Procedure Title: **DCS Cyber Security Incident Response**

Procedure Owner: **Manager - Digital, Governance, Risk, Security and Operations**

This procedure must be followed in response to responding to all Cyber Security Incidents and, ensure the University complies with its obligations under the *Security of Critical Infrastructure Act 2018* for applicable cyber security incident categories defined by the Act.

---

1. INTENT

The purpose of this procedure is to document the process for triaging and managing Cyber Security Incidents.

2. ORGANISATIONAL SCOPE

The scope of this procedure applies to Digital and Campus Services staff, contractors, vendors and outsourced personnel.

3. DEFINITIONS

The University Glossary and the following definitions apply to this procedure:

Term:	Definition:
Critical Incident	A critical incident is an event that poses a significant risk to the continuity of core University-wide operations.
Cyber Security Incident	One or more acts, events or circumstances involving any of the following: (a) unauthorised access to (i) computer data or (ii) a computer program; (b) unauthorised modification of (i) computer data or (ii) a computer program;

Term:	Definition:
	(c) unauthorised impairment of electronic communication to or from a computer; or (d) unauthorised impairment of the availability, reliability, security or operation of (i) a computer, (ii) computer data or (iii) a computer program.
Data Breach	The loss, unauthorised access or unauthorised disclosure of Personal Information.
DCS	Digital and Campus Services
Incident Manager	A role of co-ordinating and liaising between the Service Desk and the technical leads. Incident Managers handle direct communication with the service owner (and any stakeholders). They can orchestrate additional resource and replacement resource if timelines become extended. After a Global email, they may initiate further emails for IT Service Desk to send and are a source of information and advice during an outage.
Major Incident	A major incident is an event that has significantly impacted the operations of a specific School, Centre, or campus location.
Playbook	A procedural guideline referred to by Security Operations in responding and closing out a cyber incident.
Security Operations	ECU Digital Governance, Risk, Security and Operations - Information Security Analysts with roles and responsibilities for the implementation, operations and management of information security within ECU.
SLA	Service Level Agreement for Tier Application delivery.
SOC	Security Operations Centre managed through AARNet.

4. PROCEDURE CONTENT

4.1. The DCS Cyber Security Incident Response Process appended to this procedure will govern the general approach to Cyber Security Incidents together with the consideration of any potential external reporting requirement as described in the addendum.

4.2. **Detect Incident.** Cyber Security Incident detection may appear from one or several simultaneous sources i.e. staff, students, concerned citizens, statutory/government bodies, cyber monitoring or management systems. Upon detection a ServiceNow Incident Ticket is required to be opened.

4.3. **Investigate Incident**. Security Operations Team analyse, validate and investigate a Cyber Security Incident threat to inform decisions on how to respond or escalate.

4.4. **Respond to Incident**. Security Operations utilise tools, techniques, processes, playbooks, services or third parties to respond to the Cyber Security Incident threats. The goals are to 1) contain the incident ; 2) eradicate the threat footprint; 3) provide recovery advice or plans for the incident targets; and 4) close out the issue.

4.5. **Escalation points**. There are criteria that may require further actions potentially from outside of the Security Operations Team. DCS personnel should be aware of these criteria and potential impacts on individual teams when a Cyber Security Incident is to be escalated.

4.5.1. **A Major Incident or SLA Breach**. A Cyber Security Incident may interrupt ECU's ability to function in a partial manner or disrupt DCS services that breaches a SLA while the Security Operations Team investigate or respond. A DCS service breach of 30 minutes will initiate this process. Determination of a Major Incident is impact based and determined by the Incident Manager.

4.5.2. **Escalation of the Major Incident or SLA Breach.** This is subject to the incident causing a longer disruption of service or the impact of the incident increases. This cycle may have a small number of iterations before the Incident Manager escalates to the university's enterprise process.

4.5.3. **Invoke ECU Critical response process**. The Critical Incident Management Team will be formed at the time of invoking a Critical Incident with ECU executive membership, that will include the DCS Director and CIO or his nominee.

4.5.4. **Data Breach**. The Director, Strategic and Governance Services must be notified of any Data Breach, for action in accordance with the Data Breach Response Procedure.

4.6. **Escalation to DCS Management or CIMT.** While the incident is active and escalation has occurred, the DCS management function is to provide decision support to ensure that communication and further escalation are managed to DCS Service Management and Critical Incident Response processes while the Security Operations Team continue resolution action. The Security Operations Team's work instruction include notifying DCS Management or the CIMT of statutory reporting obligations. A copy of these instructions are included in this document as an addendum.

4.7. **Post Incident Actions**. During the **Respond to Incident** cycle, the Cyber Security Incident will be resolved. Within a reasonable timeframe following the end of a major or critical incident, the Security Operations Team is responsible to 1) Conduct a Post Incident Review; 2) Implement Improvements and 3) Review and update the Security Work instructions and processes for effectiveness. The Security Operations Team will complete administrative actions to close out the Service Now Incident Ticket and ensure that appropriate reporting is conducted and submitted to the Recovery Director and the Risk and Incident Management Committee.

5. ACCOUNTABILITIES AND RESPONSIBILITIES

The Procedure Owner is the Manager - Digital Governance, Security, Risk and Operations who is responsible for currency of information and provision of advice relating to these procedures.

6. RELATED DOCUMENTS

Acts

- Security of Critical Infrastructure Act 2018

Policies

- Information Security and Information Technology Policy
- Acceptable Use of Information Systems Policy
- Critical Incident and Business Continuity Management Policy
- Critical Incident and Business Continuity Management Guidelines
- Privacy Policy
- Data Breach Response Procedure

7. CONTACT INFORMATION

For queries relating to this document please contact:

Procedure Owner	Manager - Digital Governance, Security, Risk and Operations
All Enquiries Contact	Manager - Digital Governance, Security, Risk and Operations
Telephone:	6304 7129
Email address:	m.alberghini@ecu.edu.au

8. APPROVAL HISTORY

Procedure approved by:	Manager - Digital Governance, Security, Risk and Operations
Date procedure first approved:	May 2022
Date last modified:	May 2022: July 2022
Revision history:	Included references to Australian Cyber Security Center reporting obligations
Next revision due:	July 2025
HPCM file reference:	SUB/105687 DOC11150/22

Addendum

Mandatory Reporting of Cyber Security Incidents for Critical Infrastructure Process

After becoming aware of any Cyber Security Incident of any ECU asset used for research that is critical to another critical infrastructure sector, the defence of Australia or national security, ECU must notify the Australian Cyber Security Centre (ACSC) as soon as practicable and, in any event, within:

Critical Infrastructure entities are required to report cyber security incidents to the ACSC within:

- 12 hours, if the incident is having a significant impact on the availability of the asset, or
- 72 hours, if the incident is having an impact on the availability, integrity, reliability or confidentiality of information about, or held by, the asset.

The Cyber Security Incident timer commences at the time the "incident notifier" becomes aware of the incident.

A Cyber Security Incident that causes a disruption of 30 minutes in any DCS service category (T1-T4) is treated as a T1 service level response. Investigation of the incident will determine escalation to Manager – Digital Governance, Security, Risk and Operations and DCS Director and CIO who will make judgement on the 12- or 72-hour requirement and authorise submission to ACSC. In the event of their absence then the InfoSec Analyst is authorised to submit an ACSC report at the 11-hour mark, noting the reasons for the decision at the time of submission.

In the event of a CIMT being formed, the DCS nominee will inform the CIMT of their statutory obligations regarding ACSC reporting requirements.

Reporting Instructions

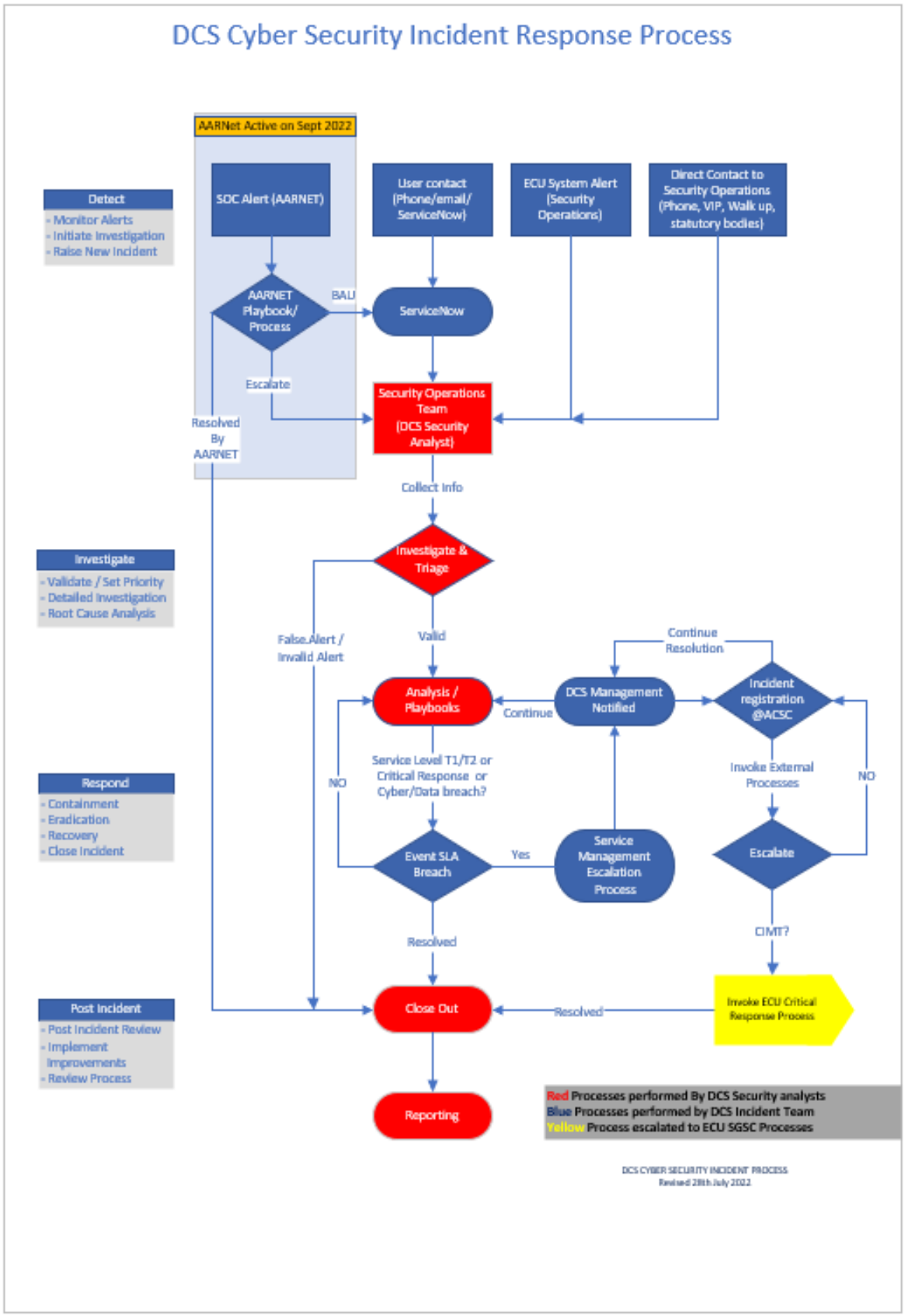
1. Report the cyber incident through the ACSC reporting web site https://www.cyber.gov.au/acsc/report/report-a-cyber-security-incident.

   Alternatively, a report can be made verbally through the Australian Cyber Security Hotline – 1300 CYBER1 (1300 292 371). If a report was made verbally, a written report is required within 84 hours for critical infrastructure or within 48 hours for other cyber security incidents after the verbal notification.
2. Select "To inform the ACSC" as the reason for reporting.
3. Provide the contact details of the authorised person reporting the incident.
4. Provide the organisation details

Question Header	Details
Organisation name	Edith Cowan University
ABN	54 361 485 361
State / Territory	WA
Postcode	6027
Website address	https://www.ecu.edu.au/
Is your organisation part of a critical infrastructure sector	Yes
Critical Infrastructure sector	Higher education and research
Are you making a mandatory cyber incident report under the Security of Critical Infrastructure Act 2018?	Yes
Do you content for this information to be provided to the relevant regulator?	Yes

5. Provide the incident details
   Date and time the incident was identified or the "noticed period" refers to the time when the incident was first observed or when a person become aware of the incident. This will be the start time for the 12- or 72- hour mark.

6. Submit the report and record the CIRS report number (Example: CIRS-20180512-1), the details of the incident and the email address used to submit the report into the Information Security, Risk and Governance site.


DCS Cyber Security Incident Response Process
AARNet Active on Sept 2022
SOC Alert (AARNET)
User contact (Phone/email/ ServiceNow)
ECU System Alert (Security Operations)
Direct Contact to Security Operations (Phone, VIP, Walk up, statutory bodies)
Detect
- Monitor Alerts
- Initiate Investigation
- Raise New Incident
AARNET Playbook/ Process
BAU
ServiceNow
Escalate
Security Operations Team (DCS Security Analyst)
Resolved By AARNET
Collect Info
Investigate & Triage
Investigate
- Validate / Set Priority
- Detailed Investigation
- Root Cause Analysis
False Alert / Invalid Alert
Valid
Continue Resolution
Analysis / Playbooks
DCS Management Notified
Incident registration @ACSC
Continue
Service Level T1/T2 or Critical Response or Cyber/Data breach?
NO
Invoke External Processes
NO
Respond
- Containment
- Eradication
- Recovery
- Close Incident
Event SLA Breach
Yes
Service Management Escalation Process
Escalate
CIMT?
Resolved
Post Incident
- Post Incident Review
- Implement Improvements
- Review Process
Close Out
Resolved
Invoke ECU Critical Response Process
Reporting
Red Processes performed By DCS Security analysts
Blue Processes performed by DCS Incident Team
Yellow Process escalated to ECU SGSC Processes
DCS CYBER SECURITY INCIDENT PROCESS
Revised 28th July 2022