NETWORK SECURITY POLICY

BADGER GROUP
Badger House
121 Glover Street
Birmingham, B9 4EY

Destroy All Previous Issues

Contents

DOCUMENT CONTROL

Document Storage

Location: P:\Ops Team\Central Policies & Procedures - Development - Word Docs\IG - IGSoc - GDPR Policies\IG-34 - Network Security Policy V1.9.docx

Version Control Log (Only last 3 versions, earlier versions can be found in the appropriate Archive directory for the document)

Version	Date	Author	Description of Changes
V1.7	Apr 2022	A Savage	Reviewed, Updates to sections 5, 14, 21.1
V1.8	Apr 2023	A Savage	Reviewed, minor changes, contract due for review Octo 2023
V1.9	Oct 2023	Jo Carey	Reviewed, minor changes

Approval

Version	Name	Position	Signature	Approved Date
V1.3	IGSG	IG Steering Group		22 Feb 2017
V1.5	Badger Executive	Executive Team		25 July 2019

Glossary

Term	Description
CEO	Chair Executive Officer
IG	Information Governance
SIRO	Senior Information Risk Officer

1 INTRODUCTION

This document defines the Network Security Policy for Badger.

This 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 Badger policy for the protection of the confidentiality, integrity and availability of the network.
- Establishes the responsibilities for network security.
- Provides reference to documentation relevant to this policy.

2 PURPOSE

The purpose of this policy is to ensure the proper use of the Badger network and make users aware of what Badger deems as acceptable and unacceptable use of its network. Further information on acceptable use can also be found in related policies listed in Appendix A.

If there is evidence that any user is not adhering to the guidelines set out in this policy, this may be dealt with under Badger's Disciplinary Procedure.

3 AIM

The aim of this policy is to ensure the security of the network. To do this Badger will:

- Ensure that Badger's network is available to authorised users only.
- Preserve the integrity of all information and data on the network by protecting the network from unauthorised or accidental modification ensuring the accuracy of Badger's assets.
- Preserve confidentiality of all information and data on the network by protecting against unauthorised disclosure.

4 SCOPE OF POLICY

This policy applies to all networks within Badger used for:

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

This policy applies to anyone using Badger's computer network including any staff seconded to Badger, contractors, temporary and agency staff, students and other staff.

Badger's information network will be available when needed and can only be accessed by authorised users. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality.

To satisfy this, Badger will undertake the following:

- 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.
- 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.

5 NETWORK DEFINITION

The network is a collection of communication equipment such as servers, computers, printers, switches, hubs, and routers, which have been connected. The network is created to share data, software, and peripherals such as printers, photocopiers, Internet connections, Email connections, hard disks, and other data storage equipment.

6 RISK MANAGEMENT

Badger will carry out security risk assessments in relation to all the business processes covered by this policy as part of business continuity and disaster recovery planning.

These risk assessments will cover all aspects of the network that are used to support business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity, and availability.

7 PHYSICAL & ENVIRONMENTAL SECURITY

1. 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.
2. Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and access controls.
3. The Chief Executive is responsible for ensuring the security and safety of the equipment.
4. Critical or sensitive network equipment will be protected from power supply failures by the use of UPS devices.
5. Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.
6. All visitors to secure network areas must be authorised by the Chief Executive, or appropriately authorised staff.
7. All visitors to secure network areas must be made aware of network security requirements.
8. 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.
9. The Chief Executive will ensure that all relevant staff are made aware of procedures for visitors and those visitors are escorted, when necessary.
10. Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The Head of Technology will maintain and periodically review a list of those with unsupervised access.

8 ACCESS CONTROL TO THE NETWORK

1. 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 is allowed for key workers, IG-17 applies, as deemed appropriate by the CEO
2. There is a formal, documented user registration and de-registration procedure for access to the network. Forms for new user, changes and leavers are available from the shared pool area or the Mission Control desk.
3. The CEO must approve user access.
4. Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis.
5. 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.
6. Access will not be granted until a user is fully registered, and duly authorised the CEO.
7. Administrative staff who access the network will have their own individual user identification and password.
8. Call centre agents access the network via individual user accounts. There is also a generic account with restricted access. Once on the network, the agent logs into Adastra with their own individual user identification and password.
9. Users are responsible for ensuring their password is kept secret (see Section 21 Responsibilities).

10. User access rights will be immediately removed or reviewed for those users who have left Badger or changed jobs.

9 THIRD PARTY ACCESS CONTROL TO THE NETWORK

Third party access to the network will be based on a formal contract that includes a standard clause which satisfies all necessary NHS confidentiality and security conditions, and completion of a New User Form must also be completed and all third party access to the network must be logged.

10 MAINTENANCE CONTRACTS

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

11 DATA EXCHANGES

Data exchanges must be registered with the IG Lead. Exchange of any data must be approved for person-identifiable or commercially sensitive information.

12 FAULT LOGGING

The IT Lead is responsible for ensuring that a log of all faults on the network is maintained and reviewed. All faults are reported via the team leader report or in person to the IT team.

13 NETWORK OPERATING PROCEDURES

Documented operating procedures should be prepared for the operation of the network, to ensure its correct, secure operation. Changes to operating procedures must be authorised by the Head of Technology.

14 DATA BACKUP AND RESTORATION

The network provider is responsible for ensuring that backup copies of network configuration data are taken daily. Backups are stored securely in the provider datacentre.

15 MALICIOUS SOFTWARE

Badger will use security products to detect and protect the network from viruses and other malicious software – viruses, spyware, Trojan horses, worms etc.

16 UNAUTHORISED SOFTWARE

Required use of any non-standard software on Badger equipment must be notified to the Head of Technology before installation. All software used on Badger equipment must have a valid licence agreement - it is the responsibility of the "owner" or Responsible User of non-standard software to ensure that this is the case.

17 SECURE DISPOSAL OR RE-USE OF EQUIPMENT

Where equipment is being disposed of, the IT Lead will ensure that all data on the equipment (e.g. on hard disks or tapes) is securely overwritten. Where this is not possible, the IT Lead will physically destroy the disk or tape.

In the event of the need for disposal of storage media, this will be done through a company who should conform to the BS EN 15713:2009 (Secure Destruction of Confidential Material)

18 CHANGES TO THE NETWORK

1. Any proposed changes to the network will be reviewed and approved by the Head of Technology
2. Adastra are responsible for updating all relevant design documentation, security operating procedures and network operating procedures.

3. The Head of Technology may require checks on, or an assessment of the actual implementation based on the proposed changes.
4. The Head of Technology is responsible for ensuring that selected hardware or software meets agreed security standards.
5. Testing facilities will be used for all new network systems. Development and operational facilities will be separated.

19 SECURITY MONITORING

The Information Security Officer will ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

20 REPORTING SECURITY INCIDENTS & WEAKNESSES

All potential security breaches must be reported in accordance with the requirements of CG-02 Adverse Events including IG Serious Incidents Policy. Investigations will be undertaken by the Information Security Officer or a nominated person.

Incidents will be reviewed by the Information Governance Steering Group. Any Serious Untoward Incidents (SUI) will be immediately reported to the IG Lead and Caldicott Guardian where appropriate.

A major incident would constitute a loss of function of a clinical system or breach of confidential information for one or more individuals or a breach of information which is likely to lead to harm to an individual.

21 RESPONSIBILITIES

Responsibility for information security resides ultimately with the Chief Executive who is also the designated SIRO and supported by the IG Lead.

21.2 Information Security Officers

ISOs have lead responsibility for information security management within Badger acting as a central point of contact on information security for both staff and external organisations.

1. Produce organisational standards, procedures and guidance on Information Security matters for approval by the Information Governance Steering Group.
2. Co-ordinate information security activities particularly those related to shared information systems or IT infrastructures.
3. Be responsible for the deployment of Department of Health approved encryption software within Badger.
4. Ensure risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of risk.
5. Ensuring that access to Badger's network is limited to those who have the necessary authority and clearance.
6. Advise users of information systems, applications and networks of their responsibilities under the Data Protection Act 2018 and the UK's implementation of the General Data Protection Regulation (GDPR).

21.3 User Responsibilities / All Staff

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

Badger 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 if a workstation is to be left unattended for a short time.

All users have a responsibility to safeguard hardware, software and information in their care and prevent the introduction of malicious software to Badger's systems.

Any suspected or actual breaches in security must be reported to the Information Security Officer.

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

Departmental managers must ensure that the IT Department is promptly notified when new accounts are required, or staff leave Badger.

22 MONITORING AND REVIEW

All breaches of this policy should be reported in line with the Badger CG-02 Adverse Events including IG Serious Incidents Policy.

A report of breaches of this policy shall be presented to the Badger's Information Governance Steering Group. The information will enable the monitoring of compliance and enable improvements to be made to the policy.

23 REFERENCE DOCUMENTS

- Badger IG-01 - Information Governance Policy & Management Framework
- Badger IG-05 - Information Security Policy
- Badger IG-17 - Mobile Computing and Tele-working Policy
- Badger IG-33 – Checklist for New and Changed Systems, Processes and Services
- Badger CG-02 – Adverse Events Policy inc Serious Incidents