network security policy

 template

# Authority and review

## Document control and review

|  |  |
| --- | --- |
| **Document check**  |  |
| Author  |  |
| Owner |  |
| Date created |  |
| Last revised by  |  |
| Last revision date |  |

.

## Version management

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Date of approval** | **Approved by**  | **Description of change** |
| 1.0 |  |  |  |

# Intro

Network security within the organisation is important because it is your first defence against outside attacks. By implementing effective technical and organisational network security measures, you can prevent cybercriminals from mapping your infrastructure, disrupting your communications, unlawfully gathering data or reaching critical applications and devices.

This policy document is part of a set of policy documents that support **[Organisation]** in establishing a sound cybersecurity strategy.

# Network security

## Physical security

Network components such as firewalls and switches should be located in dedicated cabinets. Access to these cabinets should be restricted to specially designated personnel. Data and power cables should be protected from damage.

## Segregation of networks

To prevent malware and other abuse from spreading across the network, the network should be designed as a segregated topology. Systems should reside in designated VLANs, separated by firewall access rules.

The following VLAN segregation rules must be observed:

* Systems providing online services (i.e. accepting incoming traffic from the internet) should be separated from other systems.
* Network management is via a separate VLAN.
* Systems providing connected services (i.e. accepting incoming traffic from untrusted networks other than the internet) should be separated from other systems
* End-user devices should be separated from servers.
* Unmanaged devices should be separated from managed devices.
* Systems with different purposes should be separated.
* Physical locations should be separated.
* Development, testing and production systems should be separated.

## Firewalling

VLANs should be separated by firewalls. Network traffic between VLANs and traffic to or from untrusted networks should be blocked unless explicitly required to be open. Outbound Internet access for office user VLANs is allowed unless it adversely affects the security or performance of the business. Traffic can be prioritised, for example to prevent video or music streams from affecting work-related office traffic.

## VPN

For teleworking or machine-to-machine communication over untrusted networks, VPN can be used to encrypt network traffic that is not encrypted by default.

Access to the VPN, and thus to all underlying **[Organisation]** systems, should, where possible, be configured to use some form of Multi Factor Authentication such that an unauthorised person in possession of compromised **[Organisation]** credentials cannot use the **[Organisation]** VPN.

## Securing wired networks

# Network ports should be protected from untrusted devices. When physical security is low, network security techniques such as MAC filtering or network access security should be used to block or isolate untrusted devices.

## Wireless network security

Wi-Fi uses different standards for encryption and authentication. Below are the methods in order of best security (the first is the only secure method):

1. WPA2 + AES
2. WPA + AES (not preferred)
3. WPA + TKIP (not preferred)
4. WEP (never use)
5. Open Network (never use)

User access should be verified. For authentication of WIFI networks, a central user database by name is preferred. Most corporate Wi-Fi access points provide LDAP or RADIUS support.
Unmanaged devices should only be allowed to access **[dedicated guest WIFI networks].** Network traffic between guest networks and those managed by **[Organisation]** should be prevented.

# Network management

* A high-level network diagram is developed and stored (printed) securely. This schema includes the hardware and function description, as well as the necessary (IP) addressing. This schema is updated on a regular basis.
* Management ports should be restricted to authorised personnel and should not be connected to the internet, unless via VPN.
* User access to management ports should be monitored regularly. A central user database by name is preferable for management access authentication.
* Installation or modification of network devices must be done by or in consultation with **[Organisation]** IT.
* Network infrastructure devices feature logging, focusing on monitoring and controlling traffic flows through network zones and different trust levels. Examples include important administrator events such as login, system changes, password resets...
* To ensure the availability and performance of critical and confidential systems, the presence of service level agreements (SLAs) for these network components should be considered.