Resilience Policy

Section 1 - Purpose

(1) The purpose of this policy is to set out the elements of organisational processes that are required to be in place to ensure the preparedness of Charles Sturt University (the University) to be able to effectively plan for, respond to, and recover from, disruptions.

(2) This policy is derived from the University's resilience framework set out in this policy.

Scope

(3) This policy applies to all academic and professional/general staff of the University, controlled entities, educational partnerships, contractors and adjunct staff.

Section 2 - Glossary

(4) For the purpose of this policy, the University has adopted the following definitions:

a. Business continuity – the capability of the University to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption (AS ISO 22301:2020).
b. Crisis – the 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 (Int):2020).
c. Disruption – an unplanned negative deviation from the expected delivery of products and services according to the University's objectives (AS ISO 22301:2020).
d. Emergency – 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 3745:2010).
e. Incident – 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 22301:2020).
f. Resilience – 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 (Int):2020).

Section 3 - Policy

Part A - Resilience framework

(5) The University's resilience framework is based on the following standards: 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 - Planning for emergencies in facilities.

(6) 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.

Phase 1: Planning

(7) Planning and preparing to respond to a disruption requires areas to evaluate the potential disruption, design a response and implement the following planning strategies, processes, oversighting and implementation responsibilities.

Planning strategies

(8) Awareness and anticipation strategies: to enable the University to understand potential sources and types of disruptions, as well as establish mechanisms to identify disruptive events and respond flexibly in a timely fashion. Such strategies may involve developing monitoring mechanisms to detect early warnings of change, scenario analysis, and awareness training.

(9) Prevention and protection strategies: to remove or reduce potential sources of disruption and minimise interaction with sources of disruption. For example, these strategies include establishing effective controls to prevent unwanted behaviour, ceasing activities with undue exposure to risk, developing safety procedures, relocating people away from sources of harm.

(10) Preparedness strategies: to improve the University's capability to respond to and withstand disruptive events. This entails improving the capability of people (e.g. leadership and team skills), infrastructure (e.g. reducing logical security vulnerabilities), contingency arrangements (e.g. manual workarounds), and management systems (e.g. reporting). Preparedness strategies include actively anticipating and mitigating the impacts of incidents on staff and student wellbeing.

Planning processes

(11) Risk assessment: to identify, analyse, and evaluate potential threats and sources of disruption.

a. Risk assessments should be conducted according to the Risk Management Procedure.
b. Threat identification may include incident reviews from within the University as well as across the higher education sector and the broader context.

(12) Business impact analysis (BIA): to assess the impact of a potential disruption and determine business continuity priorities and requirements. The BIA defines the types of impacts, criteria for assessing the impacts over time, maximum tolerable period of disruption, activities and resources to be prioritised, as well as dependencies (e.g. partners and suppliers).

(13) Response procedures and plans: to be activated by relevant areas and response teams when addressing a disruption. Procedures and plans must specify practical steps to respond to a disruption, be flexible in responding to any changes in internal and external conditions of a disruption, be effective in minimising the effects of a disruption, and assign roles and responsibilities for tasks. These procedures and plans should consider wellbeing and support protocols, succession plans, and staff emergency contact and next of kin notification.

(14) Training and testing: to ensure individuals and teams are enabled to respond to disruptions and enact relevant response procedures and plans, as well as to validate the effectiveness of resilience strategies (e.g. through drills and simulations).

Oversighting the planning phase

(15) Oversighting the development of plans to respond to a disruption will involve the following areas across the University:

a. The Risk and Compliance Unit will oversight:
    i. the implementation of the University's resilience framework to provide reasonable assurance that areas are preparing to respond to potential disruptions according to the planning strategies outlined above,
    ii. the development of standardised processes and templates to assist areas to prepare for potential disruptions,
    iii. the development and delivery of training to enhance the University's capability to plan, respond to, and recover from, disruptions, and
    iv. the testing and review of the University's preparedness to respond to disruptions.
b. The Division of Facilities Management will oversight the University's emergency management process to ensure the completion of the planning strategies and development of attendant structures, policies, procedures and plans.
c. The Division of Information Technology will oversight the development, maintenance, testing, and update of the University's IT disaster recovery plan.
d. Portfolio leaders will oversight the development of the planning strategies and planning processes outlined above within their respective portfolios.

Implementing the planning phase

(16) The following areas will implement the strategies and processes associated with the planning phase:

a. Emergency Planning Committees will develop University-wide and/or facility specific emergency plans.
b. Business owners of critical functions are to develop business continuity plans for their areas.
c. Portfolio or cross-portfolio teams, as identified by portfolio leaders, to develop response procedures and plans for other incidents (e.g. for an incident involving an overseas student).

Phase 2: Response

(17) Responding to a disruption requires areas to design and implement the following response strategies, processes, oversighting and implementation responsibilities.

Response strategies

(18) Communication strategies: to inform stakeholders about disruptive events, as well as the University's responses and expected adjustments to processes and behaviours. Communications strategies include the provision of timely and accurate advice about the disruption, alternative arrangements to respond to the disruption, and approaches to recovery.

(19) Containment strategies: to prevent the spread of disruption effects, including the potential use of quarantine, isolation, evacuation, relocation, and hibernation responses.

(20) Stabilisation strategies: to prevent further incident and volatility. These strategies may include, for example, senior management involvement, reprioritising workloads, ceasing non-essential activities, and enhancing information provision.

(21) Suppression strategies: to reduce the sources and effects of an incident. Countermeasures aimed at reducing the source of an incident include, for example, removing an insider threat. Countermeasures focused on addressing effects involve, for instance, responding to cybersecurity incidents.

(22) Contingency strategies: to safeguard the continuity of critical business functions, including the reprioritisation of objectives, redeployment of resources, activating emergency response, business continuity or disaster recovery plans and adjusting supplier arrangements.

(23) These response strategies should include considerations to support the wellbeing of persons directly or indirectly affected by an incident.

Response processes

(24) Emergency management: to ensure that resources and services are efficiently mobilised and deployed in response to an emergency.

(25) Critical incident management: to ensure that predetermined or bespoke leadership arrangements and functional teams are mobilised and deployed to manage the disruption on behalf of the University.

(26) Crisis management: to ensure that crises are adequately managed by a Crisis Management Team made up of representatives of the Vice-Chancellor's Leadership Team and specialist expert advisers.

(27) Business continuity management: to safeguard the University’s capability to maintain its critical functions and areas, as well as deliver essential products and services during a disruption, while supporting the recovery towards pre-existing or modified business as usual operations.

(28) IT disaster recovery: to ensure the timely response and restoration of the University’s IT infrastructure, electronic data and access to applications, in the event of a disruption. IT disaster recovery also entails the re-establishment of cybersecurity protocols for affected information systems.

(29) Response processes should be carried out in accordance with relevant procedures and/or plans.

Oversighting the response phase

(30) Oversighting the response to a disruption will involve the portfolio leader of the portfolio of origin of the incident. In general, portfolio leaders will oversight incidents as set out below:

a. Chief Operating Officer: Incidents involving emergencies, staff, campus security, facilities, contractors, suppliers, and IT.
b. Deputy Vice-Chancellor (Students): All incidents involving students, whether domestic or international, onshore or offshore.
c. Deputy Vice-Chancellor (Research and Engagement): Incidents involving the functioning of educational partnerships, industry engagement, research, as well as centres and institutes within the portfolio.
d. Provost and Deputy Vice-Chancellor (Academic): Incidents involving learning and teaching and library services, the functioning of the faculties, schools, library, laboratories, as well as centres within the portfolio.

(31) If necessary, portfolio leaders responsible for oversighting a particular incident may convene a cross-portfolio Critical Incident Management Team (CIMT), to be chaired by the responsible portfolio leader or another member of the CIMT. The aim of a CIMT is to draw on multidisciplinary expertise to respond to an incident. A CIMT may also be appointed by the Crisis Management Team (see below).

(32) A Crisis Management Team (CMT) chaired by the Vice-Chancellor and composed of representatives of the Vice-Chancellor's Leadership Team, and other representatives as required, will oversight the University's response to a crisis. The CMT have the authority to approve and provide clarity in relation to working arrangements and circumstances otherwise unanticipated by standing policy and procedure. The purpose of the CMT is to ultimately guide response teams while also having regard to the implications of the disruptive event for the University, including internal and external stakeholders.

Implementing the response phase

(33) Incident response strategies and processes will be carried out by the following areas across the University:

a. Emergency control organisations to implement campus emergency response plans.
b. Nominated responders to implement functional area business continuity plans.
c. Response teams within or across portfolios, as identified by portfolio leaders, CIMT or CMT, to respond to other incidents.

Phase 3: Recovery

(34) Recovering from a disruption requires areas to design and implement the following recovery strategies, processes, oversighting and implementation responsibilities.

Recovery strategies

(35) Strategic recovery: to reconfirm, modify or reprioritise the University's strategic plan in light of the disruption. While strategic recovery at the University-level is managed by the Vice-Chancellor's Leadership Team, at the portfolio-level it is managed by portfolio leaders.

(36) Functional recovery: to re-establish or introduce changes to the organisational structures and functions with a view to deliver existing or modified products or services (e.g. re-structuring areas to reflect new strategic objectives).

(37) People recovery: to assist individuals and teams to return to previous or modified work arrangements, organisational structures, and processes, as well as support their wellbeing (e.g. through mentoring, counselling, coaching).

(38) Infrastructure recovery: to restore affected facilities, equipment, IT and telecommunications, and other physical assets (e.g. equipment repair). Infrastructure recovery arrangements should include assets owned or operated by third-parties to provide services to the University (e.g. partnership facilities).

(39) Process, systems and information recovery, including the restoration of IT systems, data, and information, as well as the re-design of processes (e.g. learning and teaching processes).

Recovery processes

(40) Recovery from the effects of a disruption and restoring capability will be driven by business continuity management and IT disaster recovery processes. Both processes should be designed to deliver on the recovery strategies outlined above, including where interdependencies exist with University suppliers, partners or other third parties.

Oversighting the recovery phase

(41) Oversighting the recovery to a disruption will involve the following:

a. Portfolio leaders will oversight the recovery from disruptions originating from their respective portfolios. In general, portfolio leaders will oversight disruptions associated with the incidents outlined in clause 30.
b. A recovery committee may also be appointed by portfolio leaders, CIMT or CMT to oversight recovery from certain incidents, as required.
c. Debrief of the overall incident management response and recovery processes.

Implementing the recovery phase

(42) Disruption recovery strategies and processes will be carried out by the following areas across the University:

a. Portfolio leaders responsible for managing the disruption within their portfolios.
b. Recovery teams appointed by portfolio leaders, recovery committee, CIMT or CMT.

(43) In implementing a return to business as usual operations, consideration should be given to learnings and opportunities that have been realised throughout the incident management phase, recognising that post-incident operations may include considered varied business processes arising from the incident itself.

(44) Student and staff wellbeing should be considered throughout the implementation of the recovery phase.

Hierarchy of supporting documentation

(45) The resilience framework will be supported by the hierarchy of policy, procedures and plans.

Part B - Responsibilities

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

(47) The Vice-Chancellor is responsible for the following:

a. The overall management of the University's capability to prepare for, respond to and recover from incidents.
b. Establishing and chairing a Crisis Management Team to address crises impacting the University and to transition temporary crisis management arrangements to recovery as crises are resolved.
c. Ensuring adequate provision is made across the University for communications to staff during incident management.
d. Delegating, as appropriate (e.g. via the Office of the Vice-Chancellor), the following operational responsibilities to implement the University's Resilience Policy:
    i. designing, deploying and oversighting resilience strategies and processes to plan for, respond to, and recover from, incidents under the responsibility of the Office of the Vice-Chancellor (e.g. the functioning of the University's governance structures, such as the University Council)
    ii. developing and maintaining business continuity plans to support relevant procedures within each portfolio
    iii. carrying out regular reviews to test the validity and practicality of relevant resilience strategies, processes, procedures and plans
    iv. ensuring that staff within each portfolio are trained to implement relevant resilience strategies, processes, procedures, and plans.

(48) The Chief Operating Officer is responsible for the following:

a. Designing, deploying and oversighting resilience strategies and processes to plan for, respond to, and recover from, incidents involving emergencies, staff, campus security, facilities, contractors, suppliers and IT.
b. Developing and maintaining the following procedures to support relevant resilience strategies and processes:
    i. Emergency management procedure
    ii. IT disaster recovery procedure
c. Developing and maintaining the following plans to support relevant procedures:
    i. Emergency plans
    ii. Incident management plans within their portfolio (e.g. staff wellbeing plan, contractor incident plan)
    iii. Business continuity plans within their portfolio

(49) The Deputy Vice-Chancellor (Students) is responsible for the following within their portfolio:

a. Designing, deploying and oversighting resilience strategies and processes to plan for, respond to, and recover from, incidents involving domestic and international students, both onshore and offshore.

b. Developing and maintaining the following plans to support relevant procedures:
    i. Incident management plans (e.g. student wellbeing plan, international student incident plan)
    ii. Business continuity plans
c. Ensuring adequate provision is made across the University for communications to students during periods of incident management.

(50) The Deputy Vice-Chancellor (Research and Engagement) is responsible for the following within their portfolio:

a. Designing, deploying and oversighting resilience strategies and processes to plan for, respond to, and recover from, incidents involving the functioning of educational partnerships, industry engagement, research, as well as centres and institutes.
b. Developing and maintaining the following plans to support relevant procedures:
    i. Incident management plans (e.g. partnership incident management plans)
    ii. Business continuity plans

(51) The Provost and Deputy Vice-Chancellor (Academic) is responsible for the following within their portfolio:

a. Designing, deploying and oversighting resilience strategies and processes to plan for, respond to, and recover from, incidents involving the functioning of the faculties, schools, library, laboratories, as well as centres.
b. Developing and maintaining the following plans to support relevant procedures:
    i. Incident management plans
    ii. Business continuity plans

(52) All portfolio leaders are responsible for the following within their portfolio:

a. Carrying out regular reviews to test the validity and practicality of relevant resilience strategies, processes, and plans.
b. Ensuring that staff are trained to implement relevant resilience strategies, processes, and plans.
c. Establishing a Critical Incident Management Team to address issues arising from their portfolio but which requires cross-portfolio collaboration.
d. Conducting incident management debriefings.
e. Ensuring adequate provision is made to support staff and student wellbeing during periods of incident management.

(53) The Risk and Compliance Unit is responsible for the following:

a. Reviewing the efficacy of and maintaining this Resilience Policy and framework.
b. Implementing procedures to routinely review the design, implementation, and operating effectiveness of the procedures and plans associated with this Resilience Policy and framework.
c. Developing and maintaining the following procedures to support relevant resilience strategies and processes:
    i. Critical incident management procedure
    ii. Crisis management procedure
    iii. Business continuity management procedure
d. Assisting areas to design and deploy resilience strategies, processes, procedures, and plans, as well as to train their staff on these approaches.

(54) Where convened in accordance with the critical incident management procedure, Critical Incident Management Teams are responsible for the following:

a. Leading and coordinating the response to incidents that require cross-portfolio collaboration.
b. Oversighting the deployment of applicable resilience strategies, processes, procedures, and plans to respond to incidents.
c. Appointing and oversighting response teams to assist in the response to incidents at an operational level.
d. Appointing and oversighting recovery teams to assist in the recovery from incidents at an operational level.
e. Advising the need to establish a Crisis Management Team, as appropriate.
f. Providing regular reports to the Crisis Management Team, where convened.
g. Conducting incident management debriefings, where applicable.

(55) Where convened in accordance with the crisis management procedure, the Crisis Management Team is responsible for the following:

a. Oversighting the deployment of applicable resilience strategies, processes, procedures, and plans to respond to crisis.
b. Oversighting Critical Incident Management Teams, where convened.
c. Appointing and oversighting response teams to assist in the response to crisis at an operational level.
d. Appointing and oversighting recovery teams to assist in the recovery from crisis at an operational level.
e. Conducting incident management debriefings, where applicable.

Section 4 - Guidelines

(56) Nil.

Status and Details

Status	Current
Effective Date	2nd March 2021
Review Date	2nd March 2024
Approval Authority	University Council
Approval Date	2nd March 2021
Expiry Date	Not Applicable
Unit Head	Natalie Nixon University Secretary
Author	Marcos Tabacow Director, Risk and Compliance
Enquiries Contact	Risk and Compliance Unit