Information Security Incident Management Guidelines

Section 1 - Guidelines

Audience

(1) The intended audience of this guide are:

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

Executive Summary

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

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

(4) 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.

Purpose

(5) 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.

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

a. Detect, report and assess information security incidents.
b. Respond to and manage information security incidents.
c. Continuously improve incident response as a result of managing information security incidents.

Section 2 - Information Security Incident Management Process

Introduction

(7) 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.

Phase 1: Preparation

(8) 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.

Preparing to handle an Incident

(9) 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, Information Security Policy, and Information Technology Conditions of use Policy must readily be available for use as reference.
b. ISIRT Member nomination – Appropriately skilled ISIRT members must 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 (ie 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.

Phase 2: Detection / Incident Analysis

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

(11) 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.

(12) Refer to the University Risk Management Framework for detailed Risk Analysis guidelines to be followed.

(13) 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 the 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.

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 Information Technology Conditions of Use Policy, e.g: a. Downloading and/or using unauthorised security tools, b. Use of peer to peer applications to acquire or distribute copyrighted material. d. 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.

Incident Prioritisation

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

(15) 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 effecting the entire organisation.	-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 effecting 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 effecting 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 100 users.
Insignificant	Minor Incident	-Some localised inconvenience, but not impact to the University.

Incident Service Level Agreements (SLA)

(16) 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 types of information security incidents. Incident response times vary according to the priority level assigned to the incident.

a. Notification – Initial notification of a suspected incident to ISIRT / IT Security Teams.
b. 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 Hors	5 Business Days	IT Security Team or ISIRT
Insignificant	N/A	N/A	N/A

Incident

(17) 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.

Status	Reason
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 worfklow.

Escalation

(18) 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.

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

Phase 3: Containment, Eradication and Recovery

(20) 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.

(21) 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.

(22) 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.

(23) 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 the 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.

Phase 4: Post-Incident Activity

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

Compile Summary of Actions and Findings

(25) 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.

(26) The Incident Handle shall collate the details and prepare the Closure report.

Closure Report

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

a. Summary of the incident
b. Incident actors
c. Incident handlers
d. Detailed Incident Description
e. Relevant evidences
f. Technical details
g. Eradication actions
h. Conclusion
i. Lessons Learnt

(28) 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.

Submit Recommendations to Appropriate Management

(29) 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 fo the development of a follow-up action plan.

Lessons Learnt

(30) 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.

Section 3 - Roles and Responsibilities

ISIRT Team

(31) 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 appropriated 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.

Incident Handlers / Investigators

(32) 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 updates 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 are the ISIRT Team has accepted and approved them.
i. Adhere to Incident Response SLAs.

Status and Details

Status	Historic
Effective Date	31st March 2017
Review Date	1st July 2018
Approval Authority	Chief Information Officer
Approval Date	28th May 2018
Expiry Date	17th June 2019
Responsible Executive	David Toll 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 management" - The co-ordination of activities to optimise the management of potential opportunities and reduce the consequence or impact of adverse effects or events.

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

"Level of risk" - Magnitude of a risk or combination of risks, expressed in terms of the combination of their consequence and likelihood.

"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.

"Confidential information" - All information which is disclosed to a party by, or on behalf of, the other party, or which is otherwise acquired by a party from the other party, or any adviser engaged by the other party, which: (a) is by its nature confidential; (b) is designated by the other party as being confidential; or (c) the party knows or ought to know is confidential, but does not include information which: (d) is or becomes public knowledge other than through a breach of confidentiality; (e) was already in the possession of a party and not subject to an obligation of confidentiality; (f) is lawfully received from a third party; or (g) is independently developed by a party.

"Course" - When referring to a course offered by the University, a course is a set of learning activities or learning opportunities with defined, assessed and recorded learning outcomes. A course will be identified by an alphanumeric course code and course title. Course types include core courses, compulsory courses, directed courses, capstone courses and electives. For all other uses of this term, the generic definition applies.

"Law" - All applicable statutes, regulations, by-laws, ordinances or subordinate legislation in force from time to time anywhere in Australia, whether made by the Commonwealth, a State, a Territory or a local government and, where the context permits, includes the common law and equity.

"Third party" - A person or group other than the University or any of the University's partner institutions.