ACT Government
Transport Canberra and City Services

Policy and Procedures

Data Breach Policy

Document ID Objective: A39794268	Title Cyber Security – Data Breach Policy	
REVISION 1.2	**DOCUMENT OWNER** Chief Information Officer	**DATE PREPARED** 09/05/2024
TYPE Policy and Procedures	**APPROVED BY** Agency Security Executive	**REVIEW DATE** 09/05/2025
DATE APPROVED **17/05/2024**		

Lisa Johnson
Chief Operating Officer/Agency Security Executive

Table of Contents

1. Data breach policy statement

TCCS systems handle sensitive official information and personal information about members of the community, staff and the business community. This data is likely to have high value to a cyber attacker. While TCCS endeavours to manage cyber risks to "as low as reasonably achievable", cybersecurity breaches are inevitable, and business units must be prepared to respond.

The Director-General requires all TCCS staff and contractors to be responsible for protecting and safeguarding sensitive and personal information. Should a data breach be suspected or identified, staff must respond in accordance with this policy.

This expectation is consistent with other related recording-keeping, privacy and security practices, policies, and procedures of TCCS and the TCCS Privacy Statement. For more information on how to meet these requirements refer to the TCCS Intranet and ACT Cyber Security Portal.

2. Purpose

This policy and individual system Data Breach Plans provide TCCS business units with guidance and a templated approach to managing data breaches. By following them, business units assist TCCS to Identify, Report, Assess, Notify and Recover from data breaches when they occur.

This policy is based on the guidance provided by the Office of the Australian Information Commissioner (OAIC) and informed by ACT Cyber Security Policy.

3. Definition

A data breach happens when official information is stolen, lost or accessed or disclosed without authorisation. The severity of a data breach can vary depending on the sensitivity of the information; in the case of a serious data breach, TCCS should notify affected individuals or entities if the breach is likely to cause serious harm.

4. Scope

This policy applies to official information held in both physical and electronic form including, but not limited to:

- personal information
- personal health information
- payment card information
- unique government identifiers such as Tax File Numbers
- other data such as sensitive legal, commercial, audit or cabinet information.

Even in circumstances where information was de-identified, a data breach should be handled in accordance with this policy due to the risk of re-association with an individual.

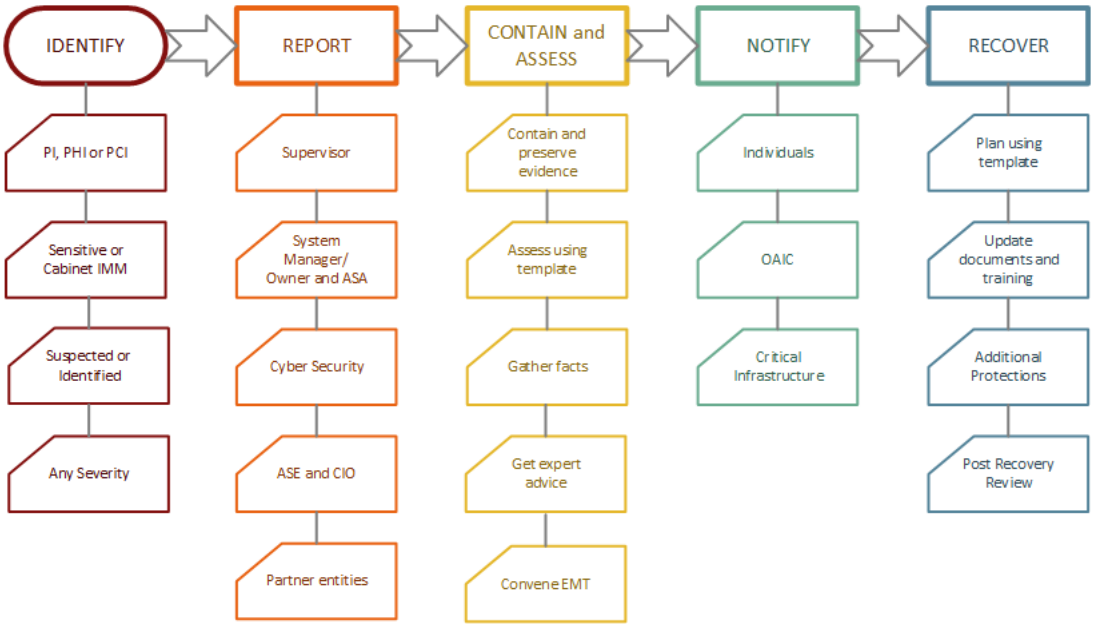
5. Prerequisites

Documenting the data sensitivity and information privacy requirements is a prerequisite to assist System Managers and System Owners in understanding the value of their information holdings and quickly assess the severity of a data breach.

ACT Government's mechanism for this is its Information Security Assessment (ISA) template. Completing this is the responsibility of the System Manager in the business unit holding the data (sometimes also the *Data Steward*), with approval of the executive System Owner (who may also be the *Data Custodian*).

The ISA should be completed early when procuring or developing an ICT solution for a business initiative but is also retroactively performed for existing systems to help manage their security posture. ISAs are approved by the System Owner and recorded in Objective as they document government decisions.

6. Data breach process



7. Identifying data breaches

All staff should remain alert to data breaches including:

- loss or theft of physical devices (such as laptops and storage devices) or physical records
- unauthorised access to data by a staff member
- inadvertent or malicious disclosure of data; and
- emailing data to unauthorised internal or external parties.

Scenarios that may indicate a data breach has occurred include but are not limited to:

- Reports from media or other sources that TCCS data are available on the dark web.
- Accidental email of reports to a customer or a vendor representative
- Downloading unrelated files from a records management system
- Exfiltration of data from a TCCS system by a malicious attacker
- Unauthorised publication of confidential data on a public website; and
- Evidence such as security alerts or audit findings that a system handling official information has been accessed by an unauthorised actor.

8. Reporting data breaches

Business units may learn of data breaches through media, contact from a member of the public, DDTS or a vendor. It is vital that TCCS staff report data breaches as soon as they are **suspected** or **identified** to enable a rapid response by security personnel and executive. Data breaches are not managed in isolation – they require a collaborative approach.

1. All staff are to report all suspected or identified data breaches **immediately** to your supervisor.
2. Supervisors are to facilitate reporting data breaches **immediately** to:
    a. the System Administrator, System Manager or executive System Owner if the breach relates to one or more ICT systems.
    b. TCCS Agency Security Advisor (ASA)

    tccs.security@act.gov.au
    mobile 0434 663 888

NOTE: All suspected or identified data breaches regardless of severity must be reported to the ASA. These contacts are monitored 24x7. TCCS will keep a register of all breach reports.

3. System Managers and Owners must report all data breaches in ICT systems, cloud services and managed services **immediately** to:
    a. TCCS Cyber Security Advisor (CSA)
    tccs.cybersecurity@act.gov.au
    b. ACT Cyber Security Centre (CSC)
    servicedesk_o365@act.gov.au
    ddtsictsecurity@act.gov.au

    NOTE: If the data breach is ICT-related, such as a breach or spill of data from a business system or incorrectly addressed email, it is also considered a cyber security incident. The CSA and CSC may recommend actions to contain or reduce immediate risks of harm to affected individual(s), the directorate and other stakeholders, and will report further in accordance with ACT Government obligations under the *Cyber Security Incident Response Plan*.
4. System Owners must make the Agency Security Executive (ASE) and Chief Information Officer (CIO) completely aware of all information in relation to the data breach:
    a. TCCS Agency Security Executive (ASE)
    tccs.chiefoperatingofficeroffice@act.gov.au
    b. TCCS Chief Information Officer (CIO)
    tccs.chiefinformationofficer@act.gov.au
    mobile 0419 408 297
5. ASE and/or CIO reports the data breach as needed to:
    a. Executive Group Managers
    b. Deputy Directors-General, and
    c. Director-General
    d. Legal and Procurement Branch tccs.legal@act.gov.au
    e. Communications and Engagement Branch tccs.communications@act.gov.au

    All staff or public messaging is to be coordinated by Communications and Engagement Branch. Do not engage with media enquiries unless instructed.
6. Director-General reports data breaches to the Head of Service and Ministers as needed.
7. System Owners must notify partner entities when the data breach involves them. Partner entities include organisations such as Australian Government, states and territories, statutory agencies such as WorkSafe ACT, Capital Metro, academic institutions, trade unions, industry and service providers, etc. TCCS is unqualified to make decisions about a data breach on their behalf.

Data breach in external organisations

TCCS is still responsible for the data breach process when a breach of TCCS data occurs in external service providers such as cloud services, system integrators or partner entities with whom TCCS has an MOU.

These organisations should in parallel follow their own data breach process appropriate to their legislated, regulatory or internal policy requirements, and support TCCS enquiries, assessment and actions in accordance with their legal agreement.

9. Assessing data breaches

System Owners must assess each data breach on a case-by-case basis to effectively manage risk and the sensitivities of the legislation each business unit must respond to. An apparently limited breach that affects only one or a few individuals could still result in risk of serious harm. Conversely, what appears to

be a widespread breach of data affecting hundreds or even thousands of individuals may not necessarily result in risk of serious harm.

System Owners must assess any suspected data breach related to their information assets to determine its likely impacts and if it is eligible for reporting to the Office of the Australian Information Commissioner (OAIC). Typically this would involve forming a team with the required expertise to:

1. Contain the breach and preserve evidence, e.g. stop the unauthorised practice, revoke or change access privileges, recover the records, or shut down the breached system.
    a. CIO branch and DDTS Security can provide technical assistance on request.
    b. ASA can provide policy advice and coordination.
2. Perform the assessment using the Data Breach Assessment template:
    https://objective.act.gov.au/documents/A40159193
3. Gather the facts:
    a. Confirm with ASA, CSA and DDTS Security as needed that suspected data breaches are actual, based on available evidence.
    b. Check within your administrative unit's subject matter experts and management for clear advice about what information was being handled by business operations.
    c. Check with system administrators, database administrators or your vendor about what information was being handled in ICT systems or cloud services, and what protective measures may have been in place.
4. Get expert advice:
    a. Legal and Procurement branch can provide legal advice and will escalate to ACT Government Solicitors as required.
5. When assessment indicates a serious data breach, the ASE, ASA or any authorised executive may convene an Emergency Management Team (EMT) to develop an Incident Action Plan. See the TCCS Emergency Management Plan for further information.

    When assessment indicates a minor data breach (such as information sent in error to another part of ACT Government where no harm to affected individuals is likely), management of actions may be conducted within the business unit provided reporting and assessment are completed.
6. Record the assessment and subsequent decisions and actions in Objective.

A Data Breach Assessment template has been developed to assist with the assessment process. Note that it may be necessary to review the assessment throughout the data preach response as information comes to light or other circumstances change.

Data breach severity

Under the Notifiable Data Breach (NDB) scheme an organisation or agency must notify affected individuals and the OAIC about an eligible data breach.

A serious data breach (eligible for notification of the OAIC) occurs when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds
- this is likely to result in serious harm to one or more individuals, and
- the administrative unit could not prevent the risk of serious harm with remedial action.

Examples of serious harm to affected individuals can include:

- financial loss or fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family or domestic violence or physical violence, or
- bullying, harassment, or intimidation.

Other factors to consider in assessment include:

- the type and sensitivity of the personal information subject of the breach

- the context of the affected persons – for example, are they working in a sensitive position, vulnerable due to domestic violence, or of an ethnicity that is vulnerable in their home country
- whether the personal information is also marked using an Information Management Marker (IMM) or subject to classification i.e. Cabinet, Protected, Secret
- the person(s) who obtained the information or could obtain the information
- the potential impact on the reputation of TCCS, ACT Government or its Ministers, or
- if electronic information was involved, were protective measures such as encryption used, and is there a likelihood that they could be circumvented.

10. Notification of data breaches

ACT Government is not currently an Australian Privacy Principles (APP) Entity under the *Privacy Act 1988* (Cth) and is governed by the *Information Privacy Act 2014* (ACT) and *Health Records (Privacy and Access) Act 1997* (ACT), which have no mandatory data breach notification requirements.

However it is the position of ACT Government to demonstrate transparency and protect the public interest, and TCCS like other directorates is committed to notification of data breaches.

1. With the approval of the Director-General, System Owners must notify any individuals whose personal information is involved in a data breach of their ICT systems, where the breach is likely to result in serious harm including (but not limited to) physical, psychological, emotional, reputational or financial impacts[1].

   For breaches of other data such as sensitive legal, commercial, audit or cabinet information, System Owners must notify affected individuals and entities.
2. With the approval of the Director General, System Owners should provide guidance to affected individuals about the steps they should take in response to the data breach, such as:
   a. Identity protection measures
   b. Advice regarding financial institutions, etc
   c. Contact information for the ACT Human Rights Commissioner (if personal health information was breached):

      ACT Human Rights Commission
      GPO Box 158
      Canberra ACT 2601
      human.rights@act.gov.au
3. With the approval of the Director-General, Legal and Procurement Branch on behalf the System Owners should notify the Office of the Australian Information Commissioner using the Notifiable Data Breach Statement form. Statements must include:
   a. the Data Custodian or System Owner of the ICT system and contact details
   b. a description of the data breach
   c. the type of information concerned, and
   d. the guidance provided to affected individuals in response to the data breach.

   NOTE: The Australian Information Commissioner is empowered to request information from System Owners and Data Custodians if there is a reasonable belief that a government system (including cloud services) is involved in a data breach.
4. If the data breach also constitutes a cyber security incident impacting a critical infrastructure asset, follow the Mandatory Cyber Incident Reporting procedure required under the *Security of Critical Infrastructure Act 2018*.

[1] In its decision to notify affected individuals, TCCS must not contravene the ACT public service principle of Procedural Fairness (p9): "[ACTPS actions] must be based on the evidence available and anyone who is adversely affected by the decision must be given the opportunity to provide their views and contribute their voice to the debate or discussion before matters are finalised."

Timeframes for action

Notification of a data breach must be performed in timeframes indicated by its severity:

- Serious data breach: Action within 3 days:
  - All reporting, internal and external
  - Contain the incident causes e.g. system shutdown
  - Urgent contact of affected individuals if required
  - Develop an Incident Action Plan
- Minor data breach: Action within the statutory 30 days
- Critical cyber incidents related to critical infrastructure: 12 hours (72 hours for other severities)

11. Recovery

In general, for minor data breaches, the System Owner in consultation with their administrative unit will be responsible for considering what actions are required to prevent or minimise the risk of a similar breach from occurring in the future, reviewing their systems or putting in place appropriate measures to prevent failures in data handling and data retention, and respond quickly to future breaches.

In the event of a serious data breach, the Emergency Management Team will review the breach response in detail, coordinate the implementation of immediate remediations and ensure all mitigation strategies are in place.

Regardless of approach, data breach assessments, Incident Management Plans and post-breach reviews must be documented and recorded in Objective.

12. Payment of ransom demands

Some data breaches involve cybercriminals taking (exfiltrating) sensitive data and demanding payment to prevent further disclosure. ACT Government does not condone the payment of a ransom to cybercriminals. Payment does not offer a guarantee that data will be removed by the attacker and is likely to invite further attacks from cybercriminals seeing a soft target.

1. The ACT Government position is to not pay ransoms (ACT Cyber Security Policy, Section 19.3)
2. Report ransom demands as part of data breach reporting, i.e. to the System Owner or Data Custodian, who reports the breach to security officials and to the Director-General via the ASE.
3. System Owners and Data Custodians must not communicate with purported cybercriminals responsible for ransomware. If circumstances justify contact, communications must be brokered between the Director-General, Head of Service, DDTS Security and law enforcement agencies.
4. For TCCS cloud applications, platforms and managed services, DDTS Security will advise on ACSC incident reporting protocol, as this may need to be performed by the service provider.

13. Responsibilities and timeframes

Table 1 – RACI – responsibilities, accountabilities, informed and consulted, with timeframes

Activity	All staff	System Owner	ASA	ASE	Director-General	Legal & Procurement	CSA	DDTS Security	OAIC	Timeframe
Perform an ISA		R			A		C	I		Prerequisite
Report a data breach	R	A	C	I	A		C	C		Immediately

Activity	All staff	System Owner	ASA	ASE	Director-General	Legal & Procurement	CSA	DDTS Security	OAIC	Timeframe
Report breach to EGM/DDG/DG		R	I	C	A					3 days
Assess a data breach		R	C	I	A	C	C	C		3 days
Notify affected individuals		R		I	A	C	I	I	I	3 days
Notify the OAIC		C		C	A	R	I	I	I	30 days
Review a serious data breach		R	R	C	A	C	C	C		30 days
Review a minor data breach		R								60 days

14. Alignment with legislation

Information Privacy Act 2014 (ACT): The governing binding law and principles that set out how ACT Government must handle the personal and sensitive personal information it collects and holds, stores and secures, uses and discloses, corrects and accesses.

Health Records (Privacy and Access) Act 1997 (ACT): Defines personal health information, its handling, and permits an individual to make a complaint to the ACT Human Rights Commissioner if, 'the act or omission contravenes the privacy principles in relation to a consumer'.

Territory Records Act 2002 (ACT): Covers, but is not limited to, 'the creation, keeping, protection, preservation, storage and disposal of, and access to, records of the agency'. Although the Act only applies to records its governing principles can be applied to all ACT Government information and data. If there is doubt as to whether ACT Government information or data meet the definition of a record, the Territory Records Office recommends the *Standard for Records, Information and Data* be applied.

Security of Critical Infrastructure Act (Cth): Covers the reporting of cyber security incidents, including data breaches that occur for cyber or ICT reasons, in critical infrastructure assets. TCCS falls under the SOCI Act as a provider of public transportation.

15. Supporting documents

DDTS Information Security Assessment: ICT Security has developed the Information Security Assessment (ISA) template to assist directorates with understanding, through self-assessment, the recordkeeping, information security and privacy requirements of new initiatives with an ICT component.

TCCS Information Security Guidelines: These Guidelines support administrative units to define the data requiring protection so appropriate protective measures can be applied such as metadata and report labelling (like Protective Markings in Outlook email); data masking and data encryption.

TCCS Emergency Management Plan: To ensure the Directorate can effectively respond to and recover from a sustained all-hazard event it is imperative that the Directorate has plans in place and operational procedures to guide our activities. The Emergency Management Plan has been prepared by the Directorate Executive Team to manage this create the framework for a coordinated and rapid response from the Directorate to a critical incident impacting the Territory.

ACT Cyber Security Policy: DDTS Security publishes the Cyber Security Framework that governs the security of electronically handled official information of the ACT Government. The keystone of this framework is the Cyber Security Policy, which derives its authority from the ACT Government Protective Security Policy Framework (PSPF) and supplements it with policies to support Information Security.

ACT Cyber Security Incident Response Plan: The Cyber Security Incident Response Plan (CSIRP) defines the Territory's approach to detecting and responding to ICT security incidents. The CSIRP ensures when

an ICT security event or incident occurs, DDTS is ready to identify and record security events and incidents; analyse the threat, nature and scope of the incident; advise leadership and other stakeholders appropriately; escalate to a Data Breach Plan or Emergency Response Plan as needed; contain spreading or ongoing damage; recover affected systems; and identify actors and preserve evidence.

16. Other resources

Business Continuity Management within TCCS

TCCS Information and Records Management

TCCS Information Privacy Policy

ACT Cyber Security Sub Plan

17. Glossary

Term	Definition
Agency Security Advisor	Responsible for day-to-day management of TCCS protective security measures. Develops, implements, and monitors protective security procedures and systems.
Agency Security Executive	The delegate of the Director-General or agency head with authority to approve protective and cyber security programs for TCCS.
Cyber Security Advisor	Responsible for day-to-day management of the cyber security measures within TCCS. Develops, implements, and monitors cyber security policies, procedures and systems. Analyses TCCS security environment and posture, and plans measures to manage cyber security risks.
System Owner	Person at executive or senior executive level within TCCS who has the authority to make binding financial and operational decisions regarding an ICT system, and to accept residual risk on behalf of the Director-General.
System Manager	An ACTPS officer who is responsible for the integrity and operation of the ICT system; negotiates service levels; authorises access levels and access for new users including staff, contractors, vendors and volunteers; reviews audit logs.
Data Custodian[2]	Data custodians are accountable for governing and overseeing the management of one or more datasets. They may be assigned both internal datasets and datasets that have been externally acquired.
Data Steward[3]	Data stewards are responsible for the day-to-day management and protection of one or more datasets, reporting to the data custodian. While they facilitate data access, sharing and use, authorisation must be provided by the data custodian.
Partner Entities	Partner entities can include organisations such as other directorates, statutory authorities, states and territories, Australian Government agencies, education institutions, trade unions, industry and service providers, etc depending on context, purpose and data handled by the system, and should be determined case by case.

18. More information

Questions or comments about this policy should be directed to the TCCS Cyber Security Advisor tccs.cybersecurity@act.gov.au

[2] There is considerable overlap between Data Custodians and System Owners, roles which may belong to the same executive position. However some System Owners own systems with multiple datasets and Data Custodians; while some Data Custodians have custody of datasets held in multiple systems or not in ICT systems.

[3] There is also overlap between Data Stewards and System Managers, noting that System Administrators, Database Administrators and other data workers answering to a System Manager may also be Data Stewards.