Personal Data Breach Procedure

Section 1 - Purpose

(1) Charles Sturt University (the University) is committed to protecting the confidentiality, integrity and availability of personal information that it collects and uses to support business operations and services to staff and students.

(2) The purpose of this Procedure is to:

a. outline responsibilities of Charles Sturt University staff and students in response to suspected or identified breaches of personal information held by Charles Sturt University;
b. determine if a personal data breach occurring after 22nd February 2018 constitutes an eligible data breach that must be reported to the Office of the Australian Information Commissioner (OAIC) as per compliance with the Privacy Act 1988 amendments; and
c. outline the steps and responsibilities in reporting eligible data breaches to the Office of the Australian Information Commissioner, described as the 'Notifiable Data Breaches scheme'.

(3) This Procedure is a key component of the University's Data Breach Response Plan. The Data Breach Response Plan outlines how the University will respond to and initiate improvements in the University's response to personal data breaches.

Scope

(4) This Procedure applies to all University staff, students and other relevant parties including visitors, contractors and associated bodies who own, manage, access or use the University's Information and Communications Technology (ICT) services.

(5) This includes all:

a. ICT systems and data attached to University computer or telephone networks;
b. University systems;
c. communications sent to or from the University; and
d. data owned by the University, either internally or on systems external to the CSU network.

References

(6) This Procedure should be read in conjunction with:

a. Privacy Act 1988 (mandatory data breach notification amendment);
b. Privacy Amendment (Notifiable Data Breaches) Act 2017;
c. Information and Communications Technology Security Policy;
d. Privacy and Personal Information Protection Act 1998 No 133;
e. Privacy Management Plan;
f. Information Technology Procedure - Acceptable Use and Access;
g. Code of Conduct; and

h. Student Charter.

Section 2 - Glossary

(7) For the purpose of this Procedure:

a. Application, Data and Information Custodians – nominated staff overseeing the management of a specified application, data or information set with regards to ensuring availability, integrity, and protection according to relevant University business requirements, policy and legislative compliance.
b. Critical Incident Response Group – as determined by the Emergency Planning Committee to plan and organise responses to Critical Incidents in accordance with this Procedure.
c. CSU Privacy Officer – oversees the maintenance of the University's Privacy Management Plan, information sessions and advice to support the University in meeting privacy legislation obligations across the various areas of organisational activity.
d. Data Breach – means personal information or data held by the University is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Data breaches can be accidental or intentional in nature.
e. Data Breach Response Team – carry out timely actions to reduce the potential impact of a data breach.
f. Data Breach Response Process – outlines the actions to be taken in the case of a suspected or identified data breach. Facilitates a swift response and ensures any legal obligations are met following a data breach.
g. Data Breach Response Plan – sets out the components, roles and responsibilities for managing the University's appropriate response to a data breach.
h. Data Security and Governance Committee (DSGC) – a subcommittee of the Technology Governance Committee (TGC). The DSGC has oversight of University information and communications technology security and for ensuring the means by which data assets are defined, controlled, used and communicated for the benefit of the University. Membership represents a cross section of the University community.
i. Eligible Data Breach – means:
    i. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information that an organisation holds;
    ii. it is likely to result in serious harm to one or more individuals; and
    iii. the organisation has not been able to prevent the likely risk of serious harm with remedial action.
j. Information and Communications Technology (ICT) - includes:
    i. computers and peripherals (e.g. printers);
    ii. communications infrastructure;
    iii. computing facilities and utilities;
    iv. information storage media; and
    v. systems and software.
k. Information Security - encompasses:
    i. ICT security policies;
    ii. organisation of information security;
    iii. ICT asset management;
    iv. information security compliance obligations;
    v. information security components of human resources management;
    vi. ICT communications and operations management;
    vii. Information security components of business continuity management;
    viii. ICT services access control;

ix. ICT security incident management;
x. ICT systems acquisition, development and maintenance; and
xi. ICT asset physical and environmental security.

l. IT Security Team – comprised of specialised Division of Information Technology resources and responsible for the confidentiality, integrity and availability of the University's information assets.

m. Loss – means the accidental or inadvertent loss of personal information held by an organisation, in circumstances where it is likely to result in unauthorised access or disclosure.

n. Notifiable Data Breach – a personal data breach that is determined as a real risk of serious harm to the affected individual/s. A notifiable data breach requires at a minimum, formal notification to the OAIC and affected individuals.

o. Notifiable Data Breaches scheme – requires regulated entities to notify impacted individuals and the Office of the Australian Information Commissioner about eligible data breaches.

p. Other Incident Management Process Owners – staff who have the responsibility to oversee the process relating to other existing organisational incident management processes in different areas of the University (such as student residences, campus security).

q. Personal Information – means electronic and physical copies of personal information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Examples include:
   i. email account or application data;
   ii. data stored on physical devices such as phone, laptop, iPad, USB storage, building; and
   iii. paper based copies of information or data.

r. Preliminary Data Breach Assessment – an initial assessment completed to determine quickly if there is a high level of risk of serious harm to affected individuals given the nature and scope of the personal data breach.
   Serious Harm – means serious harm to an individual and may include:
   i. identity theft;
   ii. financial loss;
   iii. threat to physical safety;
   iv. threat to emotional wellbeing;
   v. loss of business or employment opportunities;
   vi. humiliation;
   vii. damage to reputation;
   viii. bullying; or
   ix. marginalisation.

t. Unauthorised Access – means personal information that an organisation holds is accessed by someone who is not permitted to have access.

u. Unauthorised Disclosure – occurs when an organisation makes personal information accessible or visible to others outside the organisation, and releases that information from its effective control in a way that is not permitted by the Privacy Act 1988.

Section 3 - Policy

(8) Nil.

Section 4 - Procedure

Responsibilities

(9) Charles Sturt University staff are responsible for:

a. reporting via the IT Service Desk as soon as possible any identified, suspected or possible unauthorised disclosure of personal information held by the University; and
b. protecting personal information held by the University against unauthorised disclosure.

(10) Charles Sturt University students are responsible for:

a. reporting via Student Central as soon as possible any identified, suspected or possible unauthorised disclosure of personal information held by the University; and
b. maintaining appropriate data protection of their personal data.

(11) IT Service Desk is responsible for:

a. registering reported incidents;
b. providing specialised advice (where possible) to the individual reporting the incident on options for preventing further damage; and
c. escalating the incident within the IT Service Management Platform to IT Security Team.

(12) Student Central is responsible for:

a. registering reported incidents;
b. providing specialised advice (where possible) to the individual reporting the incident on options for preventing further damage; and
c. escalating the incident within the IT Service Management Platform to IT Security Team.

(13) The IT Security Team is responsible for:

a. assessing assigned security breaches; and
b. reporting breaches to the Data Breach Response Team.

(14) Data Breach Response Team are responsible for:

a. actioning the data breach response process within specified time constraints;
b. maintaining adequate documentation of suspected data breaches reported and steps taken to deliver on compliance and University reporting requirements;
c. preparing and submission to the CSU Privacy Officer of Notifiable Data Breach Statement - form where applicable;
d. checking personal data breach incidents to see if it also fits the critical incident classification; and
e. notifying the Critical Incident Response Group of any suspected or identified critical incident.

(15) CSU Privacy Officer is responsible for:

a. overseeing the University's compliance to Notifiable Data Breaches scheme;
b. managing the University's Data Breach Response Plan (includes Data Breach Response Procedure);

c. chairing the Data Breach Response Team meetings;
d. approving the prepared Notifiable Data Breach Statement - form (in compliance with legislation);
e. lodging the Notifiable Data Breach Statement - form to OAIC;
f. reporting to the Vice-Chancellor on notifiable data breach compliance and OAIC notifications; and
g. approving any additional information about a University data breach that is to be provided to impacted individuals or other third parties. This could be in addition, or separate to a Notifiable Data Breach Statement - form.

(16) Executive Director, Division of Information Technology is responsible for:

a. contributing as a member of the Data Breach Response Team; and
b. supporting the availability of technical expertise to undertake data breach response and remedial actions.

(17) Data Security and Governance Committee is responsible for:

a. promoting the adoption of information management and Information and Communications Technology (ICT) security controls to ensure integrity, availability and confidentiality of personal information; and
b. providing guidance on improvements to protect personal information from unauthorised disclosure.

(18) Application, Data and Information Custodians are responsible for the personal information and data within their area of responsibility for:

a. reporting via the IT Service Desk as soon as possible any identified, suspected or possible unauthorised disclosure of personal information held by the University; and
b. actively managing and maintaining protection against unauthorised disclosure. This includes aspects such as:
    i. purpose, capture, use, movement, storage and retention;
    ii. access controls, both electronic and physical records;
    iii. staff training (including manual handling); and
    iv. monitoring for unauthorised disclosure.

(19) The Emergency Planning Committee and Critical Incident Response Group are responsible for notifying the Data Breach Response Team via email of any suspected or identified personal data breaches.

Part A - Reporting a Data Breach

(20) All University staff must report any suspected or known breaches of personal information held by the University to the IT Service Desk as soon as possible.

(21) All University students must report any suspected or known breaches of personal information held by the University to Student Central as soon as possible.

Part B - Containing a Data Breach

(22) The suspected or known breach must be promptly contained to minimise scope and impact of breach.

(23) The IT Service Desk will:

a. record the incident;
b. where possible, contain the data breach; and
c. escalate the incident to the IT Security Team.

Part C - Preliminary Data Breach Assessment

(24) The IT Security Team will complete an preliminary assessment to determine the criticality and eligibility of the incident as soon as possible.

(25) On completion of preliminary assessment:

a. if it is determined that there has been an eligible data breach, the IT Security Team must notify the Data Breach Response Team with the results including the:
    i. likelihood of causing serious harm to individuals;
    ii. number of individuals impacted; and
    iii. nature and scope of the data breach.
b. if it is determined that there has not been an eligible data breach, IT Security Team must:
    i. consider how the data breach occurred;
    ii. recommend enhanced personal information security measures;
    iii. seek endorsement of recommendations from the Data Breach Response Team; and
c. if it is unable to be determined that there has been an eligible data breach, IT Security Team must:
    i. complete a more detailed risk assessment within a 30 day period in order to determine if it is an eligible data breach; and
    ii. on completion of the detailed risk assessment, if it is determined that there
        - has been an eligible data breach, see clause 25(a); and
        - has not been an eligible data breach, see clause 25(b).

Part D - Reporting a Data Breach

(26) On receipt of the data breach assessment report, the Data Breach Response Team will assess and determine if it is a notifiable breach.

(27) If it is determined that it is a notifiable breach, the Data Breach Response Team will:

a. complete a list of individuals impacted;
b. consider if there is any additional information required to support the:
    i. data custodian;
    ii. impacted individuals; and
    iii. the completion of the Notifiable Data Breach Statement - form.
c. prepare a Notifiable Data Breach Statement - form;
d. submit the Notifiable Data Breach Statement - form to the CSU Privacy Officer;

Note: on receipt of the prepared Notifiable Data Breach Statement - form, the CSU Privacy Officer approves and submits the Notifiable Data Breach Statement - form along with any approved additional information to Office of the Australian Information Commissioner;

e. notify and advise impacted individuals, relevant University areas and the Vice-Chancellor's Office that:
    i. possible vulnerabilities have been identified; and
    ii. a Notifiable Data Breach Statement - form has been lodged.
f. advise remedial actions to be undertaken by relevant stakeholders;
g. monitor the delivery of remedial actions; and
h. capture and report on success or remedial actions undertaken by relevant stakeholders.

(28) If it is determined that it is not a notifiable breach, the Data Breach Response Team will:

a. consider how the data breach occurred;
b. recommend enhanced personal information security measures; and
c. communicate and provide recommendations to the data custodian and relevant stakeholders.

Section 5 - Guidelines

(29) Nil.

Status and Details

Status	Historic
Effective Date	12th February 2019
Review Date	12th February 2021
Approval Authority	Chief Financial Officer
Approval Date	23rd January 2019
Expiry Date	31st July 2022
Unit Head	Helen Jessop Chief Information and Digital Officer
Author	Colleen Middleton
Enquiries Contact	Division of Information Technology