BrisDoc Patient care by people who care

NHS

Network Security

Version:	Owner:	Created:
1.6	Deb Lowndes (Programme and Service Director.)	1st August 2012
Published:	**Approving Director:**	**Next Review**
17/04/2025	Rhys Hancock (Director of Nursing, AHPs and Governance.)	17/04/2027

Contents

Introduction

The purpose of this document is to detail the Network Security Policy that applies within BrisDoc's Integrated Urgent Care Service and head office functions. The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network.

This document:

Sets out the organisation's policy for the protection of the confidentiality, integrity and availability of the network

Establishes the security responsibilities for network security

Provides reference to documentation relevant to this policy

Aim

The aim of this policy is to ensure the security of BrisDoc's networks. To do this BrisDoc will:

Ensure Availability

Ensure that the network is for users

Preserve Integrity

Protect the network from unauthorised or accidental modification ensuring the accuracy and completeness of the organisation's assets

Preserve Confidentiality

Protect assets against unauthorised disclosure

Network definition

The network is a collection of communication equipment such as servers, firewalls, computers, printers, and switches, which has been connected together by cables in all BrisDoc's Sites.

The network is created to share data, software, and peripherals such as printers, internet connections, disks and other data storage equipment.

Scope of this Policy

This policy applies to all networks within the Integrated Urgent Care Service and head office functions, that are used for:

The storage, sharing and transmission of non-clinical data

The storage, sharing and transmission of clinical data

Printing or scanning non-clinical or clinical data

The provision of Internet systems for receiving, sending and storing non-clinical or clinical data

The Policy

The overall Network Security Policy for BrisDoc is described below:

The BrisDoc information network will be accessible when required, limited to authorised users, and will maintain data integrity and accuracy. The network will be resilient against threats to its availability, integrity, and confidentiality.

To satisfy this, BrisDoc will undertake the following.

Protect all hardware, software and information assets under its control

Provide both effective and cost-effective protection that is commensurate with the risks to its network assets

Implement the Network Security Policy in a consistent, timely and cost-effective manner

Where relevant, BrisDoc will comply with:

Copyright, Designs & Patents Act 1988

Access to Health Records Act 1990

Computer Misuse Act 1990

Data Protection Act 2018 and UK GDPR

BrisDoc will comply with other laws and legislation as appropriate

The policy must be approved by the SIRO

Risk Assessment

BrisDoc will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

Risk assessments will be conducted to determine the appropriate security barriers to protect the network.

Physical & Environmental Security

Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality where possible.

Critical or sensitive network equipment will be housed in secure areas, with appropriate security barriers and entry controls where possible.

The ISM in conjunction with the Operational Managers are responsible for ensuring that access to network areas is secure.

Critical or sensitive network equipment will be protected from power supply failures.

Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

All visitors to secure network areas must be authorised by the Digital Team.

All visitors to secure network areas must be made aware of network security requirements.

All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out and will record in the visitor books for each site.

The Digital Team will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.

Access Control to Secure Network Areas

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it where possible.

Access Control to the Network

Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.

Remote access to the network will be restricted to 3rd Party Suppliers for supervised maintenance sessions as required or via the approved secure VPN token method as approved by the Digital Team.

The Digital Team and/or Operational Managers must approve user access.

Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis.

Security privileges (i.e. 'super-user' or network administrator rights) to the network will be allocated on the requirements of the user's job, rather than on a status basis.

Access will not be granted until the Operational Managers and/or the Digital Team registers a user.

All users to the network will have their own individual user identification and password, unless the exception is agreed.

Users are responsible for ensuring their password is kept secret (see User Responsibilities).

User access rights will be immediately removed or reviewed for those users who have left the BrisDoc or changed roles/jobs.

Third Party Access Control to the Network

Third party access to the network will be based on a formal contract that satisfies all necessary conditions.

External Network Connections

Ensure that all connections to external networks and systems have documented and approved System Security Policies.

The Digital Team must approve all connections to external networks and systems before they commence operation

Maintenance Contracts

The Programme and Service Director will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.

Data and Software Exchange

Formal agreements for the exchange of data and software between organisations must be established and approved by the SIRO, with support from the Digital Team.

Fault Logging

The Digital Team is responsible for ensuring that a log of all faults on the network is maintained and reviewed.

Data Backup and Restoration

The Programme and Service Director in conjunction with 3rd Party Suppliers are responsible for ensuring that backup copies of network configuration data are taken regularly.

Documented procedures for the backup process and storage of backup will be produced and communicated to all relevant staff.

All backups will be stored securely.

Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.

User Responsibilities, Awareness & Training

BrisDoc will ensure that all users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.

All users of the network must be made aware of the contents and implications of the Network Security Policy via IG Training and the staff fact sheet for Information Security.

Irresponsible or improper actions by users may result in disciplinary action(s).

Accreditation of Network Systems

Ensure that the network is approved by the SIRO before it commences operation. The SIRO is responsible for ensuring that the network does not pose an unacceptable security risk to the organisation.

Security Audits

The SIRO and Digital Team will require checks on, or an audit of, actual implementations based on approved security policies.

Malicious Software

Ensure that measures are in place to detect and protect the network from viruses and other malicious software.

System Change Control

The Programme and Service Director in conjunction with 3rd Party Suppliers and Digital Team are responsible for updating all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures.

The SIRO may require checks on, or an assessment of the actual implementation based on the proposed changes, as defined in Data Protection by Design Policy.

The SIRO and Digital Team are responsible for ensuring that selected hardware or software meets agreed security standards.

Security Monitoring

Ensure that the network is monitored for potential security breaches.

Reporting Security Incidents & Weaknesses

All potential security breaches must be investigated and reported to the Digital Team ity incidents and weaknesses must be reported in accordance with the requirements of the organisation's incident reporting procedure.

System Configuration Management

The SIRO and Digital Team are responsible for ensure that there is an effective configuration management system for the network, in conjunction with third party suppliers.

Business Continuity & Disaster Recovery Plans

Ensure that business continuity plans and disaster recovery plans are produced for the network.

The plans must be developed and reviewed by the SIRO and Digital Team and third-party suppliers where appropriate.

Unattended Equipment and Clear Screen

Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working.

The BrisDoc operates a clear screen policy that means that users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be locked or a screensaver password activated if a workstation is left unattended for a short time.

Security Responsibilities

The SIRO holds overall security responsibility for security, policy and implementation.

Line Manager's Responsibilities

Ensuring the security of the network, that is information, hardware and software used by staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.

Ensuring that their staff are made aware of their security responsibilities.

Ensuring that their staff have had suitable security training.

Version Control

Date	Version	Author	Change Details
31/08/12	1.0	DL	Document created.
25/09/12	1.1	DL	After discussions with HR and Ops Manager revisions to appendix B and removal of C
21/2/14	1.2	DL	Annual review, inclusion of Network Users Form
27/2/14	1.3	DL	Comments from NG review accepted
26/10/15	1.4	DL	Annual Review- change in new starter process reflected
26/11/17	1.5	DL	Annual Review
23/01/20	1.6	DL	Annual Review
10-04-25	1.7	DL	Review on change of SIRO