Data Breach Response Plan

Section 1 - Overview and Scope

(1) This Data Breach Response Plan outlines the processes and roles and responsibilities for managing data breaches at UNE and should be read in conjunction with the:

a. Data Breach Guidelines;
b. Cyber and Information Security Rule;
c. Emergency Management Plan;
d. Privacy Management Plan ; and
e. the IT Service Continuity and Disaster Recovery Plan.

(2) The purpose of this plan is to outline the identification, reporting, containment, assessment, escalation and notification process in the event of a data breach at UNE enabling the University to:

a. identify, assess, contain, escalate, and respond to data breaches in a timely manner;
b. proactively mitigate and remediate potential harm to affected individuals;
c. document processes and data breach responses;
d. identify the staff roles and responsibilities, delegations of authority and reporting lines in the event of a data breach and points of contact; and
e. Identify the staff responsible for managing the data breach response.

(3) A summary of the process can be found in the Data Breach Management Process and the Data Breach Incident Escalation Process and Team Structures.

(4) Within this plan:

a. Part A outlines identification, and reporting;
b. Part B deals with containment and analysis;
c. Part C outlines the University's response; and
d. Part D outlines notification and remediation.

Part A - Identify

Alert – Reporting a suspected data breach

(5) A data breach is unauthorised access to, disclosure of, or loss of the personal, health, and sensitive information UNE holds. All UNE staff have a responsibility to report all suspected data breaches to the UNE Privacy Officer promptly via privacy@une.edu.au and cooperate with data breach investigations as required. Information provided should include:

a. time when suspected data breach is discovered and/or disclosed, and the individual who discovered or made the report (e.g. staff, student, community member, external security providers, third party vendors);

b. details of the breach e.g. system involved, email message responded to, staff member accessing unauthorised files, loss of hardware (e.g. laptop, portable storage device), loss or disclosure of paper files, verbal disclosure;
c. number of people believed to be affected;
d. the types of information involved e.g. student details, emails, staff details, business analytics, health information, or audiovisual materials.

(6) Whatever the cause of the data breach, harm can result to students or UNE Representatives. Harm includes financial, social, reputational, psychological or physical impacts to an individual and reputational or financial damage to UNE and need only impact one person.

(7) Examples of potential data breaches include:

a. the loss of a USB, laptop or other personal device;
b. loss of hardcopy files or papers containing personal details, or disclosure of these files to the incorrect recipient;
c. email errors – emails sent to incorrect addresses, the disclosure of the email addresses of large groups of recipients via carbon copy or attaching personal information inadvertently;
d. external attack, access, loss or disclosure on a third party vendor implicating personal information for which UNE is responsible;
e. phishing, hacking or other external attacks on the University's information repositories; and
f. unauthorized access by a staff member to files containing personal, health or sensitive information.

Part B - Assess and contain

(8) The UNE Privacy Officer will immediately conduct a review of the details provided using the Harm Identification and Action Tables and Personal Information Risk Categories and the Data Breach Investigation Checklist and inform Audit & Risk where appropriate. Once the type of breach has been identified the Privacy Officer will:

a. For a non-technology related breach (e.g. hard copy files, verbal disclosure) – take necessary steps to contain and notify;
b. For an IT related breach (e.g. loss of laptop, compromised user account, social engineering, ransomware, information and email disclosure to an unintended recipient, hacking) escalate or report to the Security Incident Management Team (SIMT) who will implement necessary containment measures in accordance with the Cyber Security Incident Response Plan, minimising harm to individuals and UNE.
    i. In the case of minor breaches the Privacy Officer may have mitigated all harm during the preliminary investigation and will report all details to the SIMT including a description of the breach, action taken, outcome and reasons escalation is not required.
c. In the event that breaches may affect intellectual property, copyright or commercially sensitive information in addition to or instead of personal information, concerns will be escalated to the appropriate staff members.

(9) Once notified the SIMT will make preliminary judgement as to its severity based on the Harm Identification and Action tables and Personal Information Risk Categories. SIMT and the Privacy Officer will take reasonable steps to obtain/preserve evidence of any actual or suspected data breach.

(10) The containment measures adopted by the Privacy Officer or SIMT (in collaboration with system owners or administrators and third party vendors) could include:

a. Technological breaches
    i. isolating the causes of the data breach in the relevant system, software or database;
    ii. shutting down the compromised system, software or database;

iii. resetting log-in details and passwords(of staff, Students or administrators) for compromised devices, systems or databases;
iv. quarantining compromised devices;
v. recording evidence by taking screenshots of popups or messages, retaining emails sent and received, and collating system logs; and
vi. activating the Emergency Control Organisation (ECO)and the Emergency Management Plan.

b. Loss of personal information technical or non-technical:
   i. remotely disable or delete information on the lost device wherever technology permits; and
   ii. arrange a search of the site where the loss occurred by contacting any relevant authorities (e.g. the relevant bus company if left on a public bus or an airline if left on a plane).

c. Unauthorised disclosure of personal information technical or non-technical :
   i. by email – recall the email from the recipient and/or ask the recipient not to read and to delete the email;
   ii. by post – contact the recipient and ask them not to open or read the posted materials, and arrange for collection/return of the posted materials;
   iii. by publication online – deactivate the link to the publication; and
   iv. verbal disclosure – meeting with the recipients of the information and witnesses of the incident to discuss the importance of confidentiality, and request information not be disclosed further.

Part C - Response

(11) After initial assessment of harm by the SIMT or the Privacy Officer, subject experts will be utilised as necessary. If the extent and likelihood of harm are categorised as extreme risk on the Harm Identification Table and Personal Information Risk Categories, the Data Breach Management Team (DBMT) will be activated in consultation with the ECO (see the Data Breach Escalation and Team Structures). The team will consist of the following members as required:

a. Data Breach Coordinator – Director Governance and University Secretary or nominee;
b. Risk Coordinator – Director Audit and Risk or nominee;
c. IT Coordinator – Chief Information Officer or nominee;
d. HR Coordinator – Director People & Culture or nominee (required if the breach occurred as a result of the actions of, or impacts a staff member);
e. Communications Coordinator – Associate Director Corporate Communication and Events or nominee (required for advice and approval of large scale communications to staff, students and/or the wider community);
f. Specialist support –
   i. Privacy Officer (Advisor (Privacy and Compliance));
   ii. Chief Financial Officer or nominee (required when financial or insurance advise or financial approval for remediation measures is required);
   iii. Director Legal Services or nominee; and
   iv. Specialist (Records and Governance) or nominee.

(12) The Privacy Officer will record the membership of the formed DBMT for each breach in UNE's Records Management System and review the membership regularly to maintain currency.

(13) The associated Data Breach Management Process explains the process of identification, investigation and the escalation points.

(14) Consistent documentation of the decision, escalation, and risk assessment is required for the management of external notification and investigation, assisted by the Data Breach Investigation Checklist. The IT Security Operations Manager as part of the SIMT will ensure necessary records are stored in the Records Management System in

accordance with the Records Management Rule.

(15) Any data breach will be dealt with on a case-by-case basis utilising the Data Breach Investigation Checklist. The assessment of harm and associated risk using the Harm Identification Table and Personal Information Risk Categories, will inform the appropriate course of action, which may include:

a. containment measures;
b. retrieving the personal information if possible;
c. documentation of all evidence;
d. consultation with the SIMT & DBMT;
e. conducting initial investigation and collecting information about the breach, including:
    i. date, time, duration and location of breach;
    ii. type of personal information involved in the breach;
    iii. how the breach was discovered and by whom;
    iv. cause and extent of the breach;
    v. list of the affected individuals, or possibly affected individuals; and
    vi. the risk of harm to the affected individuals (based on the Harm Identification and Action Tables and Information Risk Categories).
f. consultation with the Information and Privacy Commission NSW (IPC) or Office of the Australian Information Commissioner (OAIC) where appropriate;
g. engaging cyber security or forensic experts where appropriate;
h. conducting risk/harm assessment; and
i. liaison with or escalation to the ECO.

Part D - Notification & Remediation

(16) UNE is subject to the national Notifiable Data Breaches (NDB) scheme, under Part IIIC of the Privacy Act 1998 which establishes a mandatory notification for federal agencies and any agency collecting TFNs, for eligible data breaches. In circumstances of unauthorised access to or disclosure of a TFN, UNE must make a mandatory report within 30 days to the OAIC, if the breach is likely to result in serious harm to any individual which could not be adequately prevented.

(17) The DBMT, with input from relevant business units or system owners or administrators, is responsible for managing any other mandatory or voluntary notifications to the following parties as appropriate(text must be reviewed by the UNE Privacy Officer, who will liaise with the Communications team and Legal Office as appropriate, prior to sending):

a. affected individuals;
b. OAIC – a formal notification through the OAIC's NDB form should be completed;
c. IPC;
d. internal staff;
e. financial services provider;
f. police or law enforcement bodies;
g. the Australian Securities & Investment Commission (ASIC);
h. the Australian Taxation Office (ATO);
i. the Australian Transaction and Reports and Analysis Centre;
j. the Australian Cyber Security Centre;

k. the Australian Digital Health Agency;
l. the NSW Department of Health;
m. professional associations and regulatory bodies;
n. insurance providers;
o. NSW Department of Finance, Service and Innovation; and
p. The NSW Chief Cyber Security Officer.

(18) The Privacy Officer will prepare mandatory notifications for the OAIC, and IPC as appropriate.

(19) The documentation compiled during the investigation, assessment and notification phases (with reference to the Data Breach Investigation Checklist) including the mandatory notification report, will inform reporting by the DBMT to the Chief Information Officer, Director Governance and University Secretary, Senior Executive Team, and Council as informed by the assigned category in the Harm Action Table.

Review and Remediation

(20) After notifications and reports have been finalised, the incident will be reviewed and changes to current procedures recommended to ensure future breaches are prevented or better managed in the future. Items for review and remediation include:

a. root cause analysis of the breach(including a full investigation if required) and report to Data Breach Coordinator, Risk Coordinator, IT Coordinator and HR Coordinator as appropriate;
b. implementation of a strategy to address any identified weaknesses in data handling that contributed to thebreach;
c. involvement of external partners (where necessary);
d. policy and procedure (including updates to the security and response plans);
e. internal processes;
f. staff training practices; and
g. the option of an audit to ensure necessary outcomes are enacted.

Prevention

(21) To prevent data breaches and mitigate the extent of harm to individuals and UNE, all UNE Representatives (including system owners or administrators) must ensure:

a. they report suspected data breach incidents to the Privacy Officer;
b. participate in data breach investigations as required;
c. assist in the prevention of data breaches through compliance with this plan and the Data breach Guidelines
d. appropriate review of all systems, applications, or services incorporating personal information has occurred prior to implementation;
e. wherever possible that contracts or service agreements incorporate clauses specifying notification timeframes and investigation support related to data breaches;
f. notification of data breaches from third party vendors should occur within 48 hours from discovery of the potential breach;
g. any notification from third party vendors is reported immediately (within 24 hours) to privacy@une.edu.au;
h. changes to privacy policies, data processing arrangements, data storage locations, service agreements or other vendor documents impacting personal information, which are communicated to system owners or administrators are also communicated to the UNE Privacy Officer and Cyber Security Team where appropriate;
i. appropriate assignment of funds to sufficiently manage risks and implement appropriate remediation measures

when considering implementation of a new application or system or renewal of an existing one;

j. they remain vigilant and sceptical of unusual circumstances or behaviors and report any concerns to immediate supervisors or privacy@une.edu.au; and

k. ensure currency of knowledge of all privacy and security policies and complete all available cyber security and privacy training.

Summary of Roles and Responsibilities

Role	Responsibilities
UNE Representatives	Report suspected data breach incidents to the Privacy Officer. Participate in data breach investigations as required. Maintain awareness and complete all required cyber security or privacy training. Assist in the prevention of data breaches through compliance with this Plan.
System owners or administrators	Report notifications of breaches received from third party vendors to privacy@une.edu.au including all relevant documentation. Assist as required with all investigations managed by the Privacy Officer, SIMT, or DBMT. Ensure appropriate mechanisms for breach management response is included in all service agreements/contracts related to systems, applications or services that incorporate personal information. Ensure appropriate assignment of funds to sufficiently manage risks and implement appropriate remediation measures when considering implementation of a new application or system or renewal of an existing one. Ensure any communications with impacted parties or external bodies are first communicated to the UNE Privacy Officer for review.
UNE Privacy Officer	Receive reports of suspected data breaches and conduct preliminary investigation utilising the Data Breach Investigation Checklist and the Harm Identification and Action Tables and Personal Information Risk Categories. Escalate technology based data breaches to the SIMT. Escalate data breaches involving fraud or misconduct to the Audit & Risk Directorate as required. Assess whether an eligible data breach has occurred. Assess containment and remediation actions of a non-technological data breach. Remediate harm and preserve evidence. Assess notification requirements. Participate in security incident response as an integral member of the Security Incident Management Team. Submit the notification report as required with the IPC and/or the OAIC.
Audit & Risk Directorate	Receive data breach reports from the Privacy Officer. Provide risk based advice on the data breach and the potential responses required. Provide information and reporting to the Independent Commission Against Corruption (ICAC), the Audit Office of New South Wales (AONSW) and the New South Wales Police Force (NSW Police) as required.
Chief Financial Officer (CFO)	Liaise with the insurer as required. Provide budget authorisation for remedial actions.
Chief Information Officer (CIO)	Coordinate internal and external communication. With assistance from the Information Technology and Digital Services Command Team, oversee the activities of the Security Incident Management Team. Participate in the Data Breach Response as part of the Data Breach Response Team. Liaise with the Cyber Security Insurance provider as required and secure forensic capabilities where necessary. Inform Australian Signals Directorate (ASD) as required.
Director of Governance and University Secretary	Lead the Data Breach Management Team. Act as an escalation point for the Privacy Officer – assess notification requirements and prepare reports where required.

Role	Responsibilities
Security Incident Management Team (SIMT)	Receive information technology related data breach reports from the Privacy Officer. Analyse, contain and investigate information technology based data breaches (breaches involving personal information stored on or in computers or digital systems within the context of UNE business operations) in alignment with the Security Incident Management Plan. Document all actions taken during the containment of a data breach in alignment with the Data Breach Investigation Checklist. Liaise with the system owner and third party vendor as required. Keep the Chief Information Officer informed. Participate in data breach investigations as required. Conduct post incident review and provide reports to the Chief Information Officer.
Data Breach Management Team (DBMT)	Assess the impact, harm and legal implications of escalated data breaches. Assess containment and remediation actions of data breaches. Remediate harm and preserve evidence. Manage and implement appropriate communications with the UNE community as required. Keep the Emergency Control Organisation informed of the status of the data breach. Escalate significant data breaches to the Emergency Control Organisation (categorised as Extreme on the Harm Action Table).
Emergency Control Organisation (ECO)	Receive assessment information (impact, harm and legal implications) on data breaches. Lead and manage the data breach response in alignment with the Emergency Management Plan. Approve external technological support where required.

Section 2 - Authority and Compliance

(22) The Director Governance and University Secretary makes this plan, which has the effect of a policy.

(23) UNE Representatives must observe this plan in relation to University matters.

(24) This Plan operates as and from the Effective Date of the Data Breach Guidelines.

(25) Notwithstanding other provisions of this Plan, the Vice-Chancellor and Chief Executive Officer may approve an exception to this Plan where the Vice-Chancellor and Chief Executive Officer determines the application of this Plan would otherwise lead to an unfair, unreasonable or absurd outcome.

Section 3 - Quality Assurance

(26) The implementation for these guidelines will be supported through;

a. Quarterly reporting to the Information Technology Governance Committee and Director of Governance and University Secretary regarding any breach notifications and investigations; and
b. The reporting of data breach notifications and post investigation recommendations to the ITD Management Team and Information System owners.

Section 4 - Definitions

(27) Data breach:

a. A data breach occurs when a failure or potential failure causes unauthorised access to UNE's data. When this access involves the unauthorised access to, disclosure of or loss of personal information of UNE staff, student's or community members it can cause serious harm to individuals.

b. Whilst external attacks are of great concern, many breaches are a result of human error, carelessness or technical faults rather than malicious intent.

(28) Emergency Control Organisation - The entity responsible for UNE's Incident and Emergency activities during the Prevention, Preparedness, Response and Recovery (PPRR) phases (the four stages of the Emergency Management Cycle).

(29) Personal Information - As defined in the Privacy and Personal Information Protection Act 1998 (section 4) and the Privacy Act 1988 (Section 6(1)) personal information, is any information or an opinion about an identified individual or information about an individual whose identity can be readily ascertained. Whether information is considered identifiable depends on a number of factors including context, access, and number of data points. It includes but is not limited to:

a. personal details such as name, address, and other contact information about an individual;
b. photographs, images, video or audio footage;
c. fingerprints, blood or DNA;
d. employee details;
e. credit information;
f. banking and financial information; and
g. unique government identifiers such as Medicare numbers or National Unique Student identifiers.

(30) Sensitive Information - In accordance with the Privacy and Personal Information Protection Act 1998 (NSW) sensitive information includes:

a. ethnic or racial origin;
b. political opinions;
c. religious or philosophical beliefs;
d. trade union membership; or
e. sexual activities.

(31) Health information - The collection and use of health information is outlined in the Health Records and Information Privacy Act 2002 which aims to promote the fair and responsible handling of health information. Health information includes:

a. any information or an opinion pertaining to the physical or mental health or disability of an individual, their express wishes about the future provision of health care and details of any health services provided or to be provided to them;
b. other personal information collected to provide, or when providing, a health service; or
c. personal information about an individual collected in connection with the donation or intended donation of an individual's body parts, organs or body substances;
d. any genetic information about an individual arising from a health service provided to that individual, that is, or could be, predictive of the health (at any time) of that individual or a genetic relative; or healthcare identifiers.

(32) The Security Incident Management Team (SIMT) - will incorporate the IT Security Operations Team, the UNE Privacy Officer, and ITD team leaders/managers as appropriate, as overseen by the Chief Information Officer and IT at UNE.