Te Rua Mahara o te Kāwanatanga Archives New Zealand,
10 Mulgrave Street, Wellington
Phone +64 499 5595
Websites www.archives.govt.nz
www.dia.govt.nz

25 Hanuere 2023

Rimmer
fyi-request-21460-788bc8c6@requests.fyi.org.nz

Tēnā koe Rimmer

Te Rua Mahara o Te Kāwanatanga Archives New Zealand's Privacy Breach Incident Response Plan

Thank you for your email, received 19 December 2022, requesting the following under the Official Information Act 1982:

1. Archives New Zealand's privacy breach incident response plan or similar

I have provided the Te Tari Taiwhenua Department of Internal Affairs Privacy Incident Response Plan 2023. This is the response plan used by Te Rua Mahara o Te Kāwanatanga Archives New Zealand.

Please note that as the Department's response provides information that is identified to be of public interest, the response will be published on the Department of Internal Affairs website. All personal information, including your name and contact details, will be removed.

You have the right under section 28 of the OIA to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint can be found at https://www.ombudsman.parliament.nz/ or freephone 0800 802 602.

Ngā mihi, nā

Anahera Morehu
Chief Archivist

Privacy Incident Response Plan

1. Background

The privacy incident response plan provides the Department of Internal Affairs (Department) with the information required to respond to a privacy incident effectively and within a timely manner.

2. Definitions

Personal information is any information that identifies, or is capable of identifying, a person.

A **privacy incident** is when a privacy breach or near miss occurs. All privacy incidents should be reported so we can learn from them.

A **privacy breach** occurs when we do not comply with one of Information Privacy Principles set out in the Privacy Act 2020 (Act). Therefore, a privacy breach could be an over-collection of personal information (an infringement of principle 1); the failure to respond to an access request (an infringement of principle 6); or an inadvertent disclosure (an infringement of principle 11). Any of these breach types should be reported.

However, for the purposes of enacting this plan, the Department will refer to the broad definition set out in the Act, which says that a privacy breach may be either one of the following:

- Confidentiality breach – unauthorised loss of, access to or disclosure of personal information
- Integrity breach – unauthorised alteration or destruction of personal information
- Availability breach – inability to access information, either temporarily or permanently, e.g. where it is encrypted by ransomware.

A **near miss** is when a privacy breach could have occurred, but the incident was prevented or avoided.

3. Reporting a breach

The business area affected by the breach should notify the Privacy Team as soon as possible when a breach has occurred, and the incident should be promptly logged in Service Desk Plus .

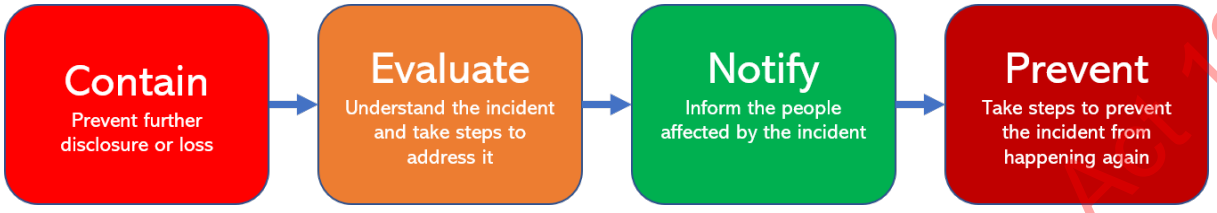
4. Responsibility for managing a privacy breach

The business area affected by a breach will manage it, with support and advice provided by the Privacy Team. However, there will be incidents that require management via a specialised team.

5. Dealing with a privacy breach

When we become aware of a privacy breach, we must respond as quickly as possible. This will help minimise any harm caused to the affected individuals and to the Department's reputation.

There are four key steps in dealing with a privacy breach:



Contain

Once a breach is discovered, we should immediately contain it. It is important to act quickly to stop or lessen further damage. This can be done by:

- Trying to get the information back
- Isolating or disabling a system that has been compromised
- Remotely wiping a device
- Stopping the practice that is causing the incident
- Cancelling or changing computer access codes
- Trying to fix any weaknesses in physical or electronic security.

Incident Management Team

Depending on the size and magnitude of the breach it might be necessary to form an Incident Management Team (IMT) at this point. The IMT will work together through the evaluation, notification and prevention steps.

Evaluate

The next step is to assess the risks of the privacy breach to help us decide how to respond, including who to inform.

Determine what information is involved

We need to promptly establish what personal information is involved.

The more sensitive the information, the higher risk of harm to the individuals affected. In New Zealand, there is no legal distinction between 'regular' personal information and 'sensitive' personal information.

However, some types of information are inherently more sensitive than others. Sensitive information is typically personal information relating to a person's**:**

- Health, genetic or ethnic background
- Finances

- Disciplinary history
- Union membership
- Criminal history
- Identity (specifically photo-ID documents such as a passport or driver licence)
- Political or religious beliefs
- Sex life or sexual orientation

Anything that might cause humiliation, loss of dignity, injury to feelings or damage to reputation of an individual could fall into the sensitive category.

A combination of personal information is usually more sensitive than a single piece of personal information. Health information, driver licence numbers, and credit card details can all cause harm on their own, but together they could be used for identity theft.

Context will matter. Personal information which might not normally be considered sensitive, such as an email address, may, in specific circumstances, be considered sensitive.

Whether the information is easy to access

If the information does not have a password or encryption, then there is a greater risk of someone misusing it.

Information which is encrypted and can be remotely wiped will have no value to a bad actor but information in hard copy or harvested unencrypted via unauthorised access might.

Identify the cause and extent of the breach

The cause of the incident must be determined and assessed as to an ongoing risk, i.e., whether it is an isolated incident or a systemic/ongoing problem.

The scale of the breach can be identified by considering:

- How many individuals can access the information
- How many individuals have lost personal information
- The risk of the information being circulated further.

Determine if anyone could be harmed

Disclosure of personal information may cause harm to the individuals to whom the information relates.

Harm is an established concept under New Zealand privacy law and it is relevant to an assessment of whether an interference with privacy has occurred. Harm in this context is broad and may fall under one of the following categories:

- Specific damage
- Loss of benefit
- Emotional harm.

Examples may include:

- Identity theft
- Financial loss
- Loss of business or employment opportunities
- Physical harm or intimidation
- Family violence
- Psychological or emotional harm
- Significant humiliation, loss of dignity or injury to feelings.

The Department must also consider impact on any employee involved, particularly if their actions resulted in the privacy incident. These can be upsetting incidents for employees and support should be offered to them.

Who holds the information

Information in the hands of individuals with unknown or malicious intentions can be of great risk to the individuals affected.

The risk will be lower if the information went to a trusted person or organisation and its return/deletion is expected.

Notify

Under the Act, if the Department has a privacy breach that that has caused or is likely to cause serious harm, it must be notified to the Privacy Commissioner and any affected individuals. However, notification is also about good customer service and being transparent. It can help individuals affected by the incident and mitigate potential reputational damage to the Department.

The Act does not define serious harm, but requires consideration of the following factors (which have already been considered during the evaluate phase):

- Nature of information – if the breach discloses sensitive information or other information that may enable fraud or ID theft it is more likely serious harm will occur
- Security measure – if the information is not protected by a security measure, such as encryption, it is more likely serious harm will occur
- Mitigations – if there are no feasible mitigations, such as retrieving lost data via backups or disabling impacted systems, it is more likely serious harm will occur
- Nature of harm – if there is the possibility of identity theft, threats to physical safety, loss of business or employment opportunities, humiliation, damage to relationships or workplace bullying it is more likely serious harm will occur
- Recipient – if the person who has obtained the personal information is known to have malicious intentions it is more likely serious harm will occur
- Other – if a large quantity of personal information is disclosed or the privacy breach has been ongoing for some time, then the risk of serious harm occurring is likely to be greater.

Assessing whether the threshold for serious harm has been reached is a judgement call that will be different in each case depending on the facts in question. The Privacy Team, in consultation with the Legal Team, will make the decision about notification on a breach-by-breach basis.

Examples of when to notify

Incident	Should we notify?
An external bad actor has harvested staff log-in details via a phishing attack. The bad actor has illegally accessed an email account and obtained the names and email addresses of customers. Those customers received an email that fraudulently claimed to be sent from the Department asking for credit card details.	In this scenario, notification is required. The attacker has used our information for the purposes of fraud, which is likely to cause serious financial harm to the relevant individuals.
SDO are despatching a passport. The passport is sent to the wrong applicant because of an addressing error. The recipient has approached another government agency using the passport as evidence of ID.	In this scenario, notification is required. The information has been used for ID theft.
TSS have identified a vulnerability in the HR Kiosk that potentially enabled staff to access the information of other staff. TSS contained and rectified the issue and confirmed that no information was viewed.	In this scenario, notification is not required. TSS have successfully mitigated any risk of disclosure and harm.
PRC have sent an email to a gambling operator. They inadvertently carbon-copied a random third party. There is no other information included apart from the email address.	In this scenario, notification is not required. While an email address may be considered personal information, it is not sensitive in nature.

Notification to the Privacy Commissioner

The Department can inform the Privacy Commissioner of any privacy incident. However, as stated above, it is compulsory to report privacy breaches that have caused serious harm or are likely to do so.

The notification must be done within **72 hours** and will be handled by the Privacy Team.

We should use the Privacy Commissioner's NotifyUs tool to help assess and report privacy breaches. We can also call 0800 803 909 and ask to speak to the Compliance Manager.

Notification to the individuals affected

If individuals could suffer serious harm because of a privacy breach, we should inform them.

Notification to the individuals affected by a breach gives them the opportunity to act to protect themselves. For instance, they may need to change their passwords, add a security question to an account or monitor their bank accounts for malicious activity.

The notification must be done as soon as **reasonably practicable**.

However, it is not always necessary to notify individuals of a breach. Sometimes, notification may do more harm than good. If the consequences from the breach are minimal or minor, of if telling individuals would cause more worry and harm than not telling them, it may be acceptable not to tell the affected individuals.

How to notify affected individuals

We should notify the individuals affected directly, such as:

- By phone
- By letter
- By email
- In person.

If we know that some individuals could be significantly upset, we should plan to do the notification with support in place.

We should only notify individuals indirectly, e.g., through our website, posted notices or the media, in the following circumstances:

- Notifying them directly could cause further harm
- We are not able to contact them directly.

What to say

Our breach notification should contain:

- Information about the incident, including when it happened
- A description of the compromised personal information
- What we are doing to control or reduce harm
- What we are doing to help individuals the breach affects
- What steps individuals can take to protect themselves – see Steps affected individuals can take
- Contact information for enquiries and complaints
- Offers of support when necessary, e.g., advice on changing passwords
- Whether we have notified the Privacy Commissioner
- Contact information for the Privacy Commissioner.

Steps affected individuals can take

As stated above, we must inform individuals what steps they should take to protect themselves. This may include a recommendation to cancel a credit card, add a security question to an account, or cancel a passport of driver licence. This may also include advice to approach any of the following:

- ID Care (www.idcare.org) – if there are concerns they have been the victim of identity fraud
- CertNZ (www.cert.govt.nz/individuals/) – if there are concerns about keeping their information safe and secure online and the risk of cyber security attacks

- Netsafe (www.netsafe.org.nz) – if there are concerns they may be the target of phishing attacks or other scams
- NZ Police (www.police.govt.nz/contact-us) – if the breach involves theft or other criminal activity.

Notifying third parties

We will need to consider any obligations of confidentiality and decide whether we should inform other agencies/organisations. This may include:

- NZ Police
- Insurers
- Professional or other regulatory bodies
- Credit card companies, financial institutions or credit reporting agencies
- Third party contractors or other parties who the breach may affect
- Internal business units
- Our Ministers
- Union or other employee representatives.

Coping with media interest

Only the Communications team should discuss privacy incidents with the media. They will:

- Coordinate the response with senior management and Privacy Team
- Act fast but ensure the message is correct before releasing it
- Appoint one spokesperson for consistency
- Consider a media conference to get the response in front of the public
- Set up a free phone enquiry line
- Continue to keep the media informed as the issue progresses
- Monitor news media reports and social media to address misinformation

Prevent

In the aftermath of the breach, we should take time to investigate the cause of the breach. This could include a:

- Security audit of both physical and technical security
- Review of policies, procedures and processes
- Review of training provided to staff and provision of additional training if required
- Review of any service delivery partners caught up in the breach.

6. Standing up an Incident Management Team

Threshold for Initiation of IMT

Incident management is used in situations with a high level of uncertainty that disrupt the core activities and/or credibility of the Department and require urgent action.

The Department has defined triggers for when our incident management arrangements are invoked. The Enterprise Incident Management Activation Levels help to determine when an incident must be escalated to a DCE.

When determining whether a privacy incident meets the activation levels, we should consider whether the following red flags are present:

- The breach involves an external bad actor who has accessed personal information via Department systems
- Control of personal information has been lost, e.g., a ransomware attack
- The breach involves the personal information of a significant number of individuals
- The breach involves the disclosure of large amounts of sensitive information
- The breach involves the disclosure of large amounts of personal information that would require the affected parties to take remedial action to thwart fraud or identity theft, such as changing passwords, changing bank accounts, cancelling credit/debit cards, cancelling a passport
- The breach is rated at impact level 5 on the Government Chief Privacy Officer's (GCPO) privacy breach impact rating scale
- The breach could have significant reputational consequences for the Department and there could be sustained media interest.

Determining when an IMT is needed for a privacy incident

The Chief Privacy Officer will provide advice to the DCE of the area affected by the breach whether an IMT is needed to manage the breach.

Leading the IMT

The DCE of the area affected by the breach will lead IMT or appoint an Incident Controller who is experienced in Coordinated Incident Management System protocols and dealing with privacy incidents. The DCE will ensure that the IMT has the necessary resources to fulfil its functions. The Privacy Team and other specialised personnel will act as advisors to the IMT.

7. Incident response roles and responsibilities

The following list indicates the high-level responsibilities of groups that should be involved in a privacy incident response.

Privacy Team

- Assist with assessing the privacy impact and risks associated with the incident
- Engage with and formally notify key stakeholders, including the Privacy Commissioner and GCPO
- Assist with queries associated with the incident and provide advice about the notification to affected individuals.

Technology Services and Solutions and Safety, Security and Risk

- Contain cyber security-related incidents
- Carry out forensic investigations
- Engage independent external providers to obtain specialised support or advice.

Legal

- Assist with any legal issues and queries associated with the incident
- Contribute to the decision on the threshold for the notification of affected individuals.

Communications

- Implement the communications plan
- Address media and public enquiries
- Amend and publish prepared key messages for different stakeholders.

DCE

- Lead the incident response until conclusion (or appoint an Incident Controller)
- Ensure the response team has access to the resources required to appropriately manage the response
- Update the CE and other Senior Leaders
- Publicly comment on the privacy incident when required.

Office of the CE

- Monitor risk in relation to the CE and Department Ministers.

7. Learning from privacy incidents

A structured approach to analysing privacy incidents enables the Department to identify possible trends, determine whether any changes are required to systems and processes, and consider if there is a need for additional privacy training.

The Privacy Team will do this in two ways. It will conduct a root-cause of analysis of all breaches. Root-cause analysis is a systematic process used to determine what happened, why it happened and what can be done to prevent another incident occurring.

The Privacy Team will also assign a rating of 1-5 using the GCPO's privacy breach impact rating scale (1 being low impact; 5 being high impact). The impact rating helps the Department to assess the actual and potential impact of privacy incidents and assist with internal reporting and analysing trends.

Lessons-Learned

When an IMT has been initiated and the incident has been managed and concluded, the Department should set up a lessons-learned session to identify and communicate what worked well, what did not, and would could be improved with how we responded to the privacy breach.

The lessons-learned session should include:

- A workshop attended by all those involved in the IMT
- Documenting and sharing the lessons learned from the incident
- Storing the lessons learned in a privacy incident repository
- A regular review of the lessons learned documents for continuous improvement.