Definitions

Terms Used in Guidelines and Survey

Term	Description	More information
Antivirus protection	Antivirus products can detect and block many forms of viruses and other malware hidden in files. Ensuring that all devices (computers, phones, laptops) have antivirus products installed and constantly kept up to date will helps ensure they are adequately protected from malicious files.	https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product
Accounts	This includes, but is not limited to; computer accounts, email accounts, internet accounts, case management accounts.	
Cloud based services	Services delivered by other parties via the public internet to which anyone can sign up or subscribe to use.	https://www.cert.govt.nz/individuals/guides/how-the-cloud-works/
Cyber security incident	Any incident that results in unauthorised access to computer data, applications, networks or devices. It results in information being accessed or blocked without authorisation. This includes breaches and near misses.	https://www.justice.govt.nz/assets/Uploads/moj-privacy-guidelines-FINAL.pdf
De-identified information	Data that has had the personal identifiers removed, such as name, address, date of birth and address.	https://www.stats.govt.nz/assets/Uploads/Integrated-data-infrastructure/de-identified-data-supporting-analytical-insights-while-maintaining-privacy-and-confidentiality.pdf
Electronic devices	This includes, but is not limited to; computers, laptops, tablets, smartphones, external hard drives (e.g. USB flash drives), printers and scanners.	
Encryption	The encoding or scrambling of information so that it cannot be accessed by people who don't have the right key (password) to decrypt it.	https://support.microsoft.com/en-us/windows/how-to-encrypt-a-file-1131805c-47b8-2e3e-a705-807e13c10da7
End user	A person or other entity that consumes or makes use of the goods or services produced by businesses. An end user may differ from a customer, since the entity or person that buys a product or service may not be the one who actually uses it.	
Firewall	A network security device that monitors and filters incoming and outgoing network traffic based on an organisation's previously established security policies.	
Hypervisors/ Virtual machine monitor	Software allowing one host computer to support multiple guest virtual monitors (VM's)	
Local Copy	A copy of a document which is stored on the device's hard drive rather than in the cloud.	
Malware	Malicious software designed to damage or harm a computer system.	https://www.cert.govt.nz/individuals/common-threats/malware/?topic=malware

Term	Description	More information
Ministry Information	Any information you obtain from the Ministry and the Court or create in the course of delivering services under your contract with the Ministry	https://www.archives.govt.nz/manage-information/how-to-manage-your-information/implementation/outsourcing-business
Multi-factor authentication	A requirement for more than one control factor to be provided in order to gain access to a system. Examples include using an ATM which requires possession of a bank card and knowledge of a PIN number, or one-time code numbers sent to a user's mobile number once a valid username and password combination has been provided.	https://www.cert.govt.nz/individuals/guides/two-factor-authentication/
Onshore/ offshore data	Onshore means data that is held in New Zealand. An offshore cloud is where we store or process information in an overseas location like Australia or the United States, instead of in New Zealand. Approval from the Judiciary is required for Court or Judicial Information to be stored or processed in an offshore location.	https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/
Patching/ patch management	The process of ensuring vulnerabilities identified in software or devices are corrected by installing security updates.	https://www.cert.govt.nz/it-specialists/critical-controls/patching/creating-a-standard-patching-process/
Privacy incident	Any actual or suspected loss, disclosure, accessing or modification of Confidential Information held by the provider or supplier. This includes breaches and near misses.	https://www.justice.govt.nz/assets/Uploads/moj-privacy-guidelines-FINAL.pdf
Confidential Information	Confidential Information means information, including personal information, that your Organisation obtains from the Ministry or others (such as programme participants) in the course of delivering services under your contract with the Ministry, which: • is by its nature confidential; • is marked as 'confidential', 'in confidence', 'restricted', or 'commercial in confidence'; • is of a sensitive nature or commercially sensitive; or • most people would consider confidential.	https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html
Remote wiping	A security feature that allows a network administrator or device owner to send a command that deletes data to a computing device. It is primarily used to erase data on a device that has been lost or stolen so that if the device falls into the wrong hands, the data won't be compromised.	
Security Testing/ certification	A process intended to reveal flaws in the security mechanisms of an information system that protect data and maintain functionality as intended. It can help to identify all the possible security threats and also help fix those errors.	
Security updates	Software updates that are primarily focused on patching existing bugs or flaws to improve software security.	
Software	A set of instructions, data or programs used to operate computers and execute specific tasks. Software is a generic term used to refer to applications, scripts and programs that run on a device.	
Strong passwords	Passwords that are difficult for others to guess, typically involving unpredictable phrases, or the use of multiple characters and symbols such as #, ?, <, % etc.	https://www.cert.govt.nz/business/guides/password-policy-for-business/
Sys Admin	A person responsible for the upkeep and operation of computer systems.	

Top Tips for Cyber Security

How to Keep Information Safe When Working

□ Choose strong passwords

Create a long, strong and unique password for each of your accounts. If one of your accounts is breached, any others will remain secured. You can use a password manager to store passwords safely

□ Set up Multi-Factor Authentication

MFA provides a second layer of security to access your accounts. Choose to receive a security verification by text message, phone call, or through an app

□ Check your wi-fi settings

Ensure your home wi-fi is password protected. Free or public wi-fi is open, meaning others can see what you're doing, so avoid using these

□ Be careful what you share on social

Anything you share online can be accessed or copied by others, so ensure you're not sharing information that could make you vulnerable

□ Back up your information

Use a cloud based (virtual) service to copy your data to a separate, safe location so it can be recovered if something happens to the original

□ Keep your systems up do date

Software updates can fix vulnerabilities and make your electronic devices more secure, so ensure you check regularly for updates

□ Using external hard drives

External hard drives such as USB's can be an easy way for viruses to spread and can also be easily lost. Ensure your stick is password protected and avoid sharing with others

□ Using email safely

Don't use your work email for personal use. Ensure your emails don't contain any protected or sensitive information. Email attachments can be encrypted if you do need to share information in this way

□ Using free services

Free services (such as antivirus software) are less safe to use than paid-for services. Paid-for services are more likely to have processes in place to protect your information

MINISTRY OF JUSTICE
Tāhū o te Ture

New Zealand Government

How to Guides

How to Better Protect Ministry Information

How do I password protect my documents?

For M365 office documents (such as Word, Excel, PowerPoint):

1. Select the ‘File’ tab
2. Select ‘Info’ from the left-hand side column
3. Select ‘Protect Document’
4. Select ‘Encrypt with Password’

For Adobe PDF’s:

1. Select the ‘Edit’ tab
2. Select ‘Protection’ then ‘Security Properties’
3. Select ‘Show Details’

How do I look after physical files?

1. Keep paper files stored in a locked area
2. Regularly review your company’s physical files and assess if you still need them
3. Don’t keep unnecessary documents such as copies of digital records
4. Ensure your original paper files are transferred to the Ministry, and consult with the Ministry on their disposal

How do I share information safely?

Email attachments can be encrypted using a file manager, so content can’t be accessed unless it’s by the intended recipient.

If it’s not appropriate to share information in an email attachment or through an online messaging service, you could:

1. Give them a call via Teams or Skype
2. Meet up in person when possible

What should I do if a privacy or cyber security incident happens?

1. Tell your contract manager as soon as possible
2. Wherever possible, find out:
   a. The nature of the breach
   b. The nature or type of information implicated
   c. What actions are proposed or can be taken to mitigate the effects
3. Keep your contract manager informed of any progress

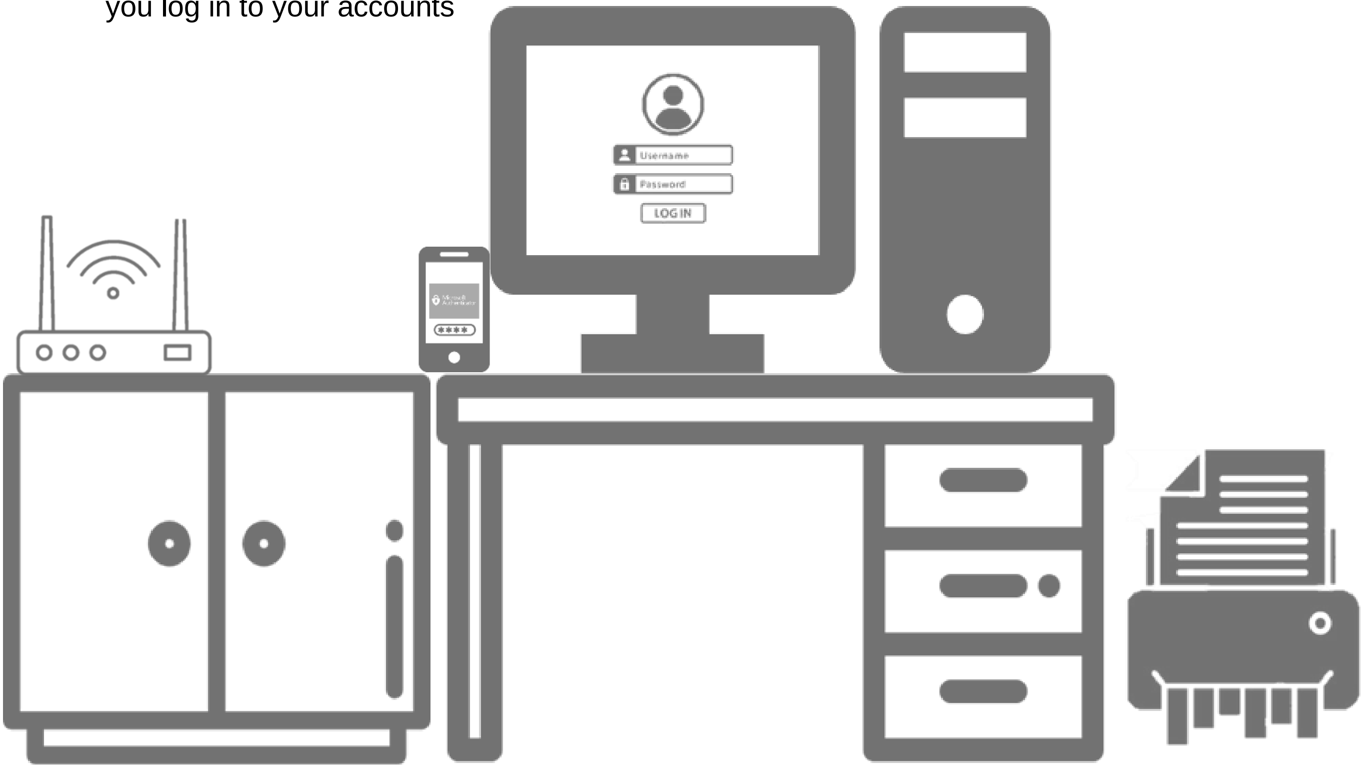
Workstation Set Up Guide

Best Practice Tips

- ✓ Create a long, strong, and unique password for all your accounts. Lock your laptop whenever you move away from your desk

- ✓ Regularly check for software updates on your electronic devices to keep

- ✓ Use Multi-Factor Authorisation (MFA) to verify your identity when you log in to your accounts



- ✓ Organise collection of files requiring archiving with your Contract Manager.

- ✓ Keep physical files in a locked area and regularly assess if you still need them

- ✓ Shred physical files you no longer to need keep. Ensure your shredder is graded to an appropriate particle size

MINISTRY OF JUSTICE
Tāhū o te Ture

New Zealand Government

Privacy Basics

The Privacy Act 2020

Privacy Rights

Everyone engaging with our justice system has privacy rights that we must uphold. People can reasonably expect that their personal information is collected, used, and shared respectfully, and adequately protected.

The Privacy Act 2020 affords privacy rights to every New Zealander. These rights include:

- their personal information is only collected, used and shared for legal purposes
- they can access any personal information an organisation holds about them
- they have the right to correct any information held about them

13 Principles to Guide Good Practice

The Act sets out 13 privacy principles that every organisation dealing with personal information must follow. Failure to meet any of these principles is considered a privacy breach.

1. Only collect the personal information you need to carry out a function of your organisation.

2. Where possible, get it directly from the person it's about.

3. Tell the person what you're going to do with it.

4. Collect it legally and fairly.

5. Take care of it once you've got it and keep it secure.

6. Allow people to see their own information if they want to.

7. Correct it if it's wrong.

8. Make sure it's accurate, up to date and relevant before you use it.

9. Securely dispose of it when you no longer have a lawful reason to keep it.

10. Use it for the purpose you collected it.

11. Only share it for a lawful reason.

12. Only transfer it to an offshore entity that is subject to privacy laws with comparable safeguards to New Zealand's.

13. Only assign and use unique identifiers as permitted.

For the full text of the principles go to:

Privacy Act and Principles

Frequently asked questions

What is a long and strong password?

A strong password uses a mix of uppercase letters, numbers and symbols. Use a catchphrase that's easy to remember but isn't linked to any personal information as this makes your password easier for someone else to guess.

https://www.cert.govt.nz/individuals/guides/how-to-create-a-good-password/

You can use a password manager to safely store your passwords to all your accounts. This means you'll only need to remember one set of login details.

Why is it important to password protect documents?

As many documents are stored on Shared Drives, password protection adds a layer of security for sensitive information and ensures only people who have the password can access the content. It's important to note that passwords need to be shared securely with the people who require access.

What information needs to be treated with care?

Information that needs to be treated with care is any information that could impact an individual or organisation if something happened to it, such as if a database was corrupted or if it was released to the media or third parties without authorisation. It could include personal information, such as a name, age, address, or information which is commercially sensitive.

Why should I not share Confidential information in emails?

Emails and email chains can very easily be sent or forwarded on to others. This means Confidential information can often be shared with people other than the original intended recipient, risking a breach of an individual's privacy. Appropriate security measures will depend on factors such as how sensitive the information is, what steps can be taken to secure the information, and what the impact would be if something did go wrong.

https://www.privacy.org.nz/tools/knowledge-base/view/229

What does cloud storage mean (offshore vs onshore, ownership of data)?

Government organisations are required to use cloud services for information systems, when possible. Public cloud services provide scalable, secure and highly resilient infrastructure tools and web applications.

Onshore means data that is held in New Zealand, and offshore means data that is held in another country. When data is held offshore, this can affect the ownership of the data, meaning the host country can have control over the data and information they hold. This is particularly important for judicial and court information, as approval from the judiciary is required is this information is to be stored offshore.

Why government organisations use public cloud services | NZ Digital government

Frequently asked questions

How should I look after information – what does ‘secure’ mean (electronic, paper)?

Looking after information to make it secure means taking all necessary steps to protect it, such as:

- leaving physical files locked away and not on your desk
- password protecting your devices and not leaving them unlocked when you step away from your desk
- not sharing sensitive or sensitive information with others, other than with the intended recipient in an appropriate manner.

How should I dispose of information (electronic, paper)?

Regularly review whether you need to keep hold of information. When managing your organisation’s physical files, ensure they are disposed of or archived correctly. Reach out to your contract manager as they can advise you on best practice

Information management requirements for outsourced business Retire information and assets securely | Protective Security Requirements

moj-privacy-guidelines-FINAL.pdf (justice.govt.nz)

What are some ministry recommended solutions?

- OneDrive – A file hosting service operated by Microsoft which allows users to store, share and synchronise their files through the cloud.
  Personal Cloud Storage – Microsoft OneDrive

- 7zip – A free and open-source file manager, allowing users to encrypt attachments before sending via email. Please note that it’s important to ensure there is an agreement in place with the recipient of the file about the future use and security of the information being shared.
  Frequently Asked Questions (FAQ) (7-zip.org)

- Microsoft Azure Multi-Factor Authorisation – This tool adds a layer of protection to the sign-in process when accessing accounts by asking for verification via a text message, one time passcode, phone call, or through the Microsoft Authenticator app.
  Multi-Factor Authentication (MFA) - Microsoft Security

- LastPass – A password manager tool that creates, remembers, and fills in long, strong, and unique passwords for all your accounts. One login allows access to all your accounts, so you only have one to remember.
  #1 Password Manager & Vault App with Single-Sign On & MFA Solutions | LastPass