Te Kāwanatanga o Aotearoa
New Zealand Government

Security advice for 2023 Election Candidates

Ensuring your safety and security during
your candidacy for the 2023 General Election.

August 2023

2023 Version 1.0

Contents

Introduction

It is important that all 2023 General Election candidates understand and consider the potential risks related to privacy, cyber security, personal security and foreign interference that may arise due to election related activities.

The security advice in this document has been put together to provide visibility of potential privacy and security issues, and to explain mitigations that can be put in place.

Contact details and additional resources and links are available at the end of each section.

This advice was produced by a sub-group of the Major Events Security Committee, comprised of

- CERT NZ
- Department of the Prime Minister and Cabinet
- Electoral Commission
- New Zealand Security Intelligence Service
- National Cyber Security Centre
- New Zealand Police
- Parliamentary Service
- Office of the Privacy Commissioner

Privacy Considerations

The issue

There are various potential privacy risks from election activities that should be considered.

Think about how your information may be exposed to the public:

- Social media accounts
- Cars with election livery
- Election advertising which requires the address of the promoter
- Personal details
- Business cards
- Mailing lists

Having publicly available information about you online could lead to the following:

- Phishing attempts (including via text message) to harvest your log-in details or banking details
- Unauthorised access to online platforms or internal systems
- Online scams delivered by messaging platforms such as Facebook, Instagram, or Whatsapp
- Public disclosure of your, or your family's, personal information
- Whānau and friends' details can be found and revealed
- Other targeting which is explored in further detail throughout this document

Remember that information can remain online for a long time and after the election neglected accounts can lead to the same risks happening over the long term.

What you can do:

Personal vs public profiles

Public-facing profiles and collateral, on and offline, are a rich source of data and information for those who want to collect it for both legitimate and illegitimate purposes. As a public figure, you're advised to separate your personal accounts completely from your public ones.

- Turn on privacy functions on all your personal accounts (for example, limiting who can interact with you online).
- Consider using a new phone number or PO Box, especially if these are going to be linked to a public profile.
- Create completely separate email and social media accounts for your public campaign.
- Ensure your accounts are protected with long, strong, unique passwords and two-factor authentication.
- Ensure you have up-to-date anti-virus software installed on any device you use to access your emails.
- Don't open attachments or click on links in emails or social media messages from strangers or if you're unsure that the sender is genuine.

If you discover that someone is impersonating you online, immediately contact the platform (such as Meta) and CERT NZ. If you believe your privacy has been breached you can contact the Privacy Commission.

Protecting the privacy of others/your obligations under the Privacy Act 2020

While it's important to keep yourself safe from privacy risks, it's also essential to consider any potential privacy risks to others, and your obligations under the Privacy Act 2020, including how you handle and dispose of information.

Some key things to consider are:

- Providing guidance for staff and volunteers about their obligations under the Privacy Act 2020 when it comes to handling voter data.
- Having a privacy breach plan ready in case of a cyber incident or any other breach of voter information.
- Implementing a data retention policy if party officials or volunteers are gathering information about voters. This should include how that information will be held, when it will be disposed of, and then how it will be disposed of.
- Ensuring you know who your appointed privacy officer is.

More information

For more advice visit the Office of the Privacy Commissioner website

Key contacts

AGENCY	PURPOSE	CONTACT
CERT NZ	General enquiry	0800 CERT NZ (0800 2378 69)
		info@cert.govt.nz
	Report an incident	https://www.cert.govt.nz/individuals/report-an-issue/
Privacy Commission	General Enquiry	0800 803 909
		enquiries@privacy.org.nz
	Make a privacy complaint	https://privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/complaint-self-assessment/

Personal Security

The issue

When standing as a candidate you will be in the public eye, which can bring scrutiny and attention from a wide range of sources. It's important to consider this, and plan how you can assure the safety and security of yourself, your supporters, and the public.

What to do

Personal security considerations

- While you are a candidate (and if you are successful in being elected) you will need to have a heightened awareness of your personal and physical security. This will continue if you are successful in being elected.
- Consider the security arrangements you have in place for your home and business and whether they need updating.
- You are more likely to be recognised and approached in public.
- Putting yourself forward as a candidate for election involves interacting up close with members of the public in ways that may be unpredictable.
- Having a robust physical safety plan allows you to engage confidently while also being prepared to expect the unexpected.
- Your personal security and that of your team will depend on planning, maintaining good situational awareness and making considered and informed decisions.
- Consider travel arrangements and how you will mitigate associated risks.
- Be aware of your information security in all areas, such as any sign writing on your personal vehicles, personal details and information readily available to the public through signage, public databases and social media.
    - This applies to family, supporters and close friends whose information may be accessible through your own personal profile. Now is a timely reminder for them to reassess the accessibility of their personal information.
- Consider the use of security professionals to provide advice, and draft plans or assessments of your individual security requirements.

Personal security at events

Hosting an event

As the organiser you have some responsibility for ensuring your safety, the safety of attendees and members of the public. Pre-planning and having a safety-first mentality are crucial to having a safe and successful event.

Site venue

- It is advised to always pre-book a location you intend to use, as others patronising this space could interfere with your event.
- Utilise traditional media, social media and local connections to scope prospective and planned venues.
- Visit the site beforehand to learn more about the venue and ensure it is appropriate:
    - If you have booked a private venue meet with the building/location venue manager.

    - If the event is being held in a public place speak with the local council, or appropriate local administrative body about your plans.
- Talk with appropriate venue staff about evacuation plans should a natural event or unplanned incident take place.
- Plan entry and multiple exit points in advance should you need to leave quickly.
- If you anticipate attendance that may affect pedestrian or vehicular traffic talk with your local council about implementing a traffic management plan.
- Consider visiting the site immediately prior to your event and have contingency plans if you have concerns about security.
- Have a plan in place should protestors attend and disrupt your event. Consider engaging security guards as a further prevention measure to enhance safety for all attendees.

Hosting a safe event

- Prior to your planned event, practice responses to a natural disaster or other threats to ensure you and your support people are all aware and familiar with these safety plans.
- Provide a safety procedure speech covering evacuation process and rally point at the start of your event. This will ensure all participants are informed and will help aid a more effective response if something does occur.
- At the event secure all personal belongings or have them looked after by a trusted associate. Don't leave valuables, personal items or sensitive information unattended.
- Utilise exit signs and emergency signage in the event of an evacuation or other emergency.
- Make sure all signage is not in breach of local bylaws, or creating hazards or obstructions for pedestrians or vehicles.
- Do not block public thoroughfares, footpaths or roads.
- If you or your supporters are driving to the event, park in a location that is both safe for others and able to be used if you need to leave quickly. Ensure when leaving your vehicle it is locked, and you have a spare set of keys easily accessible.

Communications

For all events you participate in, either as a host or attendee, make sure you have:

- Created a working and tested communication plan.
- Ensured your cell phone is fully charged, functioning normally, and has sufficient credit to check in with your support persons as planned.
- Saved all contact peoples' details to your phone.
- Tested your event location has an adequate cell or data connection.

- Nominate a safety person/s who can act should an emergency occur. This person should know:
    - Your itinerary
    - Event location and duration
    - Event organisers/key personnel contact details
    - Your essential contacts to notify in an emergency

More information

For more safety advice visit: *https://www.police.govt.nz/advice-services/personal-and-community-safety*

Key contacts

AGENCY	PURPOSE	CONTACT
NZ Police	In an emergency	Call 111 in an emergency
	Report an incident	If an incident has already happened and there’s no immediate danger, call 105 or visit *105 Police Non-Emergency | New Zealand Police*

Cyber Security

The issue

As a candidate you will be interacting with more people online than usual, which may present an increased risk to your cyber security. You should consider the advice below and ensure you have taken steps to secure your information online.

Good cyber security practices help you protect the things and people that are important to you. While there's no fool proof way to prevent an cyber incident or data breach, there are things you can do that will help to lessen the risk.

What you can do:

Two-factor authentication

Two-factor authentication – also known as two step or 2FA – is the simplest and most effective way of securing your online accounts.

After logging in, the 2FA system will ask for an extra piece of information. This is usually a code sent to your phone via text or code generating app (sometimes called a token). On your device it might also be a face ID, fingerprint, or PIN.

This means even if your password is leaked, there is still a second level of protection.

We recommend having 2FA on wherever you can. This includes your devices – laptops, tablets, smartphones – and your online accounts:

- Email
- Social media
- Internet banking

Strong, unique passwords

Having a strong and unique password for each of your accounts is solid start for anyone wanting to increase their cyber security.

- **Make your passwords long and strong:** A long unique password for each account seems like a lot of work but it pays off. If your password is leaked in a breach, or otherwise discovered, then you know attackers can't use it to get into any other accounts.

- **Don't use personal information to create your passwords**: Passphrases – four or more random words in a string with special characters and numbers – are a good way to create memorable passwords that are tough to crack (for example: RainingDalmations&17KakarikiCatfish).

- **Use a different password for every online account you have.** Doing so ensures that if one of your passwords is leaked or otherwise discovered, it cannot be used on any other account.

- **Use a password manager to store complex passwords**: A password manager is a good way to keep all those long passwords organised, all you need to remember is the password to get into the manager. Some systems have built-in managers, such as Apple and Google, but there are also a range of other password manager apps available. You can also consider writing them down in a notebook and keeping that in a secure location.

Keeping your devices secure

Most people run their lives through digital devices and it's vital to keep them secure.

- **Turn on automatic updates** to ensure you're updating your devices with new software. Sometimes the purpose of these updates is the release of a new feature, but often they are about fixing weaknesses or vulnerabilities on your device.

- **Be alert to your device behaving unusually:** this can include the battery running flat quickly, the device running hotter than normal or unexplained increases in data consumption. It might be nothing and your device just needs to be turned off and on again, but it could also be something malicious, and if you suspect that's the case, either take the device to a security professional or report it to CERT NZ.

- **Physically hold on to your hardware**: losing a device is a common way for data or credentials to be compromised. Do not give out your device's log in passwords and ensure you have location and tracking services enabled. This will also allow you to remotely wipe it in an emergency.

- **Don't connect unknown devices:** a large portion of malware is delivered by removable media like USB sticks. If you are given or find a USB device, it's best not to use that at all or to hand it to a security professional to ensure it's safe.

Personal vs public accounts

Social media accounts have become a rich source of data and information for those who want to collect it for both legitimate and illegitimate purposes. As a public figure, you're advised to separate your personal accounts completely from your public ones.

- **Turn on privacy functions** on all your personal accounts (limiting who can interact with you online).
- **Create completely separate email and social media accounts** for your public campaign.
- **Consider using a new phone number** for your public accounts.

The most important online asset most you have is the email account that password reset links to go when you have forgotten your password. Ensure this email account is protected with all the advice above.

Keeping your personal accounts locked down will help keeping private knowledge out of the public sphere.

Remember that these accounts will exist after the election. Consider deactivating the public accounts if they aren't needed, but *not* deleting them – this means no one can take the username afterwards and pretend to be you.

If you discover that someone is impersonating you online, immediately contact the platform (such as Meta) and CERT NZ.

More information

- Use two-factor authentication to protect your accounts | CERT NZ
- How to create a good password | CERT NZ
- Keep your data safe with a password manager | CERT NZ
- Keep up with your updates | CERT NZ
- General considerations using social media apps
- Assessing the risks of social media applications on government mobile devices | National Cyber Security Centre

Key contacts

AGENCY	PURPOSE	CONTACT
CERT NZ	General enquiry	0800 CERT NZ (0800 2378 69)
		info@cert.govt.nz
	Report an incident	https://www.cert.govt.nz/individuals/report-an-issue/

Foreign Interference

The issue

Foreign interference is an act by a foreign state, often through someone working on its behalf (a proxy), intended to influence, disrupt, or subvert New Zealand's national interests by deceptive, corruptive, or coercive means. It can be divided into two main forms: political and societal.

- Political interference may target governance systems (including the electoral process), the information environment, and politically influential people.

- Societal interference may target individuals, communities, businesses, social and activist groups or the information environment.

This guidance is designed to make you aware of *political interference* and how this might affect you and your staff, as you stand as a candidate for the 2023 General Election.

Why might you be targeted?

As a member, or potential member, of the New Zealand Parliament, you and your staff are of interest to foreign states.

In your role, either as a candidate or elected official, you are in a position of influence with access to a wide range of sensitive information. Additionally, your ability to steer policy and your access to other people in positions of power could make you an attractive target. New Zealand's position on international issues and our international relationships may also be of interest. There may also be particular political issues you hold views on that are sensitive to a foreign state which wants to amplify or undermine these.

How might you be targeted?

Many interactions with foreign intelligence services or those working on their behalf, will seem like normal networking opportunities. As noted above, foreign intelligence services often use third parties to conduct foreign interference; these could include diplomats, academics, business people, military personnel, and media organisations.

There are a range of ways you may be targeted, from attempting to draw information of value through targeted conversation, to more technical methods, such as interfering with your electronic devices or using cyber exploitation.

Why should you care?

Any influence a foreign state actor manages to apply over New Zealand's Parliament or other elected bodies could damage New Zealand's democratic process, undermine New Zealand's commercial edge over a competitor, compromise negotiating positions, or damage our national security. Moreover, there is potential your reputation, the reputation of your party, or New Zealand could be negatively impacted. You could also be put in a position which leaves you open to pressure or coercion.

What you can do

Keep yourself safe

Approaches by foreign state actors are unlikely to be obvious, however the below advice is intended to help protect you and your staff from being compromised if you are contacted by a third party:

- **Be vigilant:** is their interest unusual or persistent given your normal interactions? Look out for SOUP approaches: **S**uspicious, **O**ngoing, **U**nusual or **P**ersistent.
- **Check their identity and connections to foreign governments:** research any unknown individuals online and check whether the organisation they represent exists.
- **Take a trusted colleague with you when meeting someone new:** being in the presence of another person can make it harder for you to be compromised.
- **Conduct due diligence on any offer you receive:** donations and gifts are a way that foreign states have attempted to use to build influence and leverage in New Zealand's democracy. Ensure you comply with transparency rules and legislation.

More information

- For more information, go to www.protectivesecurity.govt.nz.
- For more detail on how you may be targeted and ways to keep yourself safe, read the Protective Security Requirements resource *Espionage and Foreign Interference Threats: Security Advice for members of the New Zealand Parliament and Locally Elected Representatives*
- If you believe you have been targeted, or want to report concerning behaviour, please use the reporting mechanism found here: Providing information | New Zealand Security Intelligence Service (nzsis.govt.nz).

Key contacts

AGENCY	PURPOSE	CONTACT
NZSIS	General enquiry	0800 SIS 224 (0800 747 224)
	Report concerning behaviour or an incident	Use NZSIS public contribution form here