EXPOSURE DRAFT

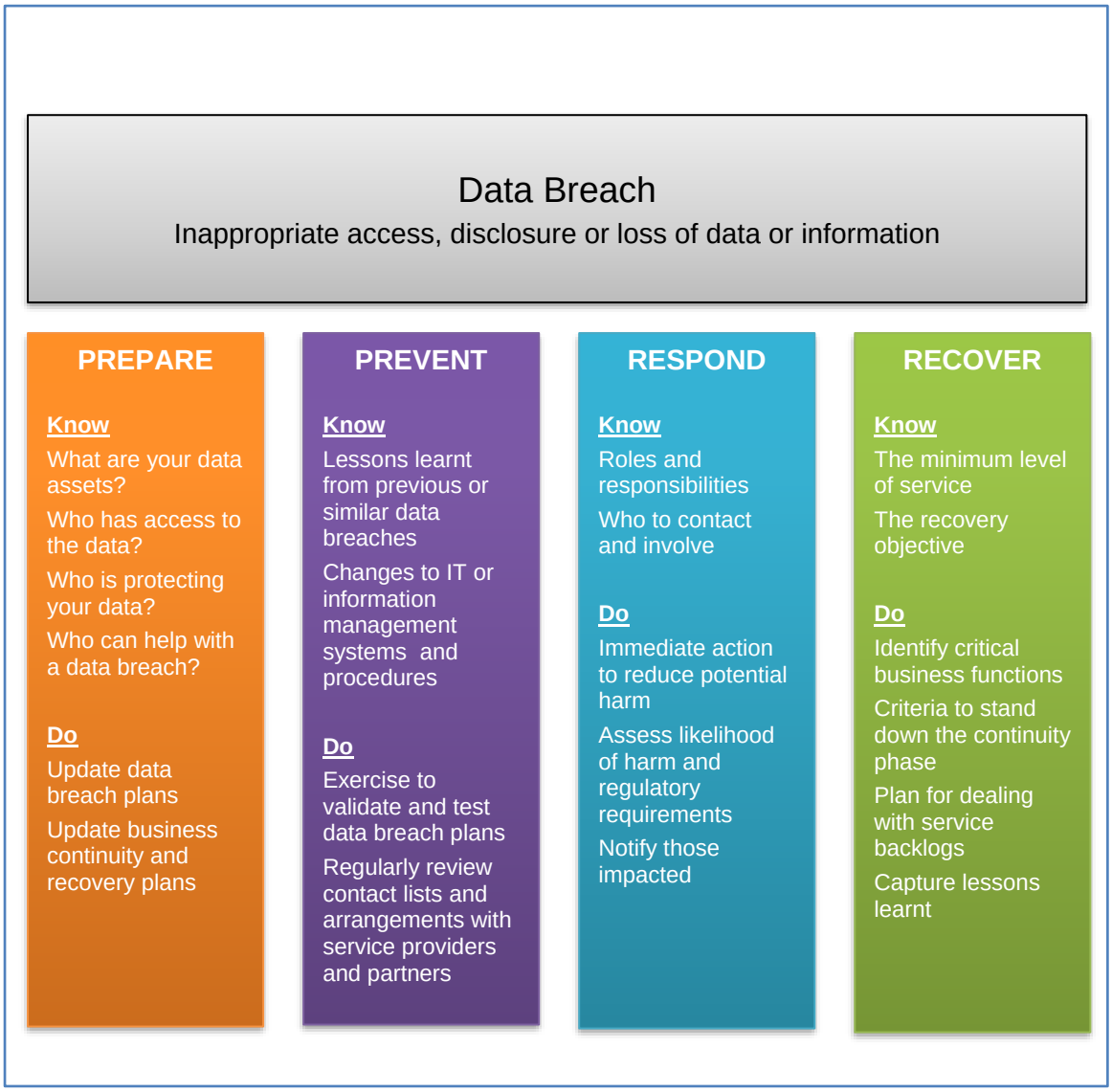
Data Breaches:

Prepare-Prevent-Respond-Recover

5 February 2019

Tasmanian Government
Office of eGovernment, Department of Premier and Cabinet

Overview


Data Breach
Inappropriate access, disclosure or loss of data or information
PREPARE
Know
What are your data assets?
Who has access to the data?
Who is protecting your data?
Who can help with a data breach?
Do
Update data breach plans
Update business continuity and recovery plans
PREVENT
Know
Lessons learnt from previous or similar data breaches
Changes to IT or information management systems and procedures
Do
Exercise to validate and test data breach plans
Regularly review contact lists and arrangements with service providers and partners
RESPOND
Know
Roles and responsibilities
Who to contact and involve
Do
Immediate action to reduce potential harm
Assess likelihood of harm and regulatory requirements
Notify those impacted
RECOVER
Know
The minimum level of service
The recovery objective
Do
Identify critical business functions
Criteria to stand down the continuity phase
Plan for dealing with service backlogs
Capture lessons learnt

1. Cybersecurity incident management

This guidance has been prepared to capture the learning from recent data breach related incidents.

It is part of a suite of cybersecurity incident management arrangements and plans that are being developed. See Figure 1.

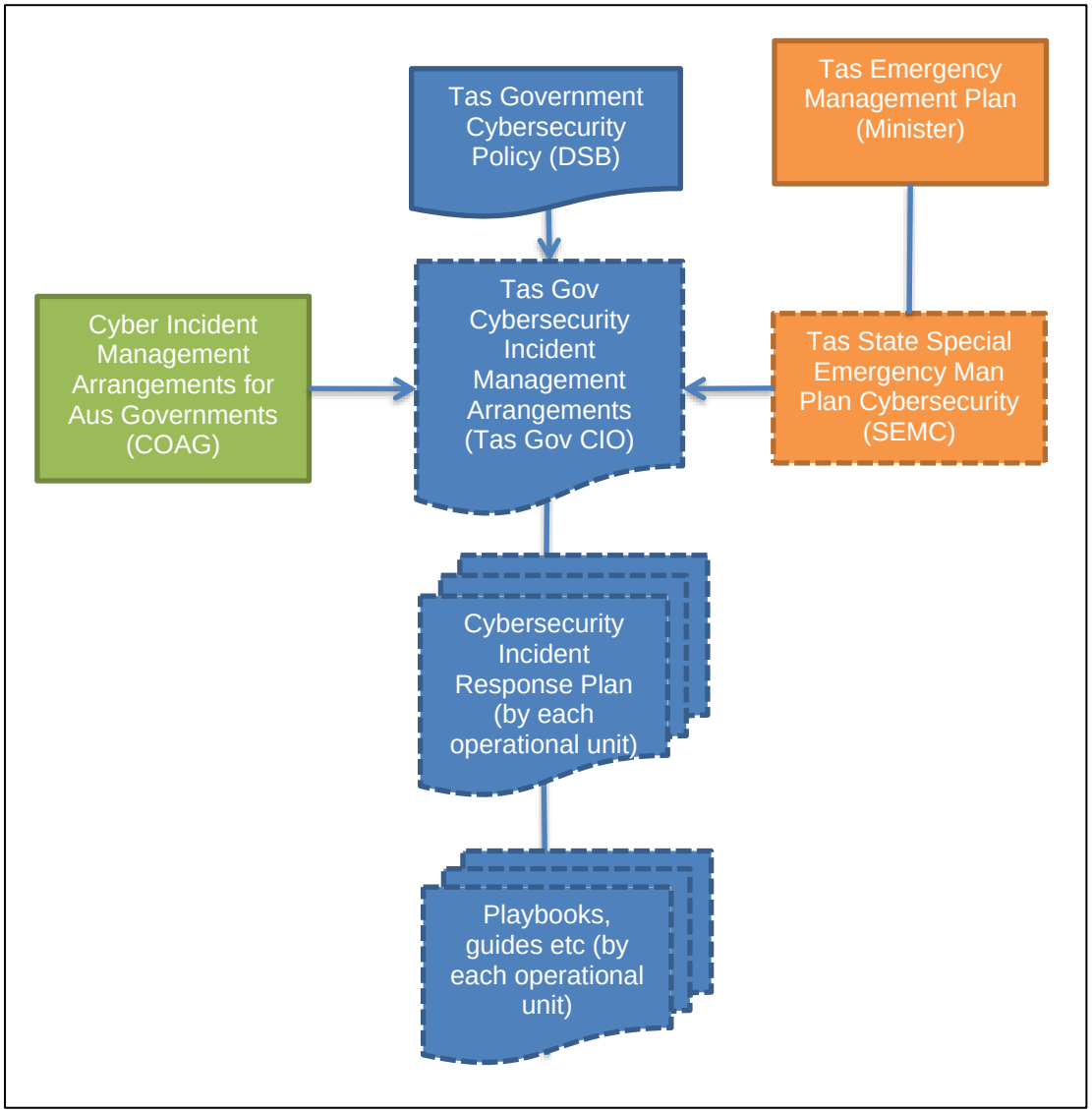


Figure 1 Key cybersecurity incident response documents. The document owner is in parentheses. Planned documents have dashed outlines.

Following is a more detailed description of the cybersecurity incident management elements:

- The Cyber Incident Management Arrangements for Australian Governments (CIMA) sets out the principles, roles and responsibilities of Australian governments to guide response to national cybersecurity incidents. This was agreed by the Council of Australian Governments (COAG) in December 2018.

- The Tasmanian Government Cybersecurity Policy outlines the principles, roles and responsibilities of agency heads and the Tasmanian Government CIO and for identifying, managing cybersecurity risks. This was agreed by the Tasmanian Government Digital Services Board (DSB) in December 2018.
- The Tasmanian Government Cybersecurity Incident Management Arrangements is intended for agency executives who are responsible for whole of government incident decision making and mobilising incident response resources. It is proposed to include principles, roles, responsibilities and high level decision making processes.
- Tasmanian Government Cybersecurity Incident Response plans are prepared by and specific to each operational unit eg an agency. Response plans are aimed at describing how incident management processes work for those involved with incident response, recovery and restoring business as usual conditions.
- Playbooks, guides etc: these are prepared by and are specific to each operational unit to capture procedures for commonly occurring cybersecurity events/incidents. These are prepared on an as need basis.
- The Tasmanian Emergency Management Plan Issue 8 (October 2015) describes the governance and coordination arrangements, roles and responsibilities for emergency management in Tasmania.
- The Tasmanian State Special Emergency Management Plan Cybersecurity is proposed to provide advice and support to government agencies that have responsibilities related to managing a cybersecurity incident that is a state or national crisis.

2. Purpose

This guidance is intended to assist Tasmanian Government organisations with planning, preparedness, response and recovery from a breach of data or information. It can form the basis of a more specific data breach plan that is tailored to the needs of your organisation.

This document should not be used as a substitute for legal advice which agencies should seek from the Solicitor-General.

This document is maintained by the Office of eGovernment, Department of Premier and Cabinet.

What is data breach and how does it occur?

A data breach occurs when official information that is not already publicly available, is lost or subjected to unauthorised access, use, modification, disclosure or misuse.

Data breaches may occur in a number of ways, including accidental loss, internal errors or deliberate actions of trusted employees, theft of physical assets or the theft or misuse of electronic information (e.g. a cyber-intrusion).

3. Scope

This guidance is intended for use by Tasmanian Government agencies.

4. Prepare

Preparedness is taking steps before an incident to support an effective response and recovery.

Personal Information

The definition of Personal Information may vary depending on the circumstances or regulations that apply. Personal information is generally information or an opinion, whether true or not, relating to an individual, or the affairs of an individual, whose identify is apparent, or can reasonably be ascertained. An individual is this context is a living human being.

Personal information can include combinations of name, address, phone number, IP address, email address, date of birth, financial or health details, ethnicity, gender, religion and other details. It may be collected in paper form, verbally or through electronic means.

How is personal information regulated?

The *Personal Information Protection Act 2004* (Tas) governs the collection, use and disclosure of personal information by Tasmanian public sector bodies. A set of Personal Information Protection Principles in the Act includes, amongst others, that a personal information custodian must take reasonable steps to protect its personal information from misuse, loss, unauthorised access, modification or disclosure. It does not include data breach reporting requirements.

The role of the Ombudsman under the *Ombudsman Act 1978* (Tas) is to enquire and investigate complaints about the administrative actions of Tasmanian Government Departments, Local Government Councils, and range of public authorities. This includes investigating complaints under the *Personal Information Protection Act 2004*.

The Commonwealth *Privacy Act 1988 (Cth)* (the Privacy Act) requires all organisations, including Tasmanian Government agencies that hold tax file number (TFN) information, to comply with the Commonwealth's Notifiable Data Breaches (NDB) scheme, but only in respect to TFN information. The scheme includes an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm.

Agencies may hold personal information jointly with another organisation, for example contracted service providers. In these cases an eligible data breach of one entity will also be considered a data breach of other entities that hold the affected information and both will have obligations under the NDB scheme.

The *European Union General Data Protection Regulation* (GDPR) may apply to Tasmanian Government organisations if they:

- offer goods or services to data subjects in the EU (regardless of whether payment is required); or
- monitor the behaviour of data subjects in the EU, in so far as the behaviour takes place within the EU, or
- have a physical or legal establishment in the EU, regardless of whether the processing takes place in the EU.

The GDPR requires data controllers to notify Data Protection Authorities in the EU and the personal data subjects within 72 hours of becoming aware of a breach if it is likely to impact the rights and freedoms of individuals.
In addition to the general regulations described above, your organisation may have regulatory bodies specific to your sector that have reporting requirements, or that you should consider.

Planning activities

Your organisational data breach response plans, should provide guidance and procedures for assigning roles and responsibilities, reporting, recording, and investigating security incidents. To prepare a plan consider the following:

1. Identify personal and other sensitive information assets and rank these based on value and criticality to the organisation.
2. Research other data breaches that have occurred that could inform the planning process. Also access information published by regulatory bodies (see Section 8).
3. Identify who has access to the data and who is managing the data. Does it involve contracted service providers? If yes, review cybersecurity in contracts and establish clear arrangements about roles and responsibilities during a data breach.
4. Conduct an information data breach risk assessment to identify threats and vulnerabilities. Contact the Office of eGovernment, DPAC for more information on risk assessments.
5. Develop a treatment plan to treat unacceptable risks, including arrangements with service providers or other parties with responsibilities
6. Identify those in your organisation to be notified of a data breach. This should also include escalation criteria and those to be notified if the impact increases.
7. Plan the communications required to notify stakeholders if a breach of personal information occurs.
8. Update business continuity plans to accommodate potential disruption from a personal data beach. For example what will happen when a business system is taken offline to respond and recover from a breach?

5. Prevent

This is taking a proactive approach to reducing the likelihood and impact of a personal information data breach.

Prevention activities

1. Implement lessons learnt from previous breaches or near misses.
2. Implement risk treatment plans from previous risk assessments.
3. Manage changes to IT systems or information processing procedures to minimise data breach risks.
4. Develop/update incident management plans setting out roles and responsibilities for managing a data breach. This should include processes for assigning additional staff to an incident response team and back filling roles that have been vacated for the incident team.
5. Developing capacity and capabilities to respond to a data breach – processes, systems and assets required to respond and recover form a data breach.
6. Review arrangements with service providers to ensure processes for managing data breach incidents are included.
7. Ensure 24x7x365 processes are in place to receive notification of a potential incident.
8. Regularly review contact lists with key stakeholders for emergency situations.
9. Conduct exercises to test and validate incident response and business continuity plans. This may be a desktop exercise to validate plans and identify gaps.

6. Respond

Actions to minimise the impacts of an actual or possible data breach.

Immediate remedial action

Can anything be done immediately to reduce adverse impacts eg taking a compromised website offline?

Triage

Determine initial response actions and priorities in consultation with key stakeholders, for example service providers, other agencies, TMD or the Office of eGovernment.

As part of the initial assessment of a serious data breach incident, inform the organisation executive immediately Law enforcement, internal investigation units, and other regulatory bodies should also be notified as required by relevant policy, plans or legislation.

If a data breach is likely to have occurred, assess the risks associated with the data breach and whether affected parties should be notified.

The following factors should be considered in the risk assessment:

The type of information involved	Does the type of compromised information create a risk of harm? • Is it personal, commercial, medical, legal, security classified or other sensitive information? • Does the aggregate of information create greater risk of harm? Who is affected by the incident? Are those affected at particular risk? Has tax file number (TFN) information been disclosed? (This may require action according to the *Privacy Act 1988.*)
The context of the information and the incident	What is the context of the information involved? What parties have gained unauthorised access to the affected information? Have there been other incidents that could have a cumulative effect? How could the information be used? Does it impact individuals in the EU? (This may require actions according to the GDPR.)
The cause and extent of the incident	Is there a risk of ongoing incidents or further exposure of the information? Is there evidence of theft? What was the source of the incident? eg Was it accidental or malicious? Is the information adequately encrypted, anonymised or otherwise not easily accessible? Has the information been recovered? What steps have already been taken to mitigate the harm? Is this a systemic problem or an isolated incident? How many individuals or organisations are affected by the incident?

The risk of harm to those affected	Who is the recipient of the information? What harm to individuals or organisations could result from the breach? Examples of harm include: • identity theft • financial loss • threat to physical safety or emotional wellbeing • loss of business or employment opportunities • damage to reputation or relationships • bullying or marginalisation • insider trading or unfair commercial advantage • identifying racial or ethnic origin, political opinions, sexual orientation, religious or philosophical beliefs • revealing genetic or biometric data for the purpose of uniquely identifying a natural person.
Risk to the data custodian	What are the risks to the data custodian? What is the likely reputation damage? Is the custodian likely to be targeted again?
The risk of other harms	Are there any other possible harms that could occur, including to the organisation that suffered the incident?

Notifying

In general, if a data breach creates a real risk of serious harm to an individual or organisation, notify the affected parties.

Prompt notification to those affected can help them mitigate the damage by taking steps to protect themselves. You should:

- take into account the ability of the individual or organisation to take specific steps to mitigate any such harm
- consider legal, regulatory or contractual obligations to notify (this may include advice from the Solicitor General)
- consider whether it is appropriate to inform third parties such as the police, or other regulators or professional bodies about the data breach incident.

It may not always be appropriate to notify in every case. Providing notification about low risk breaches can cause undue anxiety and de-sensitise individuals to notice. Each incident needs to be assessed on a case-by-case basis, to determine whether notification is required.

Sometimes the urgency or seriousness of the incident dictates that notification should happen immediately, before having all the relevant facts. Notification of a potential incident can be made if a breach is likely but cannot be confirmed.

Notifying parties affected by a data breach can support open and transparent government, assist in rebuilding public trust in government institutions and enable individuals and organisations to exercise control over their information, privacy and security.

The decision on how to notify should be made on a case-by-case basis, see Section 8 Data Breach notification process overview for a summary.
The following should be considered as part of a decision to notify:

When to notify	Those affected should be notified as soon as possible. If criminal activity is suspected, check with the law enforcement authorities before notifying so as not to compromise any ongoing investigations.
How to notify	Notify affected parties directly – by phone, letter, email or in person. Indirect notification (eg on a website) is appropriate where direct notification is impossible, unfeasible, or may cause further harm.
Who should notify	Typically, the organisation that has a direct relationship with the customer, client or employee should notify those affected. This includes where a breach may have involved handling of information by a third party service provider or contractor.
Who should be notified	Generally, the individual(s) or organisation affected by the incident should be notified. In some cases it may be appropriate to notify an individual's guardian or authorised representative on their behalf. If criminal activity is suspected contact Tasmanian Police. If the breach contains TFN information then the Office of the Australian Information Commissioner may need to be notified under the Notifiable Data Breaches Scheme, and specific requirements apply for notifying individuals affected. If the breach impacts individuals in the EU notification to the Data Protection Authority(s) may be required.
What should be included in the notification	The information in the notification should help those affected to reduce or prevent the harm that could be caused by the incident. This may include: • a description of the incident • the type of information disclosed • what has been done to respond to the incident and reduce harm • assistance available to those affected and steps they can take to reduce harm • sources of information that could assist those affected • contact information for the organisation where those affected can get more information or address concerns • whether the incident has been notified to a regulator or other external party • how individuals can lodge a complaint. The wording of the notification may have legal implications, and secrecy obligations could also apply: you should consider seeking legal advice. If the notification is required under the Australian Data Breaches Notification scheme, specific requirements apply. Notification under the GDPR has specific requirements.

Who else should be notified	Provide details of the data breach and response to the Head of agency or chief executive officer and the relevant Minister. Notifying authorities or regulators should not be a substitute for notifying those affected. In some circumstances it is appropriate or necessary to notify the following parties: • Office of the State Archivist • The Integrity Commission Tasmania • Tasmanian Ombudsman • Tasmanian Government Chief Information Security Officer • Service providers due to contractual obligations • Credit card companies or financial institutions • Regulatory bodies may have notification requirements • Australian Government Agencies that have a direct relationship with the information exposed (eg Medicare in the case of Medicare numbers)

7. Recover

Recovery is restoring the organisation to a long term sustainable position. Some parts of recovery can be planned in advance while other aspects are incident dependent.

Recovery can be in two overlapping phases:

- Continuity – to ensure the delivery of a minimum acceptable level of service continues
- Restoration – returning to a long term sustainable position

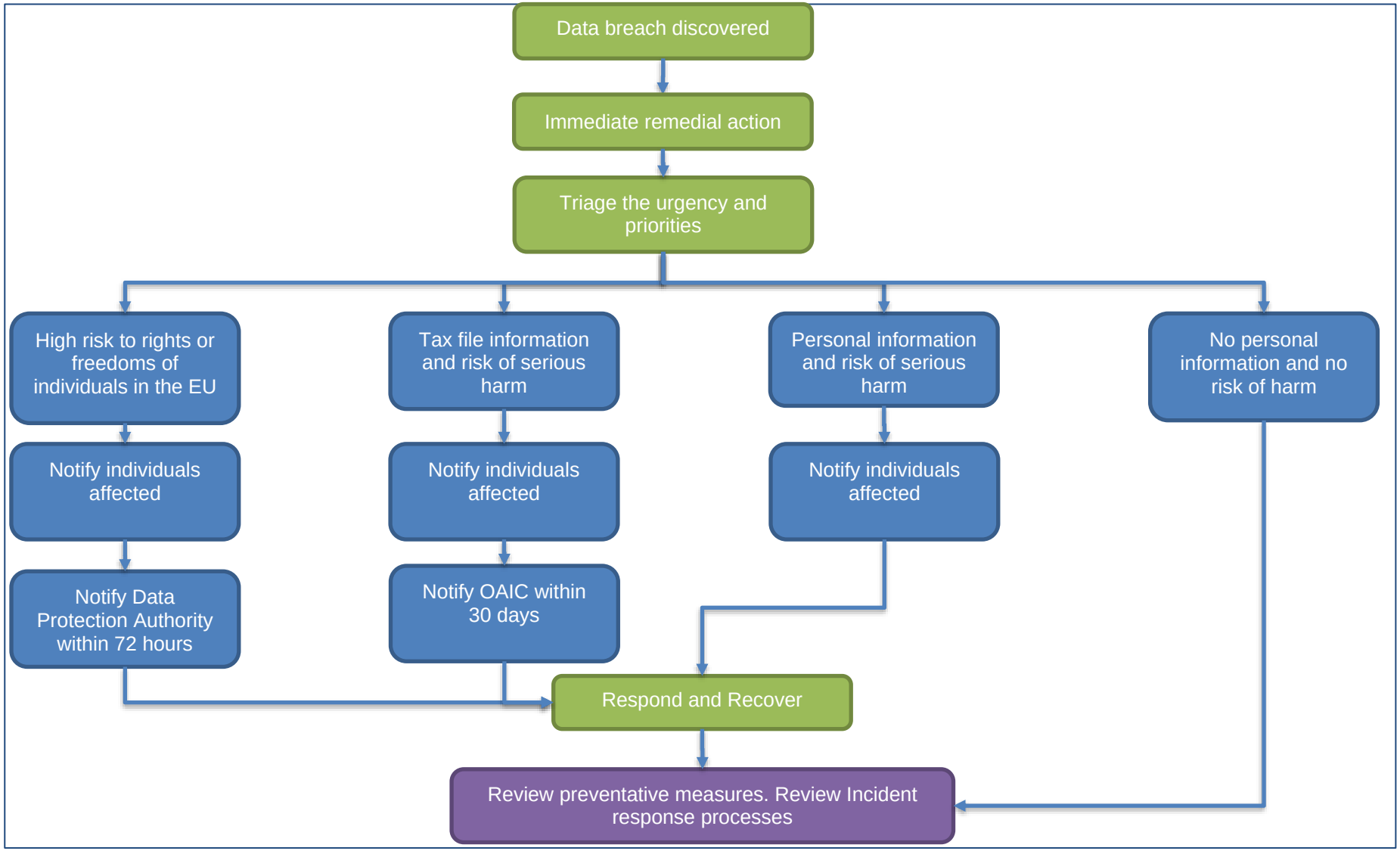
Factors to be considered for the maintaining continuity:

1. Criteria for activating a continuity phase
2. What are critical business functions?
3. What assets, facilities, and people will be required to continue critical functions?
4. What communications are required? eg notifying the public, business partners etc of a change in services
5. Criteria for deactivating or stand down of a continuity phase

Factors to be considered for long term recovery and restoration include:

1. What is the recovery objective? In some cases recovery to pre-incident operations may not be possible. Recovery to a sustainable position my require changes to reduce the likelihood of a similar incident.
2. What engagement with stakeholders is required?
3. What staff resources are available to form a recovery team?
4. What are the priorities for recovering and restoring compromised data?
5. What are the priorities for dealing with backlogs? eg catching up with processes that were delayed during the incident.
6. When is an appropriate time to review the incident response and recovery to capture lessons learnt?

8. Data Breach notification process overview



9. Other information sources

Below is a list of organisations that Tasmanian Government organisations may be required to notify, or consider contacting, when a data breach or potential data breach occurs.

- Tasmanian Police: https://www.police.tas.gov.au/
- Integrity Commission: https://www.integrity.tas.gov.au/
- Tasmanian Ombudsman: https://www.ombudsman.tas.gov.au/
- The Office of the Solicitor General (Tasmanian Government agencies): https://www.crownlaw.tas.gov.au/solicitorgeneral
- Financial institutions or credit card companies. They may be able to assist you in notifying individuals or reducing the impact on those affected.

Other internal or external parties

Consider if any other third parties may have been affected by the breach. For example, if information about a particular government tender process was breached, all organisations that submitted a tender, even if their information wasn't included in the breach, may need to be notified. Some parties to consider include:

- other internal business units in you organisation not already notified that may have a need to know (eg communications, human resources, senior management group)
- other government organisations that may experience some impact from the breach
- unions or other employee representatives, particularly if any employee information was compromised.

Regulatory bodies:

- Office of the State Archivist (OSA): https://www.informationstrategy.tas.gov.au/
- Office of the Australian Information Commissioner (OAIC): https://www.oaic.gov.au/
- European Union General Data Protection Regulation (GDPR), rules for protection of personal data inside and outside the EU: https://ec.europa.eu/info/law/law-topic/data-protection_en
- Australian Securities and Investment Commission (ASIC). Companies and registered corporations may have reporting requirements. https://www.asic.gov.au/
- Australian Competition and Consumer Commission (ACCC). The ACCC has a role in protecting the interests and safety of consumers and as such they have their own data breach notification requirements. Also consider if individuals affected may contact the ACCC to make a complaint regarding the data breach. https://www.accc.gov.au/
- Australian Communications and Media Authority (ACMA). ACMA has its own data breach reporting requirements if the data compromised includes Integrated Public Number Database (IPND) information. https://www.acma.gov.au/
- Other regulatory bodies. Your organisation may have regulatory bodies specific to your sector that have reporting requirements, or that you should consider notifying. The education, infrastructure, health, justice and child protection sectors in particular may have specific regulatory bodies that require notification in the case of a data breach.