providing assistance during incident response as required.

Incident Lead

(44) The Incident Lead is responsible for coordinating and managing the response to an incident which includes:

a. instructing incident response team members of required actions;
b. ensuring incidents are promptly reported to management and business owners;
c. ensuring that incidents are escalated to relevant stakeholders in line with the determined service level;
d. requesting, collecting, managing and securely storing evidence and artifacts related to incident response;
e. developing an incident containment, eradication, and recovery strategy;
f. preparing a written report of the incident, corrective actions taken, and recommendations to prevent recurrence; and
g. reporting Incidents involving personal information or health information breaches to the Chief Digital & Information Officer for referral to Privacy Office.

Status and Details

Status	Current
Effective Date	30th March 2023
Review Date	30th March 2026
Approval Authority	Chief Information Officer
Approval Date	20th March 2023
Expiry Date	Not Applicable
Responsible Executive	Morven Cameron Chief Operating Officer
Enquiries Contact	Information Security Team

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Risk assessment" - The overall process of risk identification, risk analysis, and risk evaluation.

"Asset" - Any tangible or intangible item (or group of items) that the University owns or has a legal or other right to control and exploit to obtain financial or other economic benefits.

"Personal information" - Has the same meaning as in the Privacy and Personal Information Protection Act 1998 (NSW).

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"External parties" - Any individual or organisation external to the University.

"Health information" - As defined in the Health Records and Information Privacy Act 2002, or any replacing legislation.

"Intellectual property" - Intellectual property (IP), as defined by the World Intellectual Property Organisation, refers to creations of the mind: inventions; literary and artistic works; and symbols, names and images used in commerce. Intellectual property is divided into two categories: Industrial property includes patents for inventions, trademarks, industrial designs and geographical indications; and Copyright covers literary works (such as novels, poems and plays), films, music, artistic works (e.g. drawings, paintings, photographs and sculptures) and architectural design. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and broadcasters in their radio and television programs.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.