02 - Information Security Policy

Version:	3
Last review date:	January 2019
Reviewed by:	Lisa Boullé, Business Support Manager
Next Review date:	January 2021
Approved by:	Glenn Atter, CTO

Contents

1. Policy aim

This information security policy is a key component of the Brain in Hand Ltd overall information security management framework and should be considered alongside more detailed information security documentation, protocols or procedures

The objectives of this Information Security Policy are to preserve:

- **Confidentiality:** Access to Data will be confined to those with appropriate authority.
- **Integrity:** Information will be complete and accurate. All systems, assets and networks will operate correctly, according to specification.
- **Availability:** Information will be available and delivered to the right person, at the time when it is needed.

2. Objectives

The aim of this policy is to establish and maintain the security and confidentiality of information systems, applications and networks owned or held by Brain in Hand Ltd by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they will be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

3. Scope

This policy applies to all information, information systems, networks, applications, locations and users of Brain in Hand Ltd or supplied under contract to it.

4. Responsibilities for Information Security

Ultimate responsibility for information security rests with the Chief Executive of Brain in Hand Ltd, but on a day-to-day basis the IG Lead will be responsible for managing and implementing the policy and related procedures.

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- The information security policies applicable in their work areas.
- Their personal responsibilities for information security.
- How to access advice on information security matters.

All staff will comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

The Information Security Policy will be maintained, reviewed and updated by the IG Lead. This review will take place annually.

Line managers will be individually responsible for the security of their physical environments where information is processed or stored.

All members of staff will be responsible for the operational security of the information systems they use.

All members of staff will comply with security requirements that are currently in force, and will also ensure that the confidentiality, integrity, and availability of the information they use is maintained to the highest standard.

Contracts or letters of understanding with external contractors that allow access to the organisation's information systems will be issued before access is allowed. These contracts will ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

5. Legislation

Brain in Hand Ltd is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of Brain in Hand Ltd who may be held personally accountable for any breaches of information security under their control. Brain in Hand Ltd will comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (2018)
- The General Data Protection Regulation (2018)
- The Data Protection (Processing of Sensitive Personal Data) Order (2000)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Right Acts (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Health and Social Care Act (2001)

6. Policy Framework

a. **Management of Security**
   - At board level, responsibility for Information Security will reside with the Chief Executive.
   - The IG Lead will be responsible for implementing, monitoring, documenting and communicating security requirements within and on behalf of the organisation.

b. **Information Security Awareness Training**
   - Information security awareness training will be included in the staff induction process.
   - An ongoing training programme will be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.
   - Trainings will be independently verified by the HSCIC IG Training Toolkit.

c. **Contracts of Employment**
   - Staff security requirements will be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause.
   - Information security expectations of staff will be included within appropriate job definitions.

d. **Secure Control of Assets**
   - Each IT asset, (hardware, software, application or data) will have a named custodian who will be responsible for the information security of that asset.

e. **Access Control**

- Only authorised personnel who have a justified and approved business need will be given access to restricted areas containing information systems or stored data.

f. **User Access Controls**

- Access to information will be restricted to authorised users who have a bona-fide business need to access the information.

g. **Computer Access Control**

- Access to computer facilities will be restricted to authorised users who have business need to use the facilities.

h. **Application Access Control**

- Access to data, system utilities and program source libraries will be controlled and restricted to those authorised users who have a legitimate business need (e.g. systems or database administrations).

i. **Equipment Access Control**

- In order to minimise loss of, or damage to, all assets, equipment will be physically protected from threats and environmental hazard.

j. **Computer and Network Procedures**

- Management of computers and networks will be controlled through standard documented procedures that have been authorised by the Executive.

k. **Information Risk Assessment**

- Once identified, information security risks will be investigated by the CTO with assistance from the IG lead as necessary. They will be recorded within a risk register and action plans will be put in place to effectively manage those risks. The risk register and all associated action actions will be reviewed at regular intervals, forming a risk management programme. These reviews will help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

l. **Information security events and weaknesses**

- All information security events and suspected weaknesses are to be reported to the IG Lead. All information security events will be investigated to establish their cause and impacts with a view to avoiding similar events.

m. **Classification of Sensitive Material**

- Where applicable, the Company will implement appropriate information classification controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure any NHS information assets.

n. **Protection from Malicious Software**

- The organisation will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff will be excepted to co-operate fully with this policy. Users will not install software on the organisation's property without permission from their line manager, with advice from the IG Lead or CTO as necessary. Users breaching this requirement maybe be subject to disciplinary action.

o. **Removable/Portable Media**

- Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of IG Lead before they may be used on Brain in Hand Ltd systems. Such media must also be fully virus checked before being used on the organisation's equipment. Staff breaching this requirement may be subject to disciplinary action.

p. **Monitoring System Access and Use**

System access and data use by staff is recorded and may be interrogated. The Company reserves the right to monitor staff or contractor activity where it suspects that there has been a breach of policy for the following reasons:

- Establishing the existence of facts.
- Investigating or detecting unauthorised use of the system.
- Preventing or detecting crime.
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by person using the system (quality control and training).
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Acts.

q. **Accreditation of Information Systems**

- The organisation will ensure that all new information systems, application and networks include a security plan and are approved by the IG Lead before they commence operation.

r. **System Change Control**

- Changes to information systems, applications or networks will be reviewed and approved by the IG Lead and CTO as necessary.

s. **Intellectual Property Rights**

- The organisation will ensure that all information products are properly licensed and approved by the IG Lead. Staff will not install software on the organisation’s property without permission from the IG Lead. Staff breaching this requirement may be subject to disciplinary action.

t. **Business Continuity and Disaster Recovery Plans**

- The organisation will ensure that business impact assessment, business continuity and disaster recovery plans are produced for all company and client critical information, applications, systems and networks.

u. **Reporting**

- The Information Security Officer will keep the Executive informed of the information security status of the organisation by means of the regular reports and presentations.

v. **Policy Review**

- This policy will be subject to review by the Executive on an annual basis.