Information Security Incident Management Guidelines

A. Guidelines

1. Audience

1.1 The intended audiences of this guide are:

(a) Individuals / ISIRT (Information Security Incident Response Team) tasked with Information security incident response and management activities.

(b) Individuals that interface with ISIRT (Information Security Incident Response Team)

2. Executive Summary

2.1 This guideline document governs the actions required for reporting, responding and managing information security incidents involving University's ICT services and system resources.

2.2 To ensure effective and consistent reporting and handling of such events, an incident response capability is necessary for rapid detection, to minimize loss and destruction, mitigate the weaknesses that were exploited and restore University ICT services and systems.

2.3 Safe use of the University's ICT services and systems is essential to keep it working effectively. All users of the University's ICT services and systems have a responsibility to

(a) Minimise the risk of vital or confidential information being lost or falling into the hands of people who do not have the right to see it

(b) Protect the security and integrity of IT systems on which vital or confidential information is held and processed

(c) Report suspected information security incidents promptly so that appropriate action can be taken to minimise harm.

3. Purpose

3.1 The intent of this guideline document is to provide a framework and procedures for managing and responding to information security incidents. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which go unreported and unnoticed, often without resolution.

3.2 This document provides guidance to the Information Security Incident Response Team (ISIRT) and associated stakeholders to better respond to information security events and incidents and provides a structured approach to:

3.3 Detect, report, and assess information security incidents.

3.4 Respond to and manage information security incidents.

3.5 Continuously improve incident response as a result of managing information security incidents.

B. Information Security Incident Management Process

4. Introduction

4.1 Information Security Incident Management is a structured approach, and is composed of four major phases:

(a) Preparation: Policies, ISIRT member nomination, stakeholder notification and ISIRT technology acquisition.

(b) Detection \ Incident Analysis: Detecting and confirming an Incident has occurred; categorising the Nature of the Incident and then prioritising the incident.

(c) Containment, Eradication and Recovery: Minimising loss, theft of information, or service disruption; eliminating the threat and restoring services quickly and securely.

(d) Post-Incident Activity: Submitting a formal closure report including lessons learned. This report must also contain recommendations for improvement, mitigation of exploited weaknesses and additional security controls to prevent similar incidents from occurring in the future.

5. Phase 1: Preparation

5.1 The first phase deals with preparing a team to be ready to handle an incident at short notice. Regardless of the cause of the incident, preparation is the most crucial phase, as it will determine how well the team will be able to respond to the event

5.2 Preparing to handle an Incident

There are several key actions that must be taken care of while responding to an incident:

(a) **Policies** – The University's Critical Incident Management Policy and the University Information Security Management, Security and Conditions of Use Policy must readily be available for use as reference.

(b) **ISIRT member nomination** - Appropriately skilled ISIRT members must be selected from employees deemed capable of adequately responding to a security incident, either from the IT services department or any external source.

(c) The ISIRT members must be apprised of their responsibilities as a team, and must prepare to undertake the relevant activities to ensure that the ISIRT is operational.

(d) The ISIRT will be managed by the Chief Information Officer (CIO), who will oversee and coordinate operations.

(e) **Stakeholder Notification** – In cases of Severe and Major Category incidents, ISIRT must immediately send an Incident Notification communication in accordance with applicable policy, legal, regulatory, or contractual requirements. Refer Critical Incident Management Communication Procedure for notification to parties outside the University.

(f) **Technology** – Required technology must be acquired to support the information security incident management process. This may include a clean laptop (i.e. not vulnerable to any network or virus attack that may be involved in the incident), a mobile internet connection (if network access is impacted) and access to copies of necessary documents such as policies and guidelines

6. Phase 2: Detection \ Incident Analysis

6.1 When an incident is reported or assigned to the IT Security team/ISIRT, the team must perform a detailed incident analysis and risk assessment.

6.2 The risk analysis considers the range of potential consequences. The risk rating determines the level of risk management required by the University. Consequence and likelihood are combined to produce a risk rating. This is achieved by applying criteria in the Risk Management Matrix to determine the level of risk to the University. These criteria include the following:

(a) Likelihood of the risk, which reflects how often a risk may occur

(b) Consequence defines the actual/potential impact that would/might occur

6.3 Refer to the University Risk Management Framework for detailed Risk Analysis guidelines to be followed

6.4 Process Steps:

(a) IT Security shares the Incident notification with ISIRT team for analysis.

(b) The IT Security/ISIRT teams will perform the incident analysis to determine whether or not a security incident has occurred.

(c) The ISIRT team will perform a detailed risk analysis of the incident as per University Risk Management Framework.

(d) ISIRT team determines the priority of the incident as per Incident Categorisation, Prioritisation and responds as per Incident SLAs.

(e) Thereafter, it assigns the case to Department Representative / Incident Handler for action.

(f) Once sufficient details are available, the Department Representative / Incident Handler will take necessary action required for the incident.

(g) Where an incident receives a priority of Severe or Major, the University Management must be notified as soon as possible.

6.5 Incident Categories

Category	Description
Unauthorised Access	Unauthorised and successful / unsuccessful logical access to the University's ICT services and systems.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorised functionality of networks, systems or applications by exhausting resources. This activity includes being the victim of, or participating in, a DoS.
Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects the ICT services and systems.
Data Leakage	Security incident involving loss of the University's critical information that can have a negative impact on the University.
Improper Usage	Actions involving ICT services and systems that violate the University Computing & Communications Use Policy, e.g.: I. Downloading and/or using unauthorised security tools, II. Use of Peer to Peer applications to acquire or distribute copyrighted material. III. Refer : Information Technology Conditions of Use Policy IV. Mis-use of UoN ICT services and systems.
Investigation	Unconfirmed incidents that have been contained, that are potentially malicious or anomalous activity deemed by the ISIRT team that warrant further review.

6.6 Incident Prioritisation

(a) The ISIRT shall perform an assessment of the incident priority using the factors in the table below.

(b) Given the established priority, the incident will be allocated a Service Level which determines the timelines attached to next steps.

Priority	Factor	Examples of Incidents
Severe	An incident affecting the entire organization	- Business disruptions resulting from malicious activity that results in > 50% degradation - Any incident that impacts the availability of perimeter security infrastructure - Exposure of unencrypted, unmasked, or insufficiently masked University confidential or sensitive information (Health Data/PII) into the public domain. This includes any data that could have a negative impact on the University's reputation.
Major	An incident affecting multiple facilities, User Groups or networks	- Compromised privileged account credentials - Incident involving Highly Critical assets - >10% of University users unable to use IT resources - Potential for involvement of law enforcement - Active attack incidents by unknown attackers that impact the University's servers - Exposure of unencrypted, unmasked, or insufficiently masked University confidential or sensitive information (Health Data/PII) into the public domain or to an unauthorised third party
Moderate	An incident affecting a facility or network	- Malware incidents that don't fall in a higher severity - Data loss incidents not involving sensitive information - Confirmed phishing campaign that impacts more than a hundred users
Insignificant	Minor Incident	- Some localised inconvenience, but no impact to the University.

6.7 Incident Service Level Agreements (SLA)

(a) The ISIRT team shall ensure that the incidents are managed and responded to as per the below SLA. This SLA applies to the Incident response commitments for all type of information security incidents. Incident response times vary according to the priority level assigned to the incident.

(i) Notification – Initial notification of a suspected incident to ISIRT / IT Security Teams

(ii) Contain/Remediate – Maximum time to either contain the threat/exposure or permanently remediate

Category	Notification	Contain / Remediate	Escalation Matrix
Severe	Immediate	8 Hours	Risk Committee, Privacy Office, University Executive & CIO
Major	8 Hours	24 Hours	Risk committee, Privacy Office & CIO
Moderate	24 Hours	5 Business Days	IT Security Team or ISIRT
Insignificant	N/A	N/A	N/A

6.8 Incident

(a) Based on the analysis of the incident category and classification, the information security incident can be addressed in the following ways:

Status	Reason
Confirmed	An incident has been confirmed and response is underway.
Disposition	**Reason**
Unidentified	A confirmed incident involving an ICT service or system which cannot be located may be resolved as Unidentified.
Transferred	A confirmed incident may be investigated and transferred to another department for further investigation or action.
Deferred	A confirmed incident may be Deferred due to resource constraints, or information type. **Note:** Critical/High Priority cases cannot be deferred without CIO approval.
False Indicator	Investigation reveals that the source indicator used as the basis for incident detection was a faulty Indicator.
Misconfiguration	An event that appeared to be a malicious activity was subsequently proven to be a false alert and determined to be a misconfiguration (malfunction) of a system.
Duplicate	An incident may be a duplicate of another record in the Service Desk, and must be merged with the existing workflow.

6.9 Escalation

(a) Severe and Major category incidents will require escalation so that senior management within the University are made aware of, and may respond accordingly to, serious and potentially serious information security incidents. The Crisis/Escalation Team consists of senior members of the relevant departments of the University. Not all members of the Crisis/Escalation Team will need to be alerted to all information security incidents immediately.

(b) Refer to the Critical Incident Management Communication Procedure for escalation procedures to be followed for Severe and Major Category incidents.

7. Phase 3: Containment, Eradication and Recovery

7.1 This phase begins once the suspected event has been classified as a Confirmed Incident. This phase involves identifying the immediate response actions to deal with the information security incident and informing the appropriate team about the required actions. The primary objective is to confine any adverse impact to the University's operations, followed by eradication of the threat and the return of the ICT services and systems to its normal productive state.

7.2 The department representative/ incident handler shall manage this phase. Incident containment, eradication and recovery steps may vary based on the incident type, and the Incident Response Responsibility may be split over multiple teams which shall be managed and coordinated by the Incident Handlers.

7.3 Incident Handlers may require investigation expertise during the course of a response or must have access to or agreements with third parties with appropriate skill sets to perform investigations.

7.4 An appropriate combination of the following actions must be used 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

(iv) Implement additional containment measures, if necessary

(b) Eradicate the incident

(i) Identify and mitigate all vulnerabilities that were exploited

(ii) The ISIRT team 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.

(iii) Remove components of the systems causing the incident.

(c) Recover from the incident

(i) Return affected systems and services to a state that is ready for operation.

(ii) Confirm that the affected systems and services are functioning normally.

8. Phase4: Post-Incident Activity

This phase takes place once the information security incident has been resolved or closed.

8.1 Compile Summary of Actions and Findings

(a) The Incident Handler(s) must document the actions taken during the process. If the incident involved support from external Investigators or Forensic Investigators, their steps and reports must also be documented and shared with the Incident Handler.

(b) The Incident Handler shall collate the details and prepare the Closure report.

8.2 Closure Report

(a) The Incident Handler is responsible for documenting an incident report which contains (at the minimum) the following information:

(i) Summary of the incident
(ii) Incident actors
(iii) Incident handlers
(iv) Detailed Incident Description
(v) Relevant evidences
(vi) Technical details
(vii) Eradication actions
(viii) Conclusion
(ix) Lessons learnt

b) The completed incident report is shared with ISIRT team for review and approval. Once the incident report is approved, it is ready for circulation to relevant stake-holders report.

8.3 Submit Recommendations to Appropriate Management

(a) The IT Security Team (or a designated member of the Incident Response team) delivers recommendations for changes in technology, process or policy to appropriate stakeholders for the development of a follow-up action plan

8.4 Lessons Learnt

(a) Information security incident management activities are iterative, and thus it is imperative that regular improvements are made to a number of information security elements over time. These improvements must be proposed on the basis of reviews of the information security incidents

C. Roles and Responsibilities

1. ISIRT Team

1.1 The primary function for tracking and managing incidents within the area of defined responsibility rests with this role. ISIRT team shall be the first responders to any incident that is reported. The responsibilities include the following:

(a) Ensure all incidents are appropriately reported, prioritised, categorised, tracked, assigned, responded to and closed with clear documentation.

(b) Ensure that all follow-up activities are conducted, e.g. work to strengthen security controls, or weaknesses, that allowed the incident to occur.

(c) Ensure incident response is conducted in compliance with this guide.

(d) Ensure incident handlers and investigators are assigned and fully supported throughout the Incident Response process, and that they have performed an adequate analysis of the incident.

(e) Ensure incidents are handled within the agreed SLA.

(f) Review and Approve authority of all incident reports as the need arises.

(g) Refer Information Security incidents that may have legal implications to responsible teams for advice and action.

(h) Liaison between the CIO office and Legal / Risk Committee on incident matters

2. Incident Handlers \ Investigators

2.1 The main responsibilities of the team are:

(a) Ensure all relevant information necessary to understand the incident is gathered

(b) Initiate incident response procedures as outlined in this guide

(c) Instruct other constituents on the response actions that may be required to contain/remediate the incident at hand

(d) Provide periodic status update to ISIRT team on the incident

(e) Prepare incident closure report and submit to the ISIRT Team for reviews

(f) In the course of the incident response, provide assistance on queries that may be raised

(g) Request, carve, collect and manage relevant artefacts for secure storage as part of the incident response

(h) Close incident tickets after the ISIRT Team has accepted and approved them.

(i) Adhere to Incident Response SLAs

3. Definitions

3.1 Refer to the Information Security Definitions document

4. Related Documents

4.1 Legislation:

(a) NSW State Records Authority Standard on Counter Disaster Strategies for Records and Recordkeeping systems (No. 6)

(b) NSW State Records Authority Standard on Managing a Records Management Program (No. 12)

(c) NSW State Records Authority Standard on Physical Storage of State Records (No. 3)

(d) Crimes Amendment (Computer Offences) Act 2001 (NSW)

(e) Cybercrime Act 2001 (Cth)

(f) Information Security Guideline for NSW Government – Part 1 Information Security Risk Management

(g) Privacy and Personal Information Protection Act 1998 No 133

(h) Health Records and Information Privacy Act 2002

(i) State Records Act 1998

(j) R39 Australian Code Responsible Conduct Research 150107

4.2 Polices:

(a) Information Security Policy

(b) Code of Conduct 000059

(c) Student Misconduct Rule 000935

(d) Records Management Policy

(e) University Risk Management Framework

(f) University Risk Management Policy

(g) Critical Incident Management Communication Procedure

(h) Incident Management Policy

(i) Information Technology Conditions of Use Policy

About this Document

Further information

TRIM Number	
Approval Authority	Chief Information Officer
Subject Matter Expert	Patrick McElhinney – Senior Security Specialist, IT Services
Contact Details	It-security@newcastle.edu.au
Review Date	1st July 2018

Approval History

No.	Effective Date	Approved by	Amendment

V1.0	31st March 2017	CIO	

D. Appendix A

1. MIR Procedure Document for P1 category incident

Resolution of P1

MIR initiation on email confirmation from Service Desk of P1 technical resolution

0 to 4 Business Hours

Change Management
Request the Primary Resolver Group Team Leader to provide the following:

i. incident overview

ii. incident timelines

iii. actions timelines

iv. communications timelines, and

v. any outstanding/remaining actions – including:

a. technical cause and/or

b. root cause resolution action items.

Team Leader
Request Resolver Group Team Leader to provide the following:

i. incident overview

ii. incident timelines

iii. actions timelines

iv. communications timelines, and

v. any outstanding/remaining actions – including:

a. root cause resolution action items, and

b. details of any participating resolver group or individuals that must also provide timelines and/or said details.

Change Management
Collate and combine independent timelines from Resolver Group(s) and Service Desk into draft MIR and forward draft MIR to Resolver Group Team Leader for review.

5 to 20 Business Hours

Team Leader

- Resolver Group Team Leader to review draft MIR.
- Team Leader to also undertake peer review if required (e.g. within own team, across resolver groups or back with Change Management).
- Provide edits and/or updates to MIR and approve draft MIR to Change Management.

Change Management

- Contribute to any required peer review with Team Leader.
- Finalise and submit approved MIR for quorum IT Management Team review and approval.

Note: Quorum consists of at least 3 x Associate Directors (CIO inclusive) and must include the Associate Director of the Primary Resolver Group.

21 to 24 Business Hours

IT Management Team

Associate Director/CIO quorum to formally review and approve final MIR.

Team Leader

Provide Change Management with any Technical Cause mitigation actions completed.

Change Management

Create draft Business Owner MIR summary.

IT Management Team

ADir Client Services or CIO review and approval for Business Owner MIR summary to be distributed.

Business Owner

Review MIR summary.

End of Reporting Period

Team Leader

Provide Change Management with any Root Cause resolution actions completed.

Change Management

Close out, archive and report on MIR summary - including any action item updates for any formal Change Management process requested by IT Management Team.