Cyber Security Incident Response Procedure

Section 1 - Purpose and Scope

(1) This Procedure sets requirements for responding to cyber security incidents and aligns with the preparedness, response and recovery phases described in the Incident Management Procedure.

(2) This Procedure aims to:

a. minimise the impact of cyber security incidents that occur; and
b. ensure continuous improvement of cyber security incident response and related security controls.

(3) This Procedure applies to UQ staff, contractors, title holders and third parties. It applies in a limited capacity to students (see 'Incident Reporting' provisions in section 2).

(4) Cyber security incident response at UQ is primarily managed and coordinated by teams within the Information Technology Services (ITS) division but relies on collaboration with multiple other organisational units and functions across UQ. Clause 24 ('Incident Response Team' provisions) and section 4 of this Procedure outline the various units and functions involved in UQ's cyber security incident response, and their responsibilities.

(5) Cyber security at UQ is everyone's responsibility. All staff and students are responsible for reporting potential cyber security concerns or incidents, including accidental incidents such as a lost device, to IT Support. UQ staff are further responsible for supporting incident response activities as requested.

Section 2 - Process and Key Controls

Incident Reporting

(6) Staff and students must report any suspicious activity they observe, and any cyber security events impacting them via the cyber security website.

(7) If IT staff receive reports of activity that could be related to a cyber security incident, they must escalate these to the Cyber Security Operations Centre (CSOC).

(8) External parties should report security incidents impacting UQ data using the cyber security incident reporting form.

Incident Handling

(9) Cyber security incident response and recovery consists of five phases occurring in the following sequence.

a. Identification: determines key facts about the incident such as timing, source, exploits, and vulnerabilities, the actual and potential impact level of the incident, correlation with existing or previous events or incidents, and notification requirements.
b. Containment: aims to minimise the actual and potential impacts of the incident as quickly as possible to avoid overwhelming resources for handling the incident, while avoiding actions that could compromise later phases.

c. Eradication: eliminates all possible components of the incident.
d. Recovery: restores normal operations and mitigates the risk of a similar incident re-occurring.
e. Lessons learned: improves security controls and future responses to similar incidents.

(10) Some phases may need to be returned to as new information and impacts are discovered or occur. The Appendix lists activities that typically occur during each phase of incident handling.

> See linked Figure 1: Cyber Security Incident Handling.

Incident Notification

(11) Incident notification is performed to minimise harm and satisfy regulatory and legal requirements. This includes (but is not limited to):

a. Obligations arising from data sharing agreements (i.e. where third party data has been provided to UQ): notifications are performed by the University owner of the data sharing agreement;
b. Obligations arising from the Privacy Act 1988 and Information Privacy Act 2009 (Qld): UQ may need to notify impacted persons and authorities in the event of a personal information breach. View the Personal Information Breach Response Plan for more detail;
c. Obligations arising from the Security of Critical Infrastructure Act 2018: UQ must notify the Australian Cyber Security Centre (ACSC) about significant incidents. Notifications are performed by the CSOC – see the Appendix 'Incident Notification – Security of Critical Infrastructure Act 2018' provisions for more detail; and
d. Obligation to notify the Queensland government: UQ must report all cyber security incidents with an impact rating of Minor and above to the Queensland Government Cyber Security Unit.

(12) Notification requirements must be identified as early as possible. Notifications must be prioritised to meet obligations and allow third parties to respond quickly to minimise potential impacts.

Section 3 - Key Requirements

Part A - Preparedness

Incident Response Capability

(13) The Chief Information Officer (CIO) and Director, Cyber Security must ensure that:

a. the CSOC and relevant IT support teams are sufficiently staffed and resourced for effective incident response; and
b. suitable arrangements are in place with external organisations to provide additional expertise and resources when required.

(14) The CSOC and IT managers must ensure staff involved in cyber security incident response receive sufficient training to enable them to follow this Procedure.

(15) The CSOC Manager is responsible for establishing and maintaining relationships with government agencies, industry peers and security service providers to improve cyber security incident response.

Incident Communication Mechanisms

(16) The CSOC Manager must ensure that suitable mechanisms are in place for reporting cyber security incidents or

suspicious activity.

(17) The Chief Information Officer (CIO) must ensure that resilient mechanisms are in place to enable communications during an incident that disrupts normal IT services.

Cyber Security Incident Plans and Procedures

(18) The Security Architect is responsible for developing and maintaining cyber security incident response plans for significant types of incidents in consultation with key stakeholders which are approved by the Cyber Security Risk and Compliance Committee (CSRCC). These plans are stored in the IT Procedures, Frameworks and Standards and must include:

a. description of the applicable incident/s;
b. key roles and responsibilities;
c. key actions and resources required as part of preparedness, identification, containment, eradication, and recovery;
d. key positions regarding incident response and relevant considerations;
e. relevant legislative requirements; and
f. communications plan and associated templates.

(19) Technical procedures for handling specific aspects of an incident are maintained by the Cyber Security Operations Centre (CSOC) and IT teams.

Cyber Security Tabletop Exercises

(20) Cyber security tabletop exercises simulate cyber security incidents to train participants, validate response plans and investigate dilemmas arising from particular scenarios. Members of the University Incident Management Team (UIMT) and Crisis Management Team (CMT) must participate in annual cyber security tabletop exercises coordinated by the Cyber Security Improvements Manager. Actions resulting from tabletop exercises are added to the IT Outstanding Actions Register for tracking.

Part B - Identification

Incident Assessment

(21) Once an incident is identified, the CSOC (with support from relevant staff) will assess the potential impact of the incident based on what has already occurred, and what could reasonably be expected to occur. A consequence rating is assigned based on UQ's risk matrix.

(22) Incidents with a large or complex scope may be difficult to assess accurately, and other phases such as containment may need to proceed first. Throughout the incident response process, the Cyber Security Incident Manager must revise incident assessments as new information is received and escalate (or deescalate) accordingly.

Part C - Response

Response Priorities

(23) Response activities must be prioritised to minimise the following impacts (listed in order of importance):

a. harm to people;
b. damage to information and operations;
c. harm to the broader community;

d. compliance with contractual agreements and government regulations; and
e. harm to UQ's reputation.

Incident Response Team

(24) The following table indicates the makeup of the incident response team, based on the potential impact rating.

Table 1: Incident Response Team Makeup

Potential impact (response tier)	Key decisions	Cyber Security Incident Manager	Technical response	General response	Internal Communications Lead	External Communications Lead
Insignificant Tier 1)	CSOC Manager	CSOC staff/IT Manager	CSOC/IT teams	As required	Cyber Security Incident Manager	N/A
Minor (Tier 1)	CSOC Manager	CSOC Manager	CSOC, IT teams	As required	Cyber Security Change and Communications	N/A
Moderate (Tier 1)	Director, Cyber Security	CSOC Manager/ Director, Cyber Security	CSOC, IT teams, external services as required	As required	Cyber Security Change and Communications Senior Manager, Internal Communication (informed)	Senior Manager, Corporate Communication
Major (Tier 2)	Chief Operating Officer (COO)	Director, Cyber Security	CSOC, IT Teams, external services as required	University Incident Management Team (UIMT)	Senior Manager, Internal Communication	Senior Manager, Corporate Communication
Critical (Tier 3)	Vice-Chancellor (VC)	Director, Cyber Security	CSOC, IT Teams, external services as required	UIMT, Crisis Management Team (CMT)	CMCO (CMT) Senior Manager, Internal Communication	Senior Manager, Corporate Communication

Cyber Security Incident Manager

(25) The Cyber Security Incident Manager is responsible for coordinating incident response activities according to this Procedure, directing teams and staff members as required, and for effective coordination between the technical and general response teams. The Cyber Security Incident Manager will activate support arrangements with external security service providers when needed and ensure that the required incident notifications occur.

(26) Incidents of a particular type may be handled by an IT support team by prior agreement with the CSOC. In these instances, the team manager acts as the Cyber Security Incident Manager, who must inform the CSOC about the incident.

(27) The Cyber Security Incident Manager has the CIO's authority to direct actions to remedy impacted IT services.

Incident Escalation

(28) Incidents are escalated to UQ's incident response teams when the potential impact of the incident is Major or Critical.

a. If the potential impact of an incident is Major then Tier 2 of the University incident response structure is activated.
b. If the potential impact is Critical then Tier 3 is activated.

(29) Escalation is initiated by the CSOC Manager. They escalate to the Chief Information Officer (CIO) or Director, Cyber Security who escalates to the Chief Operating Officer (COO) and the Crisis and Resilience Manager.

(30) The Crisis and Resilience Manager activates the University Incident Management Team (UIMT) and Crisis Management Team (CMT).

(31) The CSOC Manager will alert the Crisis and Resilience Manager if a Minor or Moderate (Tier 1) incident occurs in case further escalation is required.

Additional support

(32) Cyber security incident response may require a broad cross-section of skills and knowledge beyond cyber security and IT. Additional teams may support the general response depending on the scope of the incident, including (but not limited to):

a. Governance and Risk Division (RTI and Privacy Office) regarding personal information.
b. Legal Services regarding government regulations, contracts, and significant legal risks.
c. Integrity Unit regarding staff policy breaches or criminal activities.
d. Student Complaints and Grievance Resolution regarding student policy breaches or criminal activities.
e. Health, Safety and Wellness Division and Student Services for staff and student victim support.
f. Property and Facilities Division regarding physical security.
g. Information Domain Custodians regarding SENSITIVE or PROTECTED information.

Threat Intelligence Sharing

(33) If feasible, The CSOC should generate and distribute timely threat intelligence during or after an incident to help prevent similar attacks on other organisations. Threat intelligence must be sanitised to deidentify any third party as the victim of the attack and the University itself when appropriate. Threat intelligence must only be provided to the approved threat intelligence sharing networks listed in Appendix, ‘Approved Threat Intelligence Networks’ provisions.

Documentation

(34) Members of the incident response team must document events, actions and key discoveries as they occur to improve decision-making during the response process and for post-incident analysis. Records should be kept in a single location where they are visible to all incident responders. The cyber security incident manager must ensure that minutes are taken for meetings held to facilitate incident handling including a record of decisions. In cases that may involve legal proceedings, responders must consult the UQ Integrity Unit for advice regarding note taking, evidence collection and safe storage.

Communications

(35) The timing and quality of communications is critical to minimising harm to individuals and reducing the reputational impact of significant incidents. Communication must be timely and accurate and should convey empathy with impacted persons and demonstrate action.

(36) All communications to parties outside the incident response team must be strictly controlled by the internal and external communications leads (see Table 1), with the exception of incident notification requirements defined in the ‘Incident Notification’ provisions in section 2 and in specific incident response plans.

(37) Where possible, a thorough understanding of the incident's possible impacts should be determined before communications are released. However, communications should consider the impact on individuals and potential reputation damage caused by delays while waiting for more accurate information.

(38) The ITS Cyber Security Team are responsible for ensuring communication plans and templates are produced and approved in advance to facilitate a more rapid response. Plans should take into account that some channels may not be available during a severe incident.

(39) All communications must comply with the Communications and Public Comment Using The University of Queensland's Name Policy and the ITS Communications Local Standard Operating Procedure. Legal Services must review communications to third parties and the general public.

Part D - Containment

Authority to Disable and Modify IT Services

(40) During incident containment it may be necessary to fully or partially disable IT services at short notice to avoid significantly increased impacts. It may not be feasible to consult the key stakeholders generally required to approve such changes. Instead, incident responders may obtain timely approval from anyone listed below (in preferential order). Incident responders should seek approval from the person with the highest preference that is available within the required timeframe, while also ensuring to follow the IT Change Management Procedure:

a. Registered business or service owner;
b. Director, Cyber Security;
c. CIO;
d. CSOC Manager;
e. After-hours senior CSOC staff.

Part E - Eradication

(41) The Cyber Security Incident Manager is responsible for deciding when eradication activities can be terminated, and recovery activities can commence.

Part F - Recovery

(42) Activity to restore damaged services must align with the IT Incident Management Procedure. The Cyber Security Incident Manager directs IT staff and IT Major Incident Managers to ensure restoration activities do not conflict with cyber security incident handling. When applicable, IT service disaster recovery procedures should be enacted during this phase to facilitate rapid restoration and return to business-as-usual operations.

Part G - Lessons Learned

(43) For complex incidents, the CSOC will perform a root cause analysis during the lessons learned phase to identify vulnerabilities and control weaknesses that contributed to the incident.

(44) For incidents that caused a Moderate or higher impact, the Cyber Security Incident Manager must organise a post-incident review meeting within 10 business days of incident closure. After the review they must distribute and an incident report within 20 business days. The incident report must include key events and timings, decisions, root-cause analysis, and improvement actions.

(45) The post-incident review meeting should include members of the incident response team and the ITS Security

Architect. The objectives of the review meeting are to:

a. acknowledge contributions to the incident response,
b. discuss any issues that may have arisen as a result of the incident, including residual impacts on staff,
c. validate the findings of the root cause analysis,
d. evaluate the impacts of the incident and validate the final impact rating, and
e. identify and validate key lessons and improvement actions.

(46) Proposed improvement actions must be approved by relevant managers, assigned to responsible staff, and added to the IT Outstanding Actions Register for tracking.

Section 4 - Roles, Responsibilities and Accountabilities

Cyber Security Incident Manager

(47) The Cyber Security Incident Manager is responsible for:

a. coordinating cyber security incident response activities according to this Procedure;
b. directing teams and staff members as required;
c. coordinating technical and general response teams;
d. activating external incident response support as needed;
e. deciding when eradication activities can be terminated, and recovery activities can commence;
f. ensuring incident notifications occurs when required;
g. ensuring adequate records are kept during the incident handling process; and
h. ensuring minutes are taken for meetings held to facilitate incident handling including a record of decisions.

Vice-Chancellor

(48) The Vice-Chancellor is responsible for chairing the Crisis Management Team (CMT) and making key decisions regarding Critical (Tier 3) cyber security incidents.

Chief Operating Officer (COO)

(49) The COO is responsible for chairing the University Incident Management Team (UIMT) and key decisions regarding Major (Tier 2) cyber security incidents.

Chief Information Officer (CIO)

(50) The CIO is responsible for resourcing the technical cyber security incident response capability and associated IT functions. The CIO is also part of the UIMT and CMT when required.

Director, Cyber Security, ITS

(51) The Director, Cyber Security is accountable for cyber security incident management. They are responsible for:

a. the technical management of Major and higher (Tier 2 and Tier 3) cyber security incidents; and
b. approving cyber security incident response plans.

(52) The Director, Cyber Security is also part of the UIMT and CMT when required.

University Crisis Management Team (CMT)

(53) The CMT provides executive leadership for critical cyber security incidents.

University Incident Management Team (UIMT)

(54) The UIMT provides control and coordination of incident resolution actions across multiple UQ functions for Major (Tier 2) cyber security incidents and support to the CMT for Critical (Tier 3). It reports to the CMT as required.

Cyber Security Operations Centre (CSOC) Manager, ITS

(55) The Manager, CSOC is responsible for:

a. acting as the Cyber Security Incident Manager and making key decisions for Insignificant and Minor (Tier 1) cyber security incidents;
b. cyber security incident statistics, and
c. maintaining the register of cyber security incident reports.

Cyber Security Operation Centre

(56) The CSOC is responsible for technical cyber security incident response processes including the initial assessment of incidents.

Cyber Security Change and Communications Officer, ITS

(57) The Cyber Security Change and Communications Officer is responsible for:

a. acting as the internal communications lead for Minor and Moderate (tier 1) incidents; and
b. drafting communication templates and plans for cyber security incidents.

IT Managers

(58) IT Managers are responsible for:

a. creating and maintaining local cyber security incident response procedures related to security controls or IT systems they are responsible for, and
b. incident response activities performed by their team.

Business Resilience Manager, Governance and Risk Division

(59) The Business Resilience Manager is responsible for:

a. facilitating incident escalation from Tier 1 to Tier 2 and Tier 3 levels;
b. coordinating the standing up of the UIMT and CMT as required;
c. assisting with the coordination of the UIMT and CMT; and
d. facilitating incident de-escalation for critical and crisis incidents.

(60) The Business Resilience Manager is also a single point of contact for mobilising incident response resources in the Enterprise Governance and Risk Team.

Security Architect, ITS

(61) The Security Architect is responsible for:

a. maintaining this Procedure (including implementation and compliance monitoring) as part of the Information Security Management System (ISMS);
b. maintaining and developing cyber security incident response plans. and the overall cyber security framework; and
c. overseeing the high-level deployment of technical security controls.

Cyber Security Improvements Manager, ITS

(62) The Cyber Security Improvements Manager is responsible for:

a. organising and recording cyber security incident tabletop exercises;
b. distributing summary reports of exercises; and
c. ensuring tabletop exercises are recorded in the cyber security training register.

Senior Manager, Internal Communication, Marketing and Communication

(63) The Senior Manager, Internal Communication is responsible for communications to the UQ community that occur during Major (Tier 2) and Critical (Tier 3) incidents.

Senior Manager, Corporate Communication, Marketing and Communication

(64) The Senior Manager, Corporate Communication is responsible for communications to parties outside UQ during incidents.

IT support teams

(65) IT support teams are responsible for triaging reports of potential cyber security incidents and escalating to the CSOC as required.

Right to Information and Privacy Office

(66) The Right to Information and Privacy Office are responsible for notifying external regulators of privacy breaches.

Integrity Unit

(67) The Integrity Unit is responsible for providing advice and assistance with incidents involving internal staff actors and liaising with law enforcement agencies if required.

Student Complaints and Grievance Resolution

(68) The Student Complaints and Grievance Resolution team is responsible for providing advice and assistance with incidents involving internal student actors.

Information Domain Custodians

(69) Information Domain Custodians (see Information Governance and Management Framework for details) are responsible for key decisions impacting their information domains.

External service providers

(70) Service providers engaged by UQ are responsible for:

a. reporting potential and actual cyber security incidents that may impact UQ data or services using the cyber security incident reporting form; and

b. providing regular incident status updates and information as part of UQ’s cyber security incident response.

Section 5 - Monitoring, Review and Assurance

(71) The Security Architect will:

a. review and update this Procedure as required to ensure its accuracy and efficacy;
b. report on the maturity of cyber security incident response in the cyber security dashboard to UQ and IT risk committees; and
c. provide updates and monitoring regarding development of cyber security incident plans and execution of tabletop exercises to the Cyber Security Risk and Compliance Committee (CSRCC).

(72) Cyber Security Incident Managers will report any significant deficiencies or deviations from this Procedure (identified as part of the lessons learned phase) to the CSRCC.

Section 6 - Recording and Reporting

(73) For the purposes of reporting, the scope of an incident will include all the events within a single campaign. A campaign is a series of actions taken by the same threat actor within a specific time period. The CSOC will record the following information for each incident:

a. final impact (refer to the Consequence Rating Table);
b. number of people impacted (0, 1-100, 101-1000, 1001-10K, >10K);
c. incident category for insignificant incidents;
d. degree of effort spent on the incident resolution (see Table 4);
e. incident response time; and
f. incident resolution time.

(74) Incident statistics and summaries of significant incidents are included in quarterly cyber security reports to the IT Policy, Risk and Assurance Committee (IT PRAC), the Vice-Chancellor's Risk and Compliance Committee (VCRCC), and the Senate Risk and Audit Committee (SRAC).

(75) Cyber security incident reports are stored in the cyber security incident report register. All incident reports must be distributed to the CSRCC, VCRCC and SRAC. Incident reports are distributed to USET as required.

(76) Tabletop exercises are recorded in the cyber security training register. Summary reports of tabletop exercises must be distributed to attendees and the VCRCC and USET if required.

(77) Actions from tabletop exercises and improvement actions from post-incident reviews are recorded in the IT Outstanding Actions Register for tracking.

Section 7 - Appendix

Incident Notification – Security of Critical Infrastructure Act 2018

(78) Under the Security of Critical Infrastructure Act 2018, UQ has a responsibility to report cyber security incidents that impact its critical infrastructure assets.

(79) The CSOC will report all cyber security incidents with an impact rating (see risk matrix) of Minor and above to

the Australian Cyber Security Centre (ACSC). The following specifications apply:

a. Incidents that significantly impact the availability of an asset: UQ must notify the ACSC within 12 hours after becoming aware of the incident. If the initial report is made verbally, UQ must submit the written report within 84 hours of the verbal notification.
b. Incidents that have a relevant impact on an asset: UQ must notify the ACSC within 72 hours after becoming aware of the incident. If the initial report is made verbally, UQ must submit the written report within 48 hours of the verbal notification.

Incident Handling Activities

(80) The following table lists activities that typically occur during incident handling processes.

Table 2: Incident Handling Activities

Phase	Activities
Identification	• Monitoring threat intelligence for active threats. • Reviewing reports from UQ consumers, IT staff, external service providers and security researchers. • Collecting specific data related to the incident. • Correlating separate data sources. • Performing research into similar incidents. • Establishing additional monitoring specific to the incident. • Tuning or developing scripts to process the available data to see high-level patterns.
Containment	• Disconnecting systems from the network. • Disabling or resetting system components. • Blocking network traffic. • Backing up threatened data. • Removing malicious email messages from inboxes. • Disabling user accounts.
Eradication	• Deleting malicious code or software • Resetting passwords on compromised accounts. • Mitigating vulnerabilities exploited in the incident. • Identifying and removing persistent access.
Recovery	• System restoration. • System testing. • Remediation of vulnerabilities exploited in the incident. • Adjusting relevant controls. • Adjusting logging and monitoring systems.
Lessons learned	• Post-incident review meeting. • Determining the root cause of the incident. • Producing an incident report. • Estimating financial impact for medium and high-impact incidents. • Identifying required updates to response plans and procedures, the cyber security risk register and cyber security standards. • Identifying control improvements. • Debrief staff involved in the incident response, ensuring personal impacts are addressed.

Approved Threat Intelligence Networks

(81) The following table lists approved threat intelligence networks:

Table 3: Threat Intelligence Networks

Organisation
AusCERT
AARNet

Organisation
Australian Cyber Security Centre (ACSC)

Key Contacts

(82) Key contacts include:

a. UQ Cyber Security Operations Centre (CSOC);
b. UQ Right to Information and Privacy;
c. UQ Integrity Unit;
d. UQ Legal Services;
e. Student Complaints and Grievance Resolution;
f. Property and Facilities Security;
g. AUSCERT;
h. Australian Cyber Security Centre.

Degree of Effort

(83) The following table defines ratings for the degree of effort required to resolve an incident.

Table 4: Degree of effort

Effort Rating	Total Time Expended
Low	Up to 1 FTE day
Medium	Between 1 FTE day and 1 FTE week
High	More than 1 FTE week

Status and Details

Status	Historic
Effective Date	27th September 2023
Review Date	27th September 2026
Approval Authority	Chief Information Officer
Approval Date	27th September 2023
Expiry Date	29th January 2025
Policy Owner	Marni Jacoby Chief Information Officer
Enquiries Contact	Information Technology Services