Compliance Management Framework - Procedures

1. Purpose of procedures

1.1 The purpose of these procedures is to:

(a) provide detailed elements relating to the operation and implementation of the University's Compliance Management Framework;

(b) assign specific accountabilities and responsibilities for components of the University's Compliance Management Framework;

(c) enable the gathering of information to facilitate monitoring and reporting of compliance performance within the University;

(d) provide a systematic process for the reviewing of compliance obligations to enable the University to effectively and efficiently manage compliance risks;

(e) provide a systematic process for the reporting and investigation of compliance breaches or potential breaches so they can be appropriately addressed;

(f) reinforce the importance of compliance, so that all staff members are encouraged to proactively raise compliance issues as soon as possible and address any weaknesses in the control environment(1); and

(g) ensure that no staff member is penalised or disadvantaged as a result of reporting a compliance breach and that repercussions of breaches themselves are determined on a case-by-case basis.

1.2 These procedures must be read in conjunction with the linked Compliance Management Framework - Governing Policy.

APPROVAL AUTHORITY

Vice-Chancellor and President

RESPONSIBLE EXECUTIVE MEMBER

Vice-Chancellor and President

DESIGNATED OFFICER

Director, Governance and Risk Management

FIRST APPROVED

20 August 2013

LAST AMENDED

30 October 2023

REVIEW DATE

30 October 2024

STATUS

Active

2. Scope and application

2.1 These procedures apply to all staff, and members of University decision-making or advisory bodies.

2.2 These procedures are consistent with Australian Standard AS ISO 19600:2015: Compliance Management Systems.

3. Definitions

3.1 Refer to the University's Glossary of Terms for definitions as they specifically relate to policy documents.

4. Elements of the Compliance Management Framework

4.1 Successful achievement of the policy objectives will require recognition and incorporation of the following elements:

4.1.1 Commitment

4.1.1.1 The Compliance Management Framework - Governing Policy outlines the University's commitment to maintain and improve the Compliance Management Framework and processes. Accordingly, the University must allocate appropriate resources to the development, implementation and continuous improvement of its Compliance Management Framework.

4.1.1.2 Council, through the Audit and Risk Management Committee, is responsible for overseeing the University's compliance with legislation, regulatory requirements, reporting obligations, and University policies.

4.1.1.3 Compliance is the responsibility of all University staff.

4.1.1.4 Governance and Risk Management have overarching responsibility for:

(a) the design and implementation of the Compliance Management Framework;

University of the Sunshine Coast | CRICOS Provider Number: 01595D | Correct as at 29 April 2024

(b) coordinating, managing and maintaining the Register of Compliance Obligations; and

(c) providing oversight of compliance across the University.

4.1.1.5 All Organisational Unit Managers are accountable for ensuring compliance with all legislative obligations, standards and best practice guidance and for putting the necessary controls and processes in place to manage their compliance obligations. This includes ensuring Higher Degree Research (HDR) students are aware of their obligations, with supervisors monitoring student compliance with relevant legislative requirements. Organisational Unit Managers are responsible for keeping abreast of changes and updates to existing legislation and identifying new obligations. Responsible Officers will need to attest to compliance quarterly.

4.1.1.6 All staff must be aware of compliance responsibilities that apply to their area of work or activities and ensure that their actions on behalf of the University comply with relevant laws, industry codes and organisational standards. It is the responsibility of Organisational Unit Managers to ensure staff have appropriate information to ensure compliance.

4.1.2 Implementation

4.1.2.1 The University has adopted a risk-based approach to the implementation of its compliance obligations.

4.1.2.2 All compliance obligations are important, with the University having a conservative risk appetite for regulatory and compliance risk. Higher risk obligations require additional oversight and controls to ensure the risk of any potential non-compliance in any of these areas is minimised.

4.1.2.3 Compliance obligations are classified as High, Medium or Low risk. The classification is undertaken within Governance and Risk Management. Higher risk obligations have a major impact on the University and are critical to its functioning. The obligations are assessed against the University's risk tables.

4.1.2.4 If a Responsible Officer disagrees with the risk-rating of a compliance obligation, they should notify the Director, Governance and Risk Management.

4.1.2.5 Compliance responsibilities are identified and promulgated through the Register of Compliance Obligations. The Director, Governance and Risk Management is responsible for maintaining a Register of Compliance Obligations.

4.1.2.6 Each Responsible Officer identified in the Register of Compliance Obligations is responsible for the currency of Compliance Obligations recorded in this Register against their Organisational Unit. Responsible Officers should convey to the Director, Governance and Risk Management advice of any new obligations or any changes to existing ones.

4.1.2.7 Each Responsible Officer must liaise with other areas of the University where the relevant obligation exists to ensure they are comfortable with the controls and processes in place for managing the obligations.

4.1.2.8 Behaviours that create and support compliance will be encouraged. Behaviours that compromise compliance will be investigated.

4.1.3 Monitoring and review

4.1.3.1 Systems, procedures and controls are implemented to support the monitoring of compliance obligations against the requirements of the Compliance Management Framework.

4.1.3.2 Governance and Risk Management is responsible for reviewing and maintaining the Register of Compliance Obligations, the Compliance Management Framework - Governing Policy and systems which support the compliance management framework within the University.

4.1.3.3 The Director, Governance and Risk Management reports at least annually to Council on the University's framework program, via the Audit and Risk Management Committee.

4.1.3.4 The Compliance Management Framework is reviewed each year.

4.1.3.5 If issues impacting compliance are identified throughout the year, Organisational Unit Managers must take appropriate action to address the issue and implement additional controls to strengthen compliance.

5. Compliance reporting

5.1 The Director, Governance and Risk Management must coordinate a quarterly compliance risk report for Executive Committee and the Audit and Risk Management Committee.

5.2 An attestation process must be conducted quarterly and will require all Responsible Officer's to report on the status of compliance.

5.3 The quarterly compliance attestation process includes compliance with legislative obligations and University policy.

5.4 The Audit and Risk Management Committee is responsible for ensuring that it receives a quarterly report and any ad hoc reporting on compliance as required from the Director, Governance and Risk Management, and that it identifies and requests follow-up action on any issues of concern.

6. Breach reporting

6.1 Exclusions

6.1.1 A number of processes are established across the University to manage complaints relating to compliance or breaches of laws and regulations. These are covered in various University policies, such as:

(a) Staff Code of Conduct - Governing Policy;

(b) University of the Sunshine Coast Enterprise Agreement;

(c) Health, Safety and Wellbeing - Governing Policy;

(d) Critical Incident Management - Governing Policy;

(e) Anti-Discrimination and Freedom from Bullying and Harassment (Staff) - Governing Policy;

(f) Anti-Discrimination and Freedom from Bullying and Harassment (Students) - Governing Policy;

(g) Equity and Diversity - Governing Policy;

(h) Fraud and Corruption Control - Governing Policy;

(i) Financial Management Practices - Operational Policy;

(j) Information Management Framework - Governing Policy;

(k) Public Interest Disclosures - Governing Policy;

(l) Acceptable Use of ICT Resources - Governing Policy;

(m) Responsible Research Conduct - Governing Policy;

(n) Student Academic Integrity - Governing Policy; and

(o) Copyright - Governing Policy.

5.1.2 Any University policy or procedures or legislation that includes dedicated processes for handling compliance failures will take precedence over the following procedural steps and actions. Refer to the specific subject area policy or legislative provisions in the first instance.

5.2 Procedure steps and actions

5.2.1 It is essential that all parties involved in breach reporting, investigation and rectification act in good faith to obtain a satisfactory outcome. Good faith includes acting sincerely, without malice and being truthful.

5.2.2 The University fosters a culture of compliance and no blame should be attached to the reporting of accidental breaches or those identifying process errors.

5.2.3 It should be noted that staff committing deliberate or negligent breaches may be subject to the University's disciplinary processes or regulatory or criminal actions (where applicable or appropriate).

5.2.4 The required steps and actions to be followed for reporting and investigating compliance breaches, or potential breaches, are detailed in Table 1.

Table 1: Breach Reporting Procedures

PROCEDURE (INCLUDING KEY POINTS)	RESPONSIBILITY	TIMELINE
1. Initial identification and notification a. Staff should notify their supervisor or appropriate line manager of the breach or potential breach. Higher Degree Research Students should report the breach to their supervisor.	Staff member who notices the breach or potential breach / failure Supervisor/Organisational Unit Manager	Immediately or as soon as practicable

b. If a staff member feels they are unable to discuss the breach with their supervisor, the staff member should contact the Organisational Unit Manager, or alternatively the relevant People and Culture contact person or Director, People and Culture for further advice. c. Breaches or potential breaches can be reported anonymously. d. Upon receiving notification of a breach or potential breach, the supervisor should notify the Organisational Unit Manager by telephone or email.		
2. Breach containment a. The supervisor should take immediate, common sense steps to limit or contain the breach. Depending on the nature of the breach, different actions may be required e.g. stop the unauthorised practices; recover any records; suspension of employment in consultation with People and Culture; etc. b. Do not compromise the ability to investigate the breach. Do not destroy evidence that may be valuable in determining the cause or allow corrective action to be taken.	Supervisor/Organisational Unit Manager	Immediately or as soon as is practicable
3. Breach assessment and escalation a. Assess the concerns raised to substantiate if there is a prima facie case that a breach has occurred. b. Evaluate the risk level in accordance with the Risk Management - Procedures. In all instances, the breach should be notified to the Director, Governance and Risk Management. c. For breaches that are considered significant (2), this may require activation of an Incident Response Team (IRT) depending on the criticality of the incident. d. For significant breaches, the Vice-Chancellor and President is to be informed via the relevant Executive member (or delegate). e. The IRT will oversee the management of the incident until resolution. Relevant members of the University will be involved in the IRT as appropriate. Media communications are to be managed by the Director, Marketing. The reporting and communication of breaches must be discussed with the Senior Legal Officer and Director, Governance and Risk Management.	Organisational Unit Manager	Immediately or as soon as is practicable
4. Investigation and reporting a. If necessary, an investigation should be undertaken. The level of investigative effort should reflect the seriousness of the breach. b. Investigations should: i) determine the root causes; ii) identify whether it was a systemic breach, an isolated incident or a deliberate act; iii) identify appropriate actions to strengthen the control environment and prevent similar breaches from occurring; and iv) be completed in a timely manner. c. The investigation outcome should be reported to the relevant Executive and to the Vice-Chancellor and President.	Organisational Unit Manager where breach occurred Director, Governance and Risk Management Vice-Chancellor and President	Commence investigation immediately after the breach has been assessed and contained

d. All significant breaches should be reported to the Audit and Risk Management Committee. e. Where breaches involve alleged criminal activity, this should be referred to the appropriate law enforcement agencies or authorities for investigation. f. Mandatory reporting requirements to Regulators and relevant external bodies should be complied with. Reporting of significant breaches will be discussed and managed by the IRT that is established for any significant compliance breaches.		
5. Implementation of corrective action Corrective and/or preventative actions will be implemented within agreed timeframes. b. Where systemic issues are identified, an improvement plan should be developed to address policy and/or process improvement. In addition, the controls listed in the compliance register will be reassessed and strengthened. c. Monitoring by the appropriate manager should be undertaken to ensure corrective actions are completed.	Organisational Unit Manager where the breach occurred	As recommended or agreed
6. Breach recording/register a. A central register of compliance breaches or potential breaches will be maintained in an approved and secure recordkeeping system, in accordance with the *Information Privacy Act 2009* (Qld) and *Privacy Act 1988* (Cth) and the University's Information Management Framework - Governing Policy and associated procedures. b. The register will include a record of all reported breaches/potential breaches, investigations, corrective actions undertaken, and include breaches referred for external resolution.	Director, Governance and Risk Management	Continuously

6. Records Management

The Register of Compliance Obligations and responses that support the quarterly attestation process must be maintained according to the University's Information and Records Management - Procedures.

Footnotes:

(1) Compliance issues refer to those instances where there are concerns about the University's compliance with legislative obligations.

(2) Significant breaches are determined based on a number of factors that are maintained separately.

END

RELATED DOCUMENTS

- Audit and Assurance Framework - Governing Policy

- Compliance Management Framework - Governing Policy
- Critical Incident Management - Governing Policy
- Fraud and Corruption Control - Governing Policy
- Governance Framework - Governing Policy
- Health, Safety and Wellbeing - Governing Policy
- Incident Management - Procedures
- Risk Management - Governing Policy

LINKED DOCUMENTS

- Compliance Management Framework - Governing Policy

SUPERSEDED DOCUMENTS

- Compliance Management Framework: Annual Compliance Review - Procedures
- Compliance Management Framework: Breach Reporting - Procedures

RELATED LEGISLATION / STANDARDS

- University of the Sunshine Coast Act 1998 (Qld)
- Financial and Performance Management Standard 2009 (Qld)
- Financial Accountability Act 2009 (Qld)
- Work Health & Safety Act 2011 (Qld)
- Work Health and Safety Regulations 2011 (Qld)
- AS ISO 19600:2015 Compliance management systems