

Risk Management Policy (MPF1194)

1. Objectives

The objectives of this policy are to:

- a) outline the University's approach to risk management;
- b) align the University with best practice *AS/NZS ISO 31000:2009 Risk management – Principles and guidelines*;
- c) establish the roles and responsibilities of staff in risk management; and
- d) affirm the University's commitment to developing a compliance framework in line with *AS ISO 19600:2015 Compliance management systems – Guidelines*, incorporating a risk based approach to compliance that:
 - i. facilitates compliance with legislation and regulation (University's Regulatory Framework);
 - ii. continuously improves attention to compliance obligations within the Regulatory Framework; and
 - iii. stimulates the identification, reporting and rectification of non-compliance.

2. Scope

This policy applies to all staff and honorary appointees of the University, and to people authorised to undertake University business.

3. Authority

This policy is made under the [University of Melbourne Act 2009 \(Vic\)](#) and [Council Regulation](#), and supports management of risk according to applicable legislative and regulatory standards and codes to which the University is subject.

4. Policy

- 4.1. Council, through Council's Audit and Risk Committee, is responsible for overseeing and monitoring the assessment and management of risk and compliance.
- 4.2. Risk is managed in accordance with the University's risk process for risk assessment (identification, analysis and evaluation) developed by University Services, Legal and Risk, and approved by the Vice-Principal of Policy and Projects, informed by advice from the University's Risk Management Advisory Group (RMAG).
- 4.3. The management of risk aligns with the University's strategic risk appetite, as approved by Council.
- 4.4. The Vice-Principal, Policy and Projects oversees the development of the strategic risk profile and risk appetite statement and advises the University Executive on risk, taking into account any recommendations made by RMAG.

4.5. Risk management and compliance obligations are formally integrated into planning processes and management activities, and incorporated into ongoing 'business as usual' practices by those with management responsibilities.

4.6. The head of division is responsible for ensuring compliance breaches are monitored and reported.

4.7. In the event of a critical incident, the University's response will prioritise:

- a) human life, safety and wellbeing;
- b) animal life, safety and wellbeing;
- c) environmental protection; and
- d) the protection of property interests;

taking into account the nature of the incident and all relevant circumstances.

5. Procedural principles

5.1. University Services, Legal and Risk maintains the:

- a) University-wide Risk Register; and
- b) University-wide Compliance Obligations Register.

5.2. University Services, Legal and Risk:

- a) provides risk management advice and training;
- b) provides compliance training; and
- c) documents process in support of risk management.

5.3. University Services, Legal and Risk is responsible for internal audits, taking into account any recommendations made by RMAG in relation to the conduct of risk-related audits.

5.4. The Head of University Services is responsible for:

- a) developing and implementing a University-wide critical incident management program;
- b) developing processes to align with the Australian Inter-service Incident Management System; and
- c) coordinating the University's response to any critical incident that may occur, in accordance with the critical incident management program described in section 5.4(a) and all relevant University policies and processes.

5.5. University Services, Legal and Risk is responsible for developing and implementing the Business Continuity Management Program aligned to *ISO 22301:2012 Societal security – Business continuity management systems – Requirements*.

5.6. Risks are identified and managed to ensure that:

- a) activities on behalf of the University are performed in an informed manner; and
- b) areas of risk or potential risk undertaken in day-to-day activities are the responsibility of all staff, including persons authorised to undertake University business and/or activities (eg service providers and contractors).

5.7. All staff, including people authorised to undertake University business and/or activities (eg service providers and contractors) have a responsibility to comply with legislative and regulatory compliance obligations, specifically to ensure that:

- a) activities on behalf of the University comply with applicable laws and related University policies, and are performed in an ethical, lawful and safe manner; and
- b) they are aware of areas of legislation/regulation that affect their day-to-day work.

5.8. A breach of the University's compliance obligations may result in disciplinary and/or legal action.

6. Roles and responsibilities

<i>Role/Decision/Action</i>	<i>Responsibility</i>	<i>Conditions and limitations</i>
Oversee and monitor the assessment and management of risk and compliance	Council	Through Council's Audit and Risk Committee
Oversee development of the University's strategic risk profile and risk appetite statement	Chancellery – Vice President Policy and Projects	To be approved by Council through the Council's Audit and Risk Committee
Develop the University's risk management framework	Chancellery – Vice President Policy and Projects	In collaboration with University Services, Legal and Risk
Develop the University's risk process for assessing, evaluating and treating risk	University Services, Legal and Risk	To be approved by the Vice-Principal, Policy and Projects, informed by advice from RMAG
Incorporate risk management, including compliance obligations and business continuity management, into business practices	Management	
Oversee the University Risk Register (including University strategic, divisional strategic and operational strategic risk)	Vice-Principal, Policy and Projects	Taking into account any recommendations by RMAG
Provide risk advice to the University's Executive team	Vice-Principal, Policy and Projects	Taking into account any recommendations by RMAG
Maintain University-wide Risk Register	University Services, Legal and Risk	Strategic risk oversight is the responsibility of Chancellery
Maintain University-wide Compliance Obligations Register	University Services, Legal and Risk	
Provide training and documentation of process to support management of risk	University Services, Legal and Risk	

Conduct internal audits to support the management of risk and compliance obligations	University Services, Legal and Risk	Taking into account RMAG's recommendations in relation to risk-related audits
Develop and implement a University-wide critical incident management program	Head of University Services	Program to be reviewed and approved annually by the Vice-Principal, Policy and Projects, informed by advice from RMAG
Develop and implement the Business Continuity Program	University Services, Legal and Risk	Program to be approved by the Vice-Principal, Policy and Projects, informed by advice from RMAG
Identify and manage risk - perform day to day activities in an informed manner adhering to relevant compliance obligations	All staff including persons authorised to undertake University business and/or activities (e.g. service providers and contractors)	Identification of risk and non-compliance to be raised/reported to the next most senior person for assessment
Administer this policy, including informing and assisting staff on compliance issues and consider complaints of compliance breaches	Risk and Compliance Manager, Legal and Risk	
Compliance with relevant legislation/regulation	All staff, students, contractors and service providers	
Identify compliance risks	Compliance owner	
Mitigate compliance risks	Compliance owner	
Deliver specific compliance training	Legal and Risk	As identified by the compliance owner in conjunction with Legal and Risk
Manage and report compliance breaches	Compliance owner	Reporting of compliance breach to Legal and Risk and/or Regulatory as required

7. Definitions

Business continuity management means the identification of potential threats to the University, the impact those threats, if realised, might cause, and the management of those threats and impacts.

Compliance means meeting all of the University's compliance obligations.

Compliance obligations means the requirements and commitments of state and federal legislation and regulation, mandatory and voluntary codes and standards, and commitments made by the University.

Compliance obligations register means a comprehensive list of the compliance obligations of all University functions and activities.

Critical incident/emergency means an occurrence that significantly disrupts the normal operation of the University and possibly jeopardises the health, safety, wellbeing or sustainability of the University community.

Effect means a deviation from the expected, either positive or negative.

Risk means the effect of uncertainty on objectives.

Risk management means the coordinated activities to direct and control the University with regard to risk.

Risk register means the comprehensive list that describes the type of risk and related characteristics, inherent and residual risk ratings, controls in place, control effectiveness, risk owners and identification of a business continuity plan in place.

Uncertainty means the state of understanding or knowledge of an event, the consequence or likelihood.

University Risk Register means the database used to store data on University strategic and operational risk.

POLICY APPROVER

Council

POLICY STEWARD

Executive Director, Legal & Risk and General Counsel

REVIEW

This policy will be reviewed by 24 August 2022.

VERSION HISTORY

Version	Approved By	Approval Date	Effective Date	Sections Modified
1	Council	8 Jul 2013	8 Jul 2013	N/A
2	Governance and Nominations Committee authorised by Council	23 June 2016	21 July 2016	New version arising from the Policy Consolidation Project, incorporating the Risk Management Policy (MPF1194), Risk Management Procedure (MPF1097) and Compliance Policy (MPF1100).
3	Council	24 August 2017	28 August 2017	Roles and responsibilities updated to improve clarity.