Information security: People managers

Table of Contents

Introduction

For the purposes of this policy, the term ‘employee’ encompasses any person who provides work or services to Police, and has access to Police resources, regardless of the contractual setting under which they do so. This includes contractors, service providers and other third-party users.

As a manager, you must:

- ensure new employees are aware of the relevant security policies. Copies or access to the online version should be provided as part of the induction process. As well as general security awareness provided in the Essential Security Awareness course, they may also need specific training for the locations or roles they operate in.
- lead by example
- monitor all employees under your control to ensure they comply with legislation and security policy
- act if you become aware of any security issues or incidents, to manage the impact and prevent reoccurrence.

Segregation of duties

A variety of activities within Police need responsibilities to be segregated over two or more people to minimise the potential for a conflict of interest and to provide independent verification of due process. Activities that need segregation should be considered and defined in position descriptions, process definitions and system specifications. Examples include:

- Procurement, financial authorisation and payment.
- Salary movement and allowance approval.
- Complaints and conduct investigations.
- Vetting and security clearances.
- ICT assurance approval and administration.

Employee information

Some employee information that you deal with as a manager will be IN CONFIDENCE. For instance:

- Personal information about employees.
- Details about employment processes, including vetting, contract negotiations, interviews, and performance reviews.
- Files relating to incidents, investigations, prosecutions, complaints, or internal disciplinary matters could also reach the SENSITIVE classification level.

Some of the technology used operationally by Police also collects personal information about employees, both intentionally and inadvertently. These include location systems, event data recorders, phone calls and radio communications, multi-function printers, computer system and cloud service logs, emails and text messages, CCTV and building and vehicle logs.

Information collected electronically may be used and disclosed by Police for any business purposes, including:

- law enforcement
- to monitor safety of employees, the public and offenders
- efficient deployment of resources, including the management of human resources
- district and area operational requirements, e.g. TOR database reports
- investigating complaints or concerns about an employee's conduct
- conduct checks for the purposes of awards, commendations, progression and appointments
- analysis and statistics
- responding to Official Information Act requests.

Police will only access the collected information for official purposes and in accordance with relevant laws and policies.

An employee is entitled to request access to their personal information held by the Police, including conduct history. They may also request corrections to such information. Police may refuse to release personal information if it is not readily retrievable or if one of the withholding grounds of the Privacy Act 2020 applies.

Conduct investigations

To retrieve information about an employee for the purposes of investigating complaints or concerns, provide a written request to the Director: Integrity and Conduct or AC/ED: People Services. The request must outline:

- the reason for the request
- why the information retrieval and disclosure is necessary, the purpose
- the nature of the information or evidence sought
- whether the investigation is required to be recorded to evidential (court or disciplinary) standards.

The request must have reasonable grounds to believe that retrieval of the information is necessary for the investigation.

Access to personal and shared directories

Every user's Home drive on the Enterprise network is for their own use. So access to another person's Home drive may only occur under the following conditions:

- **Supervisors and Managers**: Supervisors and managers may access the Home drive of a user under their direct supervision without prior consent, if they:
  - have made every reasonable effort to contact the user concerned, stating the reason for the request
  - have a legitimate business reason to access the directory
  - have obtained written/email authority from the relevant District Commander, Service Centre Manager or Director. The request should note the reason(s) for access being required, the activity to be carried out, and the length of time for which access is required.
  - If access is granted to a current user's directory, the supervisor/manager must take the soonest opportunity to inform the user that access was granted and the purpose for which it was granted.
- **Investigations**: An Authorised Investigator may access the Home drive of another employee provided they have a legitimate business reason to do so (such as a criminal and/or disciplinary investigation). Access must be removed once the investigation is completed.
- **ICT**: ICT employees may access personal or secure shared directories for data administration or emergency access purposes, provided that the access is authorised, for a specific period of time sufficient to complete the task, and be 'read-delete' only. Authorisation for ICT administration access must detail the reason for the access, the activity to be carried out, and the time required, and may only be given by the directory owner, the CIO or the CISO. Every reasonable attempt must be taken by the ICT employee to inform the user of the access, both before and after the fact, and those efforts must be documented.

Access to text messages

One NZ stores the content of all text messages sent from and received by Police owned mobile phones (including personal messages), but will only provide access if specific conditions are met. In the context of employment enquiries, written consent of the employee is required. In criminal enquiries, a production order or search warrant is required.

ICT access for non-Police users

People who are not Police employees (e.g. contractors, volunteers, interns, NGO workers) accessing Police ICT could pose legal, operational, and reputational risks if they are given too much access to information held by Police. The risks must be considered before providing access. Information access and assurance controls must be in place and appropriately managed to reduce this risk and to protect individuals. Access must be approved in advance by a member of the Police Executive, a District Commander or a Director.

Standard access for non-Police users is limited to MS365 Outlook (email and calendar), Internet and Intranet. Additional access can be requested via the IT Self Service portal.

Principles

Principles applying to access for non-Police users include:

- Access is denied by default and is only granted on an exception basis, when there is a clearly identified and recorded operational need for granting access; and only to individuals who have a satisfactory vetting status.
- The requirements and obligations on non-Police users are equivalent to those of Police employees.
- Applications for non-Police access should be referenced explicitly to a contract or other agreement that has been reviewed by Police Legal Services, unless there is an emergency requirement.
- Applications for access to sensitive operational Police Information Systems must be consulted with the business owner of that system.
- Approval for access is documented, auditable and managed in an equivalent manner to Police employees by the ICT Service Desk.
- The ICT will not provide access without appropriately authorised documentation.
- There are increased levels of audits and reviews of information use by people granted access to Police Information Systems under this policy.

Requesting access

The steps to request ICT access for a non-Police user are:

Step	Action
1	Consider the need and extent of access required to Police Information Systems for the non-Police user. Be satisfied that: - the request is necessary for the effective delivery of Police services (and cannot be done by other reasonable means) - your supervision is sufficient to ensure ongoing compliance with Police requirements and any information sharing agreements; and to ensure that any access is appropriate - relevant contractual arrangements, MOUs or information sharing agreements are in place e.g. an Approved Information Sharing Agreement in accordance with the Privacy Act 2020.
2	Obtain a QID for the non-Police user.
3	Complete the 'New Employee/Non-Police User Registration' form online. **Note**: If the 'End Date of Contract' box on the form is not known then leave it blank. When the end date is not entered, the form will default to 12 months after the start date. This ensures the individual's access to Police Information Systems is reviewed at expiry. If access is to be continued after expiry period, then a new approval must be obtained.
4	s.6(a) OIA

The approving manager will determine that the request is necessary for the effective delivery of Police services and that the appropriate process has been followed and documentation completed.

Managing non-Police access

Each manager is responsible for oversight of their non-Police users' access to Police Information Systems.

To audit the records, a report of non-Police users will be periodically requested by the Head of IT Security Management and provided to the CISO. When necessary, enquiries are made to Districts, workgroups and HR of all non-Police users who are flagged as having their end date of contract expired to ensure they are no longer engaged with Police and access can be removed.

Account expiry

When non-Police users start with Police the end date of the contract should be specified. If no end date is known, then the end date will automatically default to 12 months after the start date. They will be reminded, via email, that their account is about to expire 1 month prior to the expiry date.