Information Security Policy

Contents

1 Document Control 1

1.1 Validity and Document management 1

1.2 Distribution 1

1.3 Change Record 1

2 Information Security Policy 2

3 Definitions 3

1 Document Control

1.1 Validity and Document management

Valid from	Responsibility
28-03-2018	The owner of this document is the ISWG who must check and, if necessary, update the document at least once a year. It does not contain confidential information and can be released to relevant external parties.

1.2 Distribution

Dated	Location
28-03-2018	Netnorth Management Share (ISMS) Netnorth Intranet Share (ISMS) – Accessible by all staff. Netnorth Website (Support)

1.3 Change Record

Version	Role	By	Dated	Description
v0.1	Authored	Tom Griffin	29-03-2017	First draft

Version	Role	By	Dated	Description
v1.0	Authored Approved Reviewed Reviewed Reviewed Reviewed Reviewed Reviewed	Tom Griffin G. Jackson G. Jackson G. Jackson G. Jackson G. Jackson G. Jackson G. Jackson	28-03-2018 28-03-2018 28-03-2018 14-05-2019 28-04-2020 15-01-2021 13-06-2022 09-01-2023	No Changes made

2 Information Security Policy

Netnorth is an Internet Service Provider. Netnorth have developed a range of hosting solutions on varied architectures and platforms. Security is a key aspect of all its activity and it is therefore vital that Netnorth ensures that any security breaches that are a risk to its ongoing business are mitigated.

A **SECURITY BREACH** is any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of the physical or electronic information assets of the Organisation.

The Directorate of Netnorth are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organisation, to preserve its competitive edge, cash-flow, profitability, legal, regulatory, contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Netnorth objectives and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

The organisation's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of the ISMS. The risk assessment, Statement of Applicability and risk treatment plan identify how information-related risks are controlled. The ISWG is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Manual and are supported by specific, documented policies and procedures.

All employees of the organisation and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy.

The ISMS is subject to continuous, systematic review and improvement

Netnorth has established an Information Security Working Group ISWG, chaired by the Directorate and including other executives / technical specialists / risk specialists, when relevant to support the ISMS framework and to periodically review the security policy.

Netnorth is committed to achieving certification of its ISMS to ISO27001:2013

This policy will be reviewed, to respond to any changes in the risk assessment or risk treatment plan, and at least annually.

3 Definitions

In this policy, "information security" is defined as:

Preserving

This means that management, all full time or part time staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities to preserve information security, to report security breaches (in line with the policy and procedures) and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in the Netnorth disciplinary policy. All staff will receive information security awareness training and more specialised staff will receive appropriately specialised information security training.

The Availability

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and Netnorth must be able to detect and respond rapidly to incidents (such as malware, loss of utility, DDoS etc.) that threaten the continued availability of assets, systems and information. There are appropriate disaster recovery and business continuity plans.

Confidentiality

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to Netnorth information and its systems including networks, websites, portals and extranet systems.

Integrity

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency (for networks, web sites and extranets), data back-up plans, and security incident reporting. Netnorth must comply with all relevant data-related legislation in those jurisdictions within which it operates.

Of the physical (assets)

The physical assets of Netnorth including but not limited to computer hardware, data cabling, telephone systems, filing systems and physical data files.

And information assets

The information assets include information printed or written on paper, transmitted by post or visual media, or spoken in conversation, as well as information stored electronically on servers, web sites, extranets, intranets, PCs, laptops, mobile phones and PDAs as well as on any other removable media, and information transmitted electronically by any means. In this context "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

The **ISMS** is the Information Security Management System, of which this policy, the information security manual ("the Manual") and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2013