Security and Internal access controls

Overview

Security of information and IT infrastructure is a critical component of a robust privacy programme. Both security and privacy staff must work together to identify external and internal risks, and to ensure that security is prioritised and resourced accordingly.

Cyber-attacks are on the rise and being able to respond appropriately to them is a key responsibility for organisations. You can read more about planning for, and practicing, incident response plans in our Breach Management guidance.

Organisations must take reasonable steps to make sure the information they hold is kept safe and secure. This includes making sure it's protected from loss, accidental or unauthorised disclosure, access, use, or modification or any other misuse. This obligation applies to information that is held by the organisation (for example, in on-premises servers) and information that is held on the organisation's behalf by a service provider (for example, a cloud-based data storage provider). Remember, organisations are liable under the Privacy Act for the personal information stored and processed on their behalf.

The most effective strategy is having a well-thought-out security plan for all personal information you hold.

At a high level, this pou describes key security controls across three areas – physical, technical, and organisational.

These controls are not exhaustive and are continually evolving. Organisations need to ensure that they update their knowledge on security risks, including seeking advice from external experts where necessary, and implement all reasonable security safeguards in a timely way.

Providing security and IT advice is not a core function of OPC, therefore we have provided links to advice and resources from other authoritative sources, such as CERT NZ, and others.

Who is this for?

Your privacy function and those who are responsible for, or involved in, privacy or information security within an organisation.

Key objectives of the Security and Internal access controls pou

What would we expect to see?

- Security controls are specific to the type and sensitivity of information held across the organisation, rather than a 'one size fits all' approach.
- Regular auditing of systems is undertaken to ensure appropriate access.
- Organisation follows industry guidelines and security standards relevant to its business context.

- There is a remediation plan for managing and/or replacing legacy systems (where necessary).
- Identified risks are proactively managed. For example, by incorporating them into the organisation's risk and assurance reporting processes to ensure visibility.
- Organisational controls (i.e. policies, procedures, and decisions) are regularly reviewed and fit for purpose.

Preventative controls

Keeping information secure isn't just about having encrypted databases, it also includes physical security, operational security, security during transmission and during destruction.

The guidance below covers some of the most common practices that can lead to data and privacy breaches if not appropriately monitored and managed within your organisation.

The controls available to you in these scenarios can be categorised as:

- Physical – for example, building access, physical documents, and mobile device protection.
- Technical – for example, IT systems and cyber security.
- Organisational – for example, policies and procedures, staff behaviour, training, and awareness.

Often, you will need to use a combination of controls from all three categories to ensure you have a robust security system in place to reduce the likelihood of breaches.

What steps are appropriate will depend entirely on the context of your organisation, including:

- How sensitive is the personal information involved?
- What are you using the personal information for?
- What security measures are available, and how will using these measures impact on your organisation's functions?
- What might the consequences be for the individual if the information is not kept secure?

Sending emails safely

Organisational controls

- Establish email procedures, such as:
    - Double-checking the address to ensure it is correct before pressing 'send'.
    - Ensuring the correct attachments are attached.
    - When sending mass-emails, double-checking that all email addresses are in the bcc not cc field if it's not appropriate for recipients to be able to see each other's email addresses.
    - Avoiding long chain emails, as these can increase the risk of unauthorised disclosure if the email recipients change during a lengthy discussion.
    - Requiring staff to use delay-send functions to reduce the risk of breaches.
- Have a policy on the types of information that staff can send by email.

- If sending a large volume of information, or particularly sensitive information, get employees to check if the entire document needs to be sent or if there is a way of extracting only the relevant information intended for the recipient.

Technical controls

- Spreadsheets can contain a lot of information. Protect them and other types of attachments using passwords, and check if other personal information is hidden behind spreadsheet document tabs and in pivot tables.
- Set a delay send on emails to allow for time to catch mistakes.
- Use of Data Loss Prevention tools when appropriate and available to restrict types of files which can be sent or shared.
- Disabling ‘auto-fill’ functionality in email address books and require the use of contact lists.

Physical controls

- Lock devices, such as laptops, when not using them to prevent inappropriate access or use of your email

Preventing the theft or loss of devices and documents

Organisational controls

- Review your organisation’s policy about the types of information that can be stored on a portable device.
- Have a comprehensive workplace security policy for bringing your own device.
- Have a ‘work from home’ policy in place to set rules and expectations in relation to security.

Technical controls

- Use extra security measures for portable devices such as encryption, password locks, and remote wiping.
- Delete personal information and other data when it’s no longer needed.

Physical controls

- Protect sensitive documents and information using physical security measures such as locked filing cabinets.
- Lock workstations and laptops, even when briefly stepping away.
- Ensure papers, computers or other electronic devices aren’t visible in homes, public places or in parked cars.
- Collect sensitive documents from printers and photocopiers straight away, so they aren’t lying around.

Storing personal information securely

Organisations have an obligation to store personal information securely. System errors, scams, and employee browsing can all lead to a security failure.

A secure IT network will help protect the personal information your organisation works with from hacks, viruses, and malware. CERT NZ has produced cybersecurity guidance that will help you keep personal information safe in your network.

If your organisation holds or shares personal information digitally, you should have multi-factor authentication (MFA) enabled. MFA means requiring more than just a password to verify access to systems and accounts. Some examples include phone authentication via text message, authenticator apps, or security questions. This is designed to allow you safer access to your systems, and provides an additional step of verification and greater security.

CERT's Multi-factor authentication and verification guidance has more advice on this.

Organisational controls

- Only use secure Wi-Fi networks when working with or sending data.
- Use secure sites to share information (for example, SharePoint) to avoid emailing unencrypted sensitive information.
- Check for sensitive information in email attachments, especially when forwarding them to others.
- Use security classifications on documents and ensure staff know what they mean and how to handle the documents to keep them safe.

Technical controls

- Ensure that sensitive information cannot be accessed publicly through your website, the internet, or your intranet. If you can access it online without a password, so can others.
- Where systems enable it, establish role-based access rules and review these regularly to ensure they're up to date.
- Send data safely, especially in remote access and client/server transmissions.
- Enable multi-factor authentication for access to systems holding personal information.

Physical controls

- Store sensitive paper records in locked filing cabinets.
- Know who has physical access to sensitive information – for example, secure areas or rooms in your facilities.
- Keep a register of where your physical documents are stored.

Disposing of information safely

Organisations must not keep personal information for longer than they need it. If your organisation doesn't have a specific legitimate purpose for keeping the personal information, it must be disposed of securely, whether it is in physical or digital form.

Public sector organisations have obligations to preserve records under the Public Records Act. You can find guidance on this at Manage information – Archives New Zealand.

Your organisation is responsible for working out when personal information is no longer needed, as well as a practical solution for disposing of physical documents containing personal information. For example, shredding can be an effective way to dispose of paper records and photographs.

You should also securely delete personal information before you reuse or dispose of any electronic equipment such as computers and laptops, smartphones, tablets, hard drives, USB sticks, photocopiers, and cameras.

You can read more about retention and disposal in the Know your Personal Information pou.

Organisational controls

- Ensure you have policies and procedures in place for disposing of information you no longer need.
- Establish practices for dealing with multiple copies of information. For example, ensure documents are filed in the correct place and any duplicates are securely disposed of.
- Check whether you have obligations under the Public Records Act or other legislation (for example, if your organisation is subject to anti-money laundering law) – ensure you know what these are and have them documented, for example, retention and disposal schedules.

Technical controls

- Check whether the IT systems you use, including cloud-based systems, can automate your data retention and disposal rules. This could save you time and reduce your risk.
- Destroy or securely delete sensitive information prior to re-use or disposal of equipment or media.

Physical controls

- Shred physical records of personal information you no longer need.
- Don’t re-use paper files.
- If you are disposing of filing cabinets, or other equipment used to store documents, check thoroughly to ensure that no documents have been left in there. For example, remove drawers to check that no documents have slipped behind them.

Keeping software up-to-date and using strong passwords

Organisational controls

- Carry out regular security checks and audits.
- Only click on links or attachments that are known or expected. Run training sessions across the organisation to test this so that everyone knows what to look out for.

- Avoid opening files sent via instant messaging software on a device that contains restricted data. These files can bypass anti-virus screening.
- Restrict the ability for staff to install software on your organisation's devices. Only install programmes that have been checked and approved by your organisation's security and/or IT functions.

Technical controls

- Computer operating systems and mobile device apps need to be kept up to date to avoid system vulnerabilities. Patches are regularly issued by Microsoft, Google, Apple and others. Updating your device software protects you from hackers and makes devices more secure.
- Use strong passwords – change them regularly and don't share or reveal them.

Preventing employee browsing and inappropriate disclosure of information

Organisations have an obligation to prevent their employees from inappropriately accessing and/or disclosing customer information. Where employees access customer information without a legitimate business purpose, this is called employee browsing.

Employee browsing or internal misuse of personal information is one of the most common privacy breaches, yet it is poorly understood as a breach, which is why it has been included specifically in this pou. These types of breaches risk staff and customers losing trust in your organisation and can cause serious harm to the individuals whose privacy has been breached.

In one example, a person in a position of power looked up the details of a colleague's partner then used their position to repeatedly sexually harass the partner via text message. The victim felt intimidated, scared, and fearful in their own home so contacted OPC.

Organisational controls

- Foster and maintain a culture of respect for personal information, and ensure employees understand that accessing information that isn't necessary for their role is a privacy breach.
- Include a policy about employee browsing in the code of conduct with clear consequences for violations of the code and ensure that your contracts of employment or contracts for services requires people to comply with the code of conduct.
- Run intranet stories or a poster campaign about employee browsing.
- Ensure that staff members are aware of organisational practices around monitoring and auditing of file access.
- If an employee deliberately discloses information without permission, disable their access to electronic systems and ensure they return keys and access cards.
- Make sure employees understand the importance of protecting personal information when working from home.
- Keep a log of user access to systems holding personal information and ensure your information repositories have the appropriate functionality to enable the logging and

monitoring of user access, particularly when procuring new technical solutions or updating existing systems.
- Regularly review access to systems and facilities and adjust or remove access where appropriate, for example when an employee changes their role or leaves the organisation.

Remember, organisational controls are only effective if staff are reminded of their existence.

Technical controls

- Have different levels of security for types of files, for example, general access and restricted.
- Ensure there are systems in place that monitor employee access to files. Where this is not possible, or as in interim measure, you should adopt random monitoring such as spot audits.
- If you are developing a new IT system, employ Privacy by Design and Security by Design techniques to reduce future risk.
- Use role-based access controls:
    - CERT NZ Principle of least privilege.
    - CERT NZ Enforcing the principle of least privilege.
- Keep files separate on content management systems, put in place access controls, and carry out routine audits.
- Ensure no personal information is stored on obsolete databases.
- Ensure each database or system has an assigned business owner who actively manages that system's security, data and retention.

Physical controls

- Store sensitive paper records in locked filing cabinets. Lock mobile phones, laptops, and other portable storage devices when not in use.

Quick links

- CERT NZ top online security tips for your business.
- NCSC Joint guidance: Principles for security by design and default.
- NCSC UK Cyber Assessment Framework
- Archives NZ Information and Records Management Standard (mandatory standard for public sector organisations)

Organisation examples

We've included some use cases based on fictional organisations to demonstrate each of the pou in practice. Read more about them in Introducing the Organisation Examples.

Large business – Fern Leaf

Fern Leaf has a well-established IT team. The Privacy Team recognises the IT team's expertise in this area and so have jointly worked on implementing physical, technical, and

organisational controls. As part of its work, the IT team sends out phishing exercises to ensure employees remain aware of these types of attacks.

Prior to using software, the IT team ensure that they carry out due diligence on third parties including checking what security credentials they hold.

Senior leadership have zero tolerance for employee browsing and trust that their employees will not go snooping, as their customers don't want to be ringing up and not receive help due to access being too restrictive. They send out regular communications on this and have noticed a reduction in employee browsing cases. They actively carry out random checks to ensure those who are accessing customer profiles have a legitimate business purpose. Their zero-tolerance approach is reflected in their code of conduct and forms part of staff inductions. There have been repercussions for staff who have been found to be inappropriately accessing customer profiles.

Small business (charity) – Reach High

Reach High does not have an internal IT security resource, and so it relies strongly on service providers to deliver its security capability. It addresses this in the following ways, noting that it has already identified that it has a high privacy risk profile:

- Reach High engages an IT security consultancy to conduct an annual security gap assessment and provide an action plan to address any security risks.
- As part of the security assessment, the IT security consultancy provides Reach High with an internal IT Security Policy and associated procedures.
- Reach High uses only cloud-based systems to store and process its data, including personal information. It selects these systems based on their security credentials, looking to systems that are ISO-270001 certified.
- Reach High also uses a separate managed IT services provider to run periodic tests on its systems and settings, and to generally manage day-to-day IT issues and risks.
- Reach High has robust third-party contracting processes including notification requirements in the case of a data breach.
- Finally, Reach High obtains access to an online security training service, which provides its employees with access to regular short security training modules.

Start-up – Swiftstart NZ

Security of customer information is crucial to Swiftstart NZ's success as a company. While it doesn't have a dedicated security or IT function, as a tech-savvy digital organisation, all staff have some responsibility for managing security risk. Staff have received training on this and are covered by contracts which clearly set out their responsibilities. In particular, there is a clear expectation on staff around when and how they are permitted to access client customer information, and they know that any inappropriate access will be considered serious misconduct and is grounds for dismissal.

Swiftstart NZ has designed its platform to meet best practice from the outset; it uses encryption to protect the data in transit and at rest, firewalls to prevent unauthorized network access, access controls to limit who can view or modify the data, backups to restore the data in case of disaster, audits to check the compliance and effectiveness of the security measures, and monitoring to detect and respond to any security incidents.

Small business (non-tech) – Green Gardens

Green Gardens doesn't have a dedicated security or IT function, due to its small size and low privacy risk profile. However, all staff have some responsibility for managing security risk.

The Owner/Manager and Administrator have joint responsibility for the home office that Green Gardens operates out of. For example, any physical documents containing client personal information are stored in a filing cabinet that is locked outside of business hours, and only the Owner/Manager and Administrator have a key to the cabinet. The onsite computer is password protected, and access is limited to the Owner/Manager and the Administrator.

There is a clear expectation of staff for when and how they are permitted to access client information, and they are aware that any inappropriate access will be considered serious misconduct.

Independent contractor – Jo Jones

As an independent contractor, Jo Jones doesn't have a dedicated security or IT function, but she is still responsible for managing any security risks to the personal information she holds. Jo Jones has a dedicated work device that is password protected, which is stored in her home outside of her business hours. Jo makes sure the computer operating system of her work device is kept up to date to avoid system vulnerabilities, as well as her device software.

When Jo is working for community health service providers, she has access to their systems via a password-protected account and can only access their systems when she is onsite at one of their offices or clinics. Jo is aware of each health provider's policies regarding employee browsing and understands that any inappropriate access to personal information will be considered serious misconduct and grounds for dismissal.

Government agency – The Ministry

Like Fern Leaf, the Ministry has a well-established IT team, and good relationships between IT, information management, and privacy teams. This joined up approach has enabled them to implement robust physical, technical and organisational controls. The Ministry has developed a long-term plan for updating their existing legacy systems, which has been reviewed by the governance function and approved by the Senior Leadership team. The Privacy team has taken a particular focus on ensuring that staff who are working from home know how to do so safely and that technical and organisational controls persist for those who are working remotely, even in the absence of the Office's physical controls. They also recently ran an awareness campaign during Privacy Week about employee browsing, reminding employees of the code of conduct and the Ministry's zero-tolerance policy. The Ministry undertakes regular spot audits to monitor employee access to files in their older legacy systems that don't have automated audit logs.