**Secure Internet Communications Policy**

**Template**

This is an example policy. Please ensure you update this policy template so that it’s suitable for your organisation.

## Purpose

The main purpose of this policy is to ensure the protection of information in networks and its supporting information processing facilities. The aim is to maintain the security of information transferred within <organisation> and with any external entity.

## Scope

The policy statements written in this document are applicable to all <organisation> resources, at all levels of sensitivity. This includes staff employed by, working for, or on behalf of our organisation.

This policy covers all information assets and will be used as a foundation for information security management.

## Network controls

We shall identify and implement appropriate solutions to:

* control the confidentiality and integrity of sensitive information passing over public networks
* protect the connected systems and applications
* maintain the availability of the network services and computers connected

Employees will not be allowed to connect any non-<organisation> approved device (personal computer, laptop or network equipment) to our network, without proper permission and approval.

<Organisation> will implement appropriate routing control mechanisms to restrict information flows to designated network paths.

<Organisation> will ensure proper management and technical oversight is performed over security perimeter structures (firewalls) and current configurations. As a minimum requirement, this will include:

* documenting the security perimeter rules and reviewing them on a regular basis
* documenting configuration changes and getting management approval
* getting management approval prior to applying any changes to security perimeter rules
* taking reasonable care while applying changes on the security perimeter rules to ensure minimal disruption to our environment

The connection capability of users shall be restricted through network gateways that filter traffic using pre-defined tables or rules. The restrictions will include, but not be limited to:

* messaging (electronic mail)
* file transfer
* interactive access
* application access

## Security of network services

<Organisation> will protect the network infrastructure by implementing proper network security measures and features. Security features of network services will include, but not be limited to the following:

1. Technology applied for security of network services, such as authentication, encryption and network connection controls.
2. Technical parameters required for secured connection with the network services in accordance with the security and network connection rules. This includes firewall, Virtual Private Network (VPN), intrusion detection systems (IDS), and intrusion prevention systems (IPS).
3. Procedures for the network service usage to restrict access to network services or applications, where necessary.

## Information transfer policies and procedures

Formal controls based on the criticality of information shall be defined to protect the transfer of information through the use of communication facilities. Transfer of confidential information shall be appropriately protected.

All users shall manage the creation, storage, amendment, copying and deletion or destruction of data (in electronic and paper form). This will be in a manner that’s consistent with <organisation> policies, that control and protect the confidentiality, integrity and availability of such data.

Asset Owners shall ensure appropriate mechanisms are implemented and followed to protect transfer of their information.

## Agreements on information transfer

Prior to the transfer of information with an external organisation, a formal and appropriate Service Level Agreement with an adequate level of security controls must be defined. This agreement will cover, but not be limited to:

* management responsibilities
* manual and electronic exchanges
* sensitivity of the critical information being exchanged
* protection requirements
* notification requirements
* packaging and transmission standards
* courier identification
* responsibilities and liabilities
* data and software ownership
* protection responsibilities and measures
* encryption requirements

## Electronic messaging (emails)

Security controls will be established to protect emails from unauthorised access, modifications or denial of service.

## Confidentiality or non-disclosure agreement

Requirements relating to confidentiality and non-disclosure commitments (for employees and third parties) shall be identified and regularly reviewed.

As such <organisation> will:

* define the information to be protected and required levels of sensitivity
* indicate the expected length of the commitment
* specify the terms for the return or destruction of information when the commitment is terminated
* specify the responsibilities and requirements concerning signatories in order to prevent unauthorised disclosure of information
* publish the penalties applicable in the event a user fails to respect the commitment

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and <organisation>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

Review of this document: annually by <role>.

Next review date: <date month year>.