|  |
| --- |
| Information Security Policy  (example) |

## Policy purpose

The purpose of this policy is to ensure an appropriate level of security throughout the organisation so that its people, information, assets, reputation and resources are protected from potential loss or damage.

This policy is an overarching document that provides the approach for the information security policies, standards and procedures in the organisation.

## Scope

This policy applies to all **[ORGANISATION NAME]** staff, third-party vendors and **[ORGANISATION NAME]** business.

## Definitions

**Staff:** everyone provided with a **[ORGANISATION NAME]** account. This includes all employees and contractors. It may also include consultants and third-party vendors.

## Policy requirements

All staff are expected to be aware of and adhere to this policy and take reasonable steps to mitigate any identified risks. Staff are also required to report on these risks and/or policy breaches to their manager.

All third-party vendors are expected to be aware of and adhere to **[ORGANISATION NAME]**’s ICT policies. Staff must ensure vendors are aware of this obligation and ensure they have sighted this and related policies.

All IT systems, software and services must follow the appropriate risk management and introduction process.

**[ORGANISATION NAME]** policies are required to meet all relevant security requirements and standards in the organisation.

Related ICT policies must adhere to, and be read in conjunction with, this overarching Information Security Policy. Details of these related policies are listed in the “Related policies and guidance” section.

## Policy principles

Culture: **[ORGANISATION NAME]** must encourage a culture of security awareness. All staff are responsible for security and are required to comply with the organisation policies, standards and procedures associated with security.

Proactive: All staff are required to report any identified security risks.

Risk management: To minimise the impact and likelihood of information security risks, all systems are submitted to a security assessment to evaluate the risks and understand which security controls must be implemented to minimise them.

Balance: **[ORGANISATION NAME]**’s security approach is to have a balance between appropriate security controls and the level of information it is protecting, while considering and trying to minimise the operational impact of the security controls.

Compliance: All security controls must comply with the relevant legal, regulatory and contractual requirements and obligations.

Enforcement: Breach of this policy and the related procedures and standards may result in disciplinary action against a staff member, termination of contract for third-party vendors, and civil and/or criminal prosecution under New Zealand law.

Exemption: Any deviation from this policy requires written approval from **[NAME CHIEF INFORMATION SECURITY OFFICER].**

## Security review

**[ORGANISATION NAME]** must review its security environment on an ongoing basis.

The review should measure compliance with standards and procedures associated with this policy and other associated policies.

Any significant breach of security must be reported, and mitigations put in place to address the impact.

## Responsibilities and accountabilities

|  |  |
| --- | --- |
| Position | Responsibilities |
| [ROLE TITLE] (Chief Information Security Officer) | Is accountable for information security in the organisation.  Ensures that this policy and subsequent standards and procedures comply with legal, regulatory requirements and New Zealand security requirements and standards; and are understood, implemented and complied with at all levels of the organisation.  Approves exceptions to this policy. |
| [ROLE TITLE] (IT Security Manager) | Is responsible for the operational implementation of this policy and related standards and procedures.  Ensures that security standards at **[ORGANISATION NAME]** meet the organisation’s relevant security requirements and standards.  Provides regular security reporting to the organisation and the **[Role Title]** (Chief Information Security Officer).  Ensures adequate skilled resources are available to implement, enforce and monitor effectiveness of this policy and subsequent standards and procedures.  Reviews and advises on this policy and subsequent standards and procedures.  Develops, maintains and improves operational processes to support this policy and related standards and procedures.  Engages with the organisation to ensure their work processes, systems and practices adhere to this policy and related standards and procedures.  Develops organisational training and education to enhance security awareness. |
| Managers | Ensures compliance with this policy and related standards and procedures within their business area or area of responsibility in the organisation.  Informs the **[Role Title]** (IT Security Manager) of any security issues raised to them by **[ORGANISATION NAME]** staff. |
| Staff | Complies with this policy and related standards and procedures and reports security breaches to their reporting manager and/or **[Role Title]** (IT Security Manager).  Compliance with this policy is a condition of employment.  Non-compliance with this policy may result in disciplinary action. The severity of the breach will determine the action taken. |

## Related policies and guidance

This policy is related to the following policies and guidance on **[relevant platform]:**

**[relevant policies]**

**[relevant procedures]**

## Further assistance

If you have any questions about this policy and related standards or guidelines, please contact **[ROLE TITLE]**.

Sponsor: [ROLE TITLE] (Chief Information Security Officer)

Owner: [ROLE TITLE] (IT Security Manager)

Audience: All [NAME ORGANISATION] staff

Approved by: Appropriate authority

Last approval date: MMM YYYY

Last review date: MMM YYYY

Next review date: MMM YYYY