RISK MANAGEMENT POLICY 2017

The Senate of the University of Sydney adopts the following policy.

Dated: 24 March 2017

Last amended: 10 July 2019 (commencing 1 August 2019)

Signature:

Name: Mr David Pacey

Position: Secretary to Senate

_____

_

CONTENTS

1 Name of policy

This is the Risk Management Policy 2017.

2 Commencement

This policy commences on 24 March 2017.

3 Policy is binding

Except to the extent that a contrary intention is expressed, this policy binds the University, staff and affiliates.

4 Statement of intent

This policy:

(a) enhances the University's ability to seize opportunities while reducing impacts of risk to the lowest practicable level;

(b) establishes the principles by which the University will identify, assess and manage risk;

(c) provides for the appropriate allocation of responsibilities for managing risks;

(d) establishes the framework within which risk management will be undertaken;

(e) defines organisational resilience and specifies its components; and

(f) establishes the framework within which organisational resilience will be addressed.

5 Application

This policy applies to:

(a) the University, its staff and affiliates; and

(b) all activities conducted by or on behalf of the University.

6 Definitions

business continuity	means the capability to operate the University's critical business functions during and after significant disruptions. **Note:** See ISO Standard 22300:2018, *Security and Resilience*
business continuity plan	means a plan which assists restoration of business activities after a disruption by prioritising tasks for recovery.
business sponsor	means the staff member or affiliate with a demonstrable interest in the outcome of a project who has primary responsibility to the executive sponsor for seeing that the intended benefits of the project are realised.
crisis	means an abnormal or unstable situation that threatens an organisation's strategic objectives, reputation or viability.
crisis management	means the activities required to develop, co-ordinate and implement a comprehensive plan for organisation-wide response to a crisis.
cyber security	means the measures taken to:

	• protect ICT, electronic systems, networks, devices and digital information from compromise or interruption; and • facilitate rapid and effective detection and response to any compromise or interruption.
emergency	means an incident which has immediate, serious impacts to safety, infrastructure or the environment, and which requires external emergency services to respond.
emerging risk	means a condition, situation or event that: • may impact organisational objectives; • emerges over time; and • has not previously been considered a risk.
executive sponsor	means the Principal Officer with a demonstrable interest in the outcome of a project, or a program of which the project is a part, who has primary responsibility to the University and the executive for the delivery of the outcomes of the initiative.
financial shock event	means an event which may adversely affect the University's financial viability.
hazard	has the meaning given in the *Work Health and Safety Policy 2016* which at the date of this policy is: a source of potential harm, or a situation with potential for harm, to human health or wellbeing.
ICT	means information and communications technology.
incident	means a situation or event which has, or may have, an adverse impact on the University. For the purposes of this policy, incidents include but are not limited to: • a situation that might be, or could lead to, a disruption, loss, emergency or crisis; • safety incidents; **Note:** See *Work Health and Safety Policy 2016* • compromises to or interference with ICT, electronic systems, networks, devices or digital information; • events which may adversely affect the University's reputation; and • events which may adversely affect the University's financial viability.
local risk register	means a risk register relating to a unit or project established and maintained by the head of the unit or project sponsor.

manager	means any staff member or affiliate with responsibility for managing people.
organisational resilience	means the ability to adapt to changing conditions. It includes the ability to respond to, and recover from, disruptions and the ability to change in order to prosper from adversity. This includes, but is not limited to, managing: • emergency responses; • crises; • business continuity; • ICT disaster recovery; • cyber security breaches; • financial shock event recovery; and • all other plans and activities designed to enable the University to respond to emerging risks that may impact its ongoing viability.
Organisational Resilience Framework	means the document, or set of documents, required by clause 10
Principal Officer	means any of: • Vice-Chancellor and Principal; • Deputy Vice-Chancellor; • Vice- Principal; • General Counsel; • Director, University Libraries.
risk	means the effect of uncertainty on objectives.
risk register	means a document or collection of documents containing a record of information about identified risks.
risk owner	means the role recorded against a particular risk in a risk register to discharge the responsibilities specified in clause 12.
risk management	means co-ordinated activities to direct and control the University's activities with regard to risk.
risk management culture	means the collective beliefs, values, attitudes, knowledge and understanding about risk management.
Risk Management Framework	means the set of documents required by clause 9, which provide the foundation and arrangements for designing, implementing, monitoring, reviewing and continually improving risk management at the University.

unit	means any of the following: • faculty; • University school; • a portfolio controlled by a Deputy Vice-Chancellor, a Vice-Principal, the General Counsel or the Director, University Libraries; • A professional service unit within the portfolio of the Vice-Principal (Operations); • a Level 4 centre, as defined in the *Centres: Policy for Establishment, Management and Review;* • other groups as determined by a Principal Officer from time to time
University Executive	means the committee of that name which comprises members of the University's senior leadership.
University Risk Appetite and Tolerance Statement	means the statement of the amount and type of risk the University is willing to accept, after risk treatment, in order to achieve its objectives.
University Risk Register	means the University-wide risk register established and maintained by the Chief Risk Officer as required by clause 11.

7 Risk management principles

(1) The University will embrace well-managed risk-taking in pursuit of its vision and strategic objectives, while:

(a) protecting the wellbeing, health and safety of students, staff, affiliates and the public; and

(b) minimising exposure to:

(i) any potential damage to the culture of excellence evident in its world-class research and education;

(ii) long-term brand and reputation damage; and

(iii) health and safety, compliance and financial solvency, environmental, sustainability and social responsibility related risks.

(2) All risks should be managed within the boundaries defined in the University Risk Appetite and Tolerance Statement.

(3) Subject to subclauses 7(1) and 7(2), the adverse impacts of risk should be reduced as far as reasonably practicable.

8 Organisational resilience principles

(1) The University's approach to organisational resilience is based on the following principles.

(2) **Completeness.** The University will:

(a) close gaps in controls; and

(b) adopt a comprehensive University-wide approach, using established structures and processes.

(3) **Accountability.** The University will assign clear responsibilities for aspects of organisational resilience at all levels of governance.

(4) **Flexibility.** The University will maintain flexibility by adapting the Organisational Resilience Framework to maintain relevance to the University's internal and external context.

(5) **Performance.** The University will measure its performance by:

(a) monitoring and reporting on the effect of organisational resilience activities; and

(b) identifying and acting on opportunities to adapt to changing conditions.

(6) **Continuous improvement.** The University will:

(a) regularly review organisational resilience activities and lessons learnt; and

(b) identify and act on opportunities to improve and adapt to changing conditions.

9 Risk Management Framework

(1) The Vice-Principal (Operations) will determine the Risk Management Framework, after consultation with University Executive and Senate.

(2) The Risk Management Framework must be consistent with the risk management standard *AS/NZS ISO 31000:2018 (Risk Management - Principles and Guidelines)*.

(3) The Risk Management Framework may consist of one or more documents and must contain the following:

(a) a University Risk Appetite and Tolerance Statement:

(b) provisions for the way in which risks are identified, assessed and evaluated;

(c) provisions for the ways in which risk treatment plans are designed and prioritised; and

(d) provisions for the ways in which risks are reported, escalated, and broadly communicated.

(4) The Risk Management Framework will be published and available to all staff and affiliates on the University intranet site.

(5) The Vice-Principal (Operations) will review the Risk Management Framework at least once every two years.

(6) The Risk Management Framework has the status of procedures under the *University of Sydney (Policies Development and Review) Rule 2011*.

10 Organisational Resilience Framework

(1) The Vice-Principal (Operations) will determine the Organisational Resilience Framework, after consultation with University Executive and Senate.

(2) The Organisational Resilience Framework:

(a) must be published on the University intranet site; and

(b) must contain at least the following:

(i) provisions for how organisational resilience activities work together;

(ii) provisions prescribing the governance structures, roles, responsibilities and approach for implementing each organisational resilience activity;

(iii) provisions specifying the training and guidance available to implement organisational resilience activities;

(iv) provisions for categorising and prioritising threats to organisational resilience by criticality;

(v) requirements for escalating organisational resilience activities;

(vi) requirements for reporting on, and communicating about, organisational resilience activities; and

(vii) requirements for monitoring, evaluating and improving organisational resilience activities.

(3) The Vice-Principal (Operations) will review the Organisational Resilience Framework at least once every two years.

(4) The Organisational Resilience Framework has the status of procedures under the *University of Sydney (Policies Development and Review) Rule 2011*.

11 Risk registers

(1) The Chief Risk Officer must establish and maintain a formal risk register for the University as a whole.

(2) The University Risk Register must document key risk events that would likely impact the University as a whole, in the manner and with the detail set out in the Risk Management Framework.

(3) The following must also establish local risk registers:

(a) the head of a unit, in relation to that unit; and

(b) the executive sponsor, in relation to a project;

(4) Local risk registers must document key risk events that would impact the unit or project, in the manner and with the detail set out in the Risk Management Framework.

12 Risk owners

(1) The Vice-Chancellor, on advice from the University Executive, will assign an owner to each risk listed in the University Risk Register.

(2) The head of unit or project sponsor, as appropriate, will assign an owner to each risk listed in a local register.

(3) Owners must be recorded against each risk in the relevant register.

13 Responding to organisational resilience threats

(1) Any situation or event which has, or may have, an adverse impact on the University may threaten organisational resilience. This includes but is not limited to:

(a) incidents;

(b) emergencies; and

(c) crises.

(2) The Vice-Principal (Operations), in consultation with the heads of relevant units, will document response plans for events which potentially threaten the University's resilience, including plans for:

(a) emergency response;

(b) crisis management;

(c) ICT disaster recovery;

(d) cyber security breach response;

(e) financial shock recovery;

(f) pandemic response; and

(g) organisational unit business continuity.

(3) Each plan must include:

(a) a description of the circumstances under which the plan will be activated;

(b) a description of the process to activate the plan; and

(c) staff roles and responsibilities in implementing the plan.

14 Emergency Planning Committee

(1) There will be an Emergency Planning Committee which will meet at least once every six months.

(2) The purpose of the Emergency Planning Committee is to:

(a) oversee the prevention and preparation phases of emergency response management as well as the implementation, training and evaluation of the University Emergency Response Plan; and

(b) oversee and coordinate organisational resilience activities to ensure that there is a consistent approach.

(3) The Emergency Planning Committee will be chaired by the Director, Campus Infrastructure and Services and will consist of at least one staff member from each of the following:

(a) Campus Infrastructure and Services;

(b) Information and Communications Technology;

(c) Human Resources or Safety Health and Wellbeing;

(d) External Relations;

(e) Risk Management;

(f) University of Sydney Union;

(g) University colleges;

(h) For meetings relating to clause 14(2)(b):

(i) Faculties;

(ii) University Schools;

(iii) Research Portfolio; and

(iv) Multidisciplinary initiatives;

(i) Any other members as required by the chair.

(4) In relation to clause 14(2)(b), the Emergency Planning Committee will:

(a) oversee and coordinate all organisational resilience activities;

(b) oversee, evaluate and review the outcomes of periodic testing of aspects of the Organisational Resilience Framework;

(c) oversee the continuous improvement and management of:

(i) the University Emergency Response Plan;

(ii) business continuity plans;

(iii) the pandemic response plan;

(iv) recovery plans (IT and financial shock); and

(v) management plans (reputational and crisis).

(d) review and, if appropriate, endorse organisational resilience reports to be submitted to the University Executive and Senate;

(e) review and, if appropriate, recommend amendments to this policy; and

(5) review and, as appropriate, recommend amendments to the Organisational Resilience Framework.

15 Ad hoc organisational resilience committees

(1) The following ad hoc committees will have responsibility for co-ordinating the University's responses to events which threaten its resilience:

(a) Crisis Management Committee;

(b) Emergency Response Team;

(c) Incident Response Team; and

(d) any other committee established as part of a plan referred to in clause 13(1).

(2) The committees established in clause 15(1) will operate in accordance with the requirements of the Organisational Resilience Framework.

(3) The Organisational Resilience Framework must specify at least the following in relation to each ad hoc committee:

(a) roles and responsibilities relating to organisational resilience;

(b) committee membership; and

(c) key activities.

16 Roles and responsibilities

(1) **Senate** is accountable for the oversight of risk management at the University. It is also responsible for:

(a) setting the University's risk appetite and tolerance levels;

(b) considering, and if appropriate, endorsing this policy, the Risk Management Framework and the Organisational Resilience Framework;

(c) considering and responding appropriately to reports about the University's risks and their management; and

(d) considering and responding appropriately to reports about organisational resilience in relation to crises management, including endorsing any actions for ongoing improvement.

(2) **Senate committees generally** are responsible for:

(a) monitoring the application of the Risk Management Framework in areas within their remit; and

(b) considering and responding appropriately to reports about the University's risks and their management in areas within their remit.

(3) **The Vice-Chancellor** is responsible for:

(a) overall risk management and compliance across the University;

(b) assigning an owner to each risk listed in the University Risk Register;

(c) promoting an appropriate risk management culture across the University;

(d) overseeing the allocation of resources to enable effective risk management; and

(e) reporting to Senate on key risks and their management.

(4) **The Provost** is responsible for:

(a) promoting an appropriate risk management culture across the University;

(b) receiving and acting on reports of risk management issues from faculties and University schools; and

(c) raising risk management issues with the Vice-Chancellor and University Executive where appropriate.

(5) **The Vice-Principal (Operations)** is responsible for:

(a) determining the Risk Management Framework and the Organisational Resilience Framework;

(b) reviewing the Risk Management Framework and Organisational Resilience Framework at least once every two years;

(c) documenting response plans for organisational resilience threats; and

(d) overseeing the implementation of the Risk Management Framework by the Chief Risk Officer.

(6) **The University Executive** is responsible for:

(a) overseeing and advising on the application of the Risk Management Framework and the Organisational Resilience Framework;

(b) considering and responding appropriately to reports about the University's risks and their management; and

(c) considering and responding appropriately to reports about organisational resilience in relation to crises management, including endorsing any actions for ongoing improvement.

(7) **University Executive committees** are responsible for:

(a) overseeing and advising on the application of the Risk Management Framework in areas within their remit;

(b) considering and responding appropriately to reports about the University's risks and their management in areas within their remit; and

(c) reporting to the University Executive any risks they identify which are outside their remit.

(8) **The Chief Risk Officer** is responsible for:

(a) administering this policy;

(b) maintaining the Risk Management Framework and the Organisational Resilience Framework;

(c) establishing and maintaining the University Risk Register; and

(d) reporting in accordance with this policy, the Risk Management Framework and the Organisational Resilience Framework.

(9) **The Emergency Planning Committee** is responsible for:

(a) overseeing and coordinating all organisational resilience activities, including testing of aspects of the Organisational Resilience Framework;

(b) overseeing the development, implementation and continuous improvement of the University's University Emergency Response Plan;

(c) approving all emergency response procedures;

(d) ensuring that relevant emergency information is available to the University community;

(e) monitoring the design and maintenance of facilities and emergency related infrastructure;

(f) monitoring the implementation of building emergency response procedures in University owned and occupied buildings;

(g) overseeing the development and implementation of business continuity activities across the University;

(h) training staff who may be required to participate as a member of the University's Emergency Response Team or Crisis Management Committee;

(i) evaluating and reviewing outcomes of periodic testing of the effectiveness of organisational resilience activities;

(j) monitoring and assessing incident response performance post-incident; and

(k) escalating organisational resilience issues to the University Executive when it becomes aware of them.

(10) **Heads of units** are responsible for:

(a) effectively managing risk;

(b) promoting an appropriate risk management culture within their areas of responsibility;

(c) assigning an owner to each risk listed in their local risk register;

(d) assigning day-to-day risk management responsibility within the teams reporting to them;

(e) providing clear information about, and explanations of, risk management and organisational resilience requirements to the teams reporting to them;

(f) reporting and escalating identified risks as required by the Risk Management Framework; and

(g) managing organisational resilience within their unit in accordance with the Organisational Resilience Framework as well as the corresponding risks; and

(h) discharging any additional responsibilities specified in either of the Risk Management Framework or Organisational Resilience Framework.

(11) **Risk owners** are responsible for:

(a) considering the risks assigned to them;

(b) devising and implementing appropriate risk management plans to manage risk within the boundaries of the University Risk Appetite and Tolerance Statement; and

(c) reporting and escalating to the relevant committee any identified risk which cannot be properly managed consistently with this policy and the Risk Management Framework.

(12) **All staff and affiliates** are responsible for:

(a) identifying and familiarising themselves with risks associated with their roles;

(b) managing risks consistently with this policy and the Risk Management Framework;

(c) familiarising themselves with the Organisational Resilience Framework and the specific organisational resilience plans that affect them and their workplace;

(d) contributing to risk management and organisational resilience activities as directed by management;

(e) responding independently to emergencies and following reasonable instructions provided by Emergency Wardens, Campus Security Officers and emergency officers;

(f) when teaching students, providing a safe initial response to an incident or emergency; and

(g) where appropriate, escalating incidents, risks and concerns to management.

17 Reporting

(1) Staff and affiliates must report risks in accordance with this policy and the Risk Management Framework.

(2) The Chief Risk Officer, and other individuals subject to reporting requirements in the Risk Management Framework must provide required reports as specified.

(3) Individuals subject to reporting requirements in the Organisational Resilience Framework must provide required reports as specified.

18 Breaches of this policy

Failure to comply with this policy, the Risk Management Framework or the Organisational Resilience Framework may constitute misconduct or serious misconduct and may result in disciplinary action being taken by the University, up to and including termination of employment, engagement or affiliation.

19 Rescissions and replacements

This document replaces the following documents which are rescinded as from the date of commencement of this document:

(a) the *Risk Management Policy 2013,* which commenced on 11 February 2013; and

(b) the *Serious Incident and Business Continuity Policy 2013* which commenced on 5 December 2016.

NOTES

Risk Management Policy 2017

Date adopted:	24 March 2017
Date commenced:	8 June 2017
Date amended:	10 July 2019 (commencing 1 August 2019)
Administrator:	Chief Risk Officer
Review date:	8 June 2022
Related documents:	Risk Management Standard AS/NZS ISO 31-000:2009 (Risk Management - Principles and Guidelines) Security and Resilience Standard ISO 22300: 2018 University of Sydney (Policies Development and Review) Rule 2011 Recordkeeping Policy 2017 Work Health and Safety Policy 2016

Recordkeeping Manual

Critical Incidents Involving Students Procedures 2018

Work Health and Safety Procedures 2016

Risk Management Framework 2017

Organisational Resilience Framework 2019

AMENDMENT HISTORY

Provision	Amendment	Commencing
6	Added definitions relating to organisational resilience	1 August 2019
6	Removed definitions relating to project risk management	1 August 2019
6	Added definitions for emerging risk and risk management culture	1 August 2019
6	Minor updates to grammar and hyperlinks	1 August 2019
7(b)(iii)	Amended to include consideration of environmental, sustainability and social responsibility	1 August 2019
4(e); 4(f); 8; 10; 13; 15; 17(3)	Amendments relating to the inclusion of organisational resilience provisions to the Risk Management Policy	1 August 2019
9(1); 9(2); 9(5)	Amended Senate to Vice Principal (Operations), amended clauses to specify minimum frequency and consultation requirements for reviewing the Risk Management Framework	1 August 2019
14	Clause added relating to the Emergency Planning Committee	1 August 2019
16	Amendments to the risk management responsibilities of the Senate, Senate Committees, Vice Chancellor, Provost, Chief Risk Officer and Heads of units; addition of roles including Vice President (Operations), University Executive, University Executive Committees; Heads of units and all staff and affiliates and removal of roles including the Director (Internal Audit), Director (Safety, Health and Wellbeing) and the Enterprise Portfolio Management Office	1 August 2019

16	Removed references to responsibilities for the Director (Internal Audit), Director (Safety, Health and Wellbeing) and the Enterprise Portfolio Management Office	1 August 2019
16	Added responsibilities relating to organisational resilience	1 August 2019
17(2);	Amended to include other individuals with reporting requirements outlined in the Risk Management Framework	1 August 2019
18	Updated to include reference to the Organisational Resilience Framework	1 August 2019
19	Reference to Serious Incident and Business Continuity Policy 2013 added	1 August 2019
Notes	Related documents subsection updated to correct naming conventions; addition of Security and Resilience Standard, and Organisational Resilience Framework 2019	1 August 2019