BrisDoc Patient care by people who care

Proudly employee owned.

Cyber Security

Version:	Owner:	Created:
1.0	Jon Rex (Head of DDaT)	23/10/2026
Published:	**Approving Director:**	**Next Review**
23/11/2026	Lewis Scandle	31st October 2027

Contents

Purpose 3
Scope 3
Roles and Responsibilities 3
Policy Statements 4
Compliance and Audit 5
Policy Review and Update 5
Associated Policies and Documents 6
Version Control 6

Purpose

This policy sets out BrisDoc's commitment to protecting its digital infrastructure, systems, data and services from cyber threats. Effective cyber security is fundamental to the safe delivery of care, the protection of patient and staff information, and the maintenance of public trust in BrisDoc and wider NHS services.

Scope

This policy applies to:

- All BrisDoc employees, contractors, volunteers, students and partner organisations
- All information systems and digital services owned, managed or controlled by BrisDoc
- All BrisDoc-issued and personal devices used to access BrisDoc systems or data

The policy applies across all BrisDoc service areas, including primary care, urgent care and services supporting people experiencing homelessness.

Objectives

Through this policy, BrisDoc aims to:

- Prevent, detect and respond effectively to cyber security incidents
- Meet the requirements of the **NHS Data Security and Protection Toolkit (DSPT)**, **UK GDPR** and the **Data Protection Act 2018**
- Apply good practice set out by the **National Cyber Security Centre (NCSC)**
- Embed a strong culture of cyber security awareness and responsibility across the organisation

Roles and Responsibilities

Senior Information Risk Owner (SIRO)

- Retains overall accountability for information risk, including cyber security risk
- Provides strategic oversight and ensures cyber security risks are appropriately recorded and managed through the organisational risk register

Caldicott Guardian

- Promotes the lawful and ethical use of confidential patient information
- Supports the response to incidents where the confidentiality of patient information may have been compromised

Programme and Service Director (Cyber Lead)

- Oversees implementation of BrisDoc's cyber security strategy, this policy and DSPT submissions
- Leads incident response planning and ensures alignment with NHS requirements and national standards

Digital / IT Providers and third-party Cyber Security Team

- Implement technical controls, including firewalls, endpoint protection and vulnerability scanning
- Monitor systems for suspicious activity and respond to technical security incidents
- Undertake regular system patching, backups and penetration testing

Line Managers

- Ensure that staff complete mandatory training and comply with this policy
- Report concerns and support the timely escalation of incidents

All Staff and System Users

- Complete mandatory cyber and data security training annually
- Report suspicious activity and potential security breaches promptly
- Follow secure working practices when using email, devices and information systems

Policy Statements

Access Control

- Access must be granted according to the principles of **need to know** and **least privilege**
- Every user must have a unique account and must not share their credentials
- Multifactor authentication (MFA) must be enabled for remote access and all administrative accounts
- Access for leavers must be revoked promptly in accordance with the relevant leaver process

Device and Network Security

- All BrisDoc-issued devices must use active antivirus or endpoint protection and device encryption
- Operating systems and software must be patched within 14 days of the release of critical security updates
- Only approved and appropriately secured devices may connect to the corporate network

Data Handling and Storage

- Confidential and personal data must be stored only in approved systems that provide appropriate access controls and logging
- The use of USB drives and other removable media is restricted; where authorised, the media must be encrypted
- Cloud storage must meet NHS security and compliance requirements, for example through BrisDoc's approved Microsoft 365 NHS tenancy

Secure Email and Internet Use

- NHSmail or another approved secure platform must be used when sending sensitive information

- Staff must exercise caution and must not open attachments or follow links from unknown or suspicious sources
- Personal use of the internet is permitted only where it complies with BrisDoc's acceptable use requirements

Remote and Mobile Working

- Remote access to BrisDoc systems must use an approved secure connection, including a virtual private network (VPN) where required
- Personal devices used for work must meet the minimum security requirements set out in BrisDoc's remote working requirements
- Lost or stolen devices used for BrisDoc work must be reported within 24 hours

Monitoring and Logging

- Security logs will be collected and reviewed in accordance with identified risks and compliance requirements, using BrisDoc's approved cyber security tools
- Intrusion detection and anomaly monitoring tools will be used to identify suspicious activity and potential threats
- User activity may be monitored where necessary for security investigations, incident response or compliance purposes

Cyber Incident Management

- All suspected or confirmed cyber security incidents must be reported immediately to the Digital team
- BrisDoc's incident response plan will be activated for high-severity events
- Incidents involving a personal data breach will be assessed to determine whether they must be reported to the **ICO** and through the **NHS DSPT**

Compliance and Audit

- Compliance with this policy will be assessed through internal audit, DSPT submissions and relevant external assurance activities
- Failure to comply with this policy may lead to disciplinary action, contractual review or legal consequences, as appropriate
- This policy supports BrisDoc's compliance with **UK GDPR**, the **Data Protection Act 2018**, the **NHS DSPT** and **Cyber Essentials**
- All staff must complete **mandatory cyber and data security training annually**
- Additional role-specific training will be provided for people in higher-risk roles, including system administrators and managers
- Cyber security awareness will be reinforced through regular updates, alerts and simulated phishing exercises

Policy Review and Update

This policy will be reviewed at least annually and may also be reviewed following:

- A major cyber security incident or data breach
- Changes to relevant legislation, regulation or national guidance

- Significant changes to BrisDoc's organisation, services or technology environment

The Programme and Service Director (Cyber Lead) is responsible for coordinating the review of this policy in consultation with IT providers, Information Governance and executive leadership.

Associated Policies and Documents

- Data Protection and Confidentiality Policy
- Information Governance Framework
- Cyber and Security Incident Management Plan
- IT Acceptable Use Policy
- Business Continuity and Disaster Recovery Policy
- National Data Guardian's 10 Data Security Standards
- NHS DSPT Requirements
- NCSC Cloud Security and Ransomware Guidance

Version Control

Date	Version	Author	Change Details
July 2025	1.0	DL	Document created.
Oct 2026	2.0	JR	Re-write as new policy