Information Security and Governance Policy

Version:	1.2
Ratified by:	Information Governance Group
Date ratified:	1st October 2015
Name of organisation / author:	Derek Wilkinson
Name of responsible committee / individual:	Eileen Milner – Executive Director of Customer and Corporate Services
Date issued:	31st October 2015
Review date:	October 2018
Target audience:	All Staff

Contents

1. Purpose and Scope

The security policy document set details the high level security principles for the Care Quality Commission and establishes the framework under which each of the other sections of the security document set should be interpreted, managed and applied. The document has been produced in line with the requirements and guidance contained in ISO27001 and ISO27002:2005.

The overall purpose of this policy document is to provide both an overview of CQC information security requirements and standards (section 4) and a detailed reference document which may be used to address specific queries on information security.

This security policy applies and will be available to all staff working in the Commission in whatever capacity. It is also relevant as evidence of good, recognised information security practices during internal or external audit processes. Relevant sections of the policy may also be used as a reference point in negotiating or agreeing contracts with external suppliers.

The standards and controls detailed within this policy document set the security goals within CQC in line with the security strategy to achieve compliance with ISO27001. To this end the policy document details the aspiration of CQC to comply with the standard it does not provide a summary of the current state of security controls in place at any given time.

The purpose of detailing the ISO27001 compliant controls in this policy document is to set the standards that CQC aim to achieve and to provide the detail required by the business units and, where applicable, 3rd party suppliers to ensure that both existing and planned systems comply, or work incrementally towards compliance with ISO27001.

2. Policy / Procedure Statement

This policy has been developed for use across the whole of the Commission and complies with the requirements of widely recognised good information security practice. It will:

- Assist staff to apply the correct level of security control to their day to day activities in line with good practice and applicable regulation and legislation.
- Be formatted, controlled and distributed in line with CQC requirements.
- Assist with the development and commissioning of new processes and systems by detailing the required security settings and standards.

The policy will be available, as the correct up to date version, on the intranet to all staff.

Any departments or staff who have a requirement to store or otherwise use hard copies of this policy should ensure that they frequently check that they have the latest version of the policy and refer any queries to the information security team. They should also ensure that any old, outdated versions of this document are destroyed and replaced as necessary.

3. Responsibilities

Party	Key Responsibilities

Information Governance Group	Delegated responsibility from the Audit, Risk and Assurance Committee (ARAC) for review and approval of security and IG policies. Oversight, guidance and approval of the information risk and incident management processes.
Senior information security risk owner	For ensuring that this policy and the information risk policy is implemented, reviewed and its effect is monitored.
Caldicott Guardian	The Caldicott Guardian is the senior person responsible for protecting the confidentiality of personal and sensitive data and enabling appropriate information sharing.
Information Security Manager	The Security Manager is responsible for the definition, implementation, monitoring and management of the Information Security Management System (ISMS) and information security policy documents. The Security Manager organises and manages participation in any joint information security committees with the Department of Health, 3rd party ICT providers and other external organisations.
Staff	All staff will adhere to this policy and associated procedures. They will raise any issues of non-compliance, information risk or incidents with either their line manager or directly with the security team.

4. Information security policy

4.1 Introduction

4.1.1 Overview of this document

This section of the Security Policy statement introduces the set of documents that collectively make up the new Security Policy that governs the operations of the Care Quality Commission. The new policy replaces the following previous security policy documents:

- Information Security Policy
- Information handling guidance
- Information technology security – acceptable use
- Internet – acceptable use policy

This section defines the general principles of the Security Policy, and establishes the framework under which each of the other Security Policy documents must be interpreted, approved, communicated, and managed. There is also a description of the most important roles and responsibilities for information governance within the organisation.

Appendix A provides a list of the individual sections of the document that make up the Security Policy. These documents follow the format of the international standard for

Information Security Management Systems (ISO/IEC 27001), which is widely acknowledged as good practice and referred to in the HMG Security Policy Framework.

Appendix B provides a glossary of information security terms used throughout the Security Policy documents.

4.1.2 Other legislation and policies referred to

- HMG Security Policy Framework.
- ISO27001:2005 / ISO/IEC17799:2000. *Information Technology – Information security management systems requirements.*
- ISO27002:2005. *Code of practice for* i*nformation security management systems.*
- ISO27005:*2008. Information Security Risk Management.*
- Freedom of Information Act 2000.
- Data Protection Act 1998.
- Regulation of Investigatory Powers Act 2000.
- Computer Misuse Act 1990.
- Connecting for Health (CfH) Information Governance Toolkit requirements.
- E-Government Interoperability Framework (eGIF) policies and specifications.
- Information Security management NHS Code of Practice 2007.
- CQC HR Disciplinary Policy.
- CQC HR Equality and Diversity Policy.
- CQC Records Management Policy.

Although this security policy refers to health and safety provisions, as well as compliance with other legal, regulatory and contractual obligations, they are not within the direct scope of the policy.

4.2 General principles

4.2.1 The importance of information security

Information can be defined as useful data for a particular analysis, decision or task. Information must always be protected appropriately irrespective of how it is stored, presented or communicated.

The main aims of information security are to preserve:

- **Confidentiality:** ensuring that information is accessible only to those who are authorised to have access.
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods.
- **Availability:** ensuring that authorised users have access to information when needed.

It also aims to support the requirements of:

- **Accountability:** accounting for the actions of individuals by monitoring their activities.

- **Non-Repudiation:** legally acceptable assurance that transmitted information has been issued from and received by the correct, appropriately authorised, individuals.

The Care Quality Commission has a responsibility to securely manage its information assets, the information made available to it by providers, and the people who use providers' services, as well as that provided by its own employees, contractors, and business partners, and to protect that information from unauthorised disclosure, loss of integrity or availability.

All parts of the organisation are responsible for making sure that information is protected adequately. Senior management are responsible for issuing and endorsing this Security Policy. They recognise the sensitive nature of the information that the organisation stores and processes, and the serious potential harm that could be caused by security incidents affecting this information. They will therefore give the highest priority to information security. This will mean that security matters will be considered as a high priority in making any business decisions. This will help CQC to allocate sufficient human, technical and financial resources to information security management, and to take appropriate action in response to all violations of Security Policy.

CQC will use this Security Policy as the basis for an organisation-wide strategy to set the correct level of information security.

The security efforts will be:

- **Coordinated:** security measures will be based on a common framework provided by the Security Policy, and all staff will be involved in maintaining compliance with the security policy.
- **Proactive:** we will detect, identify and manage vulnerabilities, threats, and security gaps to prevent security incidents as far as we possibly can.
- **Supported at the highest level:** senior management are actively committed to information security and give their full support to implementing the required security controls that are identified through a continuous risk assessment process.

These security efforts will be structured and directed by the Security Policy, which covers all aspects of information security within CQC's business operations.

4.2.2 Purpose of the Security Policy

This Security Policy comprises a set of decisions endorsed by the Executive Team about how CQC will address its obligations relating to information security and data protection. The policy will also address actual or potential security issues relating to the information assets that CQC either owns or handles on behalf of other parties. These decisions are documented and communicated by the Information Governance Group. They detail the intentions and commitments of the Executive Team and the obligations for all individuals regarding compliance with the Security Policy.

The Security Policy serves several purposes, it:

- Clearly defines management's expectations, so that requirements can be applied uniformly.

- Represents a framework that provides direction to CQC, so that resources are allocated efficiently.
- Acts as a measure against which compliance requirements can be validated.
- Enables the requirements of the policy and the consequences of non-compliance to be communicated.
- Assigns responsibilities and highlights the strategic value of information security throughout the organisation, and to relevant third parties.

4.2.3 Scope of the Security Policy

For the purpose of the Security Policy, “CQC services” are those services provided in relation to the core business of the organisation.

The scope of the Security Policy is defined across three dimensions:

- The people who are subject to the Policy and who need to comply with it.
- The assets that are covered by the Policy and subject to its protection.
- The regulatory and legislative obligations and requirements that the policy covers.

4.3 People

The Security Policy applies to all CQC’s staff, directly or indirectly managed, who are involved with supporting the delivery of regulatory and associated activities, including:

- Permanent employees of CQC or an affiliate organisation.
- Individuals contracted by CQC either directly or through employment agencies.
- Staff of sub-contractors of CQC.
- Any other individuals with authorised access to CQC information assets or information processing facilities.

4.3.1 CQC users

The term ‘CQC users’ denotes all staff within the organisation, including those not directly employed by CQC but with access to the organisation’s systems and information assets. Information security requirements will be communicated to these staff and will be included in all third party contracts.

4.4 Assets

The Security Policy applies to all premises, physical equipment, software and data owned or managed by CQC, directly or indirectly through sub-contractors, to deliver services. This scope particularly includes the data relating to authorised CQC users and providers that is stored or processed. Depending on the source of the data, CQC is both a ‘data processor’ and ‘controller’ according to the definitions within the *Data Protection Act 1998*.

Some computing facilities, such as the end-user client desktops with third party contractors, are outside the direct management control of CQC. However, where they are used to process CQC data they still fall within the scope of this Security Policy. The security requirements are included within the relevant contract with the contractor.

4.5 Types of security documents

The whole Security Policy comprises the set of documents listed in Appendix A. There are a number of other documents thtat support the Security Policy and provide more detailed guidance on aspects of the Policy for specific audiences and communication purposes. There are four categories of security documents of particular importance.

4.5.1 Policies

A policy consists of high-level, mandatory statements that provide direction as to *what* must be done. A policy does not address the details of *how* something should be done. Policies are largely technology-independent, and sufficiently generic that they need do not need to be updated often. Typically, a policy will have a number of supporting standards, which provide detail that would be inappropriate in a policy. For example, a policy might require that all servers be hardened. In this case, a hardening standard could be written for each type of server, providing configuration requirements specific to the server's technology that will change more frequently than the underlying policy.

4.5.2 Standards

A standard contains lower-level mandatory statements that also address *what* must be done. Standards may be technology-independent (for example, a data classification standard), or technology-specific (for example, SQL server hardening standard). In many cases, standards are tiered. A baseline standard provides the minimum requirements for a particular component or area (for example, SQL server baseline hardening standard). Additional standards may be written that are more stringent variations of the baseline (for example, SQL server hardening standard for use with systems deployed in an exposed network area).

4.5.3 Procedures

Some standards, such as hardening standards, are difficult to implement because of the large number of configuration settings that require deep knowledge of a particular system. In such cases, procedures may be developed to provide the detailed requirements. Procedures may be automated, reducing the time and resources required to perform a mandatory task, as well as ensuring more accurate application of the task. Procedures are also produced for non-technical requirements, such as incident reporting.

4.5.4 Guidelines

Guidelines are recommendations on good practice that either do not require to be mandated in the Security Policy, fall outside the scope of the Security Policy or provide 'user friendly' interpretation of the policies, standards and procedures.

4.6 Structure of policy documents

The security policy documentation set consists of 11 sections mapped to the primary ISO27001 controls objectives. Within the policy documents, the sections are mapped to the relevant ISO27002 controls.

4.7 Environments

For the purposes of applying the security policy, all the information processing environments within CQC will be regarded as a single environment that is subject to the application of all security requirements contained within the policy documents. Where any potential exceptions to this are identified, they should be documented and notified to the Information Security manager using the Security Exception Risk Acceptance (SERA) process. Appropriate security waivers will be then be considered and approved through the Information Governance Group.

4.8 Review and evaluation

4.8.1 Approval

The Security Policy document must undergo a two-step process before being approved and published. This involves:

- Internal review and approval: the security policy must be reviewed and approved by the Information Security Manager and the relevant stakeholders in the business. The policy will then be presented to the Information Governance Group for review and approval.
- Once the Information Governance Group has granted approval, the Policy will be adopted immediately. The policy will then be communicated to all staff by publishing on the intranet, and compliance with the policies will then be mandated across CQC.

4.8.2 Review

The Security Policy will be reviewed regularly and amended as necessary each time there are new threats, amendments to security-related good practice, or major changes to CQC's infrastructure, services or organisational structure. This continuous review process will be risk-driven and carried out in accordance with ISO27001:2005. The Security Policy will also be formally reviewed by the Information Governance Group on behalf of CQC every three years.

4.9 Communication and training

The Security Policy will be properly communicated to all people within its scope to ensure that all are aware of them. This will involve a combination of different communication channels, including:

- Security induction training.
- Email notification.
- Intranet-based security reminders.
- Mandatory security training packages applicable to all staff.

As well as employees, this will also include third party suppliers and CQC will ensure that all relevant contracts include the compliance requirements from this information security policy.

There will be specific standards and instructions about more specific information security requirements. These will be distributed directly to individuals to be acknowledged by signature, for example, confidentiality and non-disclosure agreements.

4.10 Managing exceptions

To accommodate new requirements or handle temporary operational issues, CQC may grant waivers covering variance from or non-compliance with the Security Policy. This will follow the SERA process as described above. Granting a waiver from a policy requirement can only be authorised by the Information Security Manager, who will seek approval from the Information Governance Group and Executive Team where necessary.

These will usually be temporary and will be reviewed regularly. Waivers will only be granted where a fully justified business need can be identified. A waiver may be granted retrospectively where an emergency situation has arisen involving an actual or potential loss of service.

The waiver categories are:

- Technical maintenance involving CQC information assets only. These need to be approved by the Information Security Manager.
- Any waiver affecting the processing of personal identifiable data will need to be approved by the Information Governance Group, SIRO or Caldicott Guardian.

For each waiver request, the Information Security Manager will decide which category applies.

Any request must specify a minimum of:

- The assets involved
- The policy statements or requirements involved
- The details of and justification for the non-compliance
- The period of time during which the exception should apply
- The details of the actions planned to remove the non-compliance
- The people affected by the exception.

At the end of the waiver period, the Information Security Manager will ensure that compliance is reinstated, and will report this to the Information Governance Group.

4.10.1 Consequences of policy violations

An internal investigation will be set up in accordance with HR policy to examine the detail of any serious untoward security incidents, and will take any necessary actions including invoking disciplinary procedures where appropriate.

Where subcontractor staff have been found to have committed a security breach or policy violation, the subcontractor may be asked to bar the responsible individual from working for CQC. In certain circumstances, the contract may be terminated.

Any person within the scope of the Security Policy can be held responsible for a violation where the violation is malicious or as a result of negligence.

Ignorance of policy requirements will not be accepted as mitigation for a security violation.

5. Information Security Infrastructure

5.1 Management information security forum

Information security requires a governance structure to ensure a coherent direction with the ability to drive the implementation of the Security Policy within the organisation and to ensure the constant monitoring and improvements of the overall security system.

CQC operates an Information Security Management System (ISMS) compliant with ISO27001:2005.

The ISMS will be supported by the Information Governance Group (Information Security Management Forum (ISMF)), which will include the Senior Information Risk Owner (SIRO), selected members of the senior management team and the information security manager. The primary tasks of the group are to assess and address security-related issues on a regular basis, provide strategic guidance, review and monitor significant information security risks, and take management decisions affecting security. The Information Governance Group meets on a regular basis.

5.2 Information security coordination

Meetings will take place as required with staff that have operational or project security responsibilities in the various areas of the organisation. These meetings will take place to address issues, review status, and monitor progress of planned security enhancements or security requirements in projects. Issues raised and actions taken are logged and tracked under the responsibility of the information security manager.

5.3 Allocation of information security responsibilities

The Chief Executive has overall responsibility for information security. This is delegated, via the SIRO, to the information security manager for all day to day operational aspects of information security. Further delegation of responsibility for specific security issues will be carried out within the IG group as appropriate. Information and physical security is also a key responsibility of all employees, and this is regularly communicated and reinforced through an ongoing security education and training programme.

5.3.1 Senior information security risk owner

The Senior Information Security Risk Owner (SIRO) is a board member with responsibility for ensuring that information risk policy is developed, implemented, reviewed and its effect monitored.

The SIRO will be familiar with information risks and their mitigations, including information risk assessment methodology. They will provide focus for the assessment and management of information risk at board level, providing briefings and reports on matters of performance, assurance and cultural impact.

In the area of risk management the SIRO will be supported by nominated Information Asset Owners (IAO's) and Information Asset Administrators (IAA's) whose responsibilities include:

- IAO - Understand and address the risks to the information assets they own and, provide assurance to the SIRO on the security and use of those assets.
- IAA - Provide support to the IAO's by:
    - Ensuring that policies and procedures are followed
    - Recognising potential or actual security incidents,
    - Consulting the IAO on incident management,
    - Ensuring that the information asset registers are accurate and maintained.

5.3.2 Caldicott Guardian

The nominated Caldicott Guardian should be:

- A member of the management board or Executive team,
- A senior health or social care official,
- A person with responsibility for promoting clinical governance or equivalent functions within the organisation.

The Caldicott Guardian will be supported by the information governance and security teams to ensure that the organisation satisfies the required standards for handling personal and sensitive data. The Guardian will actively support work regarding information sharing and advise on options for legal and ethical processing of patient information.

5.3.3 Information security manager

The information security manager has responsibility for the definition, implementation, monitoring and management of the ISMS and information security policy documents. The information security manager organises and manages CQC participation in any joint information security committees with 3rd party providers, the Department for Health and any other external organisations.

The information security manager's primary responsibilities include:

- Ensuring that other policies, procedures and working practices are aligned to the information security policy,
- Ensuring that staff receive appropriate information security training and are aware of their associated responsibilities,
- Monitoring and reporting on the status of information security within the organisation,
- Ensuring compliance with relevant legislation and regulation,
- Monitoring for potential security breaches through reported risks,
- Ensuring that risk assessments are carried out and include appropriate risk treatment plans,
- Providing input to the annual submission of the CfH IG Toolkit.

The Information security manager will be assisted by and delegate some of these tasks to other members of staff as necessary.

5.3.4 Information technology security officer

The information technology security officer has responsibility for ensuring that the technical security measures available to and deployed by ICT Live Services are implemented in line with this policy document set and provide the best available level of security support to CQC. They will also work closely with the information security manager and the IG Group to provide technical advice and assistance to the group.

The information technology security officer's primary responsibilities include:

- Application of technical security measures across the CQC IT Infrastructure
- Liaison with 3rd party IT Service providers to ensure compliance with CQC policy
- Technical assessment of new IT services and applications
- Technical advice and assistance to the IG Group and wider CQC business units

5.4 Authorisation process for information processing facilities

All requirements for additions or substantive changes to information processing facilities as operated by CQC will be subject to review by the information security manager. These reviews will ensure that the proposed system or system changes comply with the requirements of the security policy documents.

During this review process the information security manager will, if required, engage third party expertise (internal or external) to ensure all proposals are valid and comply with the requirements of the security policy.

5.5 Confidentiality agreements

Confidentiality agreements and non-disclosure agreements are required for all members of staff in CQC as well as all third party suppliers who handle, have access to or process information on behalf of CQC. The agreements should address the need to protect the organisation's data and should be expressed in legally enforceable terms.
The following elements will be included within the agreements:

- A definition of the data to be protected (personal data and sensitive information),
- The expected duration of the agreement, including cases where the agreement applies indefinitely,
- Responsibilities and required actions of the agreement signatories e.g. application of the 'need to know principle' for data distribution,
- Ownership of all information assets,
- The permitted use of information assets,
- The right to monitor and audit use of information assets,
- The process for notification of breaches of confidentiality,
- The arrangements to return or destroy information when the agreements end.

5.6 Specialist information security advice

Specialist advice on information security may be provided in different ways depending on the business area of involved, and on the skills required.

The information security manager will respond to requests for specialist advice and allocate internal or external resources to assist as necessary.

5.7 Contact with special interest groups and authorities

The Information security manager will identify and maintain the appropriate level of contact with information security special interest groups. This may involve ensuring that the team is included on distribution lists of organisations that produce information security alerts and advice, membership of special interest groups such as the DH information security team or the British Computer Society (BCS) Information Security Specialist Group. There may also be a requirement to establish points of contact with authorities such as the Information Commissioner's Office or local Police authorities. This will ensure that points of contact are in place if an incident occurs which has a requirement to involve or report to external authorities i.e. where a security breach or crime is suspected or has actually occurred.

5.7.1 Cooperation between organisations

CQC may participate in joint information security forums with other organisations' Information security teams e.g. service providers, other government departments and the Department of Health (DoH). This will help to facilitate appropriate cross-organisational information governance good practice and information sharing which in turn will help to:

- Maintain information security policies,
- define and review roles and responsibilities,
- monitor threats to information,
- review and manage security incidents,
- assess major initiatives to improve information security,
- Share good practice.

5.8 Independent review of information security

The implementation of the security policy and continuous compliance monitoring by the information security team and system managers will be carried out, as specified in section 11 of this policy or as required by central government. Independent reviews will be carried out as required at the discretion of the information security manager or senior executives with security responsibilities.

5.9 Security of external parties

CQC will control access to information processing facilities by third party organisations and individuals. Access by third party organisations will be assigned based on a risk assessment ensuring that access is only granted where there is a genuine, authorised business requirement.

Third parties may include the following:

- IT service providers
- Other IT contractors for hardware and software maintenance and support,
- 3rd party data handling providers,
- Second Opinion Appointed Doctors and Mental Health Commissioners
- student placement,

- other work placements,
- cleaners, caterers, security guards and other outsourced support services,
- Short-term temporary appointments.

5.9.1 Identification of risks from external party access

The security of remotely managed or accessed assets could be put at risk by third parties who do not have adequate security controls in place. Where a third party connection requirement is identified, a risk assessment will be carried out to ensure that adequate controls are implemented to mitigate the risk. The risk assessment will take into account the type of access required (network access, access to physical location), the sensitivity of the information potentially accessed and the existing security measures employed by the third party.

Remote access to CQC assets will be on an exception basis and will not be provided until appropriate security measure have been implemented and verified.

5.9.2 Addressing security when dealing with members of the public

Publicly available information interfaces may introduce significant risks if not correctly controlled and secured. This can arise both from potentially unauthorised access to information, availability of information not intended for public release or the ability to maliciously amend data content (hacking).

Any systems or portals permitting access to the organisation infrastructure which are made available to the public will be the subject of specific security scrutiny including penetration testing where deemed necessary.

5.9.3 Addressing security in third party contracts

In addition to non-disclosure and confidentiality agreements, arrangements involving third party access to CQC IT facilities hosting personal identifiable data will be based on a formal contract which will include the following items:

- the agreed policy on information security;
- permitted access methods and the control and use of unique identifiers (User Ids) and passwords;
- a description of each IT service to be made available;
- a requirement to maintain a list of individuals authorised to use the service;
- procedures regarding protection of CQC assets, including information;
- responsibilities with respect to legal matters e.g. data protection and freedom of information;
- the right to monitor and revoke user activity;
- responsibilities regarding hardware and software installation and maintenance;
- the right to audit against the documented contractual responsibilities;
- restrictions on copying and disclosing information (a non-disclosure agreement will be signed);
- measures to ensure the return or destruction of information at the end of the contract;
- any required physical protection measures;

- measures to ensure the protection against the spread of computer viruses;
- an authorisation process for granting user access;
- Arrangements for reporting and investigating security incidents.

5.10 Outsourcing

5.10.1 Security requirements in outsourcing contracts

Outsourcing contracts will contain detailed security requirements which the provider must comply with. Contract obligations will include adherence to CQC (this) security policy, the detailed provisions of section 4.3 above and more specific security requirements that make explicit reference to the characteristics of the provided service.

5.10.2 Relationship with security policy of involved parties

The business activities of CQC necessitate the collaboration between several parties, including:

- Direct employees of the organisation,
- Employees of sub-contractors involved in the delivery of the Services;
- Directly contracted individuals;
- Other Government organisations, CfH and DoH.
- Provider organisations

As a result, the Security Policies of the various organisations involved will overlap in some areas. In any such situation:

- Where a conflict between the content and requirements of different security policies are identified then the most restrictive provision will apply. Where this is not possible then the relevant Information security managers will agree to implement measures acceptable to all parties involved.
- If security policies do not overlap, all relevant policy provisions will apply, irrespective of the source.
- If security policies are in conflict, the following order of precedence shall apply:
    - Laws and regulations
    - CQC and its sub-contractors' Security Policies.
    - ISO27001:2005

5.10.3 Hosting provider

CQC's primary sub-contractor is the IT service provider – ATOS who manage the data centres and networks within which the large majority of CQC's technical systems are deployed. CQC will contractually require that the hosting provider complies with this Security Policy for all of its operations that affect the Commission.

6. Asset Management

6.1 Accountability for assets

6.1.1 Inventory of assets

The Commission will maintain asset registers of physical and information assets to ensure compliance with ISO27001:2005, providing 'life of asset' tracking throughout the organisation. Information about new assets should be added the appropriate register without delay. If an information asset is present in two or more forms, then the register will reflect that. Each asset register entry will clearly state the following:

- Asset owner,
- Asset user and/or custodian,
- The designated information asset owner and administrator (IAO / IAA),
- Classification or sensitivity rating of the asset,
- Date that the asset is created or obtained,
- Date that the asset is archived, deleted or retired,
- Additional data to ensure that the asset history is maintained.

The asset owner will be responsible for ensuring the register is maintained. The actual maintenance task may be delegated to the asset administrator or other named party. Changes in staff and/or organisational structure will be reflected in the asset register to ensure correct ownership and responsibility is maintained at all times.

6.1.2 Ownership of assets

All information and assets associated with information processing facilities will be owned by a designated individual within the organisation. The asset owner will be clearly shown on the central asset register and be responsible for:

- Ensuring that information and associated assets are correctly classified,
- Checking that access restrictions to the assets are being applied correctly.
- Any risks to the asset are recorded and notified to the information security manager.

Ownership for assets will be allocated to a nominated individual within the appropriate business area with responsibility for:

- A defined set of data,
- An application,
- A defined set of activities or processes.

6.1.3 Acceptable use of assets

Rules covering the acceptable use of assets will be clearly defined, documented and implemented. A separate Asset Management Policy document is available on the intranet to provide more detail on this subject.
Employees, contractors and third party suppliers using or having access to CQC assets will be made aware of the acceptable use policy and will be responsible for their access to and use of those assets.

The policy will cover all organisational assets and will specifically apply to:

- Electronic mail and internet usage
- The use of mobile devices and data taken outside of controlled premises

6.2 Information classification

6.2.1 Classification guidelines

The assets will be classified into one of the categories stated in the tables below.

6.2.2 Physical assets

Classification	Description	Examples
Level 1	Standard office supplies, low commercial value per unit	Consumables
Level 2	Typical office Capital Expenditure items	Laptop/workstation
Level 3	Core service components. High commercial value.	Application Server

6.2.3 Information assets

Classification / Protective Marking	Description	Examples
OFFICIAL	All information processed within CQC is deemed to be classified as 'Official' regardless of the associated sensitivity.	All information
Official Sensitive	Information which is deemed to be sensitive and is not intended to be released outside of the organisation. This may be personally sensitive information relating to individuals or business sensitive information.	Name, address, date of birth, health details, ethnicity, trade union membership, financial information. Legal privilege and financial planning documents

6.3 Information labelling and handling

There is no requirement to mark documents or emails which contain Official information. However, any document which contains more sensitive information should be marked as 'Official Sensitive'. If there is any doubt whether information should be protectively marked then the question should be escalated, via line management, to the records and document management or information security teams.

6.3.1 Official

Official information should not be released publically – other than in accordance with a defined organisational policy or process - without appropriate management approval and should normally only be published via the Engagement team.

6.3.2 Official Sensitive

Information should not be released, discussed, shared or modified without appropriate authorisation.

No automatic 'right of access' to official sensitive information exists, all staff must consider the 'need to know' principle, and ensure it is applied.

Any anonymised or masked data, which is used for testing purposes, will be treated as business sensitive. The integrity of this data is paramount to ensure the results of testing undertaken are valid.

There may be circumstances where information classified as official sensitive has to be released into the public domain when it is requested under the provisions of the Freedom of Information (FoI) Act 2000. However, this will be handled centrally by the information rights team and all external requests for CQC information must be passed to this team.

No automatic 'right of access' to personal or sensitive information exists for any business team or function. Access to sensitive data by staff is subject to appropriate authorisation and a legitimate business need or clinical relationship, also referred to as a Legitimate Relationship. Once the business need has been established for a team or department it may continue as a standing requirement, however this should be kept under review by senior management.

All sensitive information should (a single record can be as sensitive as a complete database) be handled in accordance with specific process and procedure documents which will apply as required. Each process/procedure will be subject to review and approval by the information security manager to ensure that the security controls applied are in line with Security policies, HMG and NHS requirements for the management of personal data and all legislative requirements (such as DPA).

All access or changes to sensitive data are logged in the Knowledge and Information Management team logs. Where the functionality exists the changes should also be recorded on other IT system logs.

Where copies of sensitive data are taken for authorised and approved quality assurance testing, the manager of the QA team will ensure that on completion of testing, data is purged from all data storage areas used within the testing environment.

Any electronic media or hard copy which includes sensitive data should be clearly identified as such.

Aggregation – Whilst the highest classification of information received, stored and processed by CQC is Official Sensitive, the databases on which this information is held aggregates the data relating to very many individuals and additional controls will be implemented, where available, to appropriately secure this data.

6.3.3 Sensitive Data disclosure

There may be occasions where sensitive data may or must be released to external individuals or authorities. Circumstances may include:

- To other regulators, or law enforcement agencies,

- As part of a Subject Access Request under the Data Protection Act,
- To the Caldicott Guardian where it is required for an internal investigation,
- By coroners offices,
- By individuals or teams responsible for safeguarding.

For these or other reasons when retrieval of sensitive data is required, the request and the reason for the request must be submitted in writing.

Official sensitive data may only be disclosed in strict accordance with CQC's 'Sharing Information' guidance, defined policies (e.g. safeguarding policy), or approved memoranda of understanding and information sharing agreements. In other cases, official sensitive data must not be released without the authorisation of the Caldicott Guardian, information rights team, information security manager or appropriate executive.

Individuals may request copies of all information held about them by CQC under the Data Protection Act. Authorities may request sensitive data as part of criminal investigations or proceedings. In all cases these requests should be passed to the information rights team. The team will obtain the necessary assurances and authority to release the data in accordance with the relevant legislation. Any request submitted via telephone or in an informal manner will be refused by CQC. It will not be processed and it will be reported to the information rights team, who will advise if any further action is required.

6.3.4 Data retention

CQC processes a significant amount of data of many types. Each type of data has a different retention requirement; these are detailed in the CQC Retention and Disposal Schedule. Records review will be carried out regularly to determine whether records are to be selected for permanent preservation, destroyed or retained for research, litigation or historical permanent preservation purposes. Where records are archived, they shall be capable of retrieval by authorised persons.

Whenever the retention schedule is used, the guidelines listed below should be followed:

- Local business requirements/instructions must be considered before activating retention periods in the schedule.
- Decisions should also be considered in the light of the need to preserve records, whose use cannot be anticipated fully at the present time, but which may be of value in the future.
- Recommended minimum retention periods should be calculated from the end of the calendar or accounting year following the last entry on the document.
- The provisions of the Data Protection Act 1998 must also be complied with i.e. personal data should not be retained longer than is necessary to fulfil the purpose for which it was collected.

6.3.5 Exceptional circumstances

The retention schedule does not cater for all eventualities. Records managers need to consider whether there are any exceptional circumstances which may extend the retention period of a particular document or document type.

6.3.6 Permanent preservation

We work with The National Archives to determine whether they wish to preserve any CQC records for historical purposes.

6.3.7 Final destruction

At the end of the relevant retention period, records should be reviewed by the nominated asset owner to ensure that they are no longer required. Once it has been confirmed that the records are no longer needed they may be destroyed by an approved method and a log of their destruction produced showing the details of the document, date of origin and destruction, the method of destruction and the person responsible for the destruction. Further detail on the destruction of information is contained in the policy document on the KIM section of the intranet at the following link:

Information Destruction Policy

7. Human Resources Security

7.1 Prior to employment

CQC will ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for to reduce the risk of fraud, misuse of the facilities or theft of the organisation's property. Security responsibilities should be addressed prior to employment in job descriptions and terms and conditions of employment. All candidates for employment should be screened in relation to the sensitivity of the role they are being considered for. All employees should sign an agreement detailing their responsibilities relating to the use of information and associated processing facilities.

7.1.1 Roles and responsibilities

Security Roles and responsibilities are documented jointly in Security Policy and the Organisation of Security Policy documents. Security roles and responsibilities of employees, contractors and third party suppliers should be defined and documented according to this security policy. The relevant roles and responsibilities should be clearly communicated to job candidates during the pre-employment process. They should include the requirement to:

- Implement and act in accordance with the information security policies,
- Protect the organisation's assets from unauthorised access, disclosure, modification, destruction or interference,
- Carry out and comply with security processes and activities detailed within their job description,
- Ensure that responsibility is assigned to individuals for actions taken,
- Report actual or potential security events or risks to the information security team.

These requirements may be summarised in job descriptions supplied to agencies and potential candidates.

7.1.2 Personnel screening

Prior to completing an unconditional employment offer, CQC will carry out the background checks, including a combination of the following:

- Verifying references from previous employers
- Confirmation of any academic or professional credentials claimed if compulsory for the role
- User identity check against passport or other approved documentation verifying an individual's right to work in the UK.
- Criminal Records Bureau (CRB) check for eligible roles in accordance with the CRB policy.

These checks are considered to comply with the cabinet office requirement for all government employees to undergo Baseline Personal Security Standard (BPSS) checks as part of the pre-employment process.

The Commission may perform other checks for certain roles for which there is a specific contractual, regulatory or legal obligation. These checks can include credit or Security Clearance checks but will be directly related to the classification of the information to be accessed and the sensitivity of the role e.g. access to public funds and accounts.

All personal information gathered in relation to individual job applications will be treated as sensitive and handled in accordance with the data protection act.

7.1.3 False or misleading credentials

An applicant who deliberately or knowingly provides misleading, erroneous, or deceptive information in an application form, CV, or during an interview may be immediately eliminated from any further consideration for employment.

Any subsequent revelation which indicates that an employee deliberately or knowingly provided incorrect information during the recruitment process may lead to dismissal and/or referral to external authorities.

7.1.4 Terms and conditions of employment

As part of their contractual obligation, employees, contractors and third party suppliers should agree and sign the terms and conditions of their employment. This should state both their and CQC's responsibilities for information security.

The security specific terms and conditions of employment should make direct reference to the security policies and state:

- That all employees, who are given access to sensitive information should sign a confidentiality and security statement or nondisclosure agreement prior to being given access to information processing facilities,

- The employees responsibilities in relation to relevant legislation i.e. data protection and freedom of information,
- The employees responsibilities to understand and comply with all organisational policies,
- Responsibilities for handling, management and protection of sensitive assets, in particular, personal data,
- Actions to be taken in the event that any employee disregards the organisation's security requirements.

The responsibility to maintain the confidentiality of CQC information stated within the terms and conditions of employment should continue beyond employment. The Terms and Conditions of employment will state that users' computers and activities may be monitored to ensure compliance with the Information Security Policy.

7.2 During employment

Employees must be aware of information security threats, their responsibilities and liabilities and be able to support the security requirements of the organisation during their work to reduce the risk of human error.

7.2.1 Management responsibilities

CQC management will require employees to apply and adhere to information security in accordance with the relevant policies. This should ensure that all employees:

- Are properly briefed on their information security roles prior to being granted access to any sensitive information or resources,
- Are provided with guidelines which state the security expectations of their role,
- Are motivated to comply with the security policies,
- Achieve and maintain a level of security awareness relevant to their role,
- Comply with the terms and conditions of their employment including the security requirements.

7.2.2 Information security awareness and training

All CQC employees, and where relevant, contractors and third party suppliers, will receive security awareness training and regular updates on security policies and procedures as well as notification of any changes to applicable legislation and guidelines. The security and awareness training given to personnel will be relevant to individuals' roles, responsibilities and skills. It will include updates on current security issues and threats and will contain reminders on the need to report any incidents or risks to the information security team. Employees will be given the opportunity to provide feedback on the relevance, content, and effectiveness of the information and training they receive.

7.2.3 New employees security briefing

All new employees, both permanent and contract must receive an initial security briefing within the first month of employment as part of an induction program. This briefing will ensure that they understand the implications of the security requirements, protection methods and controls used while performing their jobs. This includes the importance of

security, the use of security measures, asset protection rules, acceptable use policy and the process of reporting any security violations.

7.2.4 Continuous education

All staff will be regularly reminded about their obligations in respect to information security. Security reminders will be provided to all users via the intranet and other appropriate communications; these will include 'hot' topics with the aim of maintaining a high level of security awareness throughout the organisation. Where required, security courses and specifically targeted security training will be provided. These will ensure continued security education for all staff and cover at least the basic security requirements. Management are required to allocate sufficient on-the-job time for staff to familiarise themselves and remain current with security policies and procedures.

7.2.5 Disciplinary process

The HR disciplinary process will be applied to cases of employees committing a security breach. However, this will not commence prior to the verification that a security breach has occurred and will ensure that correct and fair treatment is applied. Where a serious security breach has been verified consideration will be given to the immediate revocation of employee access rights and privileges.

7.3 Termination or change of employment

The HR team has responsibility for the employment termination process and will work with the line manager of the employee leaving to ensure that all the relevant security aspects are applied to the process. The termination process for contractors or third party supplier staff will be handled by the responsible agency or direct employer. Contracts with employment agencies or third party suppliers will include the requirement to comply with this policy.

7.3.1 Return of assets

All employees are required to return all CQC assets on termination of employment, contract or agreement via their line manager, this includes:

- Hardware (laptops, PCs or smart phones)
- Media storage devices (USB drives, CDs or DVDs)
- Physical and logical access tokens (VPN tokens, door access swipe cards)
- CQC documents
- Software
- Manuals

Employees will be asked by their line manager to confirm that they no longer have any CQC assets in their possession prior to their final working day.

7.3.2 Removal of access rights

The access rights of all employees, contractors and third party users to information and information processing facilities will be removed on termination of employment, contract or

agreement, or adjusted as necessary on change of role. This is detailed in the Access Control section of this document and should be carried out by their line manager.

This aspect is of particular importance where an employee is dismissed following a disciplinary process or suspended pending the outcome of an investigation. It should take account of both physical and logical access rights. Any shared team or departmental access rights such as door codes or passwords to shared services should also be changed.

8. Physical and Environmental Security

This section of the security policy details the basic security policy for all physical environments which contain information processing facilities, primarily the communications and server rooms. The policy statements are made to ensure the organisation meets both good practice and the requirements of ISO 27001:2005. Physical security arrangements for CQC premises are controlled and co-ordinated by the facilities management team.

The policy statement, when correctly implemented, will reduce the risk of unauthorised access into CQC controlled locations and information processing facilities. It will also assist in protecting IT processing facilities and associated equipment from environmental threats.

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference.

8.1 Physical security

8.1.1 Secure areas

This section applies to CQC owned or controlled premises. Third party contracted premises such as Data Centres, will have equivalent or additional controls in place as detailed in the relevant contractual obligations. The organisation or its third party suppliers will establish secure arrangements to control access into areas where sensitive documents/material/equipment are stored or processed.

Areas that hold, store and/or process personal data are automatically classed as secure areas. Only authorised persons are permitted access to these areas, visitors must be escorted at all times. Computer screens and documents in use in such secure areas are to be protected at all times from being viewed by unauthorised persons.

8.1.2 Physical security perimeter

Physical security perimeters for CQC locations should be clearly defined and provide an appropriate level of security for the assets which they contain, the application of these controls are primarily intended for implementation where data processing takes place. A designated secure area may be a locked server room, an office area or a whole building such as a data centre.

These perimeters will vary by location and the level of public and staff access required in line with the location function.

The following measures will be implemented at CQC sites as appropriate:

- The perimeter of the building or site will be structurally sound with all access points secured against unauthorised access by control mechanisms such as locks and alarms.
- Windows should be locked when unattended and additional protection will be applied where necessary, particularly for ground floor, easily accessible windows,
- Manned reception areas to control physical access to the buildings or sites will be in place to restrict access to authorised or escorted personnel,
- All fire doors forming part of a physical security perimeter will be alarmed and monitored. They should operate in line with health and safety requirements and local fire regulations,
- Intruder detection systems will be installed to cover information processing facilities and will be activated and monitored whenever the area is left unattended. Appropriate access controls should be in place for non CQC sites where information processing facilities are located,
- Physical segregation of processing equipment will be in place where premises are shared with other organisations.

8.1.3 Physical entry controls

Secure areas will be protected by entry controls to ensure that only authorised personnel have access, these controls vary by location and are controlled by both CQC and 3rd party contractors. The following measures will apply to all CQC secure areas:

- A log of all visitors will be maintained recording the date and time of entry and departure and the reason for the visit. Visitors will be escorted unless their access has been previously approved,
- Access to areas where personal or business sensitive information is stored or processed will be restricted to authorised personnel only. All access will be by means of an access control device such as a smartcard or swipe card and an audit trail will be maintained recording all access to the facility,
- Access rights to secure areas should be regularly reviewed to ensure that the list of authorised personnel remains valid,
- All personnel working within or visiting secure areas will be required to wear visible identification.

The organisation will have a physical access control system based on a pass swipe system. The pass system will distinguish between employees, contractors and visitors.

Passes will be controlled in the following way:

- The pass is intended for the sole use of the person to whom it was issued
- The practice of “tail-gating”, (e.g. avoiding or bypassing security by following another person in), to gain access to any secured area is prohibited
- The pass holder will immediately inform their manager if a pass is lost or stolen
- All visitors passes are to be returned to reception when the visitor leaves
- All visitor passes will only be valid for the day of issue; they will not be valid outside normal working hours.
- An authorised pass holder who allows a visitor into any secure area will:
- Escort that visitor at all times,
- Assume the responsibility for that person’s activities

- Ensure the visitors log is completed.

Passes will only provide access to those areas that the pass holder is authorised to enter.

8.1.4 Securing offices, rooms and facilities

Physical security of offices, rooms and facilities should be designed or sited to:

- Avoid casual public access,
- Buildings housing sensitive processing facilities and data should be unobtrusive with no obvious signs indicating the purpose.

Protecting against external and environmental threats

Physical protection against fire and flood will be applied to locations containing information processing facilities. Considerations will also be given to any specific local conditions which may affect the threat to the facility.

The following protection measures will be applied:

- Fallback equipment and data backups will be stored at a safe distance from the processing facility,
- Appropriate fire fighting equipment will be available at all facilities,
- Hazardous or combustible material will not be stored alongside data processing equipment.

8.1.5 Working in secure areas

The arrangements for working in designated CQC secure areas will include:

- Unsupervised working in secure areas will be avoided wherever possible for both health and safety reasons and to minimise the opportunities for malicious activities,
- Personal recording devices (cameras, mobile phones etc.) will not be allowed in data processing facilities,
- CCTV systems will cover, at least the entry and exit points to secure areas to provide audit trails of access to the facility.

8.1.6 Public access, delivery and loading areas

Access points to secure areas and controlled facilities such as delivery and loading areas should be controlled and, where possible, segregated from information processing facilities. The following points should be included in the physical security plan:

- External access to delivery and loading areas should be restricted to authorised and identified personnel or vehicles,
- The delivery and loading area should be designed so that supplies can be unloaded without the delivery staff gaining access to controlled areas,
- The external doors to a loading facility should be secured when not in use,
- All IT equipment delivered to CQC sites should be checked against orders and registered, on receipt, in the asset register,

- IT equipment identified for disposal should be clearly marked and segregated from equipment received and the procedure for disposal of IT equipment should be followed.

8.2 Equipment security

8.2.1 Equipment siting and protection

All information processing equipment will be protected against physical and environmental threats. Protection of equipment, primarily in the data centres, will be implemented to reduce the risk of unauthorised access to information and to protect against loss or damage. Where equipment if located at other locations such as CQC offices, the existing protection for that site will be adopted. Controls will also need to be considered to ensure the continuity of any supporting utilities such as power and cooling.

The following guidelines will be employed to protect information processing assets:

- Equipment should be sited to minimise unnecessary access into secure areas,
- Sensitive data processing facilities should be sited to avoid the risk of it being viewed by unauthorised personnel,
- Any systems processing especially sensitive information should be physically segregated or given additional security protection within the site,
- When siting IT processing facilities the following physical threats will be considered with the aim of reducing or removing them completely:
    - Theft,
    - Fire,
    - Explosives,
    - Smoke,
    - Water (or failure of the water supply),
    - Dust,
    - Chemicals,
    - Electrical supply interference,
    - Communications interference,
    - Electromagnetic radiation,
    - Vandalism.
- Guidelines for eating, drinking and smoking near IT facilities will be established,
- Temperature and humidity monitoring will be carried out,
- Lightening protection will be supplied for all Data Centre facilities.

8.2.2 Supporting utilities

All critical information processing facilities will be protected from power failures and other disruptions caused by failure of supporting utilities. This applies primarily to the Data Centres but will be extended wherever possible to other locations at risk of power failure.

All supporting utilities including the power and water supply, heating and ventilation and air conditioning should be adequate for the systems they are supporting. They should be regularly inspected and tested to reduce the risk of failure or malfunction.

Critical facilities should be connected to two or more electricity feeds to avoid a single point of failure. All critical processing facilities will have an uninterruptable power supply (UPS) to allow a controlled close down or continuous running of applications. Back up generators and fuel supply should also be available to allow processing facilities to continue running in the event of disruption to the main power supply.

8.2.3 Cabling Security

Power and data cables will be segregated from each other as much as possible. Protective measures shall be introduced to reduce the possibility of damage to power and data cables including:

- Physical protection of the cables to avoid unauthorised access or damage,
- All cables should be clearly marked to avoid accidental patching into the wrong network,
- Fibre optic cabling should be used for sensitive systems to reduce the threat of interception or radiation.

8.2.4 Equipment maintenance

All IT equipment will be regularly maintained in accordance with manufacturer recommendations to ensure its integrity and availability. The following measures will be implemented:

- Maintenance will only be performed by authorised and qualified maintenance engineers,
- It will be maintained in accordance with the manufacturers recommended specifications,
- Records will be kept of all servicing and maintenance,
- Where equipment contains sensitive information, the maintenance personnel will be supervised.

8.2.5 Security of Equipment off Site

The use of CQC owned equipment outside of the organisation's premises will require appropriate authorisation by management. For laptop users this will take the form of a management request to issue a laptop and SRAS token.

When authorisation is granted for remote working involving sensitive business or personal identifiable data additional security measures may need to be implemented. The additional security measures will be commensurate with the classification or sensitivity level of information or data that the equipment and/or service may have access to.

Access to the equipment and/or services will not be made available to unauthorised persons.

Equipment used off site must not be used to access personal data or systems containing personal data without explicit approval.

Care should be taken that information cannot be seen by unauthorised personnel when data is being accessed in public places. Personal identifiable data will not be processed in open, public places.

Any loss or compromise of equipment or data must be reported to the Information security manager as soon as practical, during working hours, following discovery of the event.

8.2.6 Secure Disposal or Re-use of Equipment

Equipment, which holds; stores or processes CQC information, will be securely cleared or destroyed at the end of its functional life. Sensitive data, licensed software, and other material will be securely erased or overwritten prior to releasing equipment for re-use or disposal. The destruction and / or overwriting of data on redundant hardware may be contracted to a specialist third party who will use CESG approved methods of destruction and deletion and provide appropriate certificates on a per item basis. Security measures will also be employed to protect sensitive material and equipment during refurbishment or repair.

Even though encryption is used whenever person identifiable data is stored on removable media, it must be physically destroyed as soon as it is no longer needed. Removable media destruction must be carried out securely using a CESG approved method. Destruction receipts will be required and maintained by the business unit responsible as evidence of media destruction. These receipts must be retained according to retention periods stated in the CQC Retention and Disposal Schedule.

CQC will maintain and publish a procedural document detailing the working arrangements for the secure disposal of redundant IT hardware. Individual members of staff who have media which needs to be securely destroyed should refer to the Information Security team for advice and assistance.

8.2.7 Removal of Property

With the exception of approved processes, equipment, information or software will not be taken away from CQC premises.

Where staff are authorised to remove assets from CQC sites, all movement will be clearly documented showing details of removal and return plus the staff member(s) responsible for the assets.

Security staff, or other staff, should challenge anyone seen removing assets from offices or sites to check that proper authorisation is in place and, where necessary the identity of the person removing the assets.

Staff issued with laptops have default authority to remove them from CQC premises.

9. Communications and Operations Management

9.1 Operational procedures and responsibilities

9.1.1 Documented operating procedures

Documented procedures should be prepared for system activities associated with information processing and communication facilities, such as server start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling, and safety. These operating procedures should be produced and maintained for each system for which the organisation is responsible.

The operating procedures should specify the instructions for the detailed execution of each job including:

- processing and handling of information,
- backup,
- scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times,
- instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities,
- support contacts in the event of unexpected operational or technical difficulties,
- special output and media handling instructions, such as the use of special stationery or the management of sensitive output including procedures for secure disposal of output from failed jobs,
- system restart and recovery procedures for use in the event of system failure,
- The management of audit-trail and system log information.

Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools, and utilities.

All documented procedures will undergo a regular maintenance review, showing changes and updates. Previous versions of documented operating procedures will be kept for reference.

9.1.2 Operational change control

Changes to operational systems will be agreed between the system users, business management, ICT live services management teams and, if applicable, IT Service Providers.

Before any changes can be made, the following steps will be taken:

- the change owner or instigator will document the change,
- an impact analysis will be undertaken, including all relevant stakeholders for that infrastructure component or system,
- the change will be tested or otherwise quality assured before it is applied,
- The change will be subject to full review and acceptance by all relevant system stakeholders at the Change Authorisation Board.

In emergency cases, to prevent system outages or recover a failed system, the emergency change procedure will be followed.

9.1.3 Segregation of duties

All changes to and sensitive operations carried out on CQC IT systems will be subject to an authorisation process. This is to reduce the likelihood of unauthorised or unintentional modification or misuse of information or information processing assets.

9.1.4 Separation of test, development and live environments

Where different environments exist within the infrastructure, these should be segregated using either physical or logical control mechanisms to prevent unintentional or unauthorised access to live systems and the data they contain.

9.2 Third party service delivery management

Where 3rd party service delivery is used to provide operational services to CQC, security controls, service definitions and delivery levels should be specified in the relevant contracts and agreements. Services, reports and records from the 3rd party supplier should be regularly reviewed and monitored. Audits of the services provided should be planned and conducted on a regular basis.

Management of the relationship between CQC and the 3rd party service supplier should be carried out by a nominated team within the organisation. This should focus largely on the technical and security compliance of the 3rd party with the contractual agreements in place. The main areas of focus will be:

- monitoring of service levels against the agreements,
- review of service reports,
- security status and incident reporting,
- review of audit trails and records of security events, operational problems, failures and service disruption,
- Management and resolution of identified problems.

Operational changes to services and systems run by a 3rd party on behalf of CQC will be subject to the same change control process as internally owned and managed systems.

CQC and 3rd party suppliers will perform joint risk assessment(s) and will agree appropriate controls to manage and reduce the likelihood of security incidents.

9.3 System planning and acceptance

9.3.1 Capacity management

Advance planning and preparation are required to ensure that systems have adequate capacity and resources to meet both existing and future requirements. System operational requirements will be established, documented and tested prior to acceptance of a new system or upgrade to an existing system. Projections of future IT capacity requirements will be made to ensure that adequate processing power and storage remain available. These projections will take account of new system requirements as well as projections for current server and network use. For major new developments, ICT Live Services will also be

consulted at all stages in the development process to ensure the operational efficiency and maintainability of the proposed system design.

Where 3rd party services are required (i.e. new application services), CQC or its IT service provider, will liaise with the 3rd party to ensure appropriate power, space, connectivity, cooling and other resources are available to meet planned need.

9.3.2 System acceptance

All proposals for new systems will include a security plan that describes how the system satisfies the security requirements provided in this document and any other applicable security policy definitions. The system design document will also include the minimum and optimal performance and capacity requirements expected from the system.

All new application proposals will include evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times. Alternatively, they will include provision for additional equipment to maintain adequate resource levels.

All IT systems will be subject to ongoing performance monitoring. The metrics will be agreed before the system is commissioned and will cover such aspects as system processing speed, capacity and security requirements. Acceptable levels of service will be reviewed at least annually or earlier if service issues are reported.

9.4 Protection against malicious and mobile code

9.4.1 Controls against malicious code

An approved anti-virus (AV) software solution will be deployed on all CQC IT assets where AV services are required or supported.

The AV software will be properly installed and maintained. In addition, the AV will automatically perform a full scan at least monthly and on access scanning of all new files and media. This policy will flow down to the IT equipment used by any 3rd parties. System administrators will ensure the AV automatically checks for and downloads updates from the vendor's servers or from a trusted source within the IT environment. All incoming and outgoing Internet traffic will be routed through dedicated servers and other network devices that provide AV scanning.

Suspicious e-mail traffic (messages and attachments) will be routed to an isolated storage area for analysis by the system administrator.

The additional measures listed below should be followed to further reduce the risk of infection:

- ensure the AV is always running and, pro-actively checking for updates,
- never open mail, files or macros from an unknown source. Report any suspicious occurrences to the IT service desk,
- never download and install Freeware or Shareware from the Internet,

- always scan any removable media (CD, floppy disk) from an unknown or untrusted source before using it,
- back-up data and configuration settings regularly and store the back-ups in a safe place,
- Files should always be stored on dedicated servers rather than on local laptops or workstations in line with document and records management policies,
- delete spam, chain and other junk email,
- All PCs should be shut down when not in use.

9.4.2 Controls against mobile code

Where the use of mobile code is required for business or application functionality it should be acknowledged and authorised. Where there is no requirement to allow mobile code to run it should be prevented from executing.

The following protection measures should be employed to prevent mobile code performing unauthorised or unexpected actions:

- only allow execution in an isolated environment,
- blocking the use of mobile code,
- blocking the receipt of mobile code at network gateways,
- Employ cryptographic controls to authenticate authorised mobile code.

9.5 Backup

9.5.1 Information backup

The backup or restore procedures for all systems will include performing backups to a defined schedule for example, every 24 hours, at the end of each work period. The restoration process for data backups will be tested regularly to ensure the viability of the regime.

Additionally, it will be possible to perform ad-hoc backup requests e.g. before a major system change. This is done to ensure that appropriate versions of data, libraries, and files are available for recovery and restoration and to prevent the loss or corruption of data. Activities included in backup/restore management are as follows:

- backup/restore data indexing and compressing,
- backup/restore data scheduling and monitoring,
- backup/restore testing,
- Backup library maintenance.

The backup regime will include all audit log data, user security profiles and system security permissions.

9.5.2 Security and storage of backups

All backup media will be securely stored, accounted for and will only be available to authorised persons. An assessment of the storage arrangements for the backup data should be conducted and consideration be given to implementing additional controls where

necessary e.g. encryption of the backup data. Where long term storage is required for regulatory or legislative compliance, care should be taken to ensure that the media on which the data is held will not become obsolete or degrade during the mandatory storage period.

Where the data is held encrypted, it should be ensured that the cryptographic keys used also remain available to decrypt the data.

Backup media will be stored at a separate location to the servers from which the backups were taken. Any specific tools, procedures and instructions for the restoration of the data should also be stored off-site ensuring that they are separate from and do not permit the unauthorised recovery of the data.

9.5.3 Alternative hardware and physical assets

Business Continuity and Disaster Recovery plans will include details of the hardware, other equipment and other assets (e.g. Buildings, power, air supply, etc) that will be available in the event of a major incident or disaster.

9.6 Network security management

9.6.1 Network controls

The network provides the common infrastructure on which all other services and users depend. It should be managed and controlled to protect it from threats and to maintain the security of the applications and data in transit. Network configuration will only allow users access to the services they are specifically authorised to use.

Network controls are the primary defence against a number of external (cyber) threats including:

- Hackers and hacktivists
- Organised crime
- Terrorism
- Foreign intelligence services

CQC is not likely to be a target of the latter 2 categories of threat there are real chances that both hackers and criminals could attempt, by design or opportunity, to gain unauthorised access to CQC networks, resources and data. The measures detailed throughout this policy document set will provide defences against all known forms of external and cyber threats.

Any services which are not needed will be disabled and locked down by system administrators. Controls will be implemented on the network to provide security for the connected services and data. Particular attention should be given to the following areas:

- operational responsibility for network security and management should be separate from hardware and application support functions,

- procedures and responsibilities for network management including remote equipment such as switches should be documented,
- logging and monitoring of security related actions should be enabled on the network,
- Interconnection of the network, the Internet, GSI, N3 and administrative connections will be subject to particular attention. For the external network connections compliance checks will be carried out of all relevant technical, security, and administrative requirements. Network devices must be authorised by management prior to connection or attachment to the network. Technical measures will be installed to detect and isolate any unauthorised devices,
- all information sent through the network will be traceable through its source and destination addresses,
- unauthorised network addresses will not be allowed on the network. Every user, resource and service on the network will have a unique active directory object name. These objects and their associated rights and privileges will be proactively tracked and managed within active directory,
- The network architecture will be clearly documented to facilitate identification of components during network analysis and problem investigations. All changes or amendments to the network architecture will also be fully documented.

9.6.2 Firewall protection

Firewalls are an essential component of the information systems security infrastructure. Firewalls are defined as security systems that control and restrict network connectivity and network services.

Firewall protection provides a controlled and audited mechanism to restrict access for all internal or external connections to elements of the networks. All changes to firewall configuration parameters, enabled services, and permitted connectivity paths will be subject to a Change Management process, and fully logged. All suspicious activity that might be an indication of either unauthorised usage or an attempt to compromise security measures also will be logged. The integrity of these logs will be protected with checksums, digital signatures, encryption, or similar measures.

These logs will be retained for six months after the time they were recorded except where they relate to a specific event which may need further investigation or preservation as evidence. The firewall logs will be reviewed on a regular basis to check that the firewalls are operating in a secure manner and that the logs are complete and show no indication of unauthorised activity.

In some instances, systems such as routers, air gaps, telecommunications devices, or gateways may be functioning as though they are firewalls. All systems providing firewall functionality, whether they are formally called firewalls or not, will be managed according to the rules defined in this policy. If the device is performing a necessary firewall function on the network it may need to be upgraded or replaced with another device to fulfil the requirements of this policy.

All traffic crossing into or out of the network will pass through an authorised firewall, this firewall will be configured with another device to form a demilitarised zone (DMZ). The DMZ is used to house servers providing services outside of the CQC network such as mail,

DNS or web servers; this allows the network an additional layer of protection for the internal more critical servers containing proprietary and sensitive data.

Wherever possible, all traffic within CQC should be kept physically and / or logically (network segments / VLANs) separate within the network in line with user and application requirements. All connectivity paths and services that are not specifically required by applications and users will be blocked by CQC firewalls. The firewalls will be deployed in a 'default deny' configuration with only those ports and protocols opened for known and authorised requirements.

The list of currently approved paths and services (ports, IP addresses and required protocols) will be documented by the network administrators. This document will be kept up to date and used to record all changes to the firewall policies including the dates on which temporary changes can be removed.

The following rules will be applied:

- all firewalls will be configured and protected against unauthorised electronic or physical access attempts,
- all firewall configuration and security policy rules will be documented, maintained and retained in a secure location that can only be accessed by authorised persons,
- firewalls will not have the Any-to-Any rule set for any time period. The only exception to this is during installation and functionality tests
- all non-essential networking and system services will be removed from the firewall,
- the firewall will be configured to support the anonymity of the internal IT networks through 'network address translation' or other equivalent functionality,
- controls and monitoring processes will be applied to the ongoing management of all firewalls so that at any point in time it can be verified that any given firewall is effectively fulfilling its intended purpose. The verification of the firewall integrity will be done at least once a month,
- firewall audit logs will be reviewed for security breaches and attempted network intrusions on a regular basis,
- external Firewalls will run on dedicated machines that perform no other services. Second line firewalls may run on non-dedicated machines such as a router providing stateful packet inspection functionality,
- sensitive or critical CQC information will never be stored on a firewall. Such information may however be temporarily held in buffers as it passes through a firewall,
- firewalls will have only have the minimum operating system software installed and enabled on them.
- Where the supporting operating system permits it, all unnecessary and unused systems software will be removed from firewalls,
- no internal information or data will be resident on or processed by any firewall, server, or other computer that is shared with another organisation at an outsourcing facility,
- The firewalls should run the latest release of software to prevent attacks. When available, subscription to the vendors' software maintenance and software update services should be maintained. Where vulnerabilities are notified, analysis of the available patch or mitigation will take place to establish whether or not it can be installed and with what urgency that should happen.

9.6.3 Intrusion detection

The networks holding and processing sensitive data should include Intrusion Detection Systems (IDS); the system may be either network or host based. Alternatively an Intruder Prevention System (IPS) may be deployed.

Each system should be configured according to the guidelines defined by the manufacturer which should be checked by an appropriately skilled internal resource.

The system will be installed on all relevant network segments, and will automatically notify the monitoring staff that a known or suspected attack signature is occurring or has occurred so that corrective or preventative action can be taken.

9.6.4 Remote access

The purpose of this section of the policy is to define the security requirements for connecting to the network from any host. These standards are designed to minimise the potential damage which may result from unauthorised use of or access to resources. Damage many include the loss or unauthorised modification of sensitive data and intellectual property.

Users who require mobile computing will go through a specific management approval process, which will consider the potential risks it carries for the environment they connect to. Where mobile computing facilities are granted, the manager will be responsible for ensuring that the individual has all the necessary hardware and software to allow remote access to be carried out securely.

This policy applies to all employees, contractors, vendors and agents involved in service delivery who connect to the network. It applies to remote access connections used to carry out work on behalf of CQC, including reading or sending email, viewing intranet web resources and other CQC applications.

- it is the responsibility of employees, contractors, vendors and agents with remote access privileges to network to ensure that their remote access connection is given the same security protection as the user's on-site connection,
- secure remote access will be strictly controlled and will make use of strong authentication,
- at no time will any employee provide their login or password to any other person,
- IT equipment used for remote connectivity into the network will be issued and configured by the CQC IT service provider. Personally owned PCs and ancillary items may only be used when authorised for remote users via the virtual desktop facility,
- employees and contractors with remote access privileges will ensure that their PC, which is remotely connected to the corporate network, is not connected to any other network other than the broadband connection used for remote access at the same time,
- employees and contractors with remote access privileges to the corporate network will not use personal email accounts or other external resources to conduct CQC-related work, ensuring that official work is never confused with personal business,

- All hosts that are connected to the internal networks via remote access technologies will use approved anti-virus software which is automatically configured to ensure it is fully up to date.

9.7 Media handling and security

9.7.1 Management of removable computer media

Any removable media used to transport sensitive or person identifiable data must be encrypted using an approved product. The media itself must be issued by or on behalf of CQC and used only for that purpose. The use of personal media devices of any sort must not be used to download, store or transport CQC data.

Insecure or unauthorised handling of removable media presents a risk of data loss and breach of confidentiality. Controls are required for the management of media items, which include tapes, cartridges, cassettes, etc. Library procedures are necessary to ensure that media are used, maintained and transported in a safe and controlled manner. Removable media will be protected to the same level as the operational data that they contain.

9.7.2 Disposal of media

Data will be erased from media that is no longer required. Hardcopy data for disposal will be either shredded or placed in secure disposal containers. Electronic media will be disposed of by an approved secure process in line with CESG standards and the Secure IT Disposal Process.

9.7.3 Information handling procedures

Procedures for the handling and storage of information are in place to protect information assets from unauthorised disclosure or misuse. The procedures include the handling, processing, storage and communication of information in line with its classification. They take into account the following considerations:

- labelling and handling of all media in accordance with the classification of the information it contains,
- protection of the media to prevent unauthorised access,
- maintenance of a register of authorised recipients of information assets,
- secure storage of media taking account of manufacturers recommendations,
- data distribution restricted to the minimum necessary in line with business need,
- regular review of distribution lists and channels to ensure continued business need,
- Clear marking of media classification where appropriate.

9.7.4 Security of system documentation

System documentation, including systems operations manuals are considered sensitive as they may contain information including system configurations, security and audit settings and network addressing details. Therefore access to this documentation will be controlled, it should only be used or shared on a strict need to know basis.

9.8 Exchanges of information and software

9.8.1 Information and software exchange agreements

Agreements, such as formal contracts and software escrow agreements will be established for the exchange of information and software between organisations. These agreements should be compliant with the relevant legislation. Procedures should be in place within each business area where information is received or transmitted to ensure that information exchanges are carried out securely and in accordance with CQC policy requirements where applicable. The procedures should take account of the following points:

- information exchanged should be protected from interception, copying, modification, misrouting and loss or destruction,
- protection against malicious code,
- not leaving sensitive or personal data on printing facilities including copiers, printers and faxes,
- sensitive or personal data should only be transmitted by approved methods,
- All personal and sensitive information should be protected by the use of approved cryptographic methods of protection.

Clear, documented agreements should be in place where sensitive information or personal data is exchanged between CQC and an external party.

9.8.2 Acceptable Use

The acceptable use of all CQC systems is covered within this Security Policy document and applies to all employees. Access to web based services, in particular e-mail and internet connection systems are provided to employees for:

- their work duties,
- work-related educational purposes,
- work related research purposes,
- Business related communication.

Reasonable personal use of CQC provided e-mail and internet facilities is permitted subject to the following provisions:

- use does not interfere with an individual's normal duties;
- there is no absolute right of access to web based services, nor should there be any expectation of privacy when using CQC business communications systems;
- CQC will not be held liable for any financial or material loss to an individual user accessing the internet for personal use;
- No access will be permitted to 'inappropriate' content or sites including, but not limited to; gambling, pornographic or extremist political web pages or sites likely to cause offence to other employees.
- All web traffic to the internet is routed through an internet gateway where it is automatically logged. CQC maintains the right to inspect the logs and monitor compliance with this policy.

9.8.3 Security of media in transit

Any physical media used for storing or moving CQC data will be protected against unauthorised access, misuse or corruption during transportation outside of the CQC physical environment.

Risk assessments and data flow analysis will be performed to:

- Identify types of data being received and transmitted by CQC,
- Highlight areas of risk relating to data in transit
- Ensure that the transport methods for any physical media or electronic data are secure.

Particular care will be taken to secure the transmission of person identifiable data. Encryption, courier services and appropriate packaging will be used including locked or tamper evident containers for the physical transportation of personal and sensitive data.

9.8.4 Electronic messaging

When using electronic messaging to transmit any form of information care should be taken to ensure that the recipient is authorised to receive the information and that the method of messaging is sufficiently secure to protect the data being sent. Users should be aware that a number of security risks are associated with the use of electronic messaging, these include:

- viruses,
- chain e-mail,
- spam,
- Impersonation, anonymous e-mails and spoofing.

Wherever possible, CQC systems will be configured to protect against these threats. However, if a user has any suspicions about individual messages or e-mails then they should not open or respond to the message and should report the matter through line management to the IT service desk or information security team and request advice or assistance.

9.8.5 E-mail policy

CQC recognises that e-mail and the Internet are valuable resources, and wishes to encourage the use of these facilities to develop the skills and knowledge of the workforce to benefit the organisation's business objectives.

However the wide range of information available on the Internet and the ease of e-mail communication raise concerns about security, confidentiality and improper conduct. This document seeks to clarify these issues and avoid ambiguity, and to provide CQC employees with clear statements of accountability.

This policy is not a definitive statement of the purposes for which the e-mail and Internet facilities must not be used. The onus is placed upon the user to conduct themselves at all times in an appropriate manner.

CQC provides e-mail and Internet access primarily for business purposes but does allow limited personal use as defined in this policy.

9..8.6 Scope

This document will provides a secure framework relating to e-mail and Internet access and usage and is intended to provide direction and guidance and facilitate control in respect of best practice for all users.

This Policy:

- relates to the email client and web browser access provided by the CQC
- is applicable to all employees including permanent or temporary staff, contract staff, students, or any other person who is granted access
- refers to all user activity in relation to e-mail, and the Internet
- applies to all computers, managed by the IT Service provider and includes laptops, situated or used in any other location which are permanently or remotely linked to the network
- has been written with consideration to relevant legislation and guidance (see Appendix B)

9.8.7 Responsibilities

Organisational Responsibilities

- establish adverse incident and investigation procedures for the reporting of all breaches of this policy through the appropriate management channels
- ensure that line managers understand their responsibilities for the implementation of this policy within their business or clinical area and that their managed staff adhere to the principles
- provide appropriate training on the acceptable use of e-mail and the Internet
- ensure that controls are in place for the physical environment to prevent unauthorised access to the computer systems that allow access to the e-mail and Internet system
- compliance with section 46 of the Freedom of Information Act Code of Practice on Records Management with relation to disclosure of e-mails
- defining acceptable personal use of e-mail and the Internet

Caldicott Guardian Responsibilities

- ensure that the organisation is aware of key legislation relating to this policy
- ensure that systems are in place to investigate breaches of this policy
- guide the organisation on the transfer or disclosure of service user/employee person identifiable information by e-mail and the Internet

Line Managers' Responsibilities

Line Managers must ensure that permanent/temporary staff, students, trainees and contractors working in their departments are aware of:

- this policy and related policies
- the acceptable personal use of e-mail and the Internet
- how to access advice and guidance on e-mail and Internet acceptable use
- the security of the physical environment in their department
- how to report breaches or potential breaches of the e-mail and Internet policy

IT Responsibilities

- reviewing this Policy in line with changes in legislation/guidance/standards
- providing, managing, and maintaining the e-mail system and Internet access
- monitoring and auditing access
- support the investigation of reported incidents
- complying with authorised requests for access to mailboxes
- staff training on the acceptable use of e-mail and the Internet
- the content of any training package and assessing staff understanding
- username and password management
- virus control
- reporting incidents and inappropriate use to the Information Governance Group
- reporting on issues raised
- disseminating this policy in the organisation
- acting as a source of help, advice and guidance on the acceptable/unacceptable use of e-mail and the Internet and the content of this policy

Users Responsibilities

Users must:

- comply with this Policy at all times including any use of the service whilst off duty
- report any incidents such as inappropriate use or security breaches or virus infection to their line manager
- complete an electronically generated document after reading this Policy as per the instructions on the Information Assurance pages of the intranet
- always ask for advice and guidance on the content of this Policy or use of e-mail and the internet from line managers or the IT Service Helpdesk if unsure of the content.

9.8.8 Legal Implications

E-mail has been established as a means of communication for businesses and its use is now widespread. E-mail carries the same legal status as written documents and should be used with the same care.

Several factors combine to make e-mail a particularly important issue within Government legislation:

- where an e-mail contains personal information it will fall within the boundaries of the Data Protection Act 1998
- when e-mail content relates to a living individual its disclosure may be required under the Data Subjects rights within the Data Protection Act 1998

- e-mails that relate to the development of corporate business processes, may be subject to disclosure under the Freedom of Information Act 2000
- e-mails that contain inappropriate comments may constitute breaches of Equality and Diversity or Disability Discrimination, Human Rights or other similar legislation
- e-mails are considered a form of publication and inappropriate comments may constitute libel contrary to the provisions of the Defamation Act

Misuse of e-mail and the Internet may result in legal liability for CQC and, in some cases, the individual user. Inappropriate use may give rise to:

- liability for defamation
- copyright infringement
- breach of confidence
- inadvertently entering into contracts
- claims of harassment and discrimination
- claims for compensation

9.8.9 Internet Access - Principles

Access to the Internet or external web resources will be authenticated by user name and password.

Users must never access the Internet using another employee's login. It is totally unacceptable to adopt a colleague's identity on any Internet site.

Users must not download, upload, access or distribute any material whose subject matter is:

- unlawful,
- objectionable,
- causes offence, - examples of which are material which is libellous or pornographic or which includes offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability this includes incitement of hatred or violence or any activity that contravenes the Law or the CQC Policies listed in section 4.1.2 above.

IT services has blocked certain inappropriate sites to prevent accidental access. If an employee accidentally accesses material of the type referred to in the previous paragraph or other material which may be considered offensive, they should note the time and web site address, exit from the site and then inform their line manager who will instigate the CQC's reporting procedures.

Users must not sell or provide substances or conduct unauthorised business via CQC provided Internet access

If an employee is in doubt as to whether it is appropriate for them to access a site, they should speak to their line manager before doing so.

Only those staff who are specifically authorised to give media statements on behalf of the organisation may write or present views, concerning CQC and its business, on the Internet.

Internet users must be aware that the Internet is inherently insecure and confidential information in relation to the business of the CQC and/or service user/another employee's identifiable information must never be disclosed or placed on Internet sites or chat rooms.

Although anti-virus defences are in place, great care should be taken when using the Internet. The Helpdesk should be informed where any suspicion of virus infection arises; the incident will be dealt with in accordance with information security procedures.

Downloading or distribution of copyrighted material without permission of the copyright holder, or of software for which the user does not have a legitimate license is forbidden, this applies to any download for work or personal use.

The installation of downloaded software onto CQC computers, including laptops, is not permitted. Information downloaded for personal use must not be stored on the Network.

The use of peer-to-peer systems to download software is forbidden as is the installation of any such system on CQC computers. Peer to peer systems are computers that are not linked to the same network.

9.8.10 E-mail - Principles

Copyright in all documents created via e-mail is the property of the organisation and not the individual user. E-mails sent by a CQC employee are the organisations property.

If an e-mail is marked 'Personal' in the subject field it will not be opened under the Domestic Purposes Exemption of the Data Protection Act (1998) however, any e-mail marked 'Personal' may be opened if inappropriate activity as defined in this section of the policy is suspected.

Employees must not share their password and user name with any other person and should not leave their computers unattended whilst logged on, as they will be held responsible for any activity which takes place using their account. Unauthorised use of someone else's identity to send or intercept e-mail is strictly forbidden and will result in disciplinary action.

Employees must not distribute any material by e-mail which is:

- unlawful,
- objectionable
- causes offence, examples of which include but is not limited to offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability
- contains material which is libellous or pornographic includes incitement to commit a crime, hatred and violence or any activity that contravenes any of CQC's Policies including Equal Opportunities Policy.
- material that could be classed as abusive, indecent, obscene, menacing; or in breach of confidence, copyright, privacy or any other rights.

Any member of staff who receives e-mail containing material which is in breach of this policy should inform their line manager immediately, who will institute the organisations incident reporting procedures.

Distribution of such material may result in legal action and/or disciplinary procedures. CQC reserves the right to monitor e-mail usage.

Where a member of staff receives e-mails from unsolicited sources the sender should be added to their personal 'Blocked Sender List'. (Contact the IT helpdesk for information.)

Employees, who receive e-mail attachments, where there is any doubt about the origin, should contact the Help Desk for advice. Viruses can be spread through e-mail and opening suspect attachments may result in loss of or damage to the CQC IT systems. Users should exercise caution when disclosing their work e-mail address to commercial organisations, as this information may be passed to other 3rd party organisations generating 'junk' mail.

Employees must not use the organisations e-mail system to conduct any personal business enterprise.

It is considered inappropriate to forward or create chain letters to other e-mail users either within the organisation or externally. If a user receives a chain letter that has inappropriate content they must inform their line manager who will instigate the organisations reporting procedures.

Chain letters sometimes contain warnings about virus outbreaks; these are usually hoaxes and should not be forwarded or acted upon. The IT Department does not send out e-mails of this nature.

To avoid inappropriate content being circulated users should not set their e-mail to "auto forward" (Contact the IT helpdesk for information)

Only those employees who are specifically authorised to give media statements on behalf of CQC, i.e. appropriate Directors or the Communications Team, may write or present views, concerning CQC and its business, via e-mail.

E-mail is considered corporate correspondence and as such is accessible under the Freedom of Information Act 2000. It is therefore important to save e-mails that have been used to formulate corporate decisions, policy, or procedure, as they may be subject to a request. These e-mails should be referenced, saved and retained to appropriate record retention periods following advice from the records management team. Guidance on e-mail etiquette is given at the end of this section of the policy document.

9.8.11 Monitoring E-mail and Internet Activity

CQC has a legal right to monitor usage of e-mail and Internet access using the least intrusive method available. The IT service provider will carry out the following auditing on behalf of the CQC to monitor compliance with this policy.

Internet access

Access to the Internet is authenticated and logged on a user basis. Details such as the date and time of access, and the site visited, are recorded and the information is retained for one month and then archived. Further reports will be available for use when investigating an incident; these reports will only be disclosed upon receipt of a written request from the Service Director in question.

E-mail Activity

CQC retains copy of all internal and external e-mail which is received or sent. This facility will not be used to monitor individual employees e-mail traffic without written permission or unless they have a justified need to monitor or investigate an employee's e-mails.

The IT service provider will investigate inappropriate activity on behalf of CQC under the following circumstances:

- a report of or concern raised about the contents of a computer
- a report of inappropriate or unreasonable personal use of e-mail or the Internet
- routine monitoring identifies potential inappropriate use

This list is not exhaustive.

CQC reserves the right to carry out detailed inspection of any IT equipment without notice, where inappropriate activity is suspected. A more detailed investigation may involve further monitoring and examination of stored data including employee deleted data held on servers, disks, drives or other historical/archived material.

Access to the content of an employee's mailbox in their absence, other than for the monitoring purposes already referred to, will only be granted on submission of a written request from a senior manager of the area concerned.

In the event of a user being absent from work for an extended period of time, access to their inbox may be granted to their line manager. Authorisation for this to take place lies with an Head of Service, when absent this responsibility is passed to a senior Manager.

9.8.12 Sensitive Information & Encryption

Sensitive personal information that identifies a service user or member of staff, or commercially sensitive information must not be sent outside of the CQC network by standard e-mail unless it is encrypted.

Encryption facilities exist on the CQC systems and access to and advice on the encryption solution should be requested via the IT Helpdesk.

9.8.13 Instant Messaging software

The use of Instant Messaging (IM) clients and connectivity is strictly prohibited. IM is a form of text based communication from one person to another that allows users to chat back and forth in real time. IM can make a user's computer vulnerabilities carry out Denial of Service (DoS) attacks and may leave the IT infrastructure open to potentially harmful software or virus attack via file transfer.

9.8.14 Acceptable Personal Use & Disciplinary Procedures

CQC allows reasonable personal use of the e-mail and Internet system.

CQC considers that employees may browse the Internet or use e-mail within the boundaries of this policy for their own personal use prior to or after their normal working hours or during their lunch break.

Where there is a necessity to conduct such activities within working hours this should be agreed with your line manager.

Failure to comply with this Policy may result in disciplinary action being taken through HR Disciplinary Procedures.

9.9 Electronic commerce security

CQC does not currently host any electronic commerce sites either directly or indirectly. However, it has a publically available Web site which is hosted by the Club Shared Service. Where any electronic commerce activities are planned in the future, controls will be employed to protect those activities. The controls will protect transactions against fraudulent activity, contract dispute and unauthorised modification and disclosure of CQC information. The detailed security controls employed will be largely based on cryptographic techniques which will be contractually agreed with the planned service provider. Any project to implement electronic commerce will be referred to the Information Governance Group for approval prior to financial commitments being made.

9.9.1 Publicly available information

The integrity of the information published on the CQC web site must be protected to ensure that it cannot be modified or deleted by unauthorised users. Appropriate cryptographic mechanisms should be employed to ensure the integrity of the data and software used on the web sites. The systems should be tested on a regular basis to ensure that the security protection remains valid. All information intended for publication on the organisation web sites must go through a formal review and sign off process prior to inclusion on the sites. Where 3rd party providers or service hosts are used, they must be included in the authorisation process.

9.10 Monitoring

All relevant security events on CQC systems will be monitored and logged. Users should be aware that their actions whilst on any internal or CQC supplied service may be monitored and logged to ensure that systems are being used in an authorised manner. System administrative and fault logs will also be monitored to provide a view on potential security weaknesses or issues.

9.10.1 Audit logs

Audit logs will record user activities, exceptions and information security events, they should be retained for 3 months to assist with access control monitoring and any required security investigations. The audit logs should, at a minimum, contain:

- User ID
- Dates, times and details of key events such as log-on and log-off
- Workstation identity or location
- Records of successful or failed system access requests
- Changes to system configuration
- Use of high level privileges (system administration rights)
- Use of system utilities and applications e.g. user administration
- Files accessed and the type of access e.g. Read, Write, Amend
- Alarms raised by access control system e.g. attempt to access resources not authorised to the user
- Activation and de-activation of system security controls such as anti-virus, intruder detection system, firewall policy settings.

These audit logs will be available across a number of systems including active directory, system security components and windows operating systems. It is not expected that all of the above information will be available on all systems; this will depend on the capabilities of the system itself and data storage implications of the logs. However, the logs available on each system should be activated and used.

9.10.2 Protection of log information

All audit logs in use within the organisation should be protected against unauthorised access, deletion and amendment.

The data within the audit logs should be included within the wider system backup and archive process. Care needs to be taken to ensure that the audit log housekeeping tasks include checks which ensure that the log capacity is sufficient to store the data being captured. It may be necessary to clear the logs, under a system administration function immediately following a system backup routine.

In some cases there may be compliance requirements to retain audit logs. This is particularly the case where access to individual health records is being logged.

9.10.3 Fault Logging

Faults or errors reported by systems or users should be logged and investigated to ensure that they do not represent or indicate security weaknesses or potential incidents.

9.10.4 Clock Synchronisation

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in disciplinary or legal cases.

All system clocks should be synchronised with a central, reliable time source. This source in turn should be regularly synchronised with an accredited external source such as the radio time broadcast from one of the national atomic clocks.

10. Access Control Policy

Access to CQC information, information processing facilities and business processes will be controlled on the basis of business and security requirements. Access control can be grouped in two categories:

- Logical access control
- Physical access control

The 2 categories have different methods of implementation but remain complementary in providing protection and security assurance to information assets.

This policy takes account of:

- security requirements of individual business applications,
- identification of all information related to the business applications and the associated risks,
- consistency between the access controls applied and the classification of the data being protected,
- relevant legislation and compliance requirements for the protection of information assets,
- segregation of access control roles; access requests, authorisation and administration,
- requirements for review of access control rights,
- removal of access control rights,
- A clear delineation between access controls which are mandatory and those which may be applied as discretionary.

10.1 User Access Management

Formal procedures will be in place to control the allocation of access rights to information systems and services. The procedures will cover all stages in the life-cycle of user access, from initial registration of new users to deletion of access rights when they are no longer required. Special attention will be given to the allocation and management of privileged user rights such as Domain Administrator in active directory or database administration.

10.1.1 User Registration

A formal user registration and de-registration procedure will be in place for granting and revoking access to information systems and services. The procedure will include the following elements:

- unique user IDs will be used for each user who will subsequently be accountable for the actions carried out using that ID,
- checks with system owners will be carried out to ensure that the user has a valid business need prior to granting access,
- a method of ensuring that users are aware of and acknowledge their responsibilities and conditions of access,
- a record of all access rights granted to an individual is created and maintained,
- periodic checks are carried out to lock or delete redundant user accounts and that a review of continued business need is completed regularly,

- Grouping of user access rights by job function to ease the administration and review process.

10.1.2 Privilege Management

The allocation and use of system administrative privileges will be carried out strictly in line with business need. There will be a formal process covering the allocation of privileges to individual users, this process will include and take account of:

- the administrative privileges required for each system (operating system, databases, applications) and the nominated individuals who will use them need to be identified and recorded,
- administrative privileges should only be allocated on a strict business need basis, they should never be used 'for convenience'
- wherever possible system routines or batch jobs should be developed to complete routine and regular system administration functions
- Individuals who hold privileged administration accounts should also have a 'normal' (non-privileged) account for routine business use. Privileged accounts should only be used to carry out necessary system administration.

10.1.3 User Password Management

The allocation of user passwords will be part of a formal process within the organisation. This process should include the following:

- users are required to be informed about the importance of keeping their password secure and associated good practice guidelines for password use during security induction and refresher training. Each user will sign a confidentiality agreement as part of their terms and conditions of employment which will include their security responsibilities,
- when new or replacement passwords are issued users will be forced to change them at first log on,
- a users identity must be verified before they are issued with a new or replacement password,

Passwords remain the most common way of verifying a user's identity when linked to a user ID. Stronger authentication (2 factor) using physical tokens and cryptographic techniques for enabled applications and remote access will be used where available.

10.1.4 Review of User Access Rights

A formal process should be in place to ensure that user access rights are reviewed on a regular basis. This is to ensure that the rights an individual has been granted in the past remain valid and that the user has a continued business need to retain them. The reviews should take into account the following:

- reviews should be conducted regularly and routinely at no more than 6 monthly intervals for all users,
- individual user access rights should be reviewed after employment changes such as promotion or change of responsibilities or role,

- reviews of all privileged account allocation and use should take place more frequently i.e. not exceeding every 3 months,
- Account use should be checked; accounts which have remained dormant for 4 weeks or more should be disabled, accounts which remain unused for 3 months or more should be deleted. Where a user has been granted extended absence from work i.e. maternity leave, then the account should be disabled until the user returns to work which should be verified by the user's line manager.

10.2 User responsibilities

Users should be fully aware of their responsibilities in relation to system access control and the use of access mechanisms. System security depends on user compliance with this and other security policies.

10.2.1 Password use

Users are required to follow good practice guidelines in relation to the selection and use of their passwords. A summary of the guidelines is:

- keep passwords confidential,
- avoid keeping a written record of the password,
- change passwords regularly or whenever there is any indication or evidence of misuse or compromise,
- select quality passwords with a minimum of 8 characters including upper and lower case letters and numerals - special characters (!"£$%^&*) may also be used to further strengthen the passwords,
- passwords should not be written into a macro function or assigned to a function key,
- they should not be shared with any other user,
- The windows 'remember user and password' function should not be used.

If users are required to access several applications or services it is better to maintain a single good quality password for all systems which is changed on a regular basis than to try to maintain a different password for each.

10.2.2 Unattended user equipment

User equipment is not to be left unattended while a user session is active, unless secured by an appropriate locking mechanism. Engagement of the windows screensaver lock may be used for short absences from an active terminal. During longer periods of absence and at the end of the normal working period full logout from active applications and shut down of the terminal should be completed.

10.2.3 Clear desk and screen

When leaving the office at the end of each working day all users will:

- Lock all confidential documents in cupboards
- Keep his/her desk clear of sensitive documentation
- Ensure that any removable media containing sensitive data is cleared or securely locked away.

Obsolete documents that are no longer required will be destroyed by either shredding or disposed of in secure waste disposal container. When not in use, all information assets will be protected from unauthorised disclosure and secured in a suitable locked container.

Computer screens used to view sensitive and personal data will be sited to prevent them being overlooked by unauthorised personnel.

All computers accessing the network will be configured to automatically invoke a password-protected screen-saver after 10 minutes or less of inactivity. Users should not disable or extend the screen saver time out period. Users are not to work on sensitive or personal data outside of designated CQC locations unless specifically authorised to do so. Extra care should be taken where work is carried out whilst in transit e.g. on trains or other public transport.

10.3 Network Access Control

This section details the security requirements for access to all internal and external network connections. The objective of this section of the policy is detail the measures to be employed to prevent unauthorised access to networked services. More general network management controls are covered in the Communication and Operations Management Policy section of the document.

It is important that CQC maintains a minimum level of security of its network to ensure compliance with this policy and the relevant codes of connection including GSi and N3.

10.3.1 Policy on use of Network Services

CQC will only provide network access for users to the services that they have been specifically authorised for. To ensure this:

- CQC will consider any externally connected network to be untrusted and potentially hostile, and will take all reasonable precautions to protect the internal network from external threats.
- Access to networked resources will be limited to those which are specifically authorized for individual users and will be controlled through the use of unique user IDs and active directory permissions.

10.3.2 Enforced path

Three tiers of network access control will be used:

- Restrict access at the network perimeter through the use of firewalls (DMZs), domain name servers, network address translation and proxy servers.
- Restrict access at the host through the use of active directory permissions
- Restrict access to applications where separate access control mechanisms exist.

The network administrators will authorise new connections to external networks only with appropriate management approval to meet a specific business need. These connections will also be subject to a risk assessment and approval by the information security team.

10.3.3 User authentication for external connections

External connectivity for CQC users will make use of available authentication systems. Strong (2 factor authentication) facilities will be used to ensure connections are being made by authorised users. All external network connections should, wherever possible, be internally initiated and controlled.

All remote access users must utilise a VPN connection to protect CQC data. Access to sensitive data using external network connections will be the subject of specific authorisation on a case by case basis.

10.3.4 Equipment authentication

Any business partners connecting to the organisation data network use VPN technology with endnode authentication that is compatible with internal security policies and technical standards. The extent of this connectivity will be limited to the minimum necessary to provide the contracted service i.e. management and maintenance of 3rd party servers or applications.

10.3.5 Remote diagnostic port protection

Access to remote diagnostic ports on network devices will be securely controlled and opened only as required and for the minimum period necessary to allow fault diagnosis and analysis. This access, if used, should be strictly monitored and controlled by the network team. It should also be authorised on a case by case basis using the Security Exception Reporting Authorisation (SERA) process.

10.3.6 Segregation in networks.

The network should be segregated to provide additional security protection for more sensitive elements of the infrastructure. Three security zones should be configured on the network to segregate the following services:

- Publicly available, web based services and connections to external suppliers,
- Internal management services and information,
- Sensitive applications and data storage facilities.

The domains on the network should be separated using gateways (firewalls) which should be used to define the level of access granted to users based on permitted IP addresses, ports and protocols. The definition of the network domains and permitted access controls should be implemented following a risk assessment based on user business requirements. The boundaries of wireless network connections are difficult to define as access can potentially be made from unauthorised users and locations. Any requirement for wireless network connectivity should be subject to a thorough risk assessment and involve specific authorisation in consultation with the information security and IT security teams.

10.3.7 Network connection control

The ability for users to connect to the network and to individual network segments should be clearly defined in and managed by the access control system. This applies to both internal and external authorised users of networked services.

User connectivity should be limited to authorised business applications or services, examples of these services are:

- Messaging – e-mail
- Application and team drive access
- Database server access
- File transfer

Some user access rights, in particular 3rd party access requirements, may be limited to certain times and dates i.e. weekdays only between 08:00 and 17:00 or out of hours maintenance schedules. Consideration should be given to employing this level of control through scheduled connectivity windows wherever possible.

10.3.8 Network routing control

Network routing controls should be employed to reinforce the access control policy. Source and destination IP address checking and validation against polices should be applied onto network segregation device and gateways. Consideration should be given to the employment of stronger controls for external and 3rd party connections.

10.4 Operating System Access Control

Access to operating systems should be restricted to system administrators who have a requirement to carry out maintenance and manage the systems. Unauthorised access to operating systems can represent a significant security risk and every effort should be made to prevent this.

10.4.1 Secure log-on procedures

Access to operating systems will be controlled via a secure log on procedure which should minimise the possibility of unauthorised access. Log on to operating systems hosted and controlled by the organisation should:

- display a warning regarding the unauthorised use of systems and resources,
- limit the number of log on attempts to 5 then impose a time delay until log on can be attempted again,
- not indicate the reason for unsuccessful log on i.e. incorrect ID or password,
- display previous connection data following successful logon,
  - o date and time of the previous successful log-on,
  - o details of any unsuccessful log on attempts since the last successful log on,
- not transmit the password in clear over the network,
- hide the password characters by masking them at the point of entry,
- where available, network address restriction will be used to specify and limit which workstation(s) can request privileged access,
- Active application sessions will be terminated with the logoff procedure, or timed out and disconnected after 15 minutes inactivity.

10.4.2 User identification and authentication

An individual's user login name or registered user identifier will be the same on all their computing environments. However, individuals with responsibility for system administration will have a separate administration account which is unique to them. When not carrying out system administration duties they will use their normal, lower level privileges account.

The following types of accounts require special handling:

- Default accounts - Provided by the vendor of the operating system or 3rd party software will be deleted or disabled. The passwords will be changed for any default accounts which need to be retained, even if disabled. A list of any default vendor accounts will be kept for different platforms and checked on each system.
- Guest accounts - The default Guest account supplied with some systems will be deleted or disabled.
- Temporary accounts - Often assigned for temporary access for contractors or 3rd parties. These accounts will be assigned a defined date on which they will expire. Access will be re-authorised regularly where there is a continued business need.
- Vendor maintenance and installation accounts - These will be enabled for a specific time period (generally not to exceed project go live day) to enable system setup and configuration. These accounts should be disabled as soon as they are no longer needed.
- Generic team accounts – The use of generic accounts should be avoided wherever possible. Typically their use will be limited to generic e-mail accounts to allow reporting and communications to a central team. Procedures will be employed within the business team using these accounts to ensure accountability for their use is maintained.

10.4.3 Password management system

In addition to the policy requirements detailed above, administrator and super user passwords for operating systems and applications should have a minimum of 8 characters.

Other good practice administration rules that should be applied to passwords are:

- all passwords should be stored and transmitted in a protected form i.e. encrypted or as a hash,
- electronic storage of passwords should be separate to the system they give access to and stored in encrypted form or as a hash value,
- a record of previous passwords used should be stored to prevent re-use,
- Any system default passwords present following the installation of a new system must be changed or the associated account (i.e. Guest) deleted before the system is made live.

Passwords will be changed frequently. The frequency of password change is based on criticality of the system they provide access to. The normal change frequency will be every 90 days. System accounts will have a password policy applied to them that meets both operational and security requirements. Where they are used purely by applications and contain no interactive log on facility the change frequency may be extended, however, due to the potential power of these passwords they should be changed under dual control and copied securely to backup media. The backups should then be stored securely where they can be retrieved in case of system or application outage.

10.4.4 Use of system utilities

System utilities help to manage critical functions of the operating system. Use of and access to these utilities will be strictly controlled and logged.

Each operating system contains features and configurations that can provide additional protection for privileged accounts. System administrators will evaluate and implement operating system features that place limits on privileged access, provide an audit trail for, or monitor privileged access activities.

Insecure system file and directory access rights and permissions can be exploited by system intruders to copy proprietary information, plant Trojans, install viruses, modify control files, and replace programs. Insecure access rights or permissions can also leave a system vulnerable to damage from mistakes by authorised users.

Examples of system utilities which should be protected are:

- user administration,
- setting the system clock,
- control of system logs and audit trails,
- Permissions to add, modify or delete system executables or code.

10.4.5 Session time-out

All live system access sessions will be set to timeout after a defined period of inactivity, this time period will differ by application and system sensitivity.

Depending on the content and sensitivity of the system it should be configured to clear one or more of the following:

- session screen,
- application session,
- Network session.

Whenever one of the above timeouts is enforced by the system the ability to re-activate it will be password protected.

10.4.6 Limitation of connection time

Consideration should be given to applying restrictions to the connection times permissible for high risk or sensitive applications. Where connection requirements to applications are only ever during standard business hours, the application should be locked down to refuse any connection request outside these hours. An administrator override should be available on a 24x7 basis to allow for emergency access to the application. Limiting the period during which connections are allowed to computer services reduces the window of opportunity for unauthorised access.

10.5 Application Access Control

10.5.1 Information access restriction

For sensitive applications, users will be allowed access only to those functions for which they have an authorised business need. Access rights of users (for instance: read, write, delete, and execute) will be monitored and actions logged where possible. Consideration should also be given to restricting rights granted to other applications or utilities such as network attached storage facilities, backup routines, data extract and print facilities.

10.5.2 Mobile Computing and Teleworking

Information and data assets stored or processed outside of CQC controlled locations will be given the same level of protection as that which is worked on internally. The different and sometimes higher level risks of working on data outside of controlled environments should be recognised and guarded against.

This policy applies to all CQC employees, contractors, vendors and agents involved in service delivery. It applies to remote access connections used to do work on behalf of CQC, including reading or sending email and viewing intranet web resources as well as all devices used for remote access connectivity.

Staff who have a requirement to work remotely will apply for authorisation through their line manager. The authorisation process will detail the data type and volumes that they will be required to process. Where a remote working facility is granted, the user's line manager is responsible for ensuring that the individual has all the necessary hardware and software to allow secure remote connectivity.

Only encrypted, CQC issued devices will be used for mobile computing. These devices include; laptops, palmtops, notebooks, smart phones and all data bearing media used to store or transfer data. No personally owned devices are to be used to process CQC data or information. It is the user's responsibility to take all necessary precautions to prevent loss of data, damage or theft of their mobile computing device. If any issued device is lost or stolen it should be reported immediately to the information security team as soon as possible in accordance with the incident management process.

Only CQC provided and configured communication links will be used to connect to the network(s). Once authorised to work remotely on CQC equipment and data it is the employees' responsibility to ensure that encryption facilities are available and operational on the equipment they are using. The IT service desk should be contacted for advice or assistance if there are any doubts about the functionality of the encryption facility. When data records are processed remotely on non-networked systems, the data should be synchronised with the relevant centrally stored records as soon as possible. Systems used for remote, stand-alone processing should also be regularly taken into an office location and connected to the network to ensure that security tools and patches, including anti-virus programs, are correctly updated.

Devices used to transport data should only contain the minimum data necessary for a particular purpose, the data should be deleted from the device once it has been synchronised with the central records and is no longer needed on the portable device. Encryption will be applied to all removable media automatically by CQC systems.

Sensitive data should not be processed in public places. If there is a need to work on CQC data in a public place care should be taken to ensure that the work cannot be overlooked or

viewed by unauthorised personnel. Individuals will be accountable for the IT equipment they are issued with and will ensure that any faults or problems are reported promptly. Once the ability to work remotely is no longer needed or an employee leaves CQC all assets will be returned, via the line manager and reconciled on the asset register.

IT equipment and data used outside of established CQC premises will be afforded at least the same level of protection that it receives at office locations. Physical assets will be given additional protection to guard against the increased risk of loss, theft or damage. This particularly applies to assets which contain sensitive or pesonal data.

All devices connected to the managed networks will be registered assets and controlled using the MAC address or other unique network identifier (i.e. IP address) of the device. Users will not install or use removable networking components such as wireless network cards, wireless network USB tokens, Bluetooth USB tokens, etc; without the submission of justification to both the IT and information security teams using the SERA process.

Particular attention will be applied to any IT equipment and associated connectivity where this is used to provide data centre or system support activities from a remote location. The ability to remotely connect to system administration functions will require high level authorisation from the users line manager as well as the IT and information security teams.

11. Information Systems Acquisition, Development and Maintenance Policy

11.1 Security requirements of information systems

This policy applies to the development, acquisition and maintenance of all systems in use by CQC. These systems may be internally or externally developed and supported internally or as a managed service by a third party provider.

This policy should be used as guidance when assessing new products and services. Security is an integral part of new systems. The type and depth of security requirements which will be specified during the functional design or product selection phase depend on the sensitivity and availability requirements of the data in those systems.

All database or data repositories developed in house (end user computing) will be fully documented and measures will be employed to ensure that 2 or more members of staff are familiar with the ‘systems’ to ensure that there is no key person dependency. Wherever possible existing, centrally controlled systems will be used for all data recording activities. Any locally developed systems should only be used where no central functionality is available. Data used on locally developed systems will not be used to store or process any unique instances of critical or sensitive data. Staff will ensure that any locally developed systems are stored in locations which are included in the central IT controlled backup systems to ensure that they can be recovered following system errors or outages. This will also ensure that the correct access control measures are applied to team data.

Security requirements analysis and specification will also be a requirement of any infrastructure build; enhancement or outsourcing arrangement.

The information security team must liaise with the ICT live services management teams to:

- to provide input to the development or selection process,
- ensure all of CQC security requirements are covered and met,
- carry out a risk assessment to identify vulnerabilities and/or compliance in the early stages of systems development or acquisition,
- Assist and support development or adoption of new services and infrastructure.

Security involvement in all projects should take place at the earliest opportunity available. Security controls and requirements introduced at an early stage of system development are considerably more effective and cheaper than those which have to be retrospectively applied.

The security acceptance criteria may be formulated from internal policies, standards and compliance requirements, be taken from externally available security compliance and standards criteria or be a combination of the two.

The security analysis of new systems will take into account any risks to CQC data assets which may be introduced by the new system as well as risks associated with the integration of the system(s) with the existing infrastructure and services.

11.1.1 Correct processing in applications

Controls need to be available within applications and business processes to ensure that information contained within the systems is accurate, up to date and available in the correct format. To achieve this, controls should be designed into the applications and business processes which include validation of input data, internal processing and output data. The system controls which should be applied should include a combination of:

- dual input or other input checks such as boundary checking or limiting fields to specific ranges of input data to detect potential errors such as:
    - out-of-range values,
    - invalid characters in data fields,
    - missing or incomplete data,
    - exceeding upper and lower data volume limits,
    - Unauthorised or inconsistent control data.
- periodic review of the content of key fields or data files to confirm their validity and integrity,
- inspection of hard copy input documents,
- procedures for responding to validation errors i.e. checks of the original data and any application error message,
- procedures for testing the plausibility (sense checking) of input data,
- defining the responsibilities of personnel involved in the data input process,
- Ensuring that logs are used to record the activities involved in the data input process.

Where available, automated data input validation should be used to reduce the risk of errors and ensure the quality of the data input. However, full assurance can only be obtained from a combination of all data verification methods available.

11.1.2 Control of internal processing

Applications should include internal data checks to detect and alert to the corruption of information through processing errors, interrupted communications or user errors. These checks should be automated and may use cryptographic controls such as integrity checking with hashes or checksums.

A comprehensive backup regime should be used in conjunction with the application to ensure that where data corruption is detected, a true copy of the data can be restored. The frequency of the backups taken should correspond to the criticality of the data being processed.

11.1.3 Output data validation

Assumptions are often made that if input validation and processing controls are correctly implemented then the data output will always be correct, this is not always the case and output validation should also take place.

Output validation checks may include one or more of the following measures:

- Reconciliation checks to ensure that all required data has been processed,
- Plausibility (sense) checks of any output data to ensure that it is reasonable,
- The provision of sufficient information within the data records to allow the user or subsequent processing system to verify that the output is accurate, complete and precise.
- Procedures for responding to output validation tests

11.2 Cryptographic controls

The use of cryptographic controls and tools is becoming widespread in IT and particularly in relation to and support of IT security measures. However, to ensure that the use of cryptography is appropriate and provides the correct levels of protection and control, the cryptographic policy for CQC is detailed below.

Cryptographic controls can be used to achieve different objectives and apply different security control mechanisms including:

- Confidentiality – encrypt static or transitory data,
- Integrity / Authenticity – use digital signatures or message authentication codes to protect the authenticity of critical data,
- Non-repudiation – a combination of cryptographic techniques which provide a means of verifying the origin of a message or transaction.

All members of staff who have an authorised requirement to extract sensitive or personal data from CQC systems or transport such data to another location on portable IT equipment or media will ensure that the data is protected using the default encryption facility.

11.2.1 Cryptographic algorithms and key strength

The following algorithms and associated key lengths are currently approved for use within the CQC:

- Advance Encryption Standard (AES) with keys of 256 bits or greater
- Rivest, Shamir and Adelman (RSA) with keys of 2048 bits or greater
- Secure Hashing Algorithm (SHA) with keys of 256 bits or greater

Other algorithms and associated key lengths may be applicable for certain applications or security purposes. More detailed guidance may be sought from the information security or ICT Live services team.

11.2.2 Policy on the use of cryptographic controls

The primary use of cryptography in CQC is to provide confidentiality (encryption) for sensitive and personal data stored on portable devices and removable media. However, it may also be used in relation to authentication services for web and electronic commerce sites. There is also the potential for future use of cryptographic tools to provide data verification and integrity checking as well as user authentication.

Any proposed use of cryptographic controls within CQC requires both information security and ICT Live Services approval to ensure that the correct implementation is followed and that supporting processes are in place. The type of cryptographic algorithm used in conjunction with an application or dataset as well as the strength of the associated cryptographic keys will be based on a risk assessment and subject to the minimum requirements contained in this policy. This will take into account the requirement to encrypt data in transit, storage or both.

All use of cryptography will consider the implications for key management and, where necessary, have all the supporting processes and requirements implemented along with the cryptographic routine. This will make specific provision for secure key storage, backup and retrieval to ensure that encrypted data is not irretrievably lost.

Careful consideration will also be given to any operational impact of encrypting data i.e. the potential inability to effectively inspect data for viruses and malware.

Whilst it is unlikely that any sensitive CQC data will be stored or processed outside of the UK, consideration should be given to differing national cryptographic regulations throughout Europe and the rest of the world.

11.2.3 Cryptographic key management

A project or workstream employing cryptography will clearly define and allocate responsibilities for key management, including key generation. Depending on the use of cryptography, it may be necessary to ensure that key management processes and procedures are in place to support this. In-house key management will only be required where the CQC or it's service providers are directly responsible for generating and handling the keys used in conjunction with the application.

All cryptographic keys should be protected against modification, loss and destruction. All secret and private keys should be protected against unauthorised disclosure, any equipment used to generate, store and archive keys should be kept physically secure.

Any required key management system will be based on agreed standards, procedures and secure methods for:

- generating keys for different cryptographic systems and different applications,
- generating and distributing public key certificates,
- distributing keys to intended users, including how keys should be activated when received,
- storing keys, including how authorised users get access to keys,
- changing or updating keys and instructions on how often this will happen and how to effect it,
- dealing with compromised keys,
- revoking keys following compromise or security breach,
- recovering keys that become lost or corrupted i.e. in a business continuity or disaster recovery scenario,
- archiving keys,
- destroying keys,
- Logging and auditing all key management related activities.

11.3 Security of system files

Access to system files and application source code will be protected. Access to either of these areas will be strictly controlled and limited to the minimum necessary.

11.3.1 Control of operational software

The installation of software on operational systems will only be carried out in accordance with set procedures and by qualified personnel. To minimise the risk of errors and corruption of operational systems, the following guidelines will be adhered to:

- updating of operational software, applications and program libraries will only be carried out by trained administrators who have appropriate management authorisation,
- operational systems will only hold approved executable code, no compilers or development code will be present,
- application and operating system code will only be loaded following compatibility testing to make sure that it does not have any adverse effect on existing applications,
- a configuration management control system should be in place to track all implemented software and associated system documentation,
- a back out plan will be produced prior to updating or loading operational code,
- an audit log of all changes to operational software will be maintained,
- Backup copies of operational software will be taken, along with all necessary configuration parameters, prior to updates or the application of patches.

All vendor supplied operational software will be kept up to date to prevent the application going out of support. All changes will consider the security implications of the update(s).

11.3.2 Protection of system test data

The requirement for test data should be carefully examined in relation to its use. Once selected it should be protected and controlled to ensure that it cannot be confused with live data and potentially be loaded into a live system. The use of live databases containing sensitive data will not be used for testing purposes. If live data is to be anonymised for testing or training purposes, the routine used to anonymise it will be thoroughly tested and sample outputs examined to ensure that the process is complete and fit for purpose.

11.3.3 Access control to program source code

Program libraries and source code should be stored separately to the systems on which the programs are executed. Access to the source code should be strictly protected with consideration given to implementing dual control access.

11.4 Security in development and support processes

Wherever software and application development activities are carried out by or on behalf of CQC, assurances should be obtained that good practice guidelines are being observed and that the quality of the code or application delivered is of an acceptable standard. The following is a list of the main areas which need to be examined in relation to 3rd party application development:

- change control procedures,
- technical review of applications for compatibility following operating system changes,
- restrictions on changes to software packages should be minimised and strictly controlled,
- evidence of prevention of information leakage (Trojans or other covert channels) from the application and testing against this,
- technical vulnerability checking against known exploits,
- Methods of producing, testing and distributing application patches.

11.4.1 Change control procedures

The implementation of changes should be controlled by the use of formal change control procedures. They should be documented and enforced to minimise the risk of changes adversely affecting operational systems. The change control process should ensure that all changes are:

- tested or otherwise assessed as effective and compatible with existing systems,
- fully documented,
- reviewed by relevant teams or individuals,
- assessed for impact on other applications, databases, operating systems and processes,
- formally approved prior to implementation,
- recorded on audit trails,
- Implemented at a time designed to cause minimum disruption to users or other processes.

The relevant system documentation should be updated following successful completion of the change. Software version controls should also be updated, including on the asset register.

11.4.2 Technical review of applications after operating system changes

Any proposed changes to operating systems, including patching and other updates, will be thoroughly reviewed and, where necessary, tested prior to implementation to ensure that there is no adverse impact on supported applications or security controls in place.

Operating system owners will be responsible for monitoring the availability and associated urgency of patches and fixes notified by the relevant vendor(s). Any updates applied to operating systems will include consideration of the need to update the business continuity and disaster recovery plan.

The above controls will also apply to changes to software packages. However, wherever possible changes to vendor software packages will be avoided. If any changes are required to vendor supplied software packages then the vendor must be asked to provide them as updates or fixes. CQC will not modify or amend any commercial software as this will invalidate license agreements and support contracts.

11.4.3 Information leakage

Information leakage is the loss of data confidentiality through the use and exploitation of malicious covert channels or data paths. Controls will be deployed to reduce the possibility of information leakage, these include:

- Anti-virus software deployment to identify and block potential 'Trojan' code,
- Only using reputable commercial software i.e. no freeware or shareware will be allowed on CQC systems,
- Technical vulnerability testing will be carried out at appropriate intervals (see section 5 below).

11.4.4 Outsourced software development

If CQC enters into any agreement to have outsourced software development conducted, the following controls will be considered:

- licensing agreements, code ownership and intellectual property rights,
- certification of the quality and accuracy of the work carried out,
- code escrow agreements in the event of a failure of the third party business,
- rights of access for audit of the quality and accuracy of the work,
- contractual requirements for quality and security functionality of code,
- Testing before installation to detect malicious and Trojan code.

11.5 Technical vulnerability management

Technical vulnerability management will be independently conducted to reduce risks introduced through the exploitation of known technical vulnerabilities. It will be carried out for all applications and operating systems and the wider technical infrastructure used by CQC. The scope of planned tests should be discussed between the ICT live services and security teams before they are finalised with the service provider.

11.5.1 Control of technical vulnerabilities

Application and operating system vendors operate notification schemes which publish detailed information about any known vulnerabilities including regular updates and, normally, criticality ratings. These notifications should be monitored by application and operating system owners for any alerts which are relevant to the CQC IT infrastructure. The following points should be considered by CQC for inclusion within the vulnerability management process:

- roles and responsibilities for the process should be defined, including; monitoring, risk assessment, patching, asset tracking and coordination,
- sources of notifications should be identified for all of CQC's critical assets,
- timelines should be defined for the reaction to and resolution of relevant vulnerability patching,
- risk assessment of each relevant patch should carried out to compare the risk of installing it against the risk of not doing so,
- patches should be tested to ensure they are effective and do not adversely affect other system components,
- if a vulnerability is discovered and no patch is available other mitigating controls should be considered, including:
  - disabling services or capabilities related to the vulnerability,
  - adapting or adding compensating controls elsewhere i.e. disabling a port at a firewall or blocking a particular protocol,
  - increasing monitoring to detect and react to any attempted exploit,
  - raising awareness of the vulnerability to any potentially impacted users,
- the vulnerability management process should be regularly reviewed and updated to ensure its continued effectiveness,
- Any high risk or particularly sensitive systems should be prioritised within the process.

12. Information Security Incident Management

12.1 Reporting information security events and weaknesses

This policy details the requirements and arrangements for the reporting of all information security events and weaknesses associated with information handling facilities and information systems. It is designed to ensure that all relevant information is communicated correctly so that timely corrective action can be taken. This policy should be read in conjunction with CQC Risk and Incident management strategy document which contains the formal event reporting and escalation procedures. All employees (permanent, temporary and third parties) should be aware of the procedures and obligations in place for reporting the different types of events and weaknesses which may have an impact on the security of the organisation's assets.

12.1.1 Reporting information security events

All information security events should be reported to the security mailbox and through line management as soon as possible following the event or incident. The detailed reporting arrangements for different types of incidents are contained within the Risk and Incident management strategy document. The primary point of contact for all reporting covered by

this policy is the information security team; all information security related events should also be reported to the Information security manager.

The reporting procedure for all information security related events will include:

- the correct actions to be taken in case of an information security event,
- noting all important details (e.g. type of non-compliance or breach, system malfunction details, screen messages, details of unusual behaviour) immediately,
- not taking any action to resolve the issue prior to reporting it and obtaining advice,
- feedback mechanisms to ensure that employees are notified that the issue they have reported has been investigated and acted upon,
- reporting forms or mechanisms to assist the employee with recording and reporting all the necessary detail,
- Reference to CQC disciplinary process for dealing with users who commit or cause security breaches.

All employees should be aware that the earlier an actual or suspected security related incident is reported the more effectively it can be dealt with. Delay or failure to report an incident will often have greater repercussions for both any users involved and the organisation.

Common examples of information security events and incidents are:

- loss of data, equipment, service or facilities,
- system malfunctions or overloads,
- human errors,
- non-compliance with policies, procedures or guidelines,
- breaches of physical security arrangements,
- uncontrolled system changes,
- malfunction of software or hardware – these, or other anomalous system behaviour, may be an indicator of a security attack or actual breach and should always be reported and investigated,
- Access control violations.

12.1.2 Reporting security weaknesses

Security weakness may be observed by any employee, whilst they may not represent an incident they should be reported for further investigation and remedial action as necessary. They should be reported to the IT service desk and information security team, via line management, as soon as possible to prevent an incident occurring. Employees should not attempt to prove that an observed system weakness can be exploited. Testing system weaknesses could be interpreted as potential misuse of the system and may cause an information security incident to occur.

12.2 Management of information security incidents and improvements

A consistent and effective approach to the management of security incidents will be adopted by CQC. The supporting processes will ensure that all actual or suspected information security incidents and weaknesses are handled consistently. The process for

handling these will be subject to continuous improvement and will be applied to monitoring, recording, evaluating and the overall management of incidents and events.
The handling of all incidents, weaknesses and security related events will take into account the requirement, where necessary, to collect and preserve evidence to ensure compliance with any applicable legal requirements.

12.2.1 Responsibilities and procedures

In addition to, and in support of the individual reporting responsibilities of this policy, system monitoring, alerting and vulnerability checking will be carried out. This will be used to detect potential and actual security incidents which will be subject to further investigation.

The detailed procedure for information security incident management will take account of the following guidelines:

- the procedures will be designed to handle different types of information security incidents, including:
    - information system failures and loss of service,
    - malicious code,
    - denial of service,
    - errors resulting from incomplete or inaccurate data,
    - breaches of confidentiality and integrity,
    - misuse of information systems,
- the procedures should also cover:
    - analysis and identification of the cause of the incident,
    - containment,
    - planning and implementation of corrective actions to prevent recurrence,
    - communication to all necessary parties involved with the recovery from the incident,
    - reporting the incident and mitigation plans and actions to the necessary authority,
- the collection and secure storage of audit trails and other required evidence for:
    - internal analysis,
    - retention as evidence in relation to legal of regulatory requirements where the incident may incur liability for the organisation or individuals such as the Data Protection Act or Computer Misuse Act,
    - negotiation of compensation from a third party supplier of software, hardware or services,
- Actions taken to recover from security incidents and breaches should be carefully and formally controlled to ensure that:
    - only nominated, authorised personnel are allowed access to live systems and data,
    - all incident recovery actions are fully documented and retained,
    - all emergency actions taken are reported to management for review,
    - The integrity of systems, controls and data is confirmed as soon as possible.

All procedures and objectives of information security incident management should be reviewed by senior management. It should be ensured that those employees with responsibility of information security incident management understand the priorities and

policy. This will include reporting responsibilities and the arrangements for handling incidents which involve other organisations and service providers.

12.2.2 Learning from information security incidents

Information about security incidents should be recorded and collated to enable analysis of the types, volumes, costs and root causes to take place. This information should be used to provide the basis of required improvement plans with the aim of reducing the likelihood of future recurrences. The information will also be taken into account when updating and revising the security policy documents.

12.2.3 Collection of evidence

There are 2 primary categories of incident where the collection and preservation of evidence may be required. These are:

- Where internal HR disciplinary processes may be invoked or,
- Where the incident may lead to civil or criminal proceedings against CQC or an individual.

When an incident is first reported the details may be incomplete or unclear. It will not usually be obvious whether or not there are any legal or internal disciplinary implications. Consideration should be given in every investigation to the collection and preservation of original copies of any documents, material or IT hardware which may later be required as evidence. The preservation of IT system based evidence is complex and technical; it is unlikely that this could be effectively carried out by CQC personnel. Any evidence used in legal proceedings must comply with detailed rules and procedures which cover:

- admissibility of evidence - whether or not it can be used in court,
- weight of evidence - concerning its completeness and quality,
- Integrity of evidence - whether or not it may have been changed during or after collection.

During the course of any investigation if it becomes apparent that the matter could lead to legal proceedings, consideration should be given to requesting the assistance of the IT service provider specialists.

13. Business Continuity Management

13.1 Information security aspects of business continuity management

This Security Policy document has been produced to comply with the requirements of ISO 27001:2005, section 14, Business Continuity Management. It documents the policy requirements for the measures employed by CQC to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to assist with the recovery of services to their usual location.

The business continuity process should be designed to minimise the impact on the organisation and recover from the loss of information assets through a combination of

preventative and recovery controls. The process should identify and focus on the critical business assets and processes and integrate the information security management requirements of business continuity with requirements from other areas such as operations, HR and facilities.

The process should incorporate methods of identifying and reducing business continuity specific risks and limit, wherever possible, the consequences of incidents. It should also contain provision to ensure that business information required by CQC remains readily available. The business continuity plan should also take account of essential services supplied by third party providers which are outside the direct control of CQC.

13.1.1 Including information security in the business continuity management process

A managed process should be developed and maintained for business continuity throughout the organisation that addresses the information security requirements needed for the organisation's business continuity. The business continuity management process should include and coordinate the following key elements:

- identification of all critical business assets,
- understanding the risks to the prioritised business assets,
- understanding the impact on assets of information security related events,
- identifying and considering the implementation of additional preventative and mitigating controls,
- identifying sufficient financial, organisational, technical and environmental resources to address the identified information security requirements,
- ensuring the safety of personnel and the protection of information processing facilities and organisational property,
- formulating and documenting business continuity plans which address information security requirements in line with agreed strategy,
- regular testing and updating of the plans and processes,
- Ensuring that ownership of the business continuity strategy is assigned at the appropriate management level.

13.1.2 Business continuity risk assessments

The events which could cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security. Information security aspects of business continuity should be based on the identification of events or sequences of events which can cause interruptions to business processes e.g. human errors, theft, fire, equipment failures and natural disasters. A risk assessment should be carried out to quantify the likelihood and the resultant impact of these types of events in terms of time, damage and recovery times. Risk assessments should be carried out in conjunction with the owners of systems and business processes. Consideration should be given to linking relevant risks and examining the possibility of secondary risks arising from the realisation of a primary risk e.g. the loss of a network segment could cause increased risk, due to overloading of other sections of the network or the loss of security component equipment may increase the risk to unauthorised access to other systems or data.

13.1.3 Developing and implementing continuity plans including information security

Plans should be developed and implemented to maintain or restore operations and ensure availability of information in the required time scales following interruption to, or failure of, critical business processes.

The business continuity planning process should include:

- identification and agreement of all responsibilities and continuity procedures,
- identification and documentation of the acceptable loss of information and services, i.e. the maximum scale of an incident where it would not be deemed necessary to invoke continuity plans,
- documentation of agreed processes and procedures,
- education and awareness of staff on the processes and procedures including crisis management,
- Testing and updating of plans.

The planning process should focus on the business objectives of restoring specific services to staff and customers in an agreed timeframe. The resources and services required to achieve this should be identified including staff and fall back arrangements. Fallback arrangements will, wherever possible, rely on other CQC locations or services which may be shared in the event of an emergency. If temporary, alternative locations are used for the provision of services, the level of security at these locations should be equivalent to that employed at the main site.

Copies of all business continuity plans should be stored under arrangements which ensure that they are available in the event of an emergency or loss of a site or system e.g. both electronically and in hard copy or, on both the central information servers and backed up to media available at a number of CQC sites. The plans may well contain sensitive information and consideration should be given to ensuring that they are stored securely at all locations.

13.1.4 Business continuity planning framework

A single framework of business continuity plans should be maintained to ensure that all plans are consistent, consistently address information security requirements and clearly identify priorities for testing and maintenance. Each business continuity plan should describe the approach for continuity to ensure information or information systems availability and security. The business continuity framework should address the identified information security requirements and consider the following:

- the conditions for activating the plans which describe the process to be followed (e.g. how to assess the situation, who is to be involved) before each plan is activated,
- emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations,
- resumption procedures which describe the actions to be taken to return to normal business operations,
- temporary operational procedures to follow pending completion of recovery and restoration,
- a maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan,

- awareness, education, and training activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective,
- The critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures.

13.1.5 Testing, maintaining and re-assessing business continuity plans

Business continuity plans should be tested and updated regularly to ensure that they remain effective and are subject to a continuous improvement process.

Tests carried out should ensure that all members of the recovery team and other relevant staff understand their responsibilities and know the detailed requirements of the process related to their role.

A test schedule should be developed which details how each element of the plan will be practised and the frequency of the tests. A variety of techniques may be used to test the effectiveness of the plan, these include:

- table-top testing,
- simulations,
- technical recovery testing (ensuring that information systems can be recovered from backup devices etc.),
- testing recovery capability at an alternative site with representative staff from relevant business areas,
- testing of supplier services and facilities where these form part of the plan,
- Complete rehearsals of continuity arrangements where this does not introduce risk or safety issues,

The selection of the type of testing to include on the test schedule should be that which is most applicable to CQC and most comprehensively proves the continuity process in line with business requirements and limitations.

The individual sections of the plan should be allocated to business units who are responsible for regularly reviewing and updating the plan or section of the plan. Updates to the plans should take place when new equipment is acquired, systems are upgraded or there are any significant changes in:

- personnel,
- addresses or phone numbers,
- business strategy or organisational change,
- location, facilities and resources,
- legislation or regulation,
- contractors and suppliers,
- processes,
- Risk (both operational and financial).

14. Compliance, standards, policy and legal requirements

14.1 Introduction

Compliance is a necessary process to ensure that CQC meets its statutory, legal and regulatory obligations, in addition to complying with relevant policies, standards and guidelines. CQC has a large number of compliance regulations and related reporting requirements; this policy is limited to considering those which are information governance or security related.

As no CQC data should be processed or stored outside of the UK, only UK legislation has been considered within this policy document.

The organisation's level of compliance is measured in a number of ways including audits, system tests and through the monitoring of system and workplace processes.

14.1.1 Identification of applicable legislation

The statutory and regulatory requirements covered by this policy and a summary of CQC's compliance requirements is:

- Data Protection Act 1998,
- Freedom of Information Act 2000,
- Computer Misuse Act 1990,
- Regulation of Investigatory Powers Act 2000,
- NHS Confidentially Code of Practice,
- NHS Records Management Code of Practice,
- Access to Health Records Act 1990,
- Public Records Act 1958 and 1967,
- Civil contingencies Act 2004,
- Caldicott Report of Patient Identifiable Information 1997,
- Connecting for Health Information Governance Toolkit,
- ISO 27001 Information Security Standard (Discretionary compliance requirement).

Legislative compliance is primarily the responsibility of the Information Rights team within the Governance and Legal Services directorate. Authoritative policy and guidance is contained in the Information Governance Policy which should be referred to for all information access and sharing matters.

14.1.2 Intellectual Property Rights

Appropriate procedures should be in place to ensure compliance with relevant intellectual property rights in relation to CQC rights to use proprietary, licensed software products. Infringement of copyright law can lead to legal action which may involve reputational damage and possible legal proceedings.

ICT Live Services will maintain a list of approved software products in use and the associated manufacturer license agreement number. The list will be stored as an integral part of the CQC asset register. The following guidelines will be followed to ensure compliance with intellectual property rights:

- Software will only be acquired from known and reputable vendors,

- All software programs and the associated license details will be included on the asset register, it will detail any annual maintenance fees due, license renewal dates and number of licensed seats where these are not covered by IT processes.
- Retention of all proof of purchase, original licenses, manuals and any media supplied,
- Checks of all software being used by CQC will be carried out,
- The disposal of software, including transfer to another user will be annotated on the asset register,
- Backup copies of all original software will be made to enable restoration of the business function following an incident or emergency,
- Any other material protected by copyright will not be copied, in full or part, other than where permitted under the license or by copyright law.

14.1.3 Protection of organisational records

The majority of records in use by CQC fall under the remit of either legal or regulatory controls. They should at all times be protected against loss, destruction and falsification.

All organisational records should be categorised in line with the Asset Management Policy. Where applicable or necessary for business purposes the categories should be further refined into record types i.e. accounting records, database records, transaction logs etc. This will ensure that segregation, where required, of sensitive information can be more easily achieved.

CQC has a significant amount of data which is subject to the records retention policy. This requires the organisation to store and retain records for various time periods up to and including permanent preservation. These records may need to be retrieved for reference at relatively short notice e.g. as evidence for legal investigations or proceedings. Consideration should be given to the type of storage medium used for data to ensure that it will remain valid for the projected lifetime of the records. The two main considerations should be the potential deterioration of storage media and the future availability of equipment to read particular electronic media.

All storage of records should include clear labelling with the following information:

- summary of the record type and content,
- record sensitivity or classification,
- date of archive,
- details of the data asset owner, this should be a department rather than an individual,
- date on which the data may or should be destroyed,
- A central inventory of all records storage, disposal and destruction should be maintained.

14.1.4 Data protection and privacy of personal information

The lead for all data protection issues, including the receipt and handling of all Subject Access Requests (SARs) is the information rights team. Responses to such requests must be dealt with promptly (within 40 days) and as otherwise specified within the Data protection Act.

Data protection and privacy policy is one of the key compliance requirements for the CQC. It is underpinned in legislation by the Data Protection Act and reinforced by a number of compliance requirements including; NHS Confidentially Code of Practice, NHS Records Management Code of Practice and the Access to Health Records Act 1990.

Personal data is defined as any data that can uniquely identify an individual. This can include a persons name, address, date of birth, postcode, telephone number, e-mail address, photograph, national insurance number, employee number or patient reference number. However, the mention of an individuals name alone in a document will not mean that the document contains their personal data. In addition to this the organisation is also likely to hold sensitive information on individuals. Sensitive personal data includes medical records, religious beliefs, racial or ethnic origin, political opinion, trade union memberships, physical or mental health, sexual life, criminal offences or associated proceedings. Wherever personal data is referred to in this policy it should be taken to include sensitive personal data.

CQC must register the systems on which it stores and processes personal data along with a high level description of how the data is used. CQC registrations are available from the Information Commissioners website at: http://www.ico.gov.uk

Under the legislation there are a number of data protection principles which need to be understood and applied by all staff with a responsibility for handling and processing personal data. The eight principles of good practice apply to obtaining, processing, holding and storing personal data relating to living individuals. These are:

1 – Personal data shall be processed fairly and lawfully.

There is a requirement to make the general public aware of why CQC needs information about them, how this is used and to whom it may be disclosed. There must be procedures to notify staff, temporary employees, volunteers, locums etc, of the reasons why their information is required, how it will be used and to whom it may be disclosed. This may occur during induction or by their individual manager. Providers and service users will be made aware of the relevant sections of the act through the use of information provided during regular business communications and verbally by CQC professionals communicating directly with them.

2 – Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

All databases which hold and/or process personal information about living individuals must be registered with the Office of the Information Commissioner. This process is known as notification. If CQC fails to complete this process and keep the information up to date it will commit a criminal offence and could face criminal prosecution. The information rights team will ensure all relevant databases and their purposes are registered. A nominated person will be responsible as an application/system manager for each registered database. The asset register will contain a log of databases and nominated applications/system managers.

A database is any collection of personal information that can be processed by automated means:

- *Provider and service user records (names and addresses, etc)*
- *Confidential personal information used in relation to inspections and assessments*
- *Staff records*
- *Other personal data in any form*

3 – Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Information collected from individuals should be complete and should all be justified as being required for the purpose they are being requested. It may sometimes be necessary to justify information needs on an item-by-item basis.

4 – Personal data shall be accurate and, where necessary, kept up to date.
The organisation has to ensure that all information held on any media is accurate and up to date. The accuracy of the information can be achieved by implementing validation routines as detailed in the Information Systems Acquisition, Development and Maintenance Policy.

Users of software will be responsible for the quality (i.e. accuracy, timeliness, completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes. Staff should check that personal information held is kept up to date. Staff information should also be checked for accuracy on a regular basis, either by the manager or by the Human Resources department.

5 – Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

All records are affected by this requirement regardless of the media in which they may be held, stored or retained. The records and document management team provides comprehensive guidance for CQC. If personal information on a computer or in a manual record is not the main record, this is considered to be transient data. If relevant, the information should be incorporated into the main record as soon as possible or destroyed when it is no longer required. CQC has a Records Management Policy with an associated Records Retention Schedule and the storage and destruction of all records should be handled in line with these procedures.

6 – Personal data shall be processed in accordance with the rights of data subjects under the Act.

Under this principle of the Data Protection Act, individuals have the following rights:

- *Right of subject access (further information see below)*
- *Right to prevent processing likely to cause harm or distress*
- *Right to prevent processing for the purposes of direct marketing*
- *Right in relation to automated decision taking*
- *Right to take action for compensation if the individual suffers damage*
- *Right to take action to rectify, block, erase or destroy inaccurate data*
- *Right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.*

Individuals whose information is held within CQC have rights of access to it regardless of the media on which the information is held. Individuals also have a right to complain if they believe that the organisation is not complying with the requirements of the Data Protection legislation.

CQC must ensure an up to date procedure is in place to deal with requests for access to information. The Access to Health Records Act 1990 provides access rights to relatives, or those who may have a claim, to deceased patients' manual/paper records.

Individuals have a right to seek compensation for any breach of the Act that may cause them damage or distress.

7 – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The organisation will take appropriate measures to protect the security and confidentiality of the information held. This principle is applicable to all staff who handle confidential personal information relating to patients or other employees. Penalties for breaching this principle of the Act can be imposed at a personal level, i.e. the individual can be prosecuted in addition to CQC itself.

8 – Personal data may not be exported outside the European Economic Area unless to a country where the rights of the data subject can be adequately protected.

In practice CQC will not export, or allow a third party to export, any personal or sensitive data outside of the UK.

14.1.5 Freedom of Information and Access to Information

The Commission is subject to the requirements of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) and government policy on public sector transparency.

It will meet these statutory responsibilities by:

Maintaining and publishing a **publication scheme**, approved by the Information Commissioner,
Making information publicly available in accordance with the publication scheme and other government requirements on transparency (by publication on the Commission's website – www.cqc.org.uk – where possible),
Responding to requests for information within the statutory deadline (20 working days),
Providing any requested information that is held by the Commission - except where a relevant exemption from disclosure applies and (where relevant) where the exemption is engaged by an overriding public interest, and
Explaining the application and reason for applying any exemption, of the right to an Internal Review of any decision to withhold information, and of the further right of appeal to the Information Commissioner.

The Commission must also comply with the 'subject access provisions' of the Data Protection Act 1998 (DPA), which allow individuals about whom CQC holds 'personal data' a right of access to that data.

It will meet this statutory responsibility by:

Taking reasonable steps to assure itself of the identity of any person making a subject access request (SAR), so as to protect confidentiality and privacy by ensuring that personal data is only disclosed to those who are entitled to it,
Responding to SARs within the statutory deadline (40 calendar days),
Providing any requested personal data that is held by the Commission - except where a relevant exemption from disclosure applies, and
Explaining the application and reason for applying any exemption, of the right to an Internal Review of any decision to withhold information, and of the further right to seek an assessment from the Information Commissioner.

Training and guidance will be provided to Commission staff to assist them in identifying and appropriately handling statutory requests for information. These requests must be forwarded to the Information Access Team at information.access@cqc.org.uk as quickly as possible following receipt by any representative of the Commission.

The ***Information Rights Manager*** is responsible for ensuring that the Commission responds to requests for information in accordance with its legal responsibilities.

The ***Information Access Team*** coordinate and respond to requests for information under FOIA, EIR and DPA.

Information sharing with other public bodies – Policy Statement

The Commission may share information (including confidential personal information) with other public bodies - where it is lawful and in the public interest to do so - for the purpose of facilitating the exercise of the public functions of CQC, or of the body receiving the information.

Such sharing may include, but is not limited to, sharing information with other regulators, local authorities, and police organisations.

Any sharing of confidential personal information will be conducted in accordance with the **Code of Practice on Confidential Personal Information.**

The Commission will only disclose confidential information where it is reasonably assured as to the appropriate security and safeguards on onward transmission of the information by the receiving body.

Where the Commission intends to regularly share information with other bodies, or where a particular instance of sharing warrants, it may develop and publish a Memorandum of Understanding (MOU) and/or Information Sharing Agreement (ISA) that will set out the purpose, mechanisms and safeguards relating to the sharing of information.

The absence of an MOU or ISA does not prohibit the sharing of information with any public body, but each member of Commission staff has a personal, legal responsibility to ensure that any disclosure of information is lawful and appropriate.

The ***Information Access Team*** provides advice on information sharing with other public bodies, and coordinates and responds to requests for information from those bodies that fall outside of the scope of an existing MOU, ISA or relevant policy (eg Safeguarding Policy).

Caldicott Principles – Policy Statement

The Caldicott Principles provide a code for protecting patient and service user information throughout the NHS and public-sector Social Services.

The Commission will ensure that its policies, systems and processes are compliant with the Caldicott Principles.

The Caldicott Principles are incorporated into the Commission's **Code of Practice on Confidential Personal Information.**

The Commission's Caldicott Guardian will be a non-executive member of the Board.

All proposed new policies, systems or processes that will change or significantly impact upon the way in which the Commission processes identifiable (or potentially identifiable) information about people who use regulated services must be scrutinised and approved by the Caldicott Guardian.

The Information Asset Register, IG Toolkit returns, and internal audits of information governance will be regularly reviewed by the Caldicott Guardian to monitor compliance with the Caldicott Principles.

The ***Information Rights Manager*** is responsible for supporting and advising the Caldicott Guardian.

The Chair of Healthwatch England (HWE) will appoint a member of the HWE Committee to be HWE Caldicott Guardian

The HWE Caldicott Guardian will be responsible for ensuring that all processing of service user identifiable information by HWE is in accordance with the Caldicott Principles. Their primary responsibility in this regard is to the HWE Committee.

The CQC Caldicott Guardian maintains overall responsibility for compliance with the Caldicott Principles throughout CQC – including HWE. The HWE Committee will report on Caldicott issues to the CQC Caldicott Guardian.

14.1.6 Prevention of misuse of information processing facilities

The use of any of the organisation's information processing facilities will be specifically authorised, by line management, for each individual user. The use of any facilities without management approval or for unauthorised non business purposes will be regarded as

improper use. If unauthorised activities are identified they may be investigated further by the user's line manager in conjunction with the information security team and HR.

Network and system security tools will be in place and active, they will monitor system use and raise alerts to any potential security breach or indication of unauthorised activity.

Any unauthorised activity detected will be investigated further and may result in disciplinary action being taken against any individual found to be in contravention of security policy.

14.1.7 Regulation of Cryptographic Controls

Cryptographic regulations and controls largely focus on the use or cryptographic routines, import and export of cryptographic hardware and the transmission of encrypted data across international boundaries.

As CQC does not process any sensitive data outside the UK or develop or implement any hardware based cryptographic routines the legislation in this area does not currently apply to any of the organisation's activities.

The cryptography in use by CQC, via the IT Services provider uses point solutions which do not fall within the scope of the current legislation.

14.2 Compliance with security policies and standards, and technical compliance

All information systems will be specified, installed, configured and maintained in line with the security policies and good practice guidance supplied by manufacturers.

Regular technical compliance reviews, including penetration testing and IT health checks of the information systems will take place to ensure continued compliance.

System managers will be responsible for the reviews in conjunction with the ICT Live Services and security teams.

14.2.1 Compliance with security policies and standards

System managers should regularly check the systems for which they are responsible for compliance against the security policies and associated standards. If any non-compliance is found, managers should:

- determine the cause of the non-compliance,
- determine and implement appropriate corrective action(s),
- evaluate the need for actions to ensure the non-compliance does not recur,
- Review and document the corrective actions taken.

14.2.2 Technical compliance checking

The implementation security standards applied when the system is accepted into service should be regularly checked either manually by system administrators or using software monitoring tools. Penetration tests should also be considered when carrying out technical

compliance checking to ensure that critical areas of security have not been missed or that the system is not vulnerable to newly discovered threats.

Penetration tests require careful planning and consideration to ensure that they do not cause damage to systems or loss of services. A reputable test provider with qualified testers should always be used.

14.3 Information systems audit considerations

System audits should be scheduled and planned so that the impact on operational systems is kept to the minimum possible. Controls should be in place to safeguard both the systems and the audit tools themselves during the audit process. Access control should be applied to prevent misuse of the tools and to provide integrity of both the tools and the associated logs and data.

14.3.1 Information systems audit controls

When planning audit activities on operational systems the following guidelines should be observed:

- Audit requirements should be agreed with systems managers,
- The scope of the checks should be agreed and controlled,
- All audit checks should be limited to read-only access,
- Any audit which requires copies of data or software will arrange to have verified copies made by system administrators,
- Resources for performing the audit checks will be specifically identified and authorized,
- All access during an audit will itself be monitored and logged,
- Full details of all audit activities, including responsibilities, will be documented,
- The personnel conducting the audit will be independent of the activities being audited,
- The implementation of additional controls will be considered where an audit is conducted or assisted by a third party.

14.3.2 Protection of information systems audit tools

Access to information system audit tools will be protected to prevent misuse or compromise. The tools will be separated for development and live systems to prevent any information crossover between environments. Storage of software tools should not be in shared areas such as tape libraries or user areas unless they can be given additional access control protection.

15. Monitoring Compliance and Effectiveness

Monitoring compliance and effectiveness of this policy will be carried out in a number of ways:

- Review of effectiveness during the information and compliance status reviews, which are part of the annual Information Governance Toolkit submissions to the Department of Health.

- External audits commissioned in line with Department of Health (CfH) directives to check compliance with the IG Toolkit and ISO27001.
- Internal, targeted audits of specific information security areas. These will be triggered by the risk management process, incident management or areas of concern highlighted by staff or senior management of CQC.

All compliance monitoring, audits and reporting will be included on the agenda of the IG Group meetings and minutes along with any actions and responsible owners.

Appendix A

Security Policy Document Framework

This Appendix details the high level framework and subject areas for the security policy document in accordance with ISO27001:2005.

Section 1 - Security policy
- Information security policy document
- Review of the information security policy

Section 2 - Organization of information security
- Internal organization
- External parties

Section 3 - Asset management
- Responsibility for assets
- Information classification

Section 4 - Human resources security
- Prior to employment
- During employment
- Termination or change of employment

Section 5 - Physical and environmental security
- Secure areas
- Equipment security

Section 6 - Communications and operations management
- Operational procedures and responsibilities
- Third party service delivery management
- System planning and acceptance
- Protection against malicious and mobile code
- Back-up
- Network security management
- Media handling
- Exchange of information
- Electronic commerce services
- Monitoring

Section 7 - Access control
- Business requirement for access control
- User access management
- User responsibilities
- Network access control
- Operating system access control
- Application and information access control
- Mobile computing and home working

Section 8 - Information systems acquisition, development and maintenance

- Security requirements of information systems
- Correct processing in applications
- Cryptographic controls
- Security of system files
- Security in development and support processes
- Technical Vulnerability Management

Section 9 - Information security incident management

- Reporting information security events and weaknesses
- Management of information security incidents and improvements

Section 10 - Business continuity management

- Information security aspects of business continuity management

Section 11 - Compliance

- Compliance with legal requirements
- Compliance with security policies and standards, and technical compliance
- Information systems audit considerations

Appendix B

Information Security Glossary

This Appendix contains the definition of common terms and acronyms that are used throughout the Security Policy documentation set. Whenever one of the terms contained in this glossary is encountered in this document or in other policy documents, its meaning will be in accordance with the definition in this Glossary, unless otherwise explicitly stated.
It is the responsibility of the Information security manager to ensure that:

- The Glossary is kept current and comprehensive over time
- Information Security Policies are consistent with the definitions in this Glossary.

B1. Abbreviations and acronyms

The entries in the following table of abbreviations and acronyms are all defined in the Glossary below, referenced by their extended (i.e. non-abbreviated) form.

3DES	Triple-DES
ACL	Access Control List
ISO27001	International Standard for information security management systems
BS7799	British Standard 7799
CISO	Chief Information Security Officer
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DNS	Domain Name Server.
DSA	Digital Signature Algorithm
FTP	File Transfer Protocol
IGG	Information Governance Group
HTML	Hypertext Markup Language
HTTP(S)	Hypertext Transfer Protocol (Secure)
ID	Identification
IP	Internet Protocol
ISMS	Information Security Management System
RBAC	Role-Based Access Control
SSL/TLS	Secure Sockets Layer / Transport Layer Security
SIRO	Senior Information Risk Owner
VPN	Virtual Private Network

B2. Glossary

Access
Access is the ability to communicate with a system both by receiving output and sending data or instructions to a system.

Access Control
Access Control is the protection of system resources against unauthorised access. It is a process by which the use of system resources is regulated according to a security policy and is permitted only to authorised entities according to that policy.

Access Control List (ACL)
An ACL is a mechanism that implements access control for a resource by maintaining the identities of the system entities that are permitted to access the resource.

Accountability
The property of a system, including all of its system resources, that ensures that the actions are uniquely linked to a system entity which can then be held responsible for actions carried out on the system. Accountability permits the assignment of responsibility following the detection and subsequent investigation of security breaches.

Accounts
Application accounts are specific user IDs that are used by applications to access system resources. At the operating system level, an application would access file system resources. At the database level, an application would use the account to run queries. These accounts should only be used by applications, not by individual users.

ACPO
Association of Chief Police Officers. Representative body of UK Law Enforcement Agencies.

Administrative Security
The management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data. Examples include clear delineation and separation of duties and configuration control.

AES
Advanced Encryption Standard algorithm introduced to replace the weaker Data Encryption Standard (DES), can be used with key lengths of up to 256bit and is considered secure for all types of data and applications once correctly implemented.

Anonymous
An application may require security services that maintain anonymity of users or other system entities to preserve their privacy or hide them from attack. An alias may be used to hide an entity's real name or identity.

Anonymous Login

Anonymous Login is an access control feature in many Internet hosts that enables users to gain access to general purpose or public services and resources on a host without having a unique authorised system access account.

Asymmetric Cryptography
Asymmetric cryptography is a branch of cryptography popularly known as 'public-key cryptography' that employs a mathematically unique pair of keys (public and private) to provide confidentiality and integrity and authentication services to a system.

Attack
An attack is an assault on a system that is a deliberate attempt to evade or circumvent security services. An active attack attempts to alter system resources or affect their operation. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An internal attack is an attack initiated by an entity inside the security perimeter, i.e., an entity that is authorised to access system resources but uses them in an unauthorised way. An external attack is initiated from outside the perimeter, by an unauthorised user of the system.

Auditing
Auditing is the process and/or capability of gathering information on system transactions and administrative functions which can then be used to validate that the system is being used in an appropriately authorised manner.

Authentication
Authentication is the process of verifying the identity of a system entity. An authentication process consists of two steps:

- Identification step: Presenting an identifier to the security system. Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.
- Verification step: Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

Authentication Information
Information used to verify the identity of a system entity. Authentication information can be derived from one or more of the following:

- Something the entity knows
- Something the entity possesses
- Something the entity is.

Authorisation / Authorise
Authorisation is a right or a permission that is granted to a system entity to access a system resource. The authorisation process is a procedure for granting system rights. To authorise means to grant a right or permission. (See: privilege.)

Availability
Availability is a system or a system resource being accessible and usable upon demand by a system entity, according to performance specifications for the system. (See: critical, denial of service, reliability, survivability.)

Backup
Backup is to move data to a store for the purpose of creating a copy which can be used to recover the system to the point in time of the Backup.

Break or Crack
Cryptographic technique of performing cryptanalysis aimed at decrypting data or performing other cryptographic functions without initially having knowledge of the key protecting the data.

British Standard 7799 / BS7799
Part 1 is a standard code of practice and provides guidance on how to secure an information system. Part 2 specifies the management framework, objectives, and control requirements for information security management systems [B7799]. It is in use in the in a number of countries, Part 1 has also been defined as the ISO 17799 standard. This formed the baseline for, and has now been superseded by ISO27001/2.

Browser
A client computer program that can retrieve and display information from servers on the World Wide Web such as Microsoft Internet Explorer or Google Chrome.

Certification
Certification or registration is a technical evaluation (usually made in support of an accreditation action) of an information system's security features and other safeguards to establish that the system's design and implementation comply with specified security requirements.

Challenge-Response
This is an authentication process that verifies identity by requiring the correct information to be provided in response to a challenge. In a computer system, the authentication information is usually a value that is required to be computed in response to an unpredictable challenge.

Checksum
A checksum is a value which is computed by a function that is dependent on the contents of a data object and can be subsequently stored or transmitted together with the object, for the purpose of detecting changes in the data.

Senior Information Risk Officer (SIRO)
The SIRO is a senior executive within the CQC management team. Their task is to provide overall security guidance and executive support for information security measures and to provide sponsorship of security initiatives throughout the organisation. The SIRO will normally delegate the day to day responsibility for security to, and be advised by the information security manager.

Classification / Classification Level
Classification is a method of applying a caveat to items or groups of items of similar value, importance or sensitivity which form the components of the system supporting CQC operations.

Clear text
Data in which is directly available in a human readable format with no form of encryption applied.

Client
A system entity that requests and uses a service provided by another system entity normally a server. Usually, the requesting entity is a computer process which makes the request on behalf of a human user.

Compromise
A compromise is an incident where information is exposed to individuals with no authority or business need to access the information.

Computer Network
A collection of host computers which are network connected to allow the exchange of data.

Confidentiality
Confidentiality is a measure applied to data to ensure that it is not made available or disclosed to unauthorised individuals, entities, or processes.

Contingency Plan
An emergency response plan formulated to ensure that CQC services can be fully restored following a disaster at either the data centre or a support services location.

Cookie
A cookie is data exchanged between an HTTP (Web) server and a browser to store state information on the client side and retrieve it later for server use. An HTTP server, when sending data to a client, may send along a cookie, which the client retains after the HTTP connection closes. A server can use this mechanism to maintain persistent client-side state information for HTTP-based applications, retrieving the state information in later connections. Cookies can be used to generate profiles of web usage habits, and thus may infringe on personal privacy.

Covert Channel
A Covert Channel is a route that permits an unauthorised entity to transfer information, either internally or externally in breach of system security policy.

Cracker
A cracker is an individual who attempts to gain unauthorised access to a system. Cracker can also be used to describe a piece of software which can be used to carry out attacks on passwords and thereby a means to gain unauthorised access to a system.

Credential(s)
Credentials are made up of data that is transferred or presented to a system in order to establish a claimed identity.

Cryptographic Algorithm
A cryptographic algorithm is the mathematical function used for encryption, decryption and several other security related cryptographic functions.

Cryptographic Key
A cryptographic key is the secret value which is used, in conjunction with the algorithm to encrypt and decrypt data.

Cyclic Redundancy Check (CRC)
A CRC, sometimes called cyclic redundancy code, is a type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data may be expected.

Decrypt
Cryptographically restore cipher text to the plaintext form.

Default Account
A system login account (usually accessed with a user name and password) that has been predefined in a manufactured system to permit initial access when the system is first put into service. Sometimes, the default user name and password are the same in each copy of the system. When the system is put into service, the default password should immediately be changed or the default account should be disabled.

Denial of Service (DoS)
DoS is the prevention of authorised access to a system resource or the delaying of system operations and functions.

Digital Signature Algorithm (DSA)
DSA is an asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Domain
A Domain in security terms is an environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources.

Domain Name System (DNS)
The main Internet operations database, which is distributed over a collection of servers and used by client software for purposes such as translating a domain name-style host name into an IP address and locating a host that accepts mail for some mailbox addresses.

Dual Control
Dual Control is a procedure that uses two or more entities operating together to protect a system resource, such that no single entity acting alone can access that resource.

Encrypt
Cryptographically transform data to produce cipher text.

Encryption

Cryptographic transformation of data into a form that conceals the data's original meaning to prevent it from being known to or used by unauthorised users.

Fail Safe
Fail Safe is a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system.

Firewall
A firewall is an inter-network gateway that restricts data communication traffic to and from a connected network. A firewall typically protects a smaller, secure sub-network from a larger, less secure network. The firewall is installed at the point where the networks connect and the firewall applies security policy rules to control traffic that flows in and out of the protected network.

Gateway
A relay mechanism that attaches to two or more computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other.

Hash Function
An algorithm that computes a value based on a data object such as a message or file with the result of mapping the original data object to a smaller data object, the 'hash result' which is usually a fixed-size value. Any change to the input data object will, with a very high probability, alter the hash result. The cryptographic hash is therefore commonly used to provide message and data integrity checking.

Host
Host is a computer that is attached to a network and can use services provided by the network to exchange data with other attached systems.

Hypertext
A computer document, or part of a document, that contains hyperlinks to other documents; i.e., text that contains active pointers to other text. Usually written in Hypertext Markup Language and accessed using a web browser.

Hypertext Markup Language (HTML)
HTML is a platform-independent system of syntax and semantics for adding characters to data files (particularly text files) to represent the data's structure and to point to related data, thus creating hypertext for use in the World Wide Web and other applications.

Hypertext Transfer Protocol (HTTP)
A TCP-based, application-layer, client-server, Internet protocol used to carry data requests and responses in the World Wide Web. (See: hypertext.)

Identification
Identification is a process that presents an identifier to a system so that the system can recognise a system entity and distinguish it from other entities. This is typically achieved via a user-ID, employee ID, etc.

Information Asset
An Information Asset is a technological, electronic, physical, business process or human-based system, and its contents that are used to store or retrieve information. An asset is more generically defined as ‘something that has value or utility to the organisation’.

Integrity
Integrity is the assurance that data has not been altered, destroyed, or lost in an unauthorised or accidental manner.

Internet Protocol (IP)
IP is an Internet Standard protocol that moves datagrams from one computer to another across a network.

Internet
The Internet is the single, interconnected, worldwide system of commercial, government, educational, and other computer networks that share a set of protocols. The protocol set is named the "Internet Protocol Suite". It also is popularly known as "TCP/IP", two of its fundamental components. These protocols enable a user of any one of the networks in the Internet to communicate with, or use services located on, any of the other networks.

Intranet
A computer network, especially one based on Internet technology; that an organisation uses for its own internal, and usually private, purposes and that is closed to outsiders.

Intruder
An intruder is an entity that gains or attempts to gain access to a system or system resource without having authorisation to do so.

Intrusion Detection
Intruder Detection is a security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorised manner.

Information Security Management System (ISMS)
The ISMS is the combination of the people, policies, processes and technology that assures information security of an organisation or system and is maintained by Information Security Department.

ISO
International Organisation for Standardisation, a voluntary, non-treaty, non-government organisation, established to provide a system for worldwide standardisation.

Key Pair
A pair of mathematically unique related keys (a public key and a private key) that are used for asymmetric cryptography and are generated in a way that makes it computationally infeasible to derive the private key from knowledge of the public key.

A key pair's owner can use them to encrypt data, verify a digital signature, compute a protected checksum, or generate a key in a key agreement algorithm.

Least Privilege
The principle that a security system should be designed so that each participating entity is granted the minimum resource and authorisation it needs to function correctly.

Login / Logon
Logon is a process whereby a system entity gains access to a session in which it can use system resources. This is usually accomplished by providing a user name and password and therefore authentication to the system.

Logoff
Procedure used to terminate authenticated sessions on a system.

Need-To-Know
The business need for access to, knowledge of, or possession of specific information required to carry out official duties. This criterion is used in security procedures that require a custodian of a system ensures that the intended recipient has proper authorisation to access the information.

Non-Repudiation Service
This is a security service that provides protection against false denial of involvement in a communication. The service provides evidence that can be stored and later presented to a third party to resolve disputes that arise if a communication is repudiated by one of the entities involved.

Password
A password is a secret data value, usually a character string which is used as authentication information. A password is usually matched with a user identifier that is presented in the authentication process. Using a password as authentication information assumes that the password is known only by the system entity whose identity is being authenticated. Passwords are normally stored on systems in an encrypted (Hash) form.

Penetration
Penetration or breach refers to successful, unauthorised access to a protected system resource.

Penetration Test
A system test, often part of system certification, in which evaluators attempt to circumvent the security features of the system. Penetration testing is usually performed repeatedly, at regular intervals, on a stable infrastructure or following significant changes to the system or its main components.

Physical Security
Physical Security is a tangible means of preventing unauthorised physical access to a system. e.g., fences, walls, and other barriers; locks, safes, and vaults; dogs and armed guards; sensors and alarm bells.

Port Scan
An attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and subsequently exploiting a known vulnerability to breach the security of the system.

Privacy
Privacy is the right of an entity to determine the degree to which it will interact with its environment, including the degree to which it is willing to share information about itself with others.

Private Key
A Private Key is the secret component of a pair of cryptographic keys used in asymmetric cryptography.

Privilege
Privilege is an authorisation or set of authorisations to perform security controlled functions.

Proxy Server
A computer process often used as an interface between client and server on a network, this can contain a number of security features including content checking, anti-virus checking and access control mechanisms.

Public Key
This is the publicly available component of a pair of cryptographic keys used in asymmetric cryptography.

Public-Key Cryptography
This is a popular synonym for asymmetric cryptography.

Risk
A calculation of potential loss expressed as the probability that a particular threat will exploit a particular vulnerability.

Risk Analysis/Risk Assessment
A process that systematically identifies valuable system resources and threats to those resources, it then quantifies the impact of loss or compromise based on likelihood and costs of occurrence.

Risk Management
Risk Management is the process of identifying, controlling, and eliminating or minimising potential events that may affect Information Assets.

Role-Based Access Control (RBAC)
RBAC is a form of identity-based access control where the system assets are grouped and access controlled in accordance with the verified business need of requesting entities. Role-Based Access is always assigned using the principle of least privilege.

Rule-Based Security Policy.

A security policy based on global rules imposed for all users, these rules may be applied to a single system, domain or an entire system. The rules rely on comparison of the sensitivity of the resource being accessed and possession of appropriate business need of users or groups of users.

Sanitise
The deletion or redaction of sensitive data from a file, a device, or a system or modify data with the purpose of downgrading its classification or sensitivity level.

Secure Sockets Layer (SSL)
An Internet protocol that uses end-to-end encryption to provide data confidentiality, data integrity and, optionally, authentication services between a client and a server. Also known, more recently as Transport Layer Security (TLS).

Security Architecture
A plan and set of principles that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services and the performance levels required of these elements to deal with the assessed level of threat.

Security Audit
An independent review and examination of a system's records, activities and architecture to determine their adequacy to ensure compliance with established security policy and procedures and established best practice.

Security Audit Trail
A chronological record of system activities provided to enable the reconstruction and examination of a particular event or incident.

Security Event
This is an occurrence in a system that has an actual or potential impact on the security of a system.

Security Incident
An incident is an event that involves a violation of security policy or controls, or an adverse event which compromises an aspect of computer, network or information security.

Security Label
A security label is a marking that is bound to a system asset or resource to designate its sensitivity or value. It may be used to collectively group assets of a similar value when assigning access rights for system users.

Security Perimeter
A Security Perimeter is the boundary of the domain within which security policy or security architecture rules apply.

Smart Card
A device containing one or more integrated circuit chips, which perform the functions of a computer's central processor, memory, and input/output interface. In security

terms it is used to securely store a users access control credentials such as a cryptographic key pair.

Spam
Spam is a threat to a system whereby indiscriminate or unsolicited messages are sent which, in sufficient volume, can cause a denial of service.

Strong Authentication
This is an authentication process that relies on additional elements to strengthen the authentication process such as physical tokens in conjunction with personal identification numbers and unique user identification names.

Threat
A threat is a potential security incident, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. A threat can be either intentional or accidental such as a fire or flood.

Threat Analysis
Threat analysis is the assessment of the probability and consequences of damage being caused to a system.

Threat Consequence
A Threat consequence is the result of a security violation resulting from the realisation or execution of a threat.

Triple DES (3DES)
A symmetric block cipher, based on DES, that transforms each 64-bit plaintext block by applying the Data Encryption Algorithm three successive times, using either two or three different keys.

Trojan Horse
A Trojan Horse is a computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms and can be used to steal system data.

Virtual Private Network (VPN)
A VPN is a restricted-use, logical computer network that makes use of the system resources of another, less secure network, it invariably uses cryptographic techniques.

Virus
A virus is a hidden piece of code which is often malicious; it propagates by replicating itself to another program or executing self contained functionality.

Vulnerability
Vulnerability is a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Worm

A Worm is a computer program that can run independently and is another form of virus. It can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.