**Module 6**
**Police Security Awareness For Community Patrollers**

A copy of this section is provided to Community Patrollers as part of their induction package whilst either working inside Police premises or having received information from the New Zealand Police.

**Introduction**
Effective security management is an integral part of Police business. When sound security is routine and normal it:

- Enhances Police service
- Maintains public and stakeholders confidence, assuring them that their interests are met and information is protected.

**General Security Principles**
All Community Patrollers are required to be aware of their obligations and responsibilities towards the protection of information they have access to, and in their possession, while conducting their duties in a safe and secure manner consistent with Police security policies. Police stations are subject to security controls to ensure the protection of staff and information.

**Confidentiality**
NZ Police discuss and hold sensitive and confidential and restricted information on site. All Community Patrollers must comply with the Guidelines for Protection of Official Information and not discuss anything they may see or hear while working.

- You must have been successfully vetted by Police
- Do not read any Official Information on screens or desks or notice boards unless authorised
- On arrival, report to the station contact or whoever is designated for the local building
- Sign in and out as applicable
- Only access areas you are authorized to have access to. Do not wander into other areas
- Make yourself aware of the emergency evacuation procedures, emergency exits, and assembly points of the station.
- Patrollers must wear their CPNZ Identification Card visibly when on Police premises.

- Any access cards must be protected and never lent to anyone. If your access card is lost it must be immediately reported to police.
- When you enter any Police stations you must comply with all security requirements

**Protective Security Requirements**
The Protective Security Requirements (PSR) outline the Government's expectations for managing personnel, physical and information security. It includes mandatory requirements that police and other government agencies must implement to ensure a consistent and controlled security environment throughout the public sector.

Further information on the PSR can be found at https://protectivesecurity.govt.nz

The PSR extends the security obligations on Police to all volunteers, contractors and other non - police working on police projects or in

police premises.

**Essential Security Awareness**
The three elements that form the basis of this security awareness module are:

1. **Information Security** - Information is one of the most valuable resources held by Police and it must be protected from unauthorised disclosure but made available to those who have a need to know it.

2. **Personnel Security** - Measures taken to ensure that before individuals are provided with access to official resources, that they have been adequately assessed to verify their identity, suitability and eligibility.

**3. Physical Security** - Involves a mix of measures that establish a series of barriers preventing or restricting unauthorised access to Police assets and enable them to detect and respond to attempted or unauthorised access within acceptable time frames.

**Element 1 - Information Security**
Information Security is concerned with ensuring that information collected and produced by Police is appropriately protected.

The term 'information' is not just restricted to paper documents. It refers to:

- Documents and papers (this includes written and printed information as well as images)
- Electronic data (this includes all kinds of electronic files on your desktop computer, IPad, IPhone, Blackberry device and email servers)
- Software or systems and networks in which information is processed or stored
- Intellectual information acquired by individuals in or out of the organisation
- Physical items from which information about the design of components or their use, could be derived
- Police information must only be made available to authorised people who have a genuine 'need-to-know' in order to do their job

**Element 2 - Personnel Security**
The purpose of personnel security is to provide a level of assurance as to the honesty, trustworthiness and loyalty of people who access government resources.

Under PSR PERSEC, Police must ensure that employees, contractors and third parties who require ongoing access to NZ Government information and resources:

- Are eligible to have access
- Have had their identity established
- Are suitable to have access
- Are willing to comply with the standards that safeguard those resources against misuse

Historically one of the biggest threats to the security of information is from individuals who for reasons of ideology, fear, personal gain or just plain indifference, compromise Police activities by the deliberate or inadvertent exposure of classified information. Personnel Security processes are designed to counter that threat.

**Element 3 - Physical Security**
Physical Security measures, such as secure cabinets, gun safes, alarms, locks, and fences are part of a multi-layered approach to the protection of official information, official resources, equipment and Police functions.

In the same way that Police is required to provide you with a safe and secure working environment to protect you from harm, they are also required to provide an environment that ensures the security of the information and secure resources they manage.

Physical security includes policies and actions that are designed to provide for the:

- Protection of Police information and assets
- Correct handling of Police information and assets
- Suitable storage of Police information and assets
- Physical barriers that control access to Police property (includes vehicles, equipment and buildings)
- Identification and response to security breaches
- A working environment for employees and people interacting with Police to be safe and secure

**The 'Need-to-Know' Principle**

The 'need-to-know' principle says that 'the availability of Police information should be limited to those who need to use or access the information to do their work'.

So, a person's 'need-to-know' is related to only the information that they genuinely need to know to perform their job. It does NOT include 'Nice to Know' or 'Convenient to Know'.

Conversely, people who do not have a legitimate 'need-to-know' should not and must not have access to the information. The 'need-to-know' principle also applies to conversations in a business or social setting.

If you use or access Police Information it is YOUR personal responsibility to apply the 'need-to-know' principle in your official duties.
Keep in mind that rank, status, seniority, or security clearance level alone DO NOT automatically allow a person access to information.

You should not give, share or discuss information with people who do not have a legitimate 'need-to-know' purpose. If in any doubt, ask your supervisor. They are there to help you.

The 'need to access' principle is similar to 'need-to-know' except that it applies to someone's potential access that provides the opportunity to gain information which the person does not have a 'need to know'.

It is relevant to determining who has access to things such as the keys or combinations to secure rooms or containers,to secure folders or applications on ICT systems through administrator account privileges for the particular program.

**Security Breaches**

A breach of security that results in loss, compromise or misuse of Police information may cause serious damage to the Police organisation, for example:

- Negative exposure in the media
- Reduction in community confidence and trust in Police
- Compromising safety of staff or individuals

The Police have procedures designed to ensure that its approach to protective security is consistent. We need to protect property and information from loss, compromise and/or misuse. So what does this mean?

**Loss -** The inadvertent placement of information assets in an unknown location such that the responsible department cannot assure its protection from compromise or misuse

**Compromise** - Unauthorised disclosure to a person or organisation who is not entitled to have the information

**Misuse** - The use of the information in a way that it was not intended to be used

**Portable Storage Devices**

Portable Storage Devices are any devices that can store electronic files. You may know them as memory sticks, memory cards, thumb drives, flash drives, even 'sticky things'. This category also includes digital cameras and digital photo frames.

Most modern portable music players (like the iPod) and many smartphones have huge memory capacities and can hold large files like memory cards do.

Finally there are more traditional media like CDs and DVDs. The following rules apply:

- Personal portable storage devices must not be plugged into any Police computer systems
- Plugging a music player into a computer USB port for charging is allowed however using your own dedicated power charger is preferred
- Always perform a scan on a portable storage device for viruses and other malware by right-clicking the device and choosing 'Scan...'
- The amount of data on any portable storage device used for work should be kept to a minimum to reduce the loss if the device is stolen or goes missing
- Any data put on a portable storage device should be deleted when not required - use and then remove
- All portable media devices must be stored in a locked cabinet or drawer when not in use
- All portable media devices must be destroyed beyond repair when no longer needed

**Social Networks**

Social networking sites are a great way to make friends (some of them are even real) and share information. It's funny to video your mates and post it on YouTube. But you never know who might be prowling around the social networking sites looking for useful information that they can use for personal gain!

Therefore, information about the NZ Police or their employees MUST NOT be posted on social networking sites.

Social networking sites like Facebook, YouTube, MySpace, Twitter, and LinkedIn gather significant amounts of information about you from your profile and some of this is openly displayed for anyone to see. Their policies can change without notice and this can affect who gets to see your information.

As security guru, Bruce Schneier, said, "When you put private or confidential information about yourself or the company on a computer you lose some control over it. When you put this information on the internet, you lose a lot of control over it. Once it's out there, any control that you have over it is an illusion".

The simple answer is, DO NOT post private or Police information on social networking sites. You don't know who might see the information or how it might be used.

**Access Security**

Wearing your CPNZ ID card at all times while in Police stations is an essential aspect of security. Your ID card is an obvious indication that you are a volunteer and entitled to be in a particular office and/or on Police premises.

If the rule of wearing an ID card at all times is respected and enforced in CPNZ it will make it easier for Police to identify someone who is not approved to be in the building or a particular section of the building.

If you DO see someone walking around a Police Station who is unfamiliar to you or they don't have an ID card displayed, don't be afraid to ask them 'who are you?' and/or 'where is your ID card?' If they cannot present it, or you have suspicions about whether they are permitted to be in that part of the building, you should challenge them and/or contact a Police Officer immediately to report your concerns.

**Piggybacking And Tailgating**

Piggybacking refers to a situation where an unauthorised person closely follows an authorised person to gain entry into a controlled area or past a security controlled entry.

Piggybacking usually implies a level of consent on the part of the authorised person. The authorised person may hold the door open as a courtesy or the unauthorised person may ask for help as they are carrying an awkward package.

In 'tailgating' there is no implied consent. An unauthorised person follows closely behind an authorised person through an open door or shares a revolving door without awareness of the authorised person.

The rule is simple, when entering any door that is controlled by a swipe card, NEVER swipe anyone in using your swipe card and NEVER allow anyone to follow behind you unless you know they are authorised to enter the area.

ALWAYS challenge an unfamiliar or unaccompanied person who is not wearing an ID card or visitor's pass and remember that a visitor's pass DOES NOT entitle a person to enter or be in a controlled area unaccompanied at any time

**Storage Of Police Information**

All Police information supplied to Community Patrollers MUST be stored and protected both during and after business hours. If not, you are putting the organisation and yourself at risk of a security breach and the possible loss, compromise or misuse of Police information.

**Disposal Of Police Information**

There are many frightening stories around about people getting their hands on Police information that was simply thrown in a bin or a dumpster with the assumption that no-one will ever see it again. WRONG!

If the information you are tasked with destroying no longer needs to be retained and is not subject to the Archives Act then it should be destroyed by approved means only. (See your local PLO about this if you have any questions).

The three most common methods of destruction of Police Information are:

**Shredding** - destroying paper documents using approved cross-cut shredders

**Classified Waste Bags or Bins** - locked bins that receive appropriate protection during use and storage by Police before collection by a contracted company that destroys the information safely

**Disk/CD/DVD Shredders** - these shredders are used to completely destroy these types of media to prevent any useful recovery of data

As a Community Patroller you will be asked to sign a Statement of Acknowledgement that you have read and understand the 'Essential Security Awareness' requirements that apply to you while being engaged with the NZ Police.