



Information Security Policy

Alastair Taylor – Chief Executive Officer

NYnet Limited, 80 High Street, Harrogate, HG2 7LW.
Registered in England & Wales No. 06069791. VAT No. GB 123 4070 56.
NYnet is a UK limited company controlled by North Yorkshire County Council.

Telephone: +44 (0)1423 598210
Website: www.nynet.co.uk
Email: enquiries@nynet.co.uk



Information Security Policy

NYnet has a set of Information Security policies, procedures and rules which are mandatory and applicable to all staff both permanent and temporary. Failures, incidents and improvements are monitored and logged on ISO Activ improvement log and are approved and actioned at the security meeting.

These are certified as compliant with ISO 27001 and any necessary compliance requirements.

The objectives of security management at NYnet are to:

- Reassure customers, through external accreditation, that the service is unlikely to fail due to such things as security breaches or process failures, which shows NYnet is properly managing its services.
- Help NYnet remain compliant with contracts, customer expectations, legislation and regulations.
- Achieve 99.95% network availability through a High Availability Design approach.
- Reduce the risk of business disruption that might result from viruses, hacking or other types of security incident.

Security Policy and Rules

The full policies are available on ISO Activ which can be accessed via:

- <https://server1.isoinabox.co.uk/uk>

All employees should familiarise themselves with the policies and rules listed.

Continuous Improvement

Security is not perfect. All employees are mandated to support improvements. If anyone knows of or discovers security flaws, they must ensure they are logged on the *Improvement Log* (via Activ).

The **Security Manager** will track the issues and ensure that they are assigned and progressed to resolution.

Key Responsibilities and Objectives

Senior Management

The **Senior Management Team** is ultimately responsible for security. Their most important activities include the following and is a standing item on the Senior Managers meeting agenda:

- Understanding and agreeing the security requirements and objectives.
- Ensuring NYnet delivers on the security improvements through sponsorship, prioritisation and the provision of resources.

Risk Owner

The **Risk Owner** decides when NYnet has to take action to reduce risk. The Risk Owner can also take informed decisions not to address specific problems, however they must ensure they comply with NYnet's risk management rules.

Security Manager

Maintains the security management processes (the ISMS) and provides tools, measurements and insight for the management team.

The Security Manager is also the first point of call for security questions and advice, whether that advice is about security accreditation, designs or to help understand the risks and threats.

Operational and Technical Staff

Operational and technical teams will find that the work required to achieve the security objectives is largely their responsibility.

Staff must ensure they understand their responsibilities, have the necessary skills and training, and are committed to deliver improvement.

All Staff

All employees, permanent and temporary, of the company (and its contractors) must comply with NYnet's policies.

Failure to comply with security policy and requirements may lead to disciplinary action. In extreme cases it may lead to criminal proceedings.

Signed: _____

Alastair Taylor

Position: Chief Executive Officer

Date: _____