Information Security Incident Management Guidelines

Section 1 - Introduction

Purpose

(1) This guideline document describes the standard approach for planning for, and responding to, information security incidents involving the University's ICT resources and information assets. It specifies an appropriate incident response based on the nature and severity of the incident, the data involved, and other factors.

(2) This document provides guidance to the Incident Handler 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; and
c. continuously improve incident response as a result of managing information security incidents.

(3) These guidelines form part of the University's hierarchy of IT related incident management processes:

a. IT Incident Management Process;
b. Information Security Incident Management Guidelines (this document);
c. Information Technology ' Critical Incident Management Guide; and
d. University's Business Continuity Management Policy and Business Continuity Management Framework.

(4) 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 stored or processed; and
c. report suspected or actual information security incidents promptly so that appropriate action can be taken to minimise harm.

Scope

(5) This guideline applies to the ICT resources and the information assets of the University, and to any person or device who gains access to these systems or data.

(6) This guideline document must be read in conjunction with the IT Services Critical Incident Management Guide, and the University's Business Continuity Management Framework, Business Continuity Management Policy, Information Security Policy, and Information Technology Conditions of Use Policy.

Interface with IT Incident Management

(7) IT Incident Management is responsible for incident processes related to a significant deterioration, degradation, or disruption of an IT business process or service.

(8) The Information Security Team is responsible for information security incident management processes, running in conjunction with the IT incident management process.

(9) While investigating a particular IT incident, it may become evident or there may be indications that the root cause is information security related.

(10) If, during an standard IT incident response, ITS staff suspect that an outage or service disruption may be security-related, these guidelines should be followed.

(11) If it is determined that an incident is not information security related, the Information Security Team will discontinue its participation in that incident response process.

Interface with IT Services' Critical Incident Management

(12) Major and significant incidents require immediate escalation to the IT Service Continuity Coordinator, who is responsible for the Information Technology ' Critical Incident Management process.

(13) Information Technology Critical Incident Management process will in turn interface with the University Business Continuity process should an incident require such escalation.

Section 2 - Information Security Incident Management Process

Introduction

(14) Information Security Incident Management is a structured approach, and is composed of four phases:

a. Preparation: policies, stakeholder notification and technology acquisition.
b. Detection: detecting and confirming an incident has occurred; categorising the nature of the incident and then prioritising the incident.
c. Containment, Eradication and Recovery: minimising the loss or 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.

(15) The sensitivity of information communicated during all phases of incident response must be carefully considered. The University's Information Security Data Classification and Handling Manual defines the four security classification levels in use across the University.

(16) The Incident Handler may, whilst undertaking incident response, liaise with external organisations such as the ACSC, ASD, ASIO, AusCERT, CERT Australia, security consultants, application vendors and specialists in order to manage the technical incident response. This will not form part of any official notification process, and must be done in strict confidence.

(17) In cases where the Incident Handler communicates with external parties, the industry standard Traffic Light

Protocol (TLP) should be used. The four University data security classifications align closely with those of the TLP:

Table 1 – TLP Classifications and University Data Classifications

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

Phase 1: Preparation

(18) 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

(19) Preparation includes those activities that enable the Incident Handler to respond to an incident:

a. Policies – the University's Information Security Policy, Information Technology Conditions of use Policy, Business Continuity Management Policy, Business Continuity Management Framework, Risk Management Framework must readily be available for use as reference.
b. Stakeholder notification – in cases of incidents categorised as major or significant, the Incident Handler must immediately send an incident notification communication in accordance with the Information Technology Critical Incident Management Guide and the University's Business Continuity Management Policy.
c. Technology – required technology must be acquired to support the information security incident management process. This may include a laptop, a mobile internet connection (if network access is impacted), and access to copies of necessary software and documents, such as policies and guidelines.

Phase 2: Detection and Incident Analysis

(20) An information security incident begins when a security-related event is reported. This could come from an automated system diagnostic, an incident ticket submitted by a user to the IT Service Desk, or other sources.

(21) When an information security incident is reported or assigned to the Information Security Team, the incident is assigned to an Incident Handler who is responsible for investigating the incident and coordinating the response until the incident is resolved, closed or escalated to the IT Service Continuity Coordinator as an ITS Critical Incident.

(22) The first step for an Incident Handler is to perform a detailed incident analysis and risk assessment, using the University's Risk Management Framework.

(23) Process steps:

a. an information-security-related event is identified and assigned to an incident handler for management;
b. the Incident Handler will perform the incident analysis to determine whether or not a security incident has occurred;
c. the Incident Handler will perform a risk analysis of the incident as per the University Risk Management Framework.
d. the Incident handler determines the Incident Categorisation and Incident Prioritisation, and the resultant service

levels;

e. for major or significant incidents the case is assigned to the IT Service Continuity Coordinator for management, as per the ITS Critical Incident Management Guide; and
f. incidents involving personally identifiable information (PII) or protected health information (PHI) breaches must be reported to the CIO for referral to the Privacy Office.

Table 2 – 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.
Malware	Successful installation of malicious software (e.g. virus, worm, Trojan horse, or other code-based malicious entity) that infects the ICT services and systems.
Information 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 University ICT services and systems; and e. other improper usage per the Information Technology Conditions of Use Policy.
Unconfirmed	Unconfirmed incidents that have been contained, that are potentially malicious or anomalous activity deemed by the Information Security Incident Response Team (ISIRT) that warrant further review.
Collateral damage	Incidents that impact the confidentiality, integrity or availability of information, that are caused by failure of the very systems that are meant to protect University information; such as a failed security software update that impacts system availability.

Incident Prioritisation

(24) The Incident Handler shall perform an assessment of the incident priority using the factors in the table below.

Table 3 – Incident Prioritisation Levels

Priority	Factor	Examples
Major	An incident effecting the entire University.	- Substantial, possibly wide-ranging, actual or potential damage to the confidentiality, integrity or availability of the University's information assets and ICT resources. - An incident that impacts the availability of perimeter security infrastructure. - Bulk exposure of University PHI, PII or intellectual property (IP) into the public domain, where such exposure results in compliance and\or reputational consequences.
Significant	An incident effecting multiple facilities, User Groups or campuses.	- Contained actual or potential damage to the confidentiality, integrity or availability of the University's information Assets and ICT resources. - >10% of University users unable to use ICT resources. - Exposure of a small amount of confidential or sensitive University information (PHI, PII or IP) into the public domain or to an unauthorised individual.
Escalated	An incident affecting a facility or campus.	-Malware incident that doesn’t fall into a higher severity. -Data loss incidents not involving PHI or PII. -Confirmed phishing campaign that impacts more than 100 users.

Priority	Factor	Examples
Normal	Minor Incident	-Some localised inconvenience, but no significant impact to the University.

(25) Given the established priority, the incident will be allocated a service level which determines the timelines attached to next steps.

Incident Service Levels

(26) The Incident Handler shall ensure that an incident is managed and responded to as per the below service levels. This service level 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.

Table 4 – Incident Service Levels

Incident Category	Notification*	Contain / Remediate**	Stakeholders to notify
Major	Immediate	8 hours	- IT Service Continuity Coordinator - Associate Director, Enablement - CIO
Significant	4 Hours	24 Hours	- IT Service Continuity Coordinator - Associate Director, Enablement - CIO
Escalated	24 Hours	5 Business Days	- Associate Director, Enablement
Normal	N/A	N/A	- N/A
ANY Involving PII or PHI	Immediate	24 Hours	- Associate Director, Enablement - CIO for referral to the Privacy Office

*Notification – Initial notification of a suspected or actual incident to the relevant stakeholders.

**Contain / Remediate – Maximum time to either contain the threat or to permanently remediate.

Incident

(27) 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.

Escalation

(28) Major and significant incidents 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 initial point of escalation is to the IT Service Continuity Coordinator, who is responsible for the Information Technology ' Critical Incident Management Guide.

Phase 3: Containment, Eradication and Recovery

(29) 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, where applicable, informing the appropriate team of 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 their normal state.

(30) The 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 Handler.

(31) Incident Handlers will require investigation expertise to effectively manage the incident response, or must have access to or agreements with third parties with appropriate skill sets to perform investigations.

(32) 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; and
    iv. implement additional containment measures, if necessary.
b. eradicate the incident:
    i. identify and mitigate all vulnerabilities that were exploited;
    ii. the Incident Handler 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 systems 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

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

Compile Summary of Actions and Findings

(34) The Incident Handler(s) must document the actions taken during the process. If the incident involved support from external parties such as AusCERT, CERT Australia, or contracted security consultants, their steps and reports must also be documented by the Incident Handler.

(35) The Incident Handler shall collate the details and prepare the closure report.

Closure Report

(36) The Incident Handler is responsible for documenting an incident closure 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; and
i. lessons learnt.

(37) The completed incident closure report is shared with CIO for review and approval.

Submit Recommendations to Appropriate Management

(38) The Incident Handler delivers the incident closure report, including recommendations for changes in technology, process or policy, to appropriate stakeholders for the development of a follow-up action plan.

Lessons Learnt

(39) Information security threats evolve over time, and thus it is imperative that regular improvements are made to information security controls. Any proposed control improvements should consider the outcomes and findings of information security incidents investigations.

Section 3 - Roles and Responsibilities

Information and Technology Services (ITS) Staff

(40) As service owners and users of IT resources, ITS staff are expected to recognise potential security incidents. Responsibilities include:

a. promptly reporting all security incidents to the Information Security Team;
b. working with the Information Security Team to follow these Information Security Incident Management Guidelines. This includes checking with Information Security Team prior to communicating with any external unit or department about issues or problems that may have security-related components; and
c. the adequate protection of all Incident-related information that is considered Restricted or Highly-Restricted information.

Information Security Team

(41) The Information Security Team is the team of IT security professionals within Information Technology assigned to handle the information security needs for Information Technology . Responsibilities include:

a. maintaining it-security@newcastle.edu.au as the mailbox to report security incidents within Information Technology (IT);
b. receiving notification of detected or reported information security events and incidents from users and service owners of IT resources, automated detection systems, or other sources;

c. ensuring all relevant information necessary to understand the incident is gathered;
d. initiating incident response procedures as outlined in this guideline; and
e. in the course of the incident response, and where appropriate to do so, providing assistance on queries that may be raised.

Incident Handler

(42) The Incident Handler will typically be a member of the Information Security Team who is assigned operational responsibility for the management of an Information Security Incident. Responsibilities include:

a. development of an incident containment, eradication, and recovery plan;
b. instructing incident response team members of the response actions that are required;
c. requesting, collecting and managing relevant artifacts for secure storage as part of the incident management response;
d. ensuring incidents are promptly reported to management and appropriate business owners as appropriate;
e. ensuring that incidents are promptly escalated to the IT Service Continuity Coordinator when deemed major or significant;
f. preparing a written report of the incident, corrective actions taken, and recommendations to prevent recurrence; and
g. reporting Incidents involving PII or PHI breaches to the CIO for referral to Privacy Office.

Definitions

(43) In the context of this document:

a. event is defined as an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.
b. an Information Security Incident (or “incident”) is an adverse event that affects an information system and/or a network that poses a threat to the confidentiality, integrity or availability of the University's information assets; or a violation of explicit or implied University policy (e.g. the University's Information Technology Conditions of Use Policy), IT standard, or code of conduct. Examples of information security incidents include, but are not limited to:
    i. compromised user credentials;
    ii. interference with the intended use of information technology resource;
    iii. loss or theft of equipment used to store private or sensitive information;
    iv. unauthorised change to hardware, software or data;
    v. unauthorised use of systems or data; and
    vi. computer system intrusion.

Status and Details

Status	Current
Effective Date	18th June 2019
Review Date	18th June 2021
Approval Authority	Chief Information Officer
Approval Date	17th June 2019
Expiry Date	Not Applicable
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.

"ICT resources" - All information and communication technology resources and facilities.

"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.

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

"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.

"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.

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

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