Trusted Research

Guidance for Institutions and Researchers

PSR | Protective Security Requirements

Science New Zealand

Te Pōkai Tara Universities New Zealand

01 Protecting your research

Protecting your research when collaborating with international partners

Trusted Research aims to help New Zealand's world-leading research and innovation sector get the most out of international scientific collaboration while protecting their intellectual property, sensitive research, and personal information.

Securing the integrity of New Zealand's system of international research collaboration is vital to the continued success of our research and innovation sector.

This guidance is particularly relevant to researchers in STEM (science, technology, engineering, and mathematics), innovation, dual-use technologies, emerging technologies, and commercially sensitive research areas.

Trusted Research:

- Outlines the potential risks to New Zealand research and innovation
- Helps researchers, New Zealand universities, research organisations, and industry partners to have confidence in international collaboration, and make informed decisions about potential risks
- Explains how to protect research and staff from potential theft, misuse, or exploitation.

This guidance had been produced as a collaboration between New Zealand's research and university communities and Protective Security Requirements.

02 New Zealand's approach to research

New Zealand's thriving research and innovation sector attracts funding and investment from across the world. A significant amount of New Zealand research is a product of international partnerships[1].

- New Zealand has an open and collaborative research and innovation system, and values academic freedom and research conducted independently by individuals and organisations.
- The government is actively seeking to increase the international connectedness of the research and innovation system.
- We welcome international students and research collaborations.

There are risks with international partnerships that should be identified and managed to prevent damaged reputations, lost intellectual property (IP), and harm to New Zealand's national interests.

1 More than 50% of scholarly output in New Zealand occurs with international co-authorship: "Research, Science and Innovation System Performance Report 2018"

03 Why protect your research?

Whether you hold sensitive medical data for genetic research, or commercially sensitive information for yourself or on behalf of a research sponsor or business, protecting your research from misuse or exploitation is important to you, your institution/ organisation, and your partners.

All research can be at risk, but joint research and applied research are particulary vulnerable.

Joint research can be misused by organisations and institutions in nations with interests and ethical values that are different from our own. Joint research can provide opportunities for people with hostile intent to access expertise, IT networks, and research. These hostile activities may undermine New Zealand's system of international research collaboration. This system is integral to the success of New Zealand research and, ultimately, global scientific progress.

Applied research is vulnerable to exploitation, especially if you're trying to solve a specific problem or develop a commercial application. In these cases, the consequences of research outcomes being exploited could be considerable. For example, your research could be misused or you could lose your IP.

For individual researchers, interference with (or loss of) research is likely to limit your ability to publish first or take credit for the resulting IP. This could negatively affect your reputation and ability to demonstrate the impact of your research.

WHO ARE YOU AT RISK FROM?

A foreign state actor may:

- seek opportunities to develop a research and innovation base that increases its economic, military, and technological advantages over other countries
- prioritise the stability of its regime and focus on suppressing internal dissent, political opposition, or media freedoms
- seek to deploy its technological and security advantages against its own people to maintain the stability of the regime.

HOW MIGHT YOU BE TARGETED?

Foreign state actors are targeting New Zealand universities and organisations to steal personal data, research data, and intellectual property. Possible reasons for this targeting include furthering military, commercial, and technological interests.

International collaboration offers foreign state actors the opportunity to benefit from research without the need to carry out traditional espionage or cyber compromise activities. Collaboration can provide these state actors with access to people, IT networks, and participation in research — research which may be sensitive or have sensitive applications.

A foreign state actor may target you as an individual researcher. You could also be targeted by an academic institution or overseas business asking you to undertake research of strategic benefit to their country.

Traditional academic engagement provides an easy route for a foreign intelligence service to gain access to you while at events such as conferences or on research placements.

You might also be targeted through a cyberattack, such as a phishing email, which might try to trick you into revealing sensitive information or contain links to a malicious website or infected attachment.

WHAT ARE THE RISKS TO YOUR RESEARCH?

Competition and plagiarism will be familiar concerns to many working in the research and innovation sector. If a foreign state actor obtains your research, whether through legitimate means or not, you and your research could be affected in several detrimental ways.

Lost trust

Conducting research in a way that maintains the trust of the public and private industry is essential to the continued success of the research and innovation sector. To access sensitive data and funding, researchers need to show they can maintain this trust. If the data on which your research depends is stolen, not properly protected or misused, your institution may not be trusted with such data in the future.

Compromised integrity and legal compliance

As well as the ethical framework surrounding research, you must comply with any relevant legislation and regulation. For example, the Customs and Excise Act 2018 sets out New Zealand's export controls. Some of these controls apply to military and dual-use goods and technology, which may affect some types of research. Failure to comply with this legislation may expose you to criminal charges or civil action.

Over-reliance on a single source of funding

Over-dependence on a single source of funding is a significant risk for institutions and even for departments within institutions. This 'cumulative risk of investment' is present whether the funding is from a single organisation or a single nation. Such over-dependence creates the opportunity for funders to exercise inappropriate leverage across a range of areas. For example, a funder may pressure your organisation when you seek to protect freedom of speech or even academic freedom.

Lost funding opportunities and financial losses

You and your institution may find it difficult to attract future funding if it becomes known that a foreign state has stolen your research. Foreign states may not protect data privacy as required in New Zealand, or they might seek to misuse your research for unethical purposes. You could face a financial loss if a competitor were to access research data or information owned by your sponsor.

Damaged reputations

Reputation is critical to future success — for you and your institution. Both reputations could be damaged if it becomes apparent that another country has exploited your research for military or authoritarian purposes. You could also damage New Zealand's reputation.

HOW MUCH OF A TARGET ARE YOU?

To understand the risk of your research being targeted, identify the potential threats and the most valuable aspects of your work.

Most research will not have any sensitive application and will not cause concern, but being clear on which areas of research are sensitive is crucial.

You need to consider whether your research:

- is commercially sensitive
- has potential for patent
- is related to sensitive defence or national security technology
- could have future dual-use or unethical applications.

In most cases, as an expert in your field, you're ideally placed to judge the potential interest in, and broader application of, your research.

THINGS TO CONSIDER

Are there any potential ethical or moral concerns to do with the application of your research?

Could your research be used to support activities in other countries with ethical standards different from our own, such as internal surveillance and repression?

Are there any dual-use (both military and non-military) applications to your research?

Could your research be of benefit to a foreign state's military or be supplied to other foreign state actors?

Is any of your research likely to be subject to New Zealand export controls for military and dual-use technologies? For advice, ask the Ministry of Foreign Affairs and Trade's Exports Control Office.

Do you need to protect sensitive data or personally identifiable information? This may include genetic or medical information, population datasets, details of individuals, or commercial test data.

Is your research likely to have a future commercial or patentable outcome that you or your organisation would want to benefit from?

WHAT TO DO IF YOU'RE CONCERNED

Each university or research organisation has its own oversight arrangements for research activities. Many aspects of research and academic activity are managed by the head of faculty or a principal investigator of the research.

You need to achieve a balance between protecting academic freedom and raising awareness of issues such as cumulative risk of investment (where an institution becomes overly dependent on a single source of funding).

When you're concerned about a potential collaboration, seek the advice of the relevant institutional research office or governance board. They're likely to be the most appropriate bodies to consider the balance of risks for your organisation.

04 How to protect your research

As a researcher, there are steps you can take to protect your research, ensure you're meeting all your legal obligations, and can make informed decisions about research collaborations.

These steps should always be proportionate to the risks and balanced to support the benefits of international research collaboration.

To protect your research, consider the following three main areas.

01 Collaborating with research partners

Protecting intellectual property, making informed decisions about international collaboration, and managing cyber risks *(see pages 20 to 23).*

02 Using legal frameworks

Understanding contractual expectations, export controls, and privacy requirements *(see pages 24 to 29).*

03 Helping researchers to stay safe

Protecting your personal and research data, working with overseas researchers, and attending conferences abroad *(see pages 30 to 38).*

01 COLLABORATING WITH RESEARCH PARTNERS

Conduct due diligence

When you're considering a new research and/or funding collaboration, conduct due diligence. Include ethical, legal, and national security considerations as well as financial ones. You'll then have all the information you need to make an informed and balanced decision about whether it is safe to work with the potential partner.

Check for conflicts of interest

Check for potential conflicts of interests between research and funding partners you work with. Be open with your partners. Regularly discuss your security arrangements and their security needs, so you can avoid any conflicts.

Segregate research and control access

Where necessary to protect IP, research or personal data, ensure there is segregation between research programmes, both physically and online. Only give access to research to those who have a valid requirement. Also read 'Protect partners' on page 21.

Make security a feature of your funding proposal

Gaining funding for even short-term research can be a source of pressure and, understandably, security considerations may be secondary. However, legitimate industry or commercial partners who fund research increasingly expect assurance that the resulting IP will be protected, so that IP can contribute to their future commercial success and the wider economy. A 'secure research' offering could give prospective industry partners or sponsors this assurance while simultaneously protecting your existing relationships.

Protect partners

Without compromising academic freedoms or curtailing the benefit of collaboration, some degree of separation between areas of research may be necessary. If so, talk to your IT staff about segregating IT network access, information, and potentially people to prevent one partner seeing work that another partner is sponsoring.

Developing a good research security culture and having agreed guidelines between fellow researchers is a positive way of approaching this issue.

Demonstrate transparency and maintain visibility

As part of managing long-term research relationships, it's important to be transparent about new research commitments. This may mean speaking to your existing sponsors and discussing any potential implications for your ability to enter non-disclosure agreements.

Visibility of research across a laboratory, organisation, or university is also crucial. Laboratory or departmental meetings are key opportunities to provide such visibility, and your regular meetings with research partners could include discussions about security.

Manage cyber security for research collaboration

When entering a new international collaboration, including a funding arrangement, make sure you understand the cyber security risks and which security measures will reduce those risks.

Your IT department can support you to implement the following measures:

Controlling access

Controlling access to sensitive data is important, whether it's personal data or research data. Only allow users and partners with a valid requirement to have access to sensitive data, research, and other parts of your networks.

Ensure you understand the security of any collaborative IT platforms, especially those used by third parties, and establish acceptable use guidelines or policies for staff who'll use the platforms.

Monitoring and preventing unauthorised access

Even when sensitive data is separated and privileged access is limited, unauthorised access attempts can occur. These attempts could be from system users (insider threat) or from partners or other sources (external threat). Ensure there are effective cyber security arrangements in place to monitor and defend against unusual or malicious network activities. Don't assume your IT staff know which systems contain critical or highly sensitive data.

Taking care of security for supply chains or partner organisations

Many issues around supply chain security are due to the poor security practices of partner organisations or managed service providers. Working with overseas partners may present a higher level of risk. Develop an understanding of the cyber risks associated with partner organisations, managed service providers, and potentially vulnerable components at an early stage.

You may also wish to confirm whether your institution has implemented a recognised cyber security standard and the controls recommended in the **New Zealand Information Security Manual** (www.nzism.gcsb.govt.nz). This information will demonstrate to your partners that your institution is working towards having resilient cyber security practices.

What do you know about your potential research partner?

Universities and other organisations already invest significant effort in conducting due diligence on the financial sustainability or fraud risk associated with a research partner or funder. You should also consider whether a research or funding partner poses ethical or national security concerns. These considerations should go beyond questions of compliance (such as the export control regime) and consider reputational risks.

An internet search can provide a lot of information about a potential partner, their relationship with a state or state military, and the nature of any previous research they've undertaken.

Things to consider

- Is there any publicly available information about an organisation, institution, or entity which might give you cause for concern?
- Considering the public information you've gathered, what might be the broader application or unintended consequences of working with the potential partner in your intended area of research?
- Who does your potential partner get their funding from?
- What other affiliations does your potential partner have?
- What information is available about the level of freedom and state of law in the country where your potential partner is based?

The following resources could help inform your decision about research with specific partners:

- Country corruption index
- The Human Freedom Index
- The World Justice Project Rule of Law Index
- Any other sources of information you can find about the proposed research partner's academic institution and existing relationships with other organisations.

02 USING LEGAL FRAMEWORKS

To use legal frameworks correctly and protect your research, consider the following four areas:

Export controls

Some research activities come under export control legislation. Ensure you find out if your research is subject to export controls.

– *See page 27.*

Privacy legislation

Know and uphold your responsibilities for protecting the privacy of data and information you handle while conducting research.

– *See page 28.*

Legislation

When collaborating with an international research partner or funder, be aware of the different legislative frameworks they may operate under and how your agreements or partnership may be affected.

– *See page 28.*

Overseas Investment Act

Foreign investment may be subject to regulatory approval, particularly investment in entities with access to, or control over, dual-use or military technology. Make sure you're aware of the relevant parts of the Act.

– *See page 29.*

Understand the impact of contractual arrangements

Your research will often be subject to contractual arrangements that give greater certainty about the expectations of a research partner or sponsor. Equally, sponsors will have contractual expectations. It's critical to have a clear understanding of the impact these agreements will have on the research you undertake.

Unfortunately, it is common for disputes to arise over co-created materials. That is not to say you shouldn't collaborate. It is, however, essential that the collaborators agree upon the terms of the arrangement.

Maria Crimi Speth, *http://www.jaburgwilk.com/news-publications/warning-co-creation-hazard-ahead*

Consider institutional measures for increasing security

Academics and researchers being able to operate with autonomy is a strength of our university and research sector. However, it can also mean that your institutions have limited knowledge about the international collaborations taking place, and therefore difficulty providing support and advice.

As well as understanding your institution's international research relationships, you should consider having systems and processes in place to ensure staff members' funding relationships and any secondary employment is well managed.

Know about export controls that apply to academic and other research

New Zealand's export controls regime restricts the export of sensitive technology or strategic goods (military or dual-use goods), with the aim of:

- preventing the spread of weapons of mass destruction and undesirable entities from developing other military capabilities
- countering international threats such as terrorism
- protecting sensitive research and innovation.

The controls apply to the academic and research community as much as they do to any other exporter.

From an academic perspective, the controls may touch on several areas of academic exchange, particularly areas that might enable technology to be transferred, either physically or electronically. Failure to get a licence to export controlled goods or technology is an offence.

Routine academic and research activities that could be covered by export controls are:

- Transferring (exporting) research undertaken on behalf of an international partner to them
- Transferring (exporting) research undertaken as part of an international collaboration
- Taking presentations to international conferences which contain sufficient detail to materially contribute to the development, production or use of weapons/dual-use technologies
- Exporting certain materials, organisms, devices, machines, or other goods.

Your research office, legal department, or other relevant corporate services should be able to help with advice on export control issues. The Ministry of Foreign Affairs and Trade can also advise on whether a particular export may be covered by export controls.

Ministry of Foreign Affairs and Trade's Exports Control Office

Email: exportcontrols@mfat.govt.nz
DDI: 04 439 8227
Web: www.mfat.govt.nz/en/trade/trading-weapons-and-controlled-chemicals/

Be aware of legal obligations in foreign jurisdictions

If you're collaborating with an international partner, there may be laws and regulations in their country that you need to comply with.

Most countries will maintain some form of export control. They may have laws which restrict their institution's ability to share data or research outcomes, and their legal protections around IP may differ from New Zealand's.

Do not assume that your research partner will take responsibility for legal compliance, and be aware of any requirements that may affect your collaboration.

Your international partners may also be subject to intelligence laws that could compel them to share their data or research with military or intelligence personnel in their country.

Understand your legal obligations to protect personal information

The Privacy Act 2020 sets out the framework for how agencies collect, use, disclose, store, and give access to personal information in New Zealand.

Ensure that all data containing personal information (including research data) is protected in compliance with the Privacy Act.

For detailed information on the Privacy Act, including circumstances in which you'll have to report a privacy breach, check the Privacy Commissioner's website – *http://www.privacy.org.nz*

Consider how to both publish academic research and protect it

Freedom to publish is paramount to all academics, but it's possible to both publish and protect. In many cases, publishing first will be the way you protect your ideas. However, sometimes you may want to protect certain aspects of your work. For example, you may wish to protect research that has sensitive application or the potential for commercial opportunities.

Ask your research, legal department, or other relevant corporate services for advice on export control issues and contractual undertakings.

Processes for publishing and protecting research

At an early stage, before publishing or even speaking at a conference, consider whether any of your research could be patented or of commercial value.

Through the cycle of a research project, continually review your progress. Check whether any new developments are patentable.

If you're working with sponsors or partners and have a co-creation agreement for IP:

- regularly discuss what may be patentable
- explore an early framework agreement or process for agreeing which sensitive material you can sanitise without damaging your overall ability to publish.

In some cases, you'll need to consider whether your research has any national security implications.

Alternatively, you may not want to patent an area of research if your sponsor wishes to protect the information until they are closer to the point of commercialisation. In this case, you would be treating specific aspects of the research as 'trade secrets' and commercially sensitive. You'll need to have an agreed process for deciding what you can publish and what you must protect.

Think carefully before disclosing information when you do not have a patent.

03 HELPING RESEARCHERS TO STAY SAFE

To protect personal and research data, every institution, staff member, student, and researcher needs to pay attention to the following four areas.

Cyber security

Ensure everyone knows how to protect themselves and their research online. Good cyber security practices will reduce the likelihood of your research data being lost or compromised.

– *See page 32.*

Working overseas

Conduct a risk assessment for working overseas. Ensure your processes and lines of communication protect staff, researchers and their work.

– *See page 37.*

Overseas researchers and visitors

Make sure that overseas researchers with access to your facilities and IT network are centrally recorded as members of staff and have appropriate visas. Uphold your duty of care, understand their background, and help them to avoid conflicts of interest.

– *See page 36.*

Travel advice

When travelling overseas for a conference or longer period, consider local laws and customs, and how you'll protect IP and sensitive data. If you're relying on IT, make sure it can be accessed and used overseas.

– *See page 38.*

Follow best practice with cyber security

The nature of your collaborations, including how you use and share data and research online, will require a tailored approach to cyber security in line with your institution/organisation's security policies.

However, everyone can follow these tips to reduce the risk of your research being lost or compromised.

- Protect your email by using a strong and separate password.
- Install the latest software and app updates.
- Many apps demand unreasonable levels of permissions to access data and activity on your device. Consider limiting the number of apps you download onto work devices, and always consult with your IT department first so that you understand the risks you are exposing yourself to.
- Enable two-factor authentication on your email and collaboration platforms where possible.
- Use a password manager to help you create and remember passwords.
- Secure smartphones and tablets with a screen lock.
- Always back up your most important data (and keep the backup secure).

Your IT department can support you with any of the security measures in this section.

Take care when using USB drives

USB drives or memory cards are a quick and easy way to transfer files between organisations and people. However, there are risks.

If you're handed a USB drive, a dongle for an electronic pointer, or a mouse (for example, at a conference), do the following things before you insert it:

- Consider how trusted the source of the USB drive is (if in doubt, don't act)
- Make sure 'autorun' is disabled on your device via settings or system preferences, for example:
  - Windows 10: "Windows key + I -> Devices -> Autoplay -> Use Autoplay for media and devices (OFF)
  - MacOS just mounts the files rather than executing anything
- Make sure your antivirus software runs an auto-scan before your device accesses the data on the USB drive.

If you need to share information, consider alternative means, such as cloud storage, email or dedicated collaboration platforms.

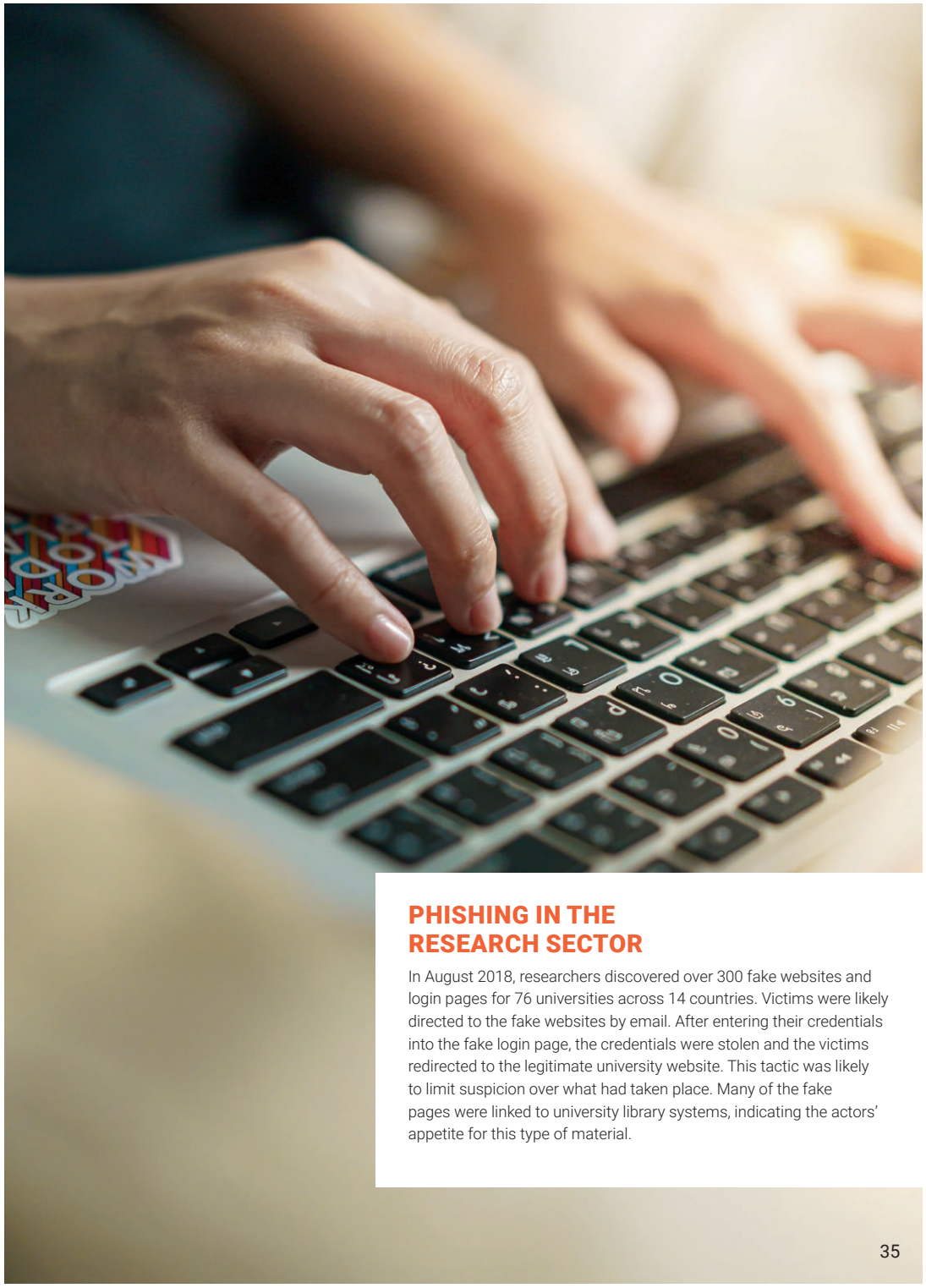
Prevent phishing attacks

Phishing attacks are one of the most common ways malicious actors obtain personal and other data, so it's worth doing whatever you can to defend yourself against them.

Phishing emails appear genuine but are fake. They might try and trick you into revealing sensitive information, or contain links to a malicious website or an infected attachment.

Taking the following actions will reduce your likelihood of being phished.

- Phishers use publicly available information about you to make their emails appear convincing. Review your privacy settings. Think about what you post and what has been posted about you, such as biographies used at conferences or by your institution.
- Know the techniques that phishers use in emails, such as urgency or authority cues that pressure you to act. Phishers may also use the visual style and branding of the organisation they are masquerading as.
- Phishers often seek to exploit 'normal business' communications and processes. Make sure you understand your organisation's policies and processes to make it easier to spot unusual activity.
- Anybody might click on a phishing email at some point. If you do, tell someone immediately (e.g. your IT team or line manager). Prompt reporting will significantly reduce the potential harm caused by cyber incidents, so don't assume that someone else will do it.



PHISHING IN THE RESEARCH SECTOR

In August 2018, researchers discovered over 300 fake websites and login pages for 76 universities across 14 countries. Victims were likely directed to the fake websites by email. After entering their credentials into the fake login page, the credentials were stolen and the victims redirected to the legitimate university website. This tactic was likely to limit suspicion over what had taken place. Many of the fake pages were linked to university library systems, indicating the actors' appetite for this type of material.

Manage your overseas researchers and visitors well

Academic and other institutions usually want to attract visitors and researchers from overseas. However, each institution needs to manage their overseas guests well so that research is protected.

Check visa requirements and ensure the correct visas are in place

If you're asked to support an application for a New Zealand visa, it's important to do due diligence on the person's suitability. This step is particularly important for international students applying for postgraduate study in certain sensitive subjects. Studying these sensitive subjects supplies knowledge that could be used in programmes for example developing weapons of mass destruction, or their means of delivery.

You must also ensure researchers from overseas have the right visas while working at your institution.

Exercise your duty of care and manage potential conflicts of interest

Every organisation has a duty of care to all staff. For visitors and researchers from overseas you also need to:

- understand enough of their backgrounds and previous work to ensure research they may access will be secure
- help them avoid conflicts of interest and uphold your security policies and processes.

Ensure visitors are recorded in your human resource system

It's vital to follow the policies and processes set by your human resources department. Anyone working on research (with access to your facilities and IT network) must have their role recorded e.g. as a member of staff, a student or a contractor. Even short-term engagements must comply with your policies.

Also consider what expectations you or sponsors may have from visitors at the end of their work, particularly to do with confidentiality and non-disclosure.

Conduct risk assessments for staff working overseas

Your broader risk assessment should include answering the following questions:

- If something happens to one of your staff when they're working overseas, who should they report it to?
- How often will you check up on whether they have any concerns or issues?
- What agreements are there with the institution that will be hosting them overseas?
- What are the rules and laws that your staff are required to comply with in that country?
- Do any of the laws in that country conflict with any of the agreements that you've made with the host institution?
- Will the work your staff do while overseas be subject to New Zealand export controls?
- Are your staff aware of the export control laws, national security laws, or intellectual property arrangements in the country that they're working in?

Protect staff going to overseas conferences: Think 'countries' as well as 'conferences'

With overseas conferences being a normal part of academic and business life, researchers will understandably focus on their presentations and potential research opportunities, rather than the security issues associated with travelling to a different country.

Part of your preparation for any overseas conference should be to:

- Consider the country that you're travelling to, and be aware of local laws and customs
- Think carefully about what information you share or present
- Make sure you understand your host's attitude to academic freedom and discussion
- Ensure that any payments you accept for attendance do not create a conflict of interest, place you in a contractual breach, or breach any organisational policies
- Be clear on the areas of research that you can and cannot talk about
- Be polite but firm if pressed to share more information
- Be aware who wants to establish further contact and cooperation
- Report any suspicions to your manager and the appropriate organisational authority
- Seek advice on whether it's safe to take your personal or work phones, computers, or other devices.

For more detailed advice, see:
Travel advice for government officials travelling overseas for business
https://protectivesecurity.govt.nz/assets/Personnel-security/2f0251f728/Travel-advice-for-government-officials-travelling-overseas-on-business.pdf

The information in this booklet is informed by research carried out by the Centre for the Protection of National Infrastructure (CPNI). CPNI is the government authority for protective security advice to the UK national infrastructure. www.cpni.gov.uk

For more information, go to:

www.protectivesecurity.govt.nz

psr@protectivesecurity.govt.nz

New Zealand Government

VERSION 1 / DECEMBER 2020

PSR | Protective Security Requirements

Science New Zealand

Te Pōkai Tara Universities New Zealand