POLICY
ICT RESOURCE SECURITY MANAGEMENT
(03.008)

POLICY

Northland Polytechnic Limited (the Polytechnic) will protect ICT resources from all threats, whether deliberate or accidental.

PURPOSE

To ensure business continuity and to preserve the security of our data and technology infrastructure to minimise the impact of security breaches.

APPLICATION AND SCOPE

This policy applies to all the Polytechnic ICT resources, staff, students and visitors.

DEFINITIONS

- *Availability*
  Ensure that authorised users have access to information when required
- *Confidentiality*
  Ensure that information is accessible only to those authorised to have access
- *Cyber Security*

  The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks
- *ICT Resources*
  Hardware and software including, but not limited to:
  - Data and communication network (LAN, WAN, Internet, and Wireless)
  - Computer and equipment (i.e. servers, computers, printers, multi-function devices, telephones, mobile devices)
  - Data storage media (i.e. backup tape, flash memory, removable hard disk) and data files
  - Business applications and software licences.
- *Information security*
  Protect information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction
- *Information security management*
  Describe controls that an organisation needs to implement to ensure that it is appropriate to manage risks
- *Integrity*
  Safeguard the accuracy and completeness of information and processing methods
- *Security incident*
  An event (e.g. unauthorised access, theft, computer virus, illegal use of software, user errors, software failure) causes or has potential to cause a breach of information security

- *Security threat*

  A potential event may result in harm to a system or the Polytechnic. Threats may be deliberate (e.g. theft, unauthorised use of storage media), accidental (e.g. user error, network component failure), or environmental (e.g. earthquake, lightning)

- *User*

  A user must be a current Polytechnic staff member or a currently enrolled student. Other individuals may also become users (with guest accounts) for the Polytechnic business purposes; examples include someone providing service to the Polytechnic and official visitors

COMPLIANCE OBLIGATIONS

Auditor General
Copyright (Infringing File Sharing) Amendment Act 2011

Responsibility	Executive manager with responsibility for ICT
Approval dates	September 2020
Next Review	September 2023

OTHER RELATED DOCUMENTS

Policy: *Acceptable use of ICT Resources (03.006)*
Policy: *Security (03.011)*
Policy: *Disciplinary Processes (04.022*)
Associated procedures and guidelines (Appendix 1)

APPENDIX 1

PROCEDURES AND GUIDELINES

1.0 In compliance with this policy computer users and departments shall ensure:

- Appropriate protection over the Polytechnic ICT resources;
- Adhere to the Cyber Security Management (3.0) Procedures and guideline.
- Information and information processing facilities are physically protected from security threats and environmental hazards;
- The safeguarding of information in networks and the protection of the supporting infrastructure and services;
- That access to information and business processes are controlled on the basis of the polytechnic security requirements;
- That users are made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and safe use of information resources;
- Information security is maintained when using alternative types of information technology and electronic devices (different from the Polytechnic standard computing and network environment);
- That information security is maintained when mobile computing equipment (e.g. Smart cell phones, laptops) and remote access facilities are used;
- Incidents affecting security are reported through appropriate management channels as quickly as possible;
- That adequate user security awareness and training is provided;
- The use of information systems in compliance with legislative and contractual requirements.

2.0 Library, Flexible Learning and ICT shall ensure:

- That formal procedures are in place to control the allocation of access rights to information systems and services;
- Adequate access controls are in place to prevent unauthorised access to the network, computers, and information held in information systems;
- That monitor mechanism is in place to detect deviation from access control policy and record system access events to provide evidence in case of security incidents;
- That all installations, implementation and maintenance of new or updated software and hardware on main Polytechnic network are controlled and will result in continued system operations, including availability and integrity of information;
- That application and system evaluation, testing, and development are conducted in an isolated environment that is separated from main Polytechnic network;
- Procedures and controls are in place to protect the integrity of software and information (e.g. Prevent and detect malicious software, virus, worms, and Trojan horses);

- That business continuity processes are implemented and maintained to reduce the disruption caused by disasters and security failures;
- That backup and recovery procedures are appropriately implemented and critical backup media are kept in a secured place offsite;
- Disaster recovery plans are appropriately documented and recovery tests are conducted regularly;
- That appropriate management processes are in place to handle security violations;
- The security of information systems is regularly reviewed and audited against the appropriate polytechnic policies, best practices and standards.

3.0 Cyber Security Management

3.1 Confidential Data

Some of the common examples of confidential data include:

- Classified financial, HR and payroll information
- Data about staff, students, partners and vendors
- Patents, formulas or new technologies
- Commercial contract and agreements
- Legal documents
- Intellectual property materials like teaching materials
- Pricing/marketing and other undisclosed strategies
- Documents and processes explicitly marked as confidential
- Unpublished goals, forecasts and initiatives marked as confidential

Employees may have various levels of authorized access to confidential information.

What employees should do

- Lock or secure confidential information at all times
- Shred confidential documents when they're no longer needed
- Make sure they only view confidential information on secure devices
- Only disclose information to other employees when it's necessary and authorized
- Keep confidential documents inside the Polytechnic premises unless it's absolutely necessary to move them

What employees shouldn't do

- Use confidential information for any personal benefit or profit
- Disclose confidential information to anyone outside of the Polytechnic
- Replicate confidential documents and files and store them on insecure devices
- When employees stop working for the Polytechnic they are to return any confidential files and delete them from their personal devices.

Confidentiality Measures

The Polytechnic will take measures to ensure that confidential information is well protected. The Polytechnic will:

- Store and lock paper documents
- Encrypt electronic information and safeguard databases

- Instruct employees to sign non-compete and/or non-disclosure agreements (NDAs)
- Request authorization by senior management to allow employees to access certain confidential information where required

Exceptions

Confidential information may occasionally have to be disclosed for legitimate reasons. Examples are:

- If a regulatory body requests it as part of an investigation or audit
- If the Polytechnic examines a venture or partnership that requires disclosing some information (within legal boundaries)

In such cases, employees involved should document their disclosure procedure and collect all needed authorizations. The Polytechnic is bound to avoid disclosing more information than needed.

3.2 Device Security - Using personal devices

When employees use their digital devices (PCs, laptops, tablets, smart phones) to access the Polytechnic emails, accounts or data, they introduce security risk to the Polytechnic data. The Polytechnic advises all employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password secured and protected.
- Upgrade antivirus software and run antivirus scan on a regular basis
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.
- Lock devices when leaving the desk

The Polytechnic advises employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

3.3 Email Security

Emails can carry scams or malevolent software (for example worms, bugs etc.). In order to avoid virus infection or data theft, the Polytechnic procedure is to inform employees to:

- Abstain from opening attachments or clicking any links in the situations when its content is not well explained
- Make sure to always check email addresses and names of senders.
- Search for inconsistencies
- Be careful with clickbait titles (for example offering prizes, advice, etc.)

In case that an employee is not sure if the email received, or any type of data is safe, they can always contact ICT.

3.4 Managing Passwords

To prevent a Polytechnic account password getting hacked, use these best practices for setting up passwords:

- At least 8 characters (must contain capital and lower-case letters, numbers and symbols)
- Do not write down password and leave it unprotected
- Do not exchange credentials when not requested or approved by supervisor

- Change passwords every 3 months
- Do not share passwords with others

3.5 Transferring Data

Data transfer is one of the most common ways cybercrimes happen. Follow these best practices when transferring data:

- Avoid transferring personal data such as customer and employee confidential data
- Adhere to personal data protection law
- Data can only be shared over company's network

3.6 Working Remotely

Even when working remotely, all the cybersecurity policies and procedures must be followed.

3.7 Disciplinary Action

Every attempt will be made to accommodate compliance with the provisions of this document in a fair and open manner that respects individual rights and by procedures that are just and equitable.

Breaches of the Professional Code of Conduct, and any other Polytechnic policies, guidelines and statutory requirements, by staff may be addressed by way of the Polytechnic Disciplinary Processes policy and procedures and include the involvement of the Police if a criminal offence has been committed.

See policy: Disciplinary Processes (04.022).

KEYWORDS

REVISION HISTORY			
Version	Description of Change	Author	Effective date
1	New – replaced T05/01 (*Information Security Management)*	QMS Team	January 2009
2	Review – management structure changes	QMS Team	January 2010
3	Re-approval	P Brimacombe	August 2015
4	Triennial review – no changes	S Milner	August 2018
5	Addition of Cyber Security Management guideline	B Kluge	September 2020