DEPARTMENT OF THE
PRIME MINISTER AND **CABINET**
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

21 May 2025

[redacted]

Ref: OIA-2024/25-0845

Dear [redacted]

Official Information Act request relating to policies and protocols that apply to the National Assessments Bureau for the use and security of information technology

Thank you for your Official Information Act 1982 (the Act) request transferred in part to the Department of the Prime Minister and Cabinet (DPMC) on 28/04/2025. Your request dated 25/03/2025 was made to the Government Communications Security Bureau (GCSB). Part [5] of your request asked about the National Assessments Bureau (NAB) policies and practices. NAB is located within DPMC and so Part [5] of your request as it related to the NAB was transferred to DPMC. Your full request is quoted below with the part transferred to DPMC in bold and underlined (numbering has been added for ease of reference):

> "*Following the story of the US administration's use of the app Signal I am interested in learning more about the GCSB's use of the app and phone communication in general.*
>
> *[1] Are there policies in place to regulate the downloading of third party apps such as Signal?*
> *[2] What security measures are in place to encrypt information that is sent from one GCSB mobile device to another?*
> *[3] What happens if a GCSB mobile device is lost?*
> *[4] How often are GCSB mobile devices replaced?*
> *[5]* ***Are these the same policies/practices/protocol applied at*** *NZSIS and* ***NAB?***
> *[6] I expect that communication regularly takes place between the Director-General of the GCSB and the Director-General of NZSIS. How many phones calls were made/received so far in 2025?*
> *[7] How many text messages were sent/received? Is it possible to have the text messages, or to be advised what the subject matter was about?*
> *[8] I am interested in text messages / iMessages / WhatsApp messages / Signal messages between the two parties, as well as with Nicky Haslem, so far in 2025*
> *[9] I am interested in the text messages/ iMessages / WhatApp messages / Signal messages between the GCSB Director-General and Minister Collins, so far in 2025.*
>
> *I understand that for security reasons you may not be able to release all the information to me. But I appreciate you considering my request*."

We have interpreted Part [5] of your request as it relates to NAB to be asking about the policies, procedures and protocols for the use and security of information technology (including mobile phones) by NAB staff.

NAB staff are covered by the same policies for information technology use and security as all DPMC officials. DPMC does not hold information on the policies, practices or protocols that might apply to GCSB officials. Accordingly, we have interpreted Part [5] of your request, as it relates to NAB, to be for the relevant information technology policies, practices or protocols that apply to DPMC officials.

Please find attached the following documents as set out in the table below which we have identified as being relevant to your request.

Item	Date	Document Title	Decision
Item 1	7/10/2022	IT Code of Conduct	Release in Full
Item 2	23/04/2024	Protective Security Policy	Release in Full
Item 3	31/08/2023	Acceptable Use of Technology Policy	Release in Full

As noted in the table, I have decided to release these three relevant documents to you in full. These are all DPMC corporate policies that sets out the policies and protocols for all DPMC staff for use and security of DPMC information technology, including DPMC mobile phones.

Item 1 "IT Code of Conduct" sets out DPMC's information technology code of conduct and is taken from DPMC's internal intranet – where DPMC staff access all DPMC corporate policies and procedures. The code of conduct sets out the three general principles to help DPMC staff make judgements about appropriate behaviour when using DPMC's information and communications technology. It links into the relevant corporate policies.

Item 2 "Protective Security Policy" is DPMC's protective security policy and applies to security for information technology. This policy is also available to all staff via the internal intranet.

Item 3 "Acceptable Use of Technology Policy" sets out the policy for acceptable use of DPMC technology which applies to all DPMC staff. This policy has been provided to DPMC by our information technology provider, Corporate and Shared Services (CSS), which is based in The Treasury. While this policy references The Treasury, it applies to DPMC staff. For DPMC, where the document mentions "Treasury", it should be read as "DPMC".

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on the Department of the Prime Minister and Cabinet's website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely

[redacted]

Bridget White
Executive Director
National Security Group

Item 01

IT Code of Conduct

Published 13/05/2025

New staff starting at DPMC are required to read and sign the Central Agencies IT Acceptable Use Policy.

The Central Agencies IT Acceptable Use Policy sets out some general principles[1] in order to help you make judgements about appropriate behaviour when using DPMC's information and communications technology (ICT)[2]. Use it as guidance to apply to a range of situations you might find yourself in. While it specifies some of your obligations it does not attempt to cover off every eventuality. If in doubt, consult your manager or ask Central Agency Shared Services (CASS) service desk x8300 for advice.

Principle 1: Fulfil your lawful obligations to government with professionalism and integrity.

All emails, documents and other material stored on DPMC's ICT systems are official information. The disclosure and handling of official information held by DPMC is subject to the Official Information Act 1982 ("OIA"), and the Privacy Act 1993 sets out principles for the collection, holding, use and disclosure of personal information. Any release of official information should follow DPMC's internal OIA processes, including sign-out procedures. Refer to DPMC's OIA policy for details.

You have a duty of care to ensure the security of information and property is effective and maintained. Refer to Central Agencies Security Policy for further detail and guidance. In particular:

- You are responsible for all activity relating to your computer user account. You must keep your password private and never share it with anyone.
- You must classify and protect official information in accordance with the Government and DPMC guidelines for protection of official information. In particular, information classified as CONFIDENTIAL, SECRET and TOP SECRET must not be transmitted or saved on DPMC's ICT systems (including computers, telephones and faxes).
- You must not connect equipment to, or install software on, DPMC's ICT systems without the approval of Central Agency Shared Services.
- You must report any actual or suspected security breaches to the Business Security Officer (BSO) immediately.

You must make a permanent record of substantive business emails and other forms of communication. Refer to Central Agencies IT Acceptable Use Policy for guidance on using and saving emails. You must summarise substantive business telephone calls, mobile phone texts or instant messages in a file note.

Principle 2: Behave honestly, faithfully and efficiently, respecting the rights of the public and your colleagues.

You must ensure your use of DPMC resources is appropriate (particularly in relation to personal use of DPMC's resources), lawful, and shows reasonable care.

Reasonable and limited use of DPMC's ICT resources for personal reasons is acceptable. Use a private email account to avoid any misconceptions that might arise from using a DPMC email address for personal messages. Use your own mobile phone or calling card for expensive personal phone calls.

You must not make or transmit unauthorised digital or paper copies of published material that is protected by copyright or under any other law.

Other examples of inappropriate or unlawful behaviour include, but are not limited to: harassment, libel, unauthorised access to ICT systems, sending unsolicited "spam" email, and the transmission or display of text or graphics which may reasonably be considered to be obscene or offensive.

Principle 3: Avoid any activities, whether connected with your official duties or otherwise, which might bring DPMC into disrepute, or jeopardise its relationships with Ministers, clients or the general public.

All material stored on the computer system - including jokes, graphics and personal emails - is likely to be official information for the purposes of the OIA, and may be subject to a request under the OIA. Therefore, there is scope for considerable damage to DPMC's reputation if any objectionable, obscene or offensive material is held on our system.

Monitoring compliance with the ICT Usage - Code of Conduct

All ICT usage activity at DPMC is monitored for accounting and audit purposes. Misconduct may lead to disciplinary action or, in serious cases, dismissal or other appropriate action will be taken.

1. The principles are derived from DPMC's Terms of Employment – Code of Conduct.
2. For example: computers, telephones, BlackBerrys, fax machines, photocopiers.

Owner: Joanna Hodgson [TSY]
Team: Technology Infrastructure
Email: N/A
Modified: 7/10/2022

Properties

ContentOwner

Joanna Hodgson [CASS]

Team

Information Technology

Kāinga | Help me with Edit Feedback

Protective Security Policy

Original policy approved by:

i-Manage reference	4342432	**Approved by**	Brook Barrington, Chief Executive
Date originally approved			1/07/2020

Amended policy approved by:

i-Manage version	Version Number	**Contact**	Executive Director, Strategy, Governance and Engagement Group
Amended version approved by	Executive Director, Strategy, Governance and Engagement Group	**Name** **Signature**	Clare Ward Clare Ward
Date amended version approved	23/04/2024	**Date for review**	23/04/2027

Objective

1. This policy sets out the high-level principles to enable proportionate and effective management of our security environment and identified security risks.

Principles

2. The Department of the Prime Minister and Cabinet (DPMC) and National Emergency Management Agency (NEMA) is committed to maintaining the security of its people, information, and assets through delivery of the Government's Protective Security Requirements (PSR). We commit to:

   a) developing a consistent, strong, and sustainable security culture to ensure that employees are fully informed of and engaged in active security practices;

   b) incorporating our risk and security management processes with consideration of security, privacy, and health and safety principles to ensure a comprehensive understanding of, and response to these critical aspects of delivering on our core functions; and

   c) developing our security policies, procedures, and guidelines to align with the PSR, to ensure that we can identify and respond to changes in our security risk environment and establish security practices that are commensurate with identified risk levels and business needs.

Applies to

3. This policy applies to everyone in DPMC and NEMA, including permanent, fixed-term, secondee, casual and agency temporary staff, self-employed and independent contractors[1] (together referred to in this policy as 'staff'), regardless of position or seniority.

4. It applies to all premises and places where employees legitimately conduct departmental business, and all information, resources, and assets that DPMC owns or is accountable for.

Background

5. DPMC and NEMA perform a range of functions which are exposed to a variety of potential security threats, and each present a unique security risk profile. It is important that we understand and respond to these risks in a managed and consistent way in order to protect national interests, personal privacy and DPMC and NEMA's reputation.

Principles of Security Management and Governance

6. DPMC and NEMA will:

   a. maintain a governance structure that enables effective management of a secure operating environment and ensures the confident and secure conduct of departmental business

   b. follow a risk-based approach to ensure the safety of staff and visitors, the protection of departmental premises and assets, and the security of information

   c. develop and maintain a protective security framework and work programme to address priorities and meet specific business needs. These will be regularly reviewed and updated as required and will enable regular reporting on organisational maturity and security awareness

   d. ensure that all staff receive security good practice education and understand security requirements and risks relative to their role and will promote a culture that supports and encourages effective security practices across the department

   e. investigate security incidents quickly and effectively and take corrective action as appropriate, and

   f. maintain a business continuity management programme to ensure continued availability of essential services and assets during an emergency incident, or in the case of heightened threat levels.

Personnel Security

7. Our recruitment and ongoing staff management processes will ensure that all staff are eligible and suitable to have ongoing access to New Zealand government information and resources at levels of classification appropriate for their role.

8. We will follow consistent processes for the application and granting of national security clearances and ensure that staff in these roles have appropriate security clearances and

[1] For the avoidance of doubt, the reference to contractors including any Treasury staff, including permanent, fixed term, secondee, casual and agency temporary staff, self-employed and independent contractors, providing services to DPMC (or any departmental agency or functional chief executive hosted by DPMC) under the Central Agencies Shared Services (CASS) agreement.

briefings prior to being granted access to any information or assets. We will ensure ongoing suitability of staff to hold a clearance through the clearance management process.

9. We will manage staff movements and exits to ensure any security risks are identified and managed and that departing staff understand their ongoing security obligations.

Physical Security

10. We will ensure that appropriate physical security measures are in place to provide secure working environments for staff and visitors, and to protect the security of information and assets.

11. We are committed to protecting the safety and security of all staff, and will ensure any proposed security measures align with the DPMC Health and Safety Policy and relevant legislation.

12. We will respond to security threats and identified risks quickly, effectively, and professionally, including making referrals to other agencies if appropriate.

Information Security

13. We will ensure that all official information held by DPMC and NEMA is classified and handled appropriately, in accordance with the Protective Security Requirements Classification Handbook and the Classification Quick Guide.

14. All information held by DPMC and NEMA will be subject to effective security management to protect national interests, personal privacy, and departmental reputation.

15. We will maintain formal processes alongside CASS to ensure the security of IT systems used by DPMC and NEMA, in line with PSR and the New Zealand Information Security Manual (NZISM).

16. We operate to a clear-desk policy to ensure all work-related documents are handled in accordance with the Classification Quick Guide and kept out of sight when not being used, including where required the storage of official information in access-controlled lockers and/or drawers.

17. The clear-desk policy applies to staff while working remotely offshore, at home, and shared office spaces.

Responsibilities

Role	Responsibilities
Chief Executive (CE)	The CE has ultimate responsibility and accountability for the security of DPMC's people (including staff and visitors), information and assets and ensuring the department maintains effective security management arrangements.
Chief Security Officer (CSO)	The CSO is appointed under the delegated authority of the CE and is responsible for all security policies and oversight of protective security practices. The CSO is also the delegated accreditation authority for all DPMC ICT systems.

Role	Responsibilities
Deputy Chief Security Officer (DCSO)	The DCSO is appointed under the delegated authority of the CE and is responsible for the ‘classified’ environment. The DCSO also provides additional oversight of security practices and assumes responsibility for security if the CSO is unavailable.
CASS Chief Information Security Officer (CISO)	The CISO is appointed under the delegated authority of the CE and is responsible for leading and overseeing information security within DPMC and NEMA. The CISO is also responsible for ensuring compliance with information security policies and the NZISM.
CASS IT Security Manager (ITSM)	The ITSM is reponsible for ensuring that the department’s information security objectives are met. They oversee ICT risk management and certification processes and maintain the operational information security management framework.
Board Subcommittee	The Board Subcommittee supports the CSO to provide assurance to the CE and DPMC’s Executive Leadership Team of the effectiveness of the security work programme and progress against the implementation of PSR.
Strategy, Governance and Engagement (SGE)	The relevant team in SGE will be responsible for ensuring the PSR is implemented appropriately and effectively, leading continuous improvement of integrated security management across DPMC, and ensuring delivery of mandatory PSR reporting requirements.
People Leaders	People leaders will ensure that all staff receive security induction and refresher training and understand the requirements for security incident reporting. People leaders will promote and demonstrate good security practice and actively monitor identified/emerging security risks within their business group or team.
Staff	All staff will follow DPMC/NEMA’s security policies, procedures and guidelines and complete security training and education as required. Staff will take all necessary steps to ensure the security of themselves and others, and of information held by the DPMC and NEMA.

Related policies, guidance, and information

Protective Security Requirements

Protective Security Framework

DPMC Health and Safety Policy

New Zealand Government Security Classification System

Handling Requirements for Protectively Marked Information and Equipment

New Zealand Information Security Manual (NZISM)

Item 03

Treasury Acceptable Use of Technology Policy

Version	3	**Contact**	Information Technology Security Manager
Status	**Current** – in effect 31 August 2023	**Approved**	Chief Information Officer 31 August 2020
Owner Group(s)	Corporate Shared Services	**Owner(s)**	Chief Information Officer
iManage	2491514	**Due for Revision**	31 August 2025
File Reference	MG-0-10	**Revision History**	Register (1934553)

Please do not make unauthorised electronic copies or new versions (drafts) of this Treasury corporate policy. Contact governance&accountability@treasury.govt.nz, to have new drafts initiated and recorded in the Register of Treasury Corporate Policies (1934553).

Contents

Purpose

This policy relates to the acceptable use of Information Technology (IT), associated applications (including web-enabled tools), and third party systems in the Treasury. The intention of this policy is to provide further detailed guidance to support the Treasury Corporate Security Policy.

This policy outlines the minimum requirements for the acceptable use of technology, including what constitutes reasonable personal use of departmental IT resources. This helps to protect and manage the integrity of IT systems and information; to minimise productivity loss; and to protect the Treasury's reputation from being adversely impacted by inappropriate IT use.

It also aims to ensure the Treasury meets legal obligations and government policy requirements (including any changes to these that post-date the date of this policy) concerning the use, integrity and protection of information including, without limitation, state sector employment, privacy and human rights, health and safety, official information and public records, copyright, and prohibitions on the use of information that would constitute a crime.

Scope

This policy applies to everyone in the Treasury, including seconded, contracted and temporary staff and consultants and visitors, who accesses any Treasury technology, equipment, systems, information and data, regardless of classification ("people").

This policy takes into account Government Chief Digital Officer/Government Chief Information Security Officer (GCDO/GCISO) rules and guidance, supports the New Zealand Government Security Classification System and contributes to the implementation of the Government's Protective Security Requirements (PSR) and New Zealand Information Security Manual (NZISM).

Definitions

- **Incident:** An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
- **Information/official information:** official information is any information that is held, developed, received, collected or spoken by or on behalf of the Government.
- **IT Equipment:** Any equipment to support the acquisition, processing and storage of information.

Requirements of access and acceptable use of Technology

As a condition of access to Treasury IT systems and equipment, all users agree to comply with the provisions set out in this policy and to seek up to date security advice on how to protect IT systems and official information.

This policy is regularly reviewed, communicated, and updated according to its review schedule or when the security environment or business requirements change. All security procedures should be regularly reviewed and communicated as well. These are all designed to make security requirements clear and to promote security awareness.

You must

- use IT systems and equipment appropriately and legally, in compliance with corporate policies, and in a way that withstands public scrutiny.
- keep access details such as passwords or access tokens for accessing Treasury or third-party systems confidential and not share with any other person.
- take reasonable steps to protect all the Treasury IT systems and equipment and information in our care from loss, damage, unauthorised disclosure and misuse, and will be held personally accountable for any carelessness or negligence.
- create and retain full and accurate records as described in our Information and Records Management Policy. All information (including emails, documents and other recorded information) created or received by the Treasury in the course of our work is official information and a public record as defined by the Public Records Act 2005.
- not use IT systems for unauthorised duplication or dissemination of information, including unauthorised downloading or forwarding of copyright information without the copyright holder's permission.
- include a classification on every piece of official information you create, to protect it from risks to privacy, policy or national security and to limit its access to only those who have a legitimate 'need to know' as part of their role. There is guidance on how to do this on our Information security page on Huihui.
- use only approved Artificial Intelligence (AI) applications or systems and this must be inline with the Government Chief Digital Officer's (GCDO) Responsible AI Guidance for the Public Service. Parata is currently approved for use Paerata User Guidelines 2024(4961339.2).docx - iManage Work

Your user account activity is logged and actively monitored including through services provided by authorised third parties. Such third parties can access information processed by and stored on Treasury technology platforms when formally requested to do so by the Treasury.

If you become aware of an actual, or suspected, security incident, then you must immediately report it to via the See Something - Say Something portal. This includes the loss or suspected compromise of IT devices, and suspicious email links or phone calls.

Treasury IT systems access

Access to the Treasury IT systems must be authorised by a manager as part of the on-boarding process via the Shiva system. Standard user account access will be granted, unless special access rights or restrictions are required.

You must

- use in a responsible manner the user accounts you've been granted, for Treasury IT systems and/or third-parties, and account for all the activity relating to them
- select a unique password for each account that meets the system password composition requirements
- keep all account passwords private and never share them with any other person

You must not

- attempt to gain unauthorised access to the Treasury IT systems, or damage or alter any software components of the Treasury's network or systems
- use anyone else's user account
- use systems that are logged into by someone else
- use unapproved Artificial Intelligence websites or applications

Reasonable personal use

Your personal use of Treasury-supplied systems and equipment should be reasonable, in terms of both frequency of use and time, and must be consistent with the Code of Conduct and the Treasury Security Policy. It must not interfere with your duties or work obligations or put unreasonable load on Treasury's network and or systems. If you have any concerns or questions, check with your people leader.

Personal use of the Treasury IT systems and devices is at your own risk. The Treasury accepts no liability for loss or harm to people as a result of personal use of the Treasury IT systems and devices.

Personal use of Treasury Email accounts for external websites and third party services is not permitted. This is to reduce the risk of a third-party data breach.

The Treasury does not guarantee privacy for any information created, stored or transmitted through personal use of the Treasury IT systems and equipment.

IT devices and device connectivity

Installation and use of IT equipment

You must receive approval from the Information Technology Security Manager (ITSM) before connecting non-Treasury owned equipment to IT systems, networks or devices. The ITSM will conduct a security risk assessment prior to the equipment being connected.

If you require a specific device in the office for health and safety reasons, talk to your manager first. Requests for IT equipment should then be logged in the CSS Service Portal , or to facilities@treasury.govt.nz for non-IT equipment or a workstation assessment.

Personal devices (mobile phones, computers or tablets) may be connected to the Treasury Guest Wi-Fi (Rangatira), but must **not** be used for creating, storing or processing Treasury information except through authorised applications. Personal devices with authorised applications must be kept up to date and have password/PIN protection to the same level as corporate devices.

Authorised applications consist of the Microsoft suite but are subject to Security and CSS IT Management endorsement if not located under the Company Portal Application for Mobility or ServiceNow for Desktop Applications. All Microsoft applications will require a second level of verification (two factor authentication) prior to accessing, for this step the "Microsoft Authenticator" application should be installed. All approved applications can be found on our ServiceNow Portal for further guidance.

It is ok to plug personal devices in for charging purposes. If you are unsure how to set your device to charge only, please check your user manual first. Please do not plug in any untrusted or suspicious USB or external storage devices into your work device.

Software and protection from malicious viruses

The Treasury systems and devices are well protected and software updates are automatically deployed to keep information and systems safe. You will usually receive notification messages to restart devices to enable updates and you must follow this instruction as soon as possible.

You should exercise appropriate caution when visiting websites or opening email attachments, to minimise the risk of damage by viruses and other malicious software. There is guidance on how to do this safely on our Security pages on Huihui.

If you mistakenly open a suspicious attachment, click on a link, or receive suspicious emails or phone calls you must notify the CSS Service Desk immediately and report the incident via See Something Say Something

Only software that is authorised by CSS I&T may be installed on Treasury IT equipment. Do not download software or applications (including executable files) from the internet
or saved from other electronic devices onto IT systems. You can find a list of products approved for use on Treasury systems on our ServiceNow Portal or within the Company Portal Application on your mobile phone.

You must use only cloud and third-party services that Chief Information Officer has approved for creating, storing or processing the Treasury's information. This will ensure that using such services will not expose the Treasury to excessive risk. The Treasury has developed its own Generative AI tool, Paerata, using Azure OpenAI within the Treasury's Microsoft cloud environment. As Paerata has been developed in a way that contains inputs and outputs within Treasury's access only, the Treasury has developed new guidance that is more permissive than if the tool shared information external to the Treasury. Therefore, use of any other GenAI must comply with the existing Treasury guidelines: Safely Using Generative AI

If you wish to use an application that does not appear on our ServiceNow Portal or Company Portal, please log a request via the iCAN Process where this will be reviewed by the Security and CSS IT Management team for possible endorsement

The Microsoft Office 365 platform allows users to create their own applications and add-ins for existing applications. If you wish to develop an app or add-in, you must follow the IT Applications Development Policy.

Lost or damaged equipment

You must report the loss or suspected compromise of any IT device to the CSS Service Desk immediately, tell someone more senior, and must report it to security.team@treasury.govt.nz

Send all reports of damage and requests for IT repairs to the Service Desk. Do not try to repair the device yourself or take it to an external provider. Contact the Service Desk to arrange to return the damaged device directly to them or to return a device that you no longer require.

Working away from the office

Treasury-approved devices, such as laptops, tablets and mobile phones, may be used for business-related activity outside the office. Refer to our Tāne Whakapiri 'new ways of working' information and guidance on working away from the office on Huihui.

Power down your laptop or tablet when not in use if you are taking it out of the office, to enable the Bitlocker encryption protection.

You should keep Treasury devices under direct supervision when outside the office. If it is not practical to do so, they must be powered off and stored as securely as possible. Out of sight in the locked boot of car is ok for short-term storage (e.g. while shopping) but for longer periods or in high-risk areas, it is recommended to store them out of sight at home.

You need to be alert to the potential for compromise of information when using equipment outside of the office, ensuring that it is not overlooked or overheard by unauthorised persons. An example is working on the train on the way to or from work where other people may be able to see the documents you are reading.

You can connect to the Treasury network remotely if you can do so through a trusted Wi-Fi network. A trusted Wi-Fi network is one where you are confident of the security status of the connection (for example, your home Wi-Fi, NOT public Wi-Fi available in cafés or hotels). If the security of a Wi-Fi connection cannot be assured, you must hot spot off a Treasury mobile phone or your personal phone.

Overseas travel

Contact travel@treasury.govt.nz prior to travel to receive the necessary travel briefings and details of current IT security requirements and advice. The Travel page on HuiHui has some general information.

You may carry Treasury devices overseas only if it is essential for business purposes and necessary security requirements are met, as determined by the locations travelled to and known security risks at the time of travel.

Approval to take devices overseas:

1. Management: Approval must be granted from your people leader to ensure there is a valid business need and costs will be covered by the organisation.
2. Security: Approval must be granted from the Chief Information Security Officer to ensure any country specific guidance can be issued and travel itinerary will be documented for information security monitoring purposes.

Whilst traveling overseas you must:

- Maintain positive control of your devices and store them property and safely. When left unattended make sure they are secure and locked in the hotel safe.

- Powering devices off when not in use and making sure that any updates are applied before leaving.
- Only connect devices to trusted wireless networks and tether/hot spot from your work phone if you are unsure.
- Carry your device as hand luggage and always know where it is when travelling.
- Report any issues, ether physical or technical, when you return

It is recommended that all mobile devices are connected to a trusted Wi-Fi to reduce the possibility of using excessive data use. Mobile Application and Operating System updates should be completed whilst connected to Wi-Fi where possible.

Prohibited and inappropriate use

You must not disable, weaken or attempt to disable or weaken any security settings or feature on your authorised account/s or devices (e.g., disable the anti-malware or elevate your access privileges)

Treasury IT systems and equipment must not be used in any of the following ways:

- in contravention of this policy.
- to endanger or cause distress to any other person (such as through harassing, bullying or otherwise intimidating behaviour).
- to criticise unfairly or defame any person or business.
- to solicit for personal gain or profit, where any gain or profit is more than minor.
- for any illegal purposes (including but not limited to downloading music or publications).
- for any purpose that is not consistent with our Code of Conduct or the Code of Conduct for the State Services (Standards of Integrity and Conduct); or
- to generate, access, or send pornographic, sexually explicit or offensive material.
- To breach or attempt to breach the security of Treasury and non-Treasury systems

Policy exceptions

Exceptions from this policy (such as temporarily seeking to transfer a file type that would normally be blocked or quarantined) may be granted to meet new or changed business requirements when there is a justifiable business purpose. Refer to the Treasury Security Policy for details of the exception approval process.

All exceptions must be reviewed, risk assessed and approved by the Chief Information Officer.

References

- Public Records Act (2005)
- New Zealand Protective Security Requirements (PSR)
- New Zealand Information Security Manual (NZISM)
- Code of conduct for the State Services - Standards of Integrity and Conduct
- Code of Conduct Policy (Treasury:1963916)
- Information and Records Management Policy (Treasury:1096384)
- IT Applications Policy (currently in draft – contact infosec@treasury.govt.nz)
- Media Policy (Treasury:2274494)
- Social Media Policy (Treasury: 4360107)
- Security Policy (Treasury: 904973)
- Travel Policy (Treasury:2543173)
- How to Protect Official Information (Treasury:831445)
- Guidelines for using Paerata, the Treasury's GenAI tool (4961339)
- Information Security on Huihui
- 'Our future focused workplace' on Huihui
- Security on Huihui
- Security + You module on Tipu
- SeeMail help – on Huihui
- Travel page on Huihui
- Wellbeing Assistance Policy (3045909)
- Working Remotely page on Huihui