# Business Continuity Management Procedure

# Section 1 - Purpose

(1) The Business Continuity Management Procedure forms part of Charles Sturt University's (the University) overall resilience framework.

(2) In circumstances where there is a disruption event that interferes with the normal operations and functions of the University, this procedure outlines the University's approach in preparing, responding and recovering from disruptions and the prioritisation of resources required to minimise impacts to the University's critical business processes.

(3) The purpose of this procedure is to:

a. identify and address business continuity risks, with a focus on building resilience and response capabilities
b. provide a structured and consistent approach to business continuity to enable a timely and effective response to disruption and minimise any potential detriment to students, staff, University partnerships and other stakeholders
c. provide a set of recovery priorities aligned to the University's strategic objectives to guide the criticality of the University's business processes and prioritise resources in the event of a disruption, and
d. communicate effectively, both internally and externally, throughout a disruption event.

### Scope

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

(5) Where a disruption occurs, the following elements of the resilience framework should be enacted:

a. For immediate emergency response, see the Emergency Management Procedure.
b. For escalation of emergencies, crises, critical incidents, disruptions or other significant incidents, see the Crisis Management Procedure.
c. For operational management of critical incidents, see Crisis Management Plan.
d. For information technology (IT) planning, response and recovery, see the IT Disaster Recovery Procedure maintained by the Division of Information Technology.
e. The Student Critical Incident Plan may also apply for on or off-campus student-related emergencies.

# Section 2 - Policy

(6) This procedure supports the Resilience Policy.

# Section 3 - Procedure

(7) The first priority in any disruption event will be the ongoing safety of students, staff and visitors. Staff are to follow

the directions of wardens during any emergency event.

(8) This procedure incorporates principles from AS ISO 22301:2020 Security and resilience – business continuity management systems – requirements.

## Disruption scenarios

(9) The following range of scenarios are considered in scope for the response and recovery processes outlined in this procedure:

a. Technology or data event – cyber security breach, data or privacy breach, lack of availability of critical IT networks, systems or applications, lack of availability of critical information or data.
b. Safety, security or wellness event – student, visitor or staff serious injury or fatality, child-related incident, pandemic or health-related incident that impacts normal operations.
c. Physical infrastructure and assets – loss of access to critical premises or infrastructure, natural disaster, environmental incident, supply chain incident, loss of or contamination to water or sewer, animal welfare incident.
d. Political event – geopolitical risk, international or domestic travel bans, substantial change to education or migration frameworks.
e. Reputational event – key person or third-party provider loss, loss of professional accreditation, loss of registration or application of registration conditions, material financial event, change management event, public relations incident on or off campus that impacts normal operations.

## Methodology

(10) Business continuity management encompasses the identification and risk management of critical business processes in line with the University's Risk Management Policy. The University’s approach to managing business continuity includes:

a. Risk assessment – disruption-related risks are identified, including the assessment of potential disruption scenarios and identification of recovery priorities defined by the University's strategic objectives.
b. Business impact analysis – focused on the identification and prioritisation of critical business processes in line with agreed recovery priorities.
c. Business continuity plans – aimed at the full restoration of critical business processes to business as usual.
d. Critical IT services – third-party and IT service dependencies are identified in assessing the critical business processes.
e. Validating capability – business continuity plans and IT service testing is performed to validate recovery capability.

(11) The University’s recovery priorities are determined in line with the University's strategic objectives and are used, in conjunction with business impact analysis results, to guide the criticality of the University's business processes and prioritise recovery. The University’s recovery priorities are outlined below:

a. Learning and teaching
b. Technology
c. Security, safety and wellbeing
d. Infrastructure and assets
e. Payments – including staff payroll
f. Student support services – including student admissions and enrolments
g. Regulatory requirements

h. Research

## Business impact analysis

(12) A business impact analysis process will be undertaken annually, facilitated by Risk and Compliance Unit in conjunction with each portfolio and faculty to identify and validate critical business processes. Performing business impact analysis assesses the impact of disruptions to the University's business processes, including:

a. identifying realistic disruption scenarios and the likelihood of scenarios leading to a short, medium or long-term disruption
b. identifying business processes supporting the University's recovery priorities
c. assessing the time impact of disruptions to business processes, including determining the maximum tolerable outage timeframes to prioritise response and recovery activities
d. the minimum level of resources required to respond to and recover critical business processes
e. the impact to, and the reasonable expectations of, students, suppliers and stakeholders, including impact to third-party partnerships
f. the critical IT systems and infrastructure required to respond to and recover critical business processes
g. the critical interdependencies that are not within the University's direct control, such as third-party partners key suppliers, the ongoing access to utilities, etc
h. the impact of environmental factors such as natural disasters, and the impact to local communities
i. identifying monitoring and surveillance indicators to improve anticipatory awareness, and
j. confirming awareness and anticipatory, prevention and protection, preparedness, response, relief and recovery strategies and controls.

(13) Maximum tolerable outage times for IT systems identified through the business impact analysis process should reconcile with recovery times defined in the University's IT Disaster Recovery Procedure.

(14) Maximum tolerable outage (MTO) times across critical business processes will be based on:

| High or very high impact timeframe | MTO |
|---|---|
| Immediate | 4 hours |
| Today | 12 hours |
| Next day | 24 hours |
| Two calendar days | 48 hours |
| More than two calendar days | 48+ hours |

(15) If a business process supports a recovery priority and has an MTO of less than 48 hours (two calendar days), it must be classified as a critical business process.

(16) For each identified critical business process, identify:

a. the type of impact a disruption may have on the business process
b. the impact of disruption on students, staff and stakeholders
c. critical IT systems including recovery timeframes
d. minimum resource requirements, including but not limited to:
    i. people
    ii. high risk and high value information, records and data
    iii. physical infrastructure and associated utilities

iv. assets and equipment
v. transportation
vi. finance, and
vii. third-party partners and key suppliers, and

e. the impact of disruption to the critical business process in various scenarios and over varying periods of time.

## Business continuity strategies and planning

(17) A business continuity plan (BCP) will apply for each portfolio and faculty, detailing how to prepare for, prevent, respond to and recover from a disruption event for all relevant critical business processes.

(18) Each BCP should define:

a. actions to prepare for and/or prevent a business disruption event
b. how to respond to and restore critical business processes in a timely manner
c. the maximum tolerable outage period
d. critical IT systems and telephony requirements, and their priority of recovery
e. records considered to be high risk and high value
f. key internal and external interdependencies
g. key internal and external contact details and communication requirements
h. workarounds and/or alternatives to maintain critical business processes, including IT systems, on a short-term basis until recovery can occur, and
i. key BCP roles and responsibilities and reporting requirements.

(19) BCPs do not attempt to identify and plan for every contingency or outage that could occur and should focus on the relevant critical business processes. The BCP should provide a flexible framework for BCP owners to identify, plan and develop resilience in their critical business processes.

(20) BCPs must be approved by the relevant Executive Leadership Team member (the BCP owner).

(21) A copy of each BCP will be retained by the BCP owner and the Risk and Compliance Unit.

(22) The Crisis Management Team and/or Critical Incident Management Team will determine whether a business continuity plan is to be activated in response to a disruption event. Once activated, the BCP owner is responsible for coordinating response and recovery activities in line with the BCP.

## Communication

(23) The manner in which the University conveys information during a disruption event is critical to students, staff and the public’s understanding and perception of the University's management of a situation.

(24) Each BCP will include provision for internal and external communication requirements during a disruption event. Messaging to students, staff, regulators, government partners, third-party partners, stakeholders and the media must be coordinated through the Crisis Management Team to ensure the accuracy and continuity of messaging. BCP owners are to direct all communication requests, including communication requests to be issued by third-party education partners, for management through the Crisis Management Procedure.

(25) Communication with staff on BCP response and recovery activities is the responsibility of the BCP owner and should include:

a. the nature and extent of the event

b. services affected and the expected duration of the disruption
c. specific instructions on where staff are to go and any actions they should take
d. where, how and from whom staff are to receive further instructions, and
e. remind staff of their media and social media responsibilities.

## Third-party arrangements

(26) Where critical business processes are supported by a third party, the University must satisfy itself that the third party's business continuity management arrangements are adequate to meet the University's recovery priorities.

(27) The University must also satisfy itself that the third party adequately reviews and tests its business continuity plan.

## Education and training

(28) The Risk and Compliance Unit will provide training to BCP owners to raise awareness of roles, responsibilities before, during and after a business disruption event, and the practical application of their BCPs.

(29) BCP owners are responsible for ensuring their staff are trained and aware of the BCPs.

(30) Test exercises conducted in line with clauses 31 and 32 will also be considered a form of ongoing training that supports awareness of business continuity management at the University.

## Testing

(31) The purpose of testing BCPs is to:

a. validate the information in each plan
b. confirm the University's ability to maintain critical business processes and identify any tools or support required to do so
c. familiarise staff with their roles, responsibilities and ensure an awareness of business continuity management, and
d. identify opportunities for improvement in the overarching recovery priorities, business impact analysis and business continuity plans.

(32) BCP owners are responsible for carrying out regular reviews to test the validity and practicality of their BCPs.

(33) The Risk and Compliance Unit will coordinate annual testing of BCPs, noting that not all BCPs may be tested each year based on the scenario and method of testing used.

(34) BCPs must be reviewed by the BCP owner following each test exercise to address learnings and implement opportunities for improvement identified.

## Monitoring, review and reporting

(35) Following a disruption event, a post incident review will be conducted in consultation with the Risk and Compliance Unit to identify and address lessons learnt and implement opportunities for improvement.

(36) In all other instances, BCPs must be reviewed by the BCP owner at least annually, or earlier following a BCP event or a major change to the University.

(37) Recovery priorities, business impact analysis and BCPs will be reviewed more frequently than annually in the event of major change.

(38) The Risk and Compliance Unit will report the following to the Executive Leadership Team and Audit and Risk Committee at least annually:

a. a summary of the control arrangements in place to support crisis management and business continuity management
b. a summary of outcomes and key learning from test exercises, and
c. advice of actual critical incident or business continuity events in which components of one or more business continuity plan(s) were enacted.

# Section 4 - Guidelines

(39) Nil

# Section 5 - Glossary

(40) This procedure uses the following terms:

a. BCP owner – Executive Leadership Team members are ultimately responsible for their respective portfolio/faculty BCPs.
b. Business continuity management – is an enterprise approach for ensuring that critical business processes can be maintained or recovered in a timely manner, in the event of a disruption.
c. Business continuity plan (BCP) – a documented response and recovery procedure aimed at ensuring the continuity of agreed critical business processes. A BCP is in place and maintained for each portfolio/faculty that undertakes critical business processes.
d. Business impact analysis (BIA) – risk analysis of the impact over time of business disruption on the University. Findings from the BIA, along with agreed recovery priorities, are used to decide whether a process is a critical business process (AS ISO 22301).
e. Critical business process(es) – 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. A critical business process will be a process that aligns with the University's recovery priorities and has a maximum tolerable outage of 48 hours or less as defined through the business impact analysis process.
f. Disruption – any event or circumstance that significantly interferes with the normal operations and functions of the University (AS ISO 22301).
g. Maximum tolerable outage (MTO) – the maximum timeframe allowable to recover a critical business process to an acceptable level.
h. Recovery priorities – business processes approved by the Executive Leadership Team as critical to University operations and, therefore, take priority in the event of business disruption. Recovery priorities may change over time in line with changes to the University's strategic objectives.
i. Response and recovery – action(s) taken to return the University to business-as-usual operations.

## Status and Details

| | |
|---|---|
| **Status** | Current |
| **Effective Date** | 3rd April 2024 |
| **Review Date** | 3rd April 2029 |
| **Approval Authority** | University Secretary |
| **Approval Date** | 2nd 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 |