# Data Breach Incident Escalation Process and Team Structures

## UNE Representatives

**Suspected Privacy breach/Identified**

Privacy Management Plan

*Reported to the UNE Privacy Officer*

## Advisor (Privacy & Compliance)/ Privacy Officer

Data breach Response Plan

Privacy Management Plan

**Privacy Breach Assessed** ↔ **Harm remediated** ↔ **Breach report and notification**

*Significant data breaches escalated*

*Technology related data breaches escalated*

*SIMT communicates and consults with CIO and IT Management Team*

**DBMT Data Breach Response Invoked**

*SIMT escalates significant data breaches*

**SIMT Data Breach Response Invoked**

Data Breach Coordinator (Director of Governance & University Secretary)

Risk Coordinator

IT Coordinator

HR Coordinator

Privacy Officer/ Advisor ( Privacy & Compliance)

Communications Coordinator

Director of Legal Services or nominee

Records Management Support

CFO or nominee

### Data Breach Management Team (DBMT)

Data Breach Response Plan

IT Security Operations Manager

Senior Network Administrator ( Team Leader)

Senior Server Administrator (Team Leader Unix)

Manager, IT Support

Senior Server Administrator (Team Leader)

Senior client Services Officer & Technical Lead

Manager, Administrative Applications

Privacy Officer/Advisor (Privacy & Compliance)

Manager online & Learning Applications

Manager, Systems Support

Manager, Business Systems & Engagement

Senior Information Security Officer

MIM Coordinator

### Security Incident Management Team (SIMT)

ITSC&DR Plan

Major Incident Management Plan

Security Incident Management Plan

*Consults*

*Significant Data breaches escalated*

*DBMT consults on evolving breach and is kept informed by SIMT*

## Emergency Control Organisation (ECO)

**ECO Emergency Response Invoked**

**ECO Emergency Comms Invoked**

Emergency Management Plan