**Compliance Breach Reporting Form (for Managers/Supervisors/Compliance Coordinators)**

**Threshold for reporting pursuant to Compliance Policy (link)** *(TICK one to proceed***)**

A Compliance Breach means an act or mission (of varying consequences, depending on the nature of the breach and the harm caused) whereby the University does not meet its compliance obligations.

Staff may report concerns of a compliance breach to a manager/supervisor /compliance coordinator by phone, email, or using one of the University incident reporting systems, such as ROAR, RiskMan or OneHelp. Any campus emergencies should be reported to the Campus Emergency Centre on 9850 9999 (9999 on MQ internal phones) or directly to Emergency Services: 000

**Managers/Supervisors/Compliance Coordinators are required to use this form to report cases when a breach is deemed material in accordance with the Compliance Policy.**

When a concern is reported, the manager/supervisor/compliance coordinator will assess the information provided and if the breach is deemed material, as set out in the criteria below, will complete this form. Guidance may be sought from the Office of General Counsel (Compliance and Privacy Manager) on whether the breach/concern reaches the threshold for reporting via the form.

In accordance with the Compliance Policy, a breach is deemed material and this form must be used for reporting, if it meets one of the below criteria.

Please tick one or more criteria below to proceed:

* + 1. University-wide impact ( ) and/or
		2. Requires policy or procedure review/amendment ( ) and/or
		3. Could generate widespread media and reputational damage, ( ) and/or
		4. Requires notification to an external regulatory authority ( ) and/or
		5. is subject to a financial penalty ( )

|  |  |  |  |
| --- | --- | --- | --- |
| Faculty/Business Unit |  | Supervisor/Manager/**Compliance Coordinator** for reporting Faculty/Business Unit |  |
| Identified by |  | Date identified  |  |
| Notified to**Compliance Owner**  |  | Date approved |  |

**Breach Notifications**

|  |  |
| --- | --- |
| Have any other parts of the University or Controlled entities been notified of the breach? (For example via ROAR, OneHelp, RiskMan notification ) | Yes/No |
| If yes, to whom? (Add email) |  |

**PART 1**

**To be completed by Manager/Supervisor/Compliance Coordinator (in consultation with staff who reported the breach or concern).**

|  |
| --- |
| Summary of Compliance Breach (Include impacts and any harm)  |
| Free text field  |

**Type of Breach**

|  |  |  |  |
| --- | --- | --- | --- |
| Legislation | Open list of legislations | Industry Standard/Guideline: | Free text |
| Internal Policy/Procedure  | Open list of Policy/Procedure | Material Contract: | Free text |
| Licence/Permit Obligation  | Free text | Directive: | Free text |
| Other: |  |
| Attachment |  |

**Penalties or Referrals (*if known*)**

|  |  |
| --- | --- |
| Is there a penalty? | Yes /No/Unsure |
| Are there any regulatory reporting deadlines or other referrals required? \*(Example: some breaches under the Cmth *Privacy Act 1988* must be reported/responded to within 30 days)  |  Yes /No /Unsure |
| If yes, what are they? |  |

\*If unsure contact the Compliance Coordinator for the relevant legislation

**PART 2**

**To be completed by Manager/Supervisor/Compliance Coordinator**

|  |
| --- |
| Business Unit response/ **Remediation plan** in relation to breach  |
| Free text field |

**PART 3 (Office of General Counsel *only*)**

**Office of General Counsel review**

|  |  |
| --- | --- |
| Remediation Plan | Satisfactory/Unsatisfactory\* |
| Reported to Audit and Risk Committee  | Yes/No |
| Regulatory referral/requirement managed  | Yes/No\*/Not appliable  |
| Other relevant referrals  |  |

\*Reference in *Outcome* commentary below

**Outcome** *(circle)a*

Closed / Ongoing

|  |
| --- |
| Commentary on Outcome/Future Management and any relevant **attachments** |
|  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

Manager Compliance/ Office of General Counsel