Compliance Breach Management Policy

Section 1 - Background and Purpose

(1) The Compliance Breach Management Policy (the Policy) sets out the University's processes for managing and complying with legislative, statutory and contractual breach reporting obligations, by ensuring any actual or potential breaches are reported and actioned. All employees, contractors and volunteers play a role in ensuring compliance and using the defined channels to notify the University of actual or potential breaches.

Section 2 - Scope

(2) This Policy applies to:

a. Employees
b. Contractors
c. Volunteers

Section 3 - Policy Statement

(3) The University is committed to full compliance with all applicable laws, regulations, standards, codes, and other licensing or contractual obligations to which it is bound.

(4) This Policy applies in situations where a contravention of a Compliance Obligation (actual or potential) is identified.

(5) Employees, Contractors and Volunteers are expected to remain familiar with this Policy and any supporting procedure(s), including the prescribed timeframes for notification.

Policy Exemptions

(6) Some compliance matters, such as those provided below, may be excluded from the requirements set out in this Policy and are to be dealt with according to the prescriptions set under University Policy, Statute or Legislation as relevant in the circumstances. These include but not limited to:

a. disclosures of improper conduct relating to the University or a member, officer, or employee or contractor of the University pursuant to the Protected Disclosure Act 2012 (as amended from time to time) as covered by the University's Protected Disclosure Policy;
b. disclosures made directly to the University Ombudsman;
c. disclosures made pursuant to staff and student complaints procedures;
d. Reportable Allegations, made pursuant to the University's Reportable Conduct Policy;
e. research misconduct allegations dealt with by the Deputy Vice-Chancellor (Research and Industry Engagement) (DVC(RIE)) (University's Designated Person); and

f. disclosures of injuries, incidents and hazards made pursuant to the University's Occupational Health and Safety Policy and Procedures.

Section 4 - Procedures

Part A - Breach Reporting (actual or potential)

(7) As soon as reasonably practicable after becoming aware of an actual or potential breach, employees are required to inform:

a. their manager; and
b. the relevant Responsible Officer.

(8) Managers will be responsible for completing a Breach Notification Form and providing this to the applicable Responsible Officer Register as soon as reasonably practicable, generally within 24 hours of identification.

(9) Where in doubt, notification should be directed to the Risk Management Office via compliance@latrobe.edu.au

Part B - Breach Assessment

(10) Under this policy, Responsible Officers are ultimately accountable for:

a. overseeing investigations by management into actual or potential breaches(see part C);
b. assessing any actual or potential contraventions resulting from that event including the root cause, severity and likely impact, and documenting this assessment within the Responsible Officer - Breach Assessment Form;
c. developing remediation and or mitigation plans and ensuring the adequacy of corrective actions to reinstate compliance and mitigate the risk of reoccurrence; and
d. reporting all breaches (actual or potential) to the Risk Management Office in accordance with the timeframes contained within this Policy.

(11) In circumstances where the Responsible Officer believes management's response to an actual or potential breach is inadequate, the matter should be referred to the Risk Management Office for resolution.

Part C - Investigatory Responsibility

(12) Management remains responsible for investigating, under the direction of the applicable Responsible Officer, the circumstances of an actual or potential breach including root cause and likely impact.

(13) In the case of a criminal matter, all reasonable care must be taken to ensure the principles of natural justice are applied and any interim action does not compromise the integrity of available evidence for any subsequent detailed investigation. For matters of health and safety, occupational health and safety standards must be adhered.

Part D - Governance Clearances

(14) Where a Governing Body or Committee is responsible for overseeing compliance, notification is required to be made by the Responsible Officer to that Governance Committee, in accordance with its terms of reference. Where the matter is a material breach however, per section 4.5, the matter must be reported to the Risk Management Office within 24 hours or as soon as reasonably practicable following identification.

(15) Approval for reporting of non-material breaches is required from the relevant Committee, prior to the Quarterly

Breach Report being lodged with the Risk Management Office.

Part E - Reporting Material Breaches (actual or potential)

(16) A material breach (actual or potential) has one or more of the following characteristics:

a. indicates a systemic concern; and/or
b. is required to be reported to an external body (such as a regulator, ombudsman, or accreditation body); and/or
c. relates to a Priority One Act Regulation, Standard or Code, as determined by risk, defined as:
    i. Long term severe health impacts on significant numbers of people or multiple fatalities
    ii. Budget blow-out of >15% or losses of >$5 million
    iii. Reputation and standing of the University affected nationally and internationally. Long term irreconcilable loss of confidence in LTU, and or loss of confidence / standing for several months
    iv. Significant legal action, criminal prosecution, major negative sanctions or imposition of significant permanent onerous obligations
    v. Loss of teaching licenses
    vi. Significant penalties or fines > $5M

(17) Material breaches (actual or potential) must be reported immediately (generally within 24 hours) to the Risk Management Office (compliance@latrobe.edu.au) by the applicable Responsible Officer, and should be assessed by the Responsible Officer in consultation with the Risk Management Office.

Part F - Committee Reporting and Oversight

(18) This University requires breaches to be reported to the Corporate Governance, Audit and Risk Committee (CGARC) quarterly by the Risk Management Office.

(19) As part of this central reporting and oversight, Responsible Officers are required to collate and provide at the end of each quarter (or otherwise on request) a report on all new actual or potential breaches (including the status of the corrective action plan) for any previously reported, open and unresolved matter (Quarterly Breach Report).

Part G - Risk Management Office (Roles and Responsibilities)

(20) While the Risk Management Office retains overall responsibility for the management of the University's Compliance Management Framework, the University's model of compliance is decentralised and places reliance on appointed Responsible Officers for identifying, monitoring, reporting on and overseeing compliance with all applicable Obligations.

(21) Under this policy the Risk Management Office will be responsible to:

a. coordinating aggregate reporting to Senior Executive Group (SEG) and CGARC;
b. undertaking systemic trending analysis of breaches reported;
c. monitoring on a quarterly basis, all reported breaches to resolution;
d. providing support and guidance, as needed; and
e. reviewing the circumstances surrounding a breach, including the adequacy of the assessment and corrective action plan to ensure the actions are taken and the risk of reoccurrence is appropriately mitigated.

Part H - Privacy Breaches (actual or potential)

(22) Where there has been a contravention or likely contravention of a privacy obligation, the Privacy Officer must be notified within 24 hours or as soon as practicable following identification.

(23) The Privacy Officer will then be responsible for initiating the University's privacy breach response as set out under the University's Privacy - Personal Information Policy.

Part I - Identification Channels

(24) There are many methods in which an actual or potential breach may be identified. Including from internal employees, contractors and volunteers to external community reports. Please also refer to Compliance Management Framework - Identification Channels and Prescribed Reporting Timeframes for examples.

Part J - Whistle-blowing and Protected Disclosures

(25) La Trobe University actively encourages employees and the broader University community to report details of any actual or potential breach they identify, or that has recently been detected but are concerned may not have been adequately raised or addressed.

(26) The University also recognises that whistleblowing (otherwise known as protected disclosures) is an important way of ensuring effective governance, and encourages employees to read and understand the Protected Disclosure Policy, and avail themselves of the additional mechanisms in which they can report on any actual or suspected misconduct.

Section 5 - Definitions

(27) For the purpose of this Policy:

a. Breach: A Breach is a contravention of a Compliance Obligation. Significant or material breaches are generally reportable to the regulator(s). See Part E for more information on assessing 'materiality'.
b. Compliance Obligation: Compliance obligations are those imposed by law, regulation, standard, code, and other licensing or contractual obligations to which the University is bound.
c. Incident (Outside the scope of this Policy): An incident is a form of non-compliance or other control failure that is not a breach (i.e. contravention of a statutory or regulatory obligation). Incidents may include a breakdown of business process or operational procedures not otherwise deemed to be a contravention of a Compliance Obligation. An example of this may be system downtime that may affect compliance. Incidents fall outside the scope of this policy and are to be dealt with by the University's Responsible Officers in consultation with the relevant business unit.

Section 6 - Stakeholders

Responsibility for implementation – La Trobe University's Responsible Officers.

Responsibility for monitoring implementation and compliance – Risk Management Office.

Status and Details

Status	Current
Effective Date	9th November 2017
Review Date	9th November 2020
Approval Authority	
Approval Date	9th November 2017
Expiry Date	To Be Advised
Unit Head	
Author	
Enquiries Contact	Risk Management Office