Document number: T.2
Document Name: Communications (Network Security) Management Policy
Document Owner: Operations Director
Issue Date: 01/05/2024
Current Revision Date: 01/05/2024

Communications (Network) Security Management Policy

Objective and Scope

The objective of this document is to ensure the protection of information in networks and other related processing facilities both internally and externally.

Roles, Responsibilities and Authorities

The Operations Director or competent IT Team delegate takes ownership of the network security, controls, segregations and information transfer.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
Computer Misuse Act1990	www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2018/12/contents
Online Safety Act 2023	https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted
National Assistance Act 1948	https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
The Copyright, Designs and Patents Act 1988	https://copyrightservice.co.uk/
Market Research Society Code of Conduct	https://www.mrs.org.uk/pdf/MRS-Code-of-Conduct-2019.pdf
Market Research Society Fair Data Principles	https://www.fairdata.org.uk/10-principles/

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Network security management		13.1.		
Network controls - networks security		13.1.1		8.20
Security of network services		13.1.2		8.21
Segregation of networks		13.1.3		8.22

Web filtering				8.23
Non-disclosure agreements / confidentiality		13.2.4		6.6

Related Information

- Non Disclosure Agreements
- Information Classification Policy
- Change Management Procedure
- IS Event Reporting Policy

Policy

The Operations Director determines and implements the rules and protocols for managing the network controls.

Security measures necessary for particular services, such as security features, service levels and service requirements, are implemented. Prevision Research ensures network service providers implement these measures.

Networks may include use of servers/mainframe, computer operating systems including portable devices, printers, scanners. Network functionality may also include use of cables, telephone lines, radio waves, satellites, or wireless that allow data sharing.

Network control protocols - high risk information security

Networks and network devices are set up and controlled to provide security at a level appropriate to the data they transfer.

Consider the Information Security Classification and CIA (confidentiality, integrity and availability) needs of data to determine the suite of information requiring the highest level of security.

Network controls for this information shall be:

- Managed by the Operations Director only
- Limited to essential roles within the organisation who require access to do manage their job role
- Restricted to essential device needs only
- Safeguarded by technology solutions when there is a need to pass over public networks
- Subject to system logging and monitoring controls for the detection of suspect events
- Monitored against device access to identify any unauthorised devices

- Subject to user system network authentication such as password protection, multi factor authentication, certificate based authentication, biometric authentication or token based authentication.

Security of network services

To protect information in networks and information processing facilities from compromise via the network, the following controls are in place:

- Each network shall be assigned a classification level for the nature/type of information it transfers
- Network equipment and devices shall be assigned to personnel with the knowledge and security status to manage the asset
- Diagram and mapping of networks and files reflecting configuration management shall be maintained current
- Assigned roles and responsibilities for the network shall be segregated from ICT operational personnel responsibilities
- CIA controls over data transiting through public, third party or wireless networks shall be protected by secure transfer or Non disclosure agreements.
- Logging and monitoring of activities to detect CIA risk
- Authentication of systems on networks through Synology Directory Server.
- Controlling new connectivity of equipment and device on networks

Communications (Network) Security Management Policy

Security networks, devices and service providers include.

Device/Service	Company	Contact Name	Email	Telephone
Internet & Telecoms	GPS / City Talk / City Fibre	Dan Drake	Dan.Drake@citytalkgroup.co.uk	07776683348
Mobile Phones & Tablets	EE	Support		07953 966 150
Server & Router	Synology NAS (Managed in house)	Richi Turner	richi@previsionresearch.co.uk	01908 278303
Survey Software	Voxco	Megha Thakur	megha.thakur@voxco.com support@voxco.com	
Email and Office software	Microsoft 365		https://www.microsoft365.com/	
Cloud Backup	Synology C2		https://account.synology.com/en-uk/support/create/ticket	

Each provider is required to enter a Service Level Agreement with Prevision Research, documenting and including:

- scope of security measures provided,
- technologies applied to the services, including authentication measures, encryption use, network connection controls,
- technical parameters for connection and network services, and
- procedures in the case of a suspected network attack or restricted coverage.

Service provider agreements are held <insert details> and are subject to <insert frequency period> review.

Security of virtualised networks

To protect information passing over virtualised networks, a risk assessment of any planned or existing virtualised networks and risk controls shall be implemented including:

- limits to classified information access the VPN
- justifiable need for a VPN
- data security controls l firewalls

Communications (Network) Security Management Policy

Network segregation

Network segregation is in place to separate high risk data/information from other less sensitive and general information. Physical network segregation is in place with the high risk data network segregated from everything else.

All wireless networks must go through a network controlled gateway before granting access to the high security risk information (secure data) network or domain.

Each domain / network is gateway directed using either a firewall and/or router depending on the nature of the network.

Web filtering

Web filtering technology is practiced to prevent users from viewing some URLs or websites by preventing browsers from loading pages from restricted sites.

Firewalls are used as web filtering tools to block access to specific types of web content and high security risk sites from exposing internal services and computers to external threats.

Any website not on the White List may be subject to web filtering at the discretion of the Operations Director.

Non-disclosure Agreements or other confidentiality agreements

Confidentiality and non-disclosure agreements are in place and required to be used in circumstances where access to personal information, business sensitive information (CIA sensitive) or core software data is or may be accessible. Use the Non-disclosure Agreement (NDA) for employees and Confidentiality Agreement for external parties.

NDA’s and Confidentiality Agreements will vary according to legislative jurisdictions.

- Signatories from both Prevision Research and the recipient must be in place. Prevision Research approval for authorisations is assigned to the Centre Manager, Operations Director & Managing Director.
- NDAs and Confidentiality Agreements must be dated and have a finite life 24 months before review and re-approval with a new NDA or Confidentiality Agreement as appropriate.
- Prescribed content and approved/agreed use of content as prescribed
- Right to audit and monitor compliance to the NDA l CA
- Document destruction arrangements

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred. Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N

Communications (Network) Security Management Policy
