BLUEBIRD
NETWORK

INTERCONNECT POLICY

1 Introduction

1.1 This document defines the Interconnect Policy for Bluebird Network LLC (referred to hereafter as the Company). The Interconnect Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support and are Users of the network. This policy shall be in place in perpetuity and may be revised by Company leadership or Board of Directors.

1.2 This document:

a. Sets out the Company's policy for the protection of the confidentiality, integrity and availability of the network;
b. Establishes the security responsibilities for network security;
c. Provides reference to documentation relevant to this policy.

1.3 The network is a collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by cables or wireless devices. The network is created to share data, software, and peripherals such as printers, modems, fax machines, Internet connections, CD-ROM and tape drives, hard disks and other data storage equipment.

2 Purpose/Scope of this Policy

2.1 The purpose of this policy is to ensure the security of The Company's network. To do this the Company will:

a. Ensure Availability on a non-discriminatory basis related to interconnection obligations
Ensure that the network is available for Users;
b. Preserve Integrity
Protect the network from unauthorised or accidental modification;
c. Preserve Confidentiality
Protect assets against unauthorised disclosure.

2.2 The purpose of this policy is also to ensure the proper use of the Company's network and make Users aware of what the Company deems as acceptable and unacceptable use of its network.

2.3 Willful or negligent disregard of this policy may be investigated and dealt with under the Company Disciplinary Procedure.

2.4 This policy applies to all networks managed by The Company used for:

- The storage, sharing and transmission of data and images;
- The storage, sharing and transmission of data and images;
- Printing or scanning data or images;
- The provision of Internet systems for receiving, sending and storing data or images.

3 The Policy

3.1 The Interconnect Policy for The Company is described below:

The Company information network will be available when needed and can be accessed only by legitimate Users. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, The Company will undertake the following:

a. Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures;
b. Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
c. Implement the Interconnect Policy in a consistent, timely and cost-effective manner.
d. Where relevant, The Company will comply with:

-Copyright, Designs & Patents Act 1988
-Access to Health Records Act 1990
-Computer Misuse Act 1990
-The Data Protection Act 1998
-The Human Rights Act 1998
-Electronic Communications Act 2000
-Regulation of Investigatory Powers Act 2000
-Freedom of Information Act 2000
- Environmental Information Regulations 2004 (EIRs)
-Health & Social Care Act 2008

b. The Company will comply with other laws and legislation as appropriate.

4 Risk Assessment and audit

4.1 The Company is responsible for ensuring that appropriate risk assessment(s) are carried out in relation to all the business processes covered by this policy. The risk assessment will identify the appropriate countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.
4.2 SOC compliance and overall audits requires the Company to undertake a self-assessment audit based on defined indicators.
4.3 Internal Audit has the ability to undertake an audit of compliance with policy on request.

5 Physical & Environmental Security

5.1 Core network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that has a monitored temperature and backup power supply.
5.2 Core network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
5.3 Door lock codes will be changed periodically, following a compromise of the code or a suspected compromise.
5.4 Critical or sensitive network equipment will be protected from power supply failures.
5.5 Critical or sensitive network equipment will be protected by fire suppression systems.
5.6 Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.
5.7 All visitors to secure network areas must be authorised by a senior member of the technical support team.
5.8 All visitors to secure network areas must be made aware of security requirements.
5.9 All visitors to secure network areas must be logged in and out. The log will contain name, organization, purpose of visit, date, and time in and out.
5.10 The Company will ensure that all relevant staff are made aware of procedures for visitors.

5.11 Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The Company will maintain and periodically review a list of those with unsupervised access.

6 Access Control to the Network

6.1 Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access will be via secure two-part authentication.
6.2 There must be a formal, documented user registration and de-registration procedure for access to the network. Separate authorisation will be required for Remote Access to the network.
6.3 The departmental manager must approve User access prior to being processed by the IT Service Desk.
6.4 Access rights to the network will be allocated on the requirements of the User's job, rather than on a status basis.
6.5 Security privileges (i.e. 'Superuser' or network administrator rights) to the network will be allocated on the requirements of the User's job, rather than on a status basis.
6.6 Users will be sent a Terms of Use agreement on application, which they must familiarise themselves with.
6.7 Access will not be granted until the Service Desk registers a user.
6.8 All Users to the network will have their own individual User identification and password.
6.9 Users are responsible for ensuring their password is kept secret (see User Responsibilities 24.3).
6.10 User access rights will, upon notification from departmental managers, be immediately removed or reviewed for those Users who have left the Company or changed jobs.

7 Remote Access

7.1 Remote Access refers to any technology that enables the Company to connect users in geographically dispersed locations.
7.2 The Company is responsible for ensuring that a formal risk assessment is conducted to assess risks and identify controls needed to reduce risks to an acceptable level.
7.3 The Company is responsible for providing clear authorisation mechanisms for all remote access users.
7.4 Departmental Managers are responsible for the authorisation of all applications for remote access and for ensuring that appropriate awareness of risks is understood by proposed Users.
7.5 All remote access users are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources and notify the Company immediately of any security incidents and/or breaches.
7.6 The Company is responsible for ensuring that the Remote Access infrastructure is periodically reviewed, which could include but is not limited to independent third-party penetration testing.

8 Third Party Access Control to the Network

8.1 Third party access to the network will be based on a formal contract that satisfies all necessary NHS security conditions.
8.2 The IT Service Desk is responsible for ensuring all third-party access to the network is logged.
8.3 Access to the internet may be provided for Company staff or Company employed contractors via the IT Service Desk. Connection to the Company Wi-Fi infrastructure may be approved where a senior Company manager requests such access.

9 External Network Connections

9.1 The Company is responsible for ensuring that all connections to external networks and systems conform to the Code of Compliance and supporting guidance found in the Information Governance Toolkit.

9.2 The Company is responsible for ensuring all connections to external networks and systems are documented and approved by The Company before they commence operation.

10 Maintenance Contracts

10.1 The Company will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.

11 Data and Software Exchange

11.1 Formal agreements for the exchange of data and software between organizations must be approved by the Caldicott Guardian.

12 Fault Logging

13.1 The Service Desk is responsible for ensuring that a log of all faults on the network is maintained and reviewed.

13 Data Backup and Restoration

13.1 The Company is responsible for ensuring that backup copies of switch configuration and data stored on the network are taken regularly.

13.2 A log should be maintained of switch configuration and data backups detailing the date of backup and whether the backup was successful.

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

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

13.5 All backup tapes will be stored securely and a copy will be stored off-site.

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

13.7 Users are responsible for ensuring that they backup their own data to the network server.

13.8 Patches and any fixes will only be applied by The Company following suitable change control procedure.

14 Malicious Software

14.1 The Company must ensure that measures are in place to detect and protect the network from viruses and other malicious software.

15 Unauthorised software

16.1 Use of any non-standard software on Company equipment must be approved by The Service Desk before installation. All software used on Company equipment must have a valid licence agreement - it is the responsibility of the Information Asset Owner or Responsible User of non-standard software to ensure that this is the case.

16 Secure Disposal or Re-use of Equipment

16.1 The Company must ensure that where equipment is being disposed of all data on the equipment (e.g. on hard disks or tapes) is physically destroyed prior to leaving Company premises for disposal.

16.2 The Company must ensure that where electronic media are to be removed from the premises for repair, where possible, the data is securely overwritten.

17 System Change Control

17.1 The Company is responsible for ensuring that appropriate change management processes are in place to review changes to the network; which would include acceptance testing and authorisation. The Company is responsible for ensuring all relevant Network documentation is up to date.

17.2 The Company is responsible for ensuring that selected hardware or software meets agreed security standards.

17.3 Testing facilities will be used for all new network systems. Development and operational facilities should be separated.

18 Security Monitoring

18.1 The Company is responsible for ensuring that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

18.2 The Company reserves the right to access, modify or delete all data stored on or transmitted across its network. This includes data stored in personal network folders, mailboxes etc. Data of a personal nature should be stored in a folder marked or called ‘Private’. This does not preclude access or removal of such a folder on the authority of a senior IT manager.

18.3 The Company reserves the right to disconnect or block any device connected either by physical or wireless means to the network.

18.4 The Company reserves the right to block any physical non-approved device connected to a piece of Company owned equipment.

19 Training and Awareness

19.1 The IT team will work in conjunction with the Human Resources to provide security awareness training for all staff to ensure that they are aware of their responsibilities for security, and the actions that they need to undertake in order to discharge those responsibilities.

19.2 All users of the network must be made aware of the contents and implications of the Interconnect Policy.

20 Reporting Data Security Breaches and Weaknesses

21.1 Data Security Breaches and weaknesses, such as the loss of data or the theft of a laptop, must be reported in accordance with the requirements of the Company's incident reporting procedure and, where necessary, investigated by the IT/Security Team.

21 System Configuration Management

21.1 The Company will ensure that there is an effective configuration management process for the network.

22 Disaster Recovery Plans

22.1 The Company will ensure that disaster recovery plans are produced for the network and that these are tested on a regular basis.

23 Unattended Equipment and Clear Screen

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

23.2 The Company 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.

23.3 Users of dumb terminals must log out when not using the terminal.

24 Responsibilities

24.1 IT Team Responsibilities

24.1.1 Act as a central point of contact on network security within the organization, for both staff and external organizations.

24.1.2 Implement an effective framework for the management of network security.

24.1.3 Assist in the formulation of Interconnect Policy and related policies and procedures.

24.1.4 Advise on the content and implementation of the relevant action plans.

24.1.5 Produce organizational standards, procedures and guidance on Network Security matters for approval by the Company. All such documentation will be included in the Asset register.

24.1.6 Co-ordinate network security activities particularly those related to shared information systems or IT infrastructures.

24.1.7 Liaise with external organizations on network security matters, including representing the organization on cross-community committees.

24.1.8 Create, maintain, and give guidance on and oversee the implementation of network security.

24.1.9 Represent the organization on internal and external committees that relate to network security.

24.1.10 Ensure that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.

24.1.11 Ensure the systems, application and/or development of required policy standards and procedures in accordance with business needs, policy and guidance.

24.1.12 Ensure that access to the organization's network is limited to those who have the necessary authority and clearance.

24.1.13 Provide advice and guidance to development teams to ensure that the policy is complied with.

24.1.14 Approve system security policies for the infrastructure and common services.
24.1.15 Approve tested systems and agree plans for implementation.
24.1.16 Advise on the accreditation of IT systems, applications and networks
24.1.17 Ensure that Network Security is included within the Company Mandatory training program.
24.1.18 Support incident assessments, where necessary
24.1.19 Provide support on user matters relating to Network Security
24.1.20 Ensure 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.
24.1.21 Ensure that staff are aware of their security responsibilities.
24.1.22 Ensure that staff have had suitable security training.
24.1.23 Ensure that the IT Service Desk is promptly notified when new accounts are required.
24.1.24 Ensure that the IT Service Desk is promptly notified when existing accounts are to be reviewed or deleted, e.g. when a member of staff changes roles or leaves the organization.

24.2 User Responsibilities

All personnel or agents acting for the organization have a duty to:

24.2.1 Safeguard hardware, software and information in their care.
24.2.2 Prevent the introduction of malicious software on the organization's IT systems.
24.2.3 Users are responsible for ensuring their password is kept secret - ***passwords should not be shared under any circumstances.***
24.2.4 If a user suspects that their network password has become compromised, they should report this to the IT Service Desk and change their password.
24.2.5 Report on any suspected or actual breaches in security.

24.3 SIRO Responsibilities

The Senior Information Asset Risk Owner is responsible for:

25.3.1 Making arrangements for information security by setting an overall Interconnect Policy for the organization.
25.3.2 Meeting the legal requirement and ensuring that operational compliance is further delegated to the Information Asset Owners.
25.3.3 Ensuring that, where appropriate, staff receive Information Security awareness training.
25.3.4 Ensuring that the network is risk assessed and any risks identified either mitigated or escalated

25 Further information

26.1 If you would like any further information regarding this policy, please do not hesitate to contact the IT Security Team.

If you do not have any questions the Company presumes that you understand and are aware of the rules and guidelines in this Internet Use Policy and will adhere to them.