ICT projects and service delivery

Table of Contents

Table of Contents 2
ICT development and procurement 3
- Procuring software and hardware 3
- Balancing business needs with security 3
- ICT certification, accreditation and audit 3
- Police information in cloud and other outsourced or offshore ICT arrangements 3
- Development, test and training environments 4

Security of end user devices and other endpoints 5
Service management 6
- Specialist ICT security policies 6
- System administrator access 6

Management of records of non-Police users access 7
ICT monitoring to reveal information loss or inappropriate use 8
Decommissioning and disposing of ICT 9
- Return of assets 9
- Secure disposal or re-use of equipment 9

Physical security for ICT facilities 10

ICT development and procurement

Procuring software and hardware

All procurement of software, hardware and IT-related services must occur through CIO-approved ICT Service procurement processes.

Users may procure computer consumables, such as toner, paper and memory sticks, with the authorisation of a supervisor or manager with the appropriate financial delegation.

No new system should be brought into production until it has been assessed to ensure that it functions correctly, that is does not adversely interfere with the operation of any other Police computer system and that the security has been approved through the Certification and Accreditation process.

Balancing business needs with security

All projects that include ICT have potential security implications. The immediate business needs must be balanced against the wider organisational need to protect Police assets, services and information. This is particularly relevant if a proposal involves new applications, installations or changes in the use of Police ICT. The development process should:

- ensure adequate security is built into the system and operational processes to meet the business needs i.e., security functional requirements and NFRs
- assess and manage the security risks applicable to the system and its influence on the wider Police ecosystem
- utilise good practices, including Police approved processes and architectural building blocks (e.g., server SOE standards) and the security controls defined in the NZ Information Security Manual (NZISM).

Security risk assessment should be completed for each business case and reviewed at each stage during the development lifecycle. This is primarily the responsibility of the project manager but advice and assistance will be provided by the Protective Security and Cyber Security teams.

ICT certification, accreditation and audit

Audit of ICT systems and services should occur at several different levels:

- The business and technical owners need to assure themselves that the risks associated with their systems and services are managed adequately and that they meet any applicable minimum standards and legislation.
- The Head IT Security Management has oversight over all Police managed and procured ICT systems, and may use audit techniques to support the security management processes.
- Assurance Group - via the CISO - conducts security assurance over all information resources and services, including conducting the Certification and Accreditation (C&A) programme, which all systems and significant changes must pass through.
- Police internal and external audit programmes may include aspects of information security.

All significant changes to systems must be managed through the ICT Change Management process, raising any security-relevant changes to the Head IT Security Management.

Police information in cloud and other outsourced or offshore ICT arrangements

Police information planned for outsourced or offshore ICT arrangements must be notified to the CISO. The CISO will assess the risks and implementation of security controls for offshore ICT arrangement for the storage or processing of information protectively marked at, or below, RESTRICTED. These activities occur as part of the Certification and Accreditation process.

6(a) OIA

Where cloud services are being considered:

- follow the advice and guidance in the GCIO's 'Cloud Computing: Information Security and Privacy Considerations' (www.ict.govt.nz/)
- the provider and the project will complete the GCIO Cloud Risk Discovery Tool to identify the security and privacy requirements and controls. The tool is a spreadsheet available from digital.govt.nz.
- the Certification and Accreditation process will be used to assess the information security risks and applicable minimum

standards, and verify that the risks are being managed
- any residual risks must be accepted by the applicable risk owners

Regardless of any outsourcing arrangement, Police remains accountable for ensuring that the information in our custody is appropriately protected.

Development, test and training environments

Development, testing and training activities can cause unintended changes to software, data and services sharing the same computing environment, so they should be separated from production environments to reduce this risk. Where sensitive production information needs to be used in any of these environments, it must be secured and managed as a production environment, with strict access control and change management to ensure the protection of that information.

Therefore, the preference is to always use dummy data in development, test and training environments.

Security of end user devices and other endpoints

All laptops, smartphones and other portable devices must be protected by an approved hard disk encryption application (e.g., BitLocker), installed by the ICT group, before being used.

By default, all information written to removable media must be encrypted. Users may be able to write unencrypted, but that must either require a formal request to the Service Desk or via an explicit decision on each occasion. Once encrypted, media containing SENSITIVE or RESTRICTED information only needs to be physically protected as an IN CONFIDENCE item when it is in a locked state.

All Police devices running Microsoft or Macintosh operating systems must have an endpoint detection and response service installed and running continuously. ICT group must ensure the virus or threat databases are regularly updated and that the capability remains fit for purpose.

Any device or portable computer used for remote access must have a functional firewall and up to date malware protection approved by the ICT group. Special attention is also required to ensure that all necessary operating system security patches have been installed and remain up to date.

Service management

Segregation of duties must be implemented in situations where an administrator or developer with enhanced access could perform actions or see information that, as a user, they would not be approved or authorised for. For instance, if they want software installed of their device they must still have it approved first. In some situations, an activity audit capability by another role (e.g., Cyber Security) may be adequate.

All ICT servers, user devices and other equipment must be kept up to date in accordance with the patching standards defined by Director ICT Ops. 6(a) OIA
Exceptions must be agreed in advance with the Vulnerability Management Review Group. Outsourced services are responsible for patching in accordance with the Police patching standards unless otherwise stated in the contract.

All systems and services should have defined Service Level Agreements (e.g., availability %, recovery time objectives, recovery point objectives), backed up by disaster recovery and service continuity plans, designs and processes. As well as technology requirements, the DR plan should also cover staffing and other non-technical recovery requirements. The SLAs and plans should be made available to all key ICT and business stakeholders.

Specialist ICT security policies

ICT group maintains a set of specialised security standards that relate to the design, selection, installation and management of Police networks and systems. Because the standards and procedures are not particularly pertinent at the staff/business user level, they are not published Police-wide. Contact the Cyber Security team for more information.

System administrator access

Staff with root, superuser, Domain Administrator and other highly privileged system access have additional responsibilities to ensure that ICT systems and applications are developed and maintain to maintain information and system integrity.

Administrative rights must only be provided when necessary for the activities being conducted. At other times, such as when researching on the Internet, a normal user account should be provided and used

Multi-factor authentication should be used for administrative access. Where that is not possible, alternative controls may be needed or additional requirements may be mandated around password protection, strength and change frequency.

Non-personal identifiers and authenticators (e.g., root or local admin passwords) should be individualised for each device or application and should be managed via a formal process that is approved and monitored by the Head IT Security Management.

Remote administrative access to production systems may only be enabled through multi-factor authenticated channels approved by Director ICT Operations. 6(a) OIA

All remote access must be set up and used with care to ensure it does not enable excessive or unauthorised access to Police systems or information.

Management of records of non-Police users access

The Service Desk is responsible for maintaining records of non-Police users' enterprise login accounts (i.e., QIDs). An automated email is sent to the requestor and non-Police user one month prior to the user's contract date expiring reminding them that access will be revoked following the end date of the contract, unless a renewed approval by a Police Executive member, District Commander or Director is obtained.

To renew access the requestor must submit the 'New Employee/Non-Police User Registration' form online. Each request should include:

Type of account	**Contractor / Volunteer / Intern / NGO worker / Secondee**
Non-Police user's details and access	- Workgroup/Station/location. - Name of agency/NGO non-Police user works for. - Type and extent of information systems and applications accessed. - Start date of contract. - End date of contract.
Approval	By Police Executive member, Assistant Commissioner, District Commander or a Director authorising access.
Alert	Flagged alert when end date of contract has expired.

ICT monitoring to reveal information loss or inappropriate use

ICT carry out monitoring of Police devices and systems for the purposes of, for example:

- detecting information loss or inappropriate use or access;
- protecting employees and the organisation; or
- providing early intervention opportunities to eliminate or minimise risk.

If the monitoring by ICT group:

detects...	**then...**
deliberate misuse or misconduct under the Code of Conduct	the matter will be reported directly to Director: Integrity and Conduct for investigation.
inadvertent access, misuse or loss of information	the matter should be reported to the user's supervisor to: - apply early intervention - eliminate or minimise potential harm - introduce protection strategies for the future.

Note: Monitoring will also be used to identify areas of exposure such as unwanted user trends for the development of targeted awareness training.

Decommissioning and disposing of ICT

Return of assets

The user and staff deprovisioning process should account for all Police devices, media and other significant resources issued to the person. Instructions should cover to who and how the resources should be returned or whether they can be transferred to another staff member.

Secure disposal or re-use of equipment

ICT Operations maintains the approved ICT equipment sanitisation and disposal process, which can be arranged through the Service Desk or a District Support Engineer. The two required steps for cleaning enterprise devices that have encrypted drives from new is to destroy the decryption key, then format and overwrite the entire drive with a storage sanitization utility.

Physical security for ICT facilities

The Departmental Security chapter provides instructions for physical security measures to minimises or reduce the risk of information assets being made inoperable or inaccessible, or improperly accessed or used.

Business owners must assess and manage the risk of physical attacks and incidents to information and services, regardless of where and how they are provided (e.g. including cloud).