# Resilience Policy

# Section 1 - Purpose

(1) The purpose of this policy is to outline the resilience framework and key processes that ensure Charles Sturt University (the University) effectively plans for, responds to, and recovers from disruptions.

(2) In line with the University's low risk appetite for business and crisis disruption events, this policy outlines the principles, roles and responsibilities of the University's resilience framework, managed through:

a. Emergency management
b. Crisis management
c. Business continuity management
d. IT disaster recovery

### Scope

(3) This policy applies to all staff, students, contractors, education partners and third-party service providers of the University and its controlled entities.

# Section 2 - Policy

### Resilience framework

(4) The objectives of the University's resilience framework are to:

a. affirm the University's priority to safeguarding the ongoing safety and wellbeing of students and staff during and following any disruption
b. provide an agreed structure and systematic approach that enables the timely and effective response to disruption
c. re-establish critical business processes as quickly and efficiently as possible
d. protect University facilities, infrastructure, assets and equipment as far as reasonably practicable, and
e. minimise any financial, legal, regulatory and reputational impacts arising from a disruption.

(5) The University’s resilience framework utilises the principles of AS/NZS 5050 (Int):2020 – Managing disruption-related risk; AS ISO 22301:2020 - Security and resilience - Business continuity management systems - Requirements; and AS 3745:2010 (Amd 2:2018) - Planning for emergencies in facilities.

(6) Disruption-related risk will be identified, assessed and evaluated through the ongoing risk control self-assessment process defined in the Risk Management Policy.

(7) The University adopts a risk-based approach to resilience and prioritises activities critical to the:

a. physical and psychological safety, security and wellbeing of staff and students, and

b. the survival of the University and the achievement of its strategic objectives in line with its recovery priorities.

(8) Critical to the success of the resilience framework is robust stakeholder engagement and collaboration to ensure the University is prepared to respond and recover from disruptions.

(9) The resilience framework will be based on the following four components, designed to be flexible and adaptable based on the nature of any disruption:

| Resilience framework | Purpose | Hierarchy of resilience framework documents | Oversight responsibility |
|---|---|---|---|
| **Emergency management** | To manage emergencies where an immediate internal or external emergency services response is required. | Emergency Management Procedure | Work Health and Safety Committee (acts at the University's Emergency Planning Committee) |
| | | Emergency plans | Emergency control organisations |
| **Crisis management** | To provide a strategic and systematic approach to the management of crises. | Crisis Management Procedure | Division of Safety, Security and Wellbeing |
| **Business continuity management** | To continue or re-establish critical business processes in a timely manner, in the event of a disruption. | Business Continuity Management Procedure | Risk and Compliance Unit |
| | | Portfolio and faculty-level business continuity plans (BCPs) | Portfolio leaders and Executive Deans |
| **IT disaster recovery** | To continue or re-establish critical technology and telecommunications within acceptable timeframes. | IT Disaster Recovery Procedure | Division of Information Technology |

(10) Each component of the resilience framework will develop strategies, processes and plans for each phase of the resilience cycle:

a. Prepare - to anticipate potential disruptions, remove or reduce sources of potential disruption or prepare to withstand the potential effects of disruption. It includes risk assessment, business impact analysis, business continuity planning, training, testing and establishing communication protocols to ensure the University is ready to respond and recover from disruptions.
b. Respond – to guide the activation of the University's response strategies, processes and plans in the event of disruption, including implementing actions to safeguard people, critical infrastructure and critical business processes. The response phase aims to contain and manage the impact of disruption in real time.
c. Recover – once the immediate response is addressed, focus shifts to recovery to restore normal operations. The recovery phase aims to return the University to full functionality, learn from the experience and identify opportunities to improve the resilience framework going forward.

(11) Components of the resilience framework will be reviewed and tested periodically to:

a. validate the information and efficiency of each strategy, process and plan
b. maintain awareness and familiarise staff with their resilience roles and responsibilities, and
c. continuously improve the resilience framework.

## Responsibilities

(12) This section summarises the responsibilities across the University for implementing the Resilience Policy.

| Officer or body | Responsibility |
|---|---|
| University Council | Primary responsibility for overseeing risk management across the University and its controlled entities. |
| Vice-Chancellor | 1. The overall management of the University's capability to prepare for, respond to and recover from disruptions.<br>2. Establishing and leading a Crisis Management Team to address crises impacting the University and to transition temporary crisis management arrangements to recovery as crises are resolved.<br>3. Ensuring adequate provision is made for communications to staff during disruptions.<br>4. Allocating adequate resources to enable effective resilience management across all levels of the University. |
| Portfolio leaders | 1. Designing, deploying and oversighting resilience strategies and processes to plan for, respond to and recover from disruptions.<br>2. Conducting business impact analysis to develop and maintain incident management plans and business continuity management plans across their areas of responsibility.<br>3. Carrying out regular reviews to test the validity and practicality of resilience strategies, processes and plans.<br>4. Ensuring that staff within their portfolios are trained to implement resilience strategies, processes and plans.<br>5. Conducting incident management debriefings.<br>6. Ensuring adequate support for staff and student physical and psychological wellbeing during periods of disruption.<br>7. Supporting staff following return to business-as-usual, including providing access to external support services where required. |
| Chief Operating Officer | In addition to portfolio leader responsibilities:<br>1.<br>Developing and maintaining the following procedures:<br>a. Emergency Management Procedure<br>b. Emergency plans<br>c. Crisis Management Procedure<br>d. Critical incident management plans, including but not limited to the Student Critical Incident Plan<br>e. IT Disaster Recovery Procedure<br>2.<br>Ensuring adequate provision is made for communications across the University during disruptions. |
| Risk and Compliance Unit | 1. Developing and maintaining this Resilience Policy and framework.<br>2. Routinely reviewing the design, implementation, and operating effectiveness of the resilience framework.<br>3. Developing and maintaining the following procedures to support relevant resilience strategies and processes:<br>a. Crisis Management Procedure<br>b. Business Continuity Management Procedure<br>4. Assisting areas to analyse, design, implement and train their staff on resilience strategies, processes and plans. |
| Crisis Management Team | Where convened in accordance with the Crisis Management Procedure:<br>1. Oversighting the deployment of applicable resilience strategies, processes, and plans to respond to crisis.<br>2. Establishing, oversighting and standing down operational response teams in line with operational needs.<br>3. Conducting incident management debriefings, where applicable. |
| Critical Incident Management Teams | Where convened in accordance with the Crisis Management Procedure:<br>1. Leading and coordinating the response to incidents that require cross-portfolio collaboration in line with the Crisis Management Procedure.<br>2. Oversighting the deployment of applicable resilience strategies, processes and plans to respond to disruptions.<br>3. Appointing and oversighting response and recovery teams to assist in the response to incidents at an operational level.<br>4. Providing regular reports to the Crisis Management Team.<br>5. Conducting incident management debriefings, where applicable |

| Officer or body | Responsibility |
|---|---|
| All staff | 1. Actively participate in activities that support the resilience framework, including participating in emergency trials, business impact analysis and crisis and business continuity management test activities.<br>2. Follow the directions of wardens during an emergency event, including an emergency trial event.<br>3. Undertake training as required. |

# Section 3 - Procedure

(13) The following procedurs support this policy:

a. Business Continuity Management Procedure
b. Crisis Management Procedure

# Section 4 - Guidelines

(14) Nil.

# Section 5 - Glossary

(15) This policy uses the following terms:

a. Business continuity management – means an enterprise approach for ensuring that critical business processes can be maintained or recovered in a timely manner, in the event of a disruption.
b. Business continuity plan(s) – means a documented response and recovery procedure aimed at ensuring the continuity of agreed critical business processes.
c. Business impact analysis – means risk analysis of the impact over time of business disruption on the University (AS ISO 22301).
d. Crisis – means an unexpected non-routine situation that is beyond the capacity of normal management structures and processes to deal with effectively, has both strategic and operational implications, and is often perceived as a potential existential threat (AS/NZS 5050).
e. Critical business process(es) – means a business process that aligns with the University's recovery priorities and is essential for the survival of the University and the achievement of its strategic objectives.
f. Disruption(s) – means any event or circumstance that significantly interferes with the normal operations and functions of the University (AS ISO 22301).
g. Emergency – means an event that arises internally, or from external sources, which may adversely affect the occupants or visitors in a facility, and which requires an immediate response (AS 3745).
h. Incident – means an event that can be, or could lead to a disruption, loss, emergency or crisis, including an adverse impact on the mental or physical wellbeing of any person (AS ISO 22301).
i. Recovery priorities – means business processes approved by the Executive Leadership Team as critical to University operations and, therefore, take priority in the event of disruption. Recovery priorities may change over time in line with changes to the University's strategic objectives.
j. Resilience – means a beneficial outcome that derives from a system’s ability to withstand, react and adapt to disruption, and to achieve a stable state where its purpose and priority objectives can be achieved (AS/NZS 5050).

## Status and Details

| | |
|---|---|
| **Status** | Current |
| **Effective Date** | 3rd April 2024 |
| **Review Date** | 3rd April 2029 |
| **Approval Authority** | Audit and Risk Committee |
| **Approval Date** | 3rd April 2024 |
| **Expiry Date** | Not Applicable |
| **Unit Head** | Anthony Heywood<br>University Secretary |
| **Author** | Julie Watkins<br>Risk and Compliance Adviser |
| **Enquiries Contact** | Risk and Compliance Unit |