Southern Cross University

PRIVACY DATA BREACH REPORT

Please complete this form, providing as much detail as possible, and email to privacy@scu.edu.au within 24 hours of discovering a suspected breach.

Date and Time of suspected breach

Date: Time:

Notification Date:

If this is more than 24 hours after the date above, please provide an explanation:

Person Making Notification

Name: Position:

Work Unit:

Preferred contact phone number: Email address:

Have you notified your Supervisor and Head of Work Unit about the suspected breach?

Yes ☐ No ☐

If no, please do so immediately

Does the suspected breach involve technology-based data?

Yes ☐ No ☐

If yes, have you notified TS Help Desk? Yes ☐ No ☐

If no, please do so immediately

Description of Breach – please see notes below for assistance.

What has happened?

What type(s) of personal information has been lost or shared?

Who has been affected, e.g. one staff member, all enrolled students, one or more health clinic patients or clients etc?

Is the information still lost or being shared?

Southern Cross University

Remedial action taken to date: Please see notes below for assistance.

What action have you taken to secure information, stop unauthorised access?

Have you notified the affected individuals? If YES, when and how?

Are there any other actions that you still intend to take?

Notes for Person Giving Notification

Breach nature

Please provide as much information as possible about:

- The type(s) and amount of personal information that has been lost or shared
- The number of individuals who were or might be affected
- What happened, e.g. did someone click on a link in an email, or leave a document in an insecure place, or provide information to the wrong person?
- When, where, how and by whom the breach was discovered.

Remedial action

Measures to remove or reduce the impact can include:

- Implementing training or process improvements
- Ceasing use of a particular system if the data breach was caused by system failure
- Ceasing or changing the access rights of individuals
- Changing users' passwords and system configurations to control access and use
- Technical fixes to remedy the system security loopholes
- Notifying other relevant agencies (e.g. Police if identity theft or other criminal activities are suspected)
- Documenting the details of the data breach to assist any investigation and corrective actions