**Information Security Policy**

**Introduction**

This top-level information security policy is a key component of organizations overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

1. **Objectives, Aim and Scope**
   1. **Objectives** [Typical objectives are outlined below. Edit as appropriate].

The objectives of ***<Company Name>*** Information Security Policy are to preserve:

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

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by ***<Company Name>*** 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 principals of security and explaining how they shall be implemented in the organization.
* Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
* Creating and maintaining within the organization 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 organization.
  1. **Scope** [Edit as appropriate]

[This policy applies to all information, information systems, networks, applications, locations and users of ***<Company Name>*** or supplied under contract to it].

1. **Responsibilities for Information Security** [More responsibility details can be added if necessary]
   1. Ultimate responsibility for information security rests with the Chief Executive of ***<Company Name>***, but on a day-to-day basis the [enter officer title (and HIS if applicable)] shall be responsible for managing and implementing the policy and related procedures.
   2. 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
  1. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.
  2. The Information Security Policy shall be maintained, reviewed and updated by the [enter officer or Board title]. This review shall take place [enter review period e.g. annually].
  3. Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.
  4. Each member of staff shall be responsible for the operational security of the information systems they use.
  5. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
  6. Contracts with external contractors that allow access to the organization’s information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organization shall comply with all appropriate security policies.

1. **Legislation** 
   1. The ***<Company Name>*** is obliged to abide by all relevant legislation. The requirement to comply with legislation shall be devolved to employees and agents of the ***<Company Name>***, who may be held personally accountable for any breaches of information security for which they may be held responsible. The ***<Company Name>*** shall comply with the following legislation and other legislation as appropriate:

* The Data Protection Act
* The Data Protection (Processing of Sensitive Personal Data) Order.
* The Copyright, Designs and Patents Act
* The Computer Misuse Act
* The Health and Safety at Work Act
* Human Rights Act
* Regulation of Investigatory Powers Act
* Freedom of Information Act
* Health & Social Care Act

1. **Policy Framework**
   1. **Management of Security**

* At board level, responsibility for Information Security shall reside with the [insert appropriate director].
* The ***<Company Name>*** Security Officer [or appropriate title] shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organization.
  1. **Information Security Awareness Training**
* Information security awareness training shall be included in the staff induction process.
* An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.
  1. **Contracts of Employment**
* Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
* Information security expectations of staff shall be included within appropriate job definitions.
  1. **Security Control of Assets**

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

* 1. **Access Controls**

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

* 1. **User Access Controls**

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

* 1. **Computer Access Control**

Access to computer facilities shall be restricted to authorized users who have business need to use the facilities.

* 1. **Application Access Control**

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorized users who have a legitimate business need e.g. systems or database administrators. Authorization to use an application shall depend on the availability of a license from the supplier.

* 1. **Equipment Security**

In order to minimize loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

* 1. **Computer and Network Procedures**

Management of computers and networks shall be controlled through standard documented procedures that have been authorized by the [enter appropriate board e.g. Information Governance].

* 1. **Information Risk Assessment**

[The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence].

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of an organization’s risk management programme. These reviews shall 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.

* 1. **Information security events and weaknesses**

All information security events and suspected weaknesses are to be reported to the [insert appropriate officer title and contact details]. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

* 1. **Classification of Sensitive Information.**

A consistent system for the classification of information within the ***<Company Name>*** enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with non-***<Company Name>*** bodies.

***<Company Name>*** shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their information assets.

The classification ***<Company Name>* Confidential** – shall be used for information passing among the employees. Documents so marked shall be held securely at all times in a locked room to which only authorized persons have access. They shall not be left unattended at any time in any place where unauthorized persons might gain access to them. They should be transported securely in sealed packaging or locked containers.

The classification ***<Company Name>* Restricted -**  shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

* adversely affect the reputation of the organization or its officers or cause substantial distress to individuals;
* make it more difficult to maintain the operational effectiveness of the organization;
* cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organizations;
* prejudice the investigation, or facilitate the commission of crime or other illegal activity;
* breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
* breach statutory restrictions on disclosure of information;
* Disadvantage the organization in commercial or policy negotiations with others or undermine the proper management of the organization and its operations.

***<Company Name>*** Restricted documents should also be stored in lockable cabinets

* 1. **Protection from Malicious Software**

The ***<Company Name>***  shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the ***<Company Name>*** property without permission from the [insert appropriate officer]. Users breaching this requirement may be subject to disciplinary action.

* 1. **User 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 [the appropriate officer] before they may be used on [organization] systems. Such media must also be fully virus checked before being used on the organization’s equipment. Users breaching this requirement may be subject to disciplinary action.

* 1. **Monitoring System Access and Use**

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis. The ***<Company Name>* has** in place routines to regularly audit compliance with this and other policies. In addition it reserves the right monitor activity where it suspects that there has been a breach of policy.

* 1. **Accreditation of Information Systems**

The ***<Company Name>***  shall ensure that all new information systems, applications and networks include a security plan and are approved by the [insert appropriate security officer] before they commence operation.

* 1. **System Change Control**

Changes to information systems, applications or networks shall be reviewed and approved by the [insert appropriate security officer].

* 1. **Intellectual Property Rights**

The ***<Company Name>*** shall ensure that all information products are properly licensed and approved by the [insert appropriate security officer]. Users shall not install software on the ***<Company Name>*** property without permission from the [insert appropriate officer]. Users breaching this requirement may be subject to disciplinary action.

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

The ***<Company Name>***  shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

* 1. **Reporting**

The Information Security Officer shall keep the [insert appropriate Board] informed of the information security status of the ***<Company Name>*** by means of regular reports and presentations.

* 1. **Policy Audit**

This policy shall be subject to audit by [enter details of audit here].

* 1. **Further Information**

Further information and advice on this policy can be obtained from [insert name, email and telephone number of appropriate officer].

1. **Policy approved by:**

Signature Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Insert name, post of Chief Executive ***<Company Name>***]

**Source:** <https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwjU9sG2zLrMAhVBHaYKHSnMBgQQFghJMAM&url=https%3A%2F%2Fwww.igt.hscic.gov.uk%2FKnowledgeBaseNew%2FNHS%2520CFH_Corporate%2520InfoSec%2520Policy%2520Template%25202007.doc&usg=AFQjCNE6Auqc333eqVbpz9cuU0n8HAnyMA&bvm=bv.121070826,d.dGY&cad=rja>