Privacy Security Breach Procedure

Section 1 - Summary

(1) In the event a privacy security breach occurs with regard to personal information held by Victoria University (University), the University will take appropriate steps in response to the breach of its privacy security.

(2) For the purpose of this Procedure, a privacy security breach occurs if personal information held by the University is lost or subjected to unauthorised access, modification, disclosure or other misuses.

Section 2 - Scope

(3) This Procedure applies to all University staff, students and agents.

Section 3 - Definitions

(4) NDB Scheme means the Notifiable Data Breaches Scheme as defined in the Privacy Act 1988(Cth).

(5) Eligible Data Breach under the NDB Scheme is a breach that is deemed to be an eligible data breach according to the following:

a. There is unauthorised access or disclosure or loss of Tax File Number Information (TFN information);
b. A reasonable person would conclude that the access, disclosure or loss would likely result in serious harm to any of the affected individuals; and
c. The University has not been able to prevent the likely risk of serious harm occurring after remedial action is taken.

Section 4 - Policy / Regulation

(6) Refer to Privacy Policy.

Section 5 - Procedures

Part A - Summary of Roles and Responsibilities

Roles	Responsibilities
Director, ITS Security and Risk Assurance	Responsible for co-ordinating the University's response to the privacy security breach.

Part B - Responding to Privacy Security Breaches: Four Key Steps

(7) There is no single way the University will respond to a privacy security breach if one occurs, as privacy security breaches can be caused or exacerbated by a number of factors. Each breach will be dealt with by the University on a case-by-case basis, with the University undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.

(8) As a guide, there are four key steps that the University will generally follow when responding to a privacy security breach or suspected privacy security breach:

a. Step 1: Contain the breach
b. Step 2: Evaluate the risks associated with the breach
c. Step 3: Consider whether notification is appropriate and if so, undertake a notification process
d. Step 4: Prevent future breaches

Each of the above steps is addressed in further detail below.

Step 1: Contain the Breach

(9) If any person within the University discovers, suspects or is made aware of a privacy security breach, that person should escalate the matter immediately to the Director, ITS Security and Risk Assurance and/or the Privacy Officer so that the University can take necessary and practicable steps to address and contain the breach.

(10) What steps are necessary to contain the privacy security breach will depend on the nature of the breach but may include:

a. recovery of any records containing personal information;
b. shutting down any electronic system that has been interfered with;
c. revoking or changing access privileges; and/or
d. addressing weaknesses in physical or electronic security.

(11) The Director, ITS Security and Risk Assurance will be responsible for co-ordinating the University's response to the privacy security breach.

Step 2: Evaluate the Risks Associated with the Breach

(12) The University will assess the risks associated with the privacy security breach.

(13) In doing so, it may consider the following factors:

The type(s) of personal information involved

(14) Some types of personal information are more likely to cause individual harm if compromised (for example, an individual's academic information, financial information, or health or other sensitive information), whether that harm is physical, financial or psychological.

The context of the affected information and the breach

(15) What parties may have gained unauthorised access to the affected information?

a. Did the breach involve disclosure to an unknown party or to a party where there is a potential risk of misuse, or to a trusted, known entity or person that would reasonably be expected to return or destroy the information without disclosing or using it?

(16) Have there been other breaches that could have a cumulative effect?

a. A number of small, seemingly insignificant, breaches may have a cumulative effect. Separate breaches that might not, by themselves, be assessed as representing a real risk of serious harm to an affected individual, may meet this threshold when the cumulative effect of the breaches is considered.

(17) How could personal information be used?

a. Could the information be used for fraudulent or otherwise harmful purposes, such as to cause financial loss to the affected individual or to cause significant embarrassment to the affected individual? Could the compromised information be easily combined either with other compromised information or with publicly available information to create a greater risk of harm to the individual?

Establish the cause and extent of the breach

(18) Is there a risk of ongoing breaches or further exposure of the personal information?

a. What was the extent of the unauthorised access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?

(19) Is there evidence of theft?

a. Is there evidence that suggests theft, and was the personal information the target? For example, where a laptop is stolen, can it be determined whether the thief specifically wanted the information on the laptop?

(20) Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?

a. Is the information rendered unreadable by security measures that protect the stored personal information? Is the personal information displayed or stored in such a way so that it cannot be used if breached?

(21) What was the source of the breach?

a. For example, did it involve external or internal malicious behaviour, or was it an internal processing error? Does personal information seem to have been lost or misplaced? The risk of harm to the individual may be less where the breach is unintentional or accidental, rather than intentional or malicious.

(22) Has the personal information been recovered?

a. For example, has a lost laptop been found or returned? If the personal information has been recovered, are there any signs that it has been accessed, copied or otherwise tampered with?

(23) What steps have already been taken to mitigate the harm?

a. Has the University adequately and effectively contained the breach? Have compromised security measures such as passwords been replaced? Has the full extent of the breach been assessed? Are further steps required?

(24) How many individuals are affected by the breach?

a. If the breach is a result of a systemic problem, there may be more people affected than first anticipated. Even where the breach involves accidental and unintentional misuse of information, if the breach affects many individuals, the scale of the breach may create greater risks that the information will be misused. The

University's response to the breach will be proportionate to the scale.

Assess the risk of harm to the affected individuals

(25) Examples of the types of harm to individuals that could result from a privacy security breach include:

a. identity theft;
b. financial loss;
c. the threat to physical safety;
d. the threat to emotional wellbeing;
e. loss of academic, business or employment opportunities; and/or
f. humiliation, damage to reputation or relationships.

Assess the risk of other harms

(26) Other possible harms associated with a breach of privacy security, including to the University include:

a. the loss of public trust in the University;
b. reputational damage;
c. loss of assets (eg. stolen computers or storage devices);
d. financial exposure (eg. if bank account details are compromised or if financial compensation is paid by the University); and/or
e. legal proceedings (eg. formal complaint).

NDB Scheme

(27) If the University suspects an eligible data breach has occurred, the University must make an assessment of the suspected eligible data breach under step 2 of this procedure with 30 days.

(28) The University should take any remedial action during the assessment period that is appropriate given the circumstances of the suspected eligible data breach.

Step 3: Consider whether Notification is Appropriate and, if so, undertake a Notification Process

(29) The University will consider the particular circumstances of a privacy security breach and decide whether to notify affected individuals; and, if so consider:

a. when and how the notification should occur, who should make the notification, and who should be notified;
b. what information should be included in the notification; and
c. who else (other than the affected individuals) should be notified.

(30) Notification may be an important mitigation strategy following a privacy security breach, however, the notification will not always be an appropriate response to a breach. Each incident will be considered on a case-by-case basis to determine whether breach notification is appropriate.

Deciding whether to notify affected individuals

(31) The key consideration the University will adopt is whether notification is necessary to avoid or mitigate serious harm to an affected individual. The University may consider the following factors when deciding whether notification is required:

a. What is the risk of serious harm to the individual as determined by Step 2?
b. What is the ability of the individual to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by the University)?
c. Even if the individual would not be able to take steps to improve the situation, is the information that has been compromised sensitive, or likely to cause financial damage or humiliation or embarrassment for the individual?

Notification process

(32) If the University determines that notification is appropriate, the University will endeavour to notify affected individuals directly - by phone, letter, email or in person. The University will generally only adopt indirect notification methods, such as by website information, posted notices, media etc, where direct notification could cause further harm, is cost-prohibitive, or the contact information for affected individuals is not known.

What will be included in the notification?

(33) If the University determines that notification is appropriate, the content of the notification will depend on the particular breach and the notification method. Notification may include the following types of information:

a. incident description;
b. type(s) of personal information involved;
c. the response is taken by the University to the breach to control or reduce the harm, and proposed future steps that are planned;
d. assistance offered to affected individuals and steps the individual can take to avoid or reduce the risk of harm or to further protect themselves;
e. other information sources designed to assist individuals in protecting against identity theft or interferences with privacy; and/or
f. contact information for persons that can answer questions, provide further information or address specific privacy concerns.

Who else should be notified?

(34) If the University determines that notification is appropriate, the University may also consider that there are third parties who should also be notified about the breach. Such third parties may include:

a. Victorian Information Commissioner (Commissioner): In some circumstances, it may be appropriate to notify the Commissioner. The University may consider the following factors when deciding whether to report a breach to the Commissioner:
    i. any applicable legislation that may require notification;
    ii. the type(s) of personal information involved and whether there is a real risk of serious harm arising from the breach, including monetary and non-monetary losses;
    iii. whether a large number of people were affected by the breach;
    iv. whether the information was fully recovered without further disclosure;
    v. whether the affected individuals have been notified; and/or
    vi. if there is a reasonable expectation that the Commissioner may receive complaints or inquiries about the breach.
b. Office of the Australian Information Commissioner (OAIC): Where the University forms the opinion that an eligible data breach has occurred the University is required to notify the OAIC and affected individuals.
c. Police: If theft or other crime is suspected.
d. Insurers or others: If required by contractual obligations.

e. Professional or other regulatory bodies: If professional or regulatory standards require the University to notify such a breach.

Step 4: Prevent Future Breaches

(35) In addition to the above three steps, the University may take further steps to prevent future privacy security breaches, including:

a. undertaking a privacy security audit to ensure a similar breach does not occur again;
b. making appropriate changes to any relevant protocols or work practices; and/or
c. reviewing and, if necessary, revising staff training practices.

Status and Details

Status	Historic
Effective Date	24th June 2019
Review Date	24th June 2022
Approval Authority	Vice-Chancellor
Approval Date	24th June 2019
Expiry Date	17th July 2024
Accountable Officer	Trish Roberts Deputy Chief Financial Officer trish.roberts@vu.edu.au
Responsible Officer	Lisa Filippin General Counsel lisa.filippin@vu.edu.au
Enquiries Contact	Lisa Filippin General Counsel lisa.filippin@vu.edu.au