- 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,
  - date and time of the previous successful log-on,
  - 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.

ANNEX 2: SECURITY MANAGEMENT PLAN

NOT APPLICABLE

CALL OFF SCHEDULE 8: BUSINESS CONTINUITY AND DISASTER RECOVERY

1. BCDR POLICY

1.1 Unless the Supplier has provided a bespoke BCDR Plan during a General Further Competition Procedure, the Supplier's BCDR policy at Annex 1 will apply. Where the Customer has required a bespoke BCDR Plan during a General Further Competition Procedure, the Supplier's BCDR Plan at Annex 2 will also apply.

ANNEX 1: BCDR TENDER POLICY

ANNEX 2: BCDR PLAN

Not Applicable

CALL OFF SCHEDULE 9: EXIT MANAGEMENT

1. DEFINITIONS

1.1 In this Call Off Schedule, the following definitions shall apply:

"Exclusive Assets"	means those Supplier Assets used by the Supplier or a Key Sub-Contractor which are used exclusively in the provision of the Services;
"Exit Information"	has the meaning given to it in paragraph 4.1 of this Call Off Schedule;
"Exit Manager"	means the person appointed by each Party pursuant to paragraph 3.3 of this Call Off Schedule for managing the Parties' respective obligations under this Call Off Schedule;
"Exit Plan"	means the plan described in paragraph 5 of this Call Off Schedule
"Net Book Value"	means the net book value of the relevant Supplier Asset(s) calculated in accordance with the depreciation policy of the Supplier set out in the letter in the agreed form from the Supplier to the Customer of even date with this Call Off Contract;
"Non-Exclusive Assets"	means those Supplier Assets (if any) which are used by the Supplier or a Key Sub-Contractor in connection with the Services but which are also used by the Supplier or Key Sub-Contractor for other purposes;
"Registers"	means the register and configuration database referred to in paragraphs 3.1.1 and 3.1.2 of this Call Off Schedule;
"Termination Assistance"	means the activities to be performed by the Supplier pursuant to the Exit Plan, and any other assistance required by the Customer pursuant to the Termination Assistance Notice;
"Termination Assistance Notice"	has the meaning given to it in paragraph 6.1 of this Call Off Schedule;
"Termination Assistance Period"	means in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to paragraph 6.2 of this Call Off Schedule;
"Transferable Assets"	means those of the Exclusive Assets which are capable of legal transfer to the Customer;

"Transferable Contracts"	means the Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Customer or any Replacement Supplier to perform the Services or the Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Assets"	has the meaning given to it in paragraph 9.2.1 of this Call Off Schedule;
"Transferring Contracts"	has the meaning given to it in paragraph 9.2.3 of this Call Off Schedule.

2. INTRODUCTION

2.1 This Call Off Schedule describes provisions that should be included in the Exit Plan, the duties and responsibilities of the Supplier to the Customer leading up to and covering the Call Off Expiry Date and the transfer of service provision to the Customer and/or a Replacement Supplier.

2.2 The objectives of the exit planning and service transfer arrangements are to ensure a smooth transition of the availability of the Services from the Supplier to the Customer and/or a Replacement Supplier at the Call Off Expiry Date.

3. OBLIGATIONS DURING THE CALL OFF CONTRACT PERIOD TO FACILITATE EXIT

3.1 During the Call Off Contract Period, the Supplier shall:

3.1.1 create and maintain a Register of all:

(a) Supplier Assets, detailing their:

(A) make, model and asset number;

(B) ownership and status as either Exclusive Assets or Non-Exclusive Assets;

(C) Net Book Value;

(D) condition and physical location; and

(E) use (including technical specifications); and

(b) Sub-Contracts and other relevant agreements (including relevant software licences, maintenance and support agreements and equipment rental and lease agreements) required for the performance of the Services;

3.1.2 create and maintain a configuration database or document detailing the technical infrastructure and operating procedures through which the Supplier provides the Services, which shall contain sufficient detail to permit the Customer and/or Replacement Supplier to understand how the Supplier provides the Services and to enable the smooth transition of the Services with the minimum of disruption;

3.1.3 agree the format of the Registers with the Customer as part of the process of agreeing the Exit Plan; and

3.1.4 at all times keep the Registers up to date, in particular in the event that Supplier Assets, Sub-Contracts or other relevant agreements are added to or removed from the Services.

3.2 The Supplier shall:

3.2.1 procure that all Exclusive Assets listed in the Registers are clearly marked to identify that they are exclusively used for the provision of the Services under this Call Off Contract.

3.3 Each Party shall appoint a person for the purposes of managing the Parties' respective obligations under this Call Off Schedule and provide written notification of such appointment to the other Party within three (3) months of the Call Off Commencement Date. The Supplier's Exit Manager shall be responsible for ensuring that the Supplier and its employees, agents and Sub-Contractors comply with this Call Off Schedule. The Supplier shall ensure that its Exit Manager has the requisite Authority to arrange and procure any resources of the Supplier as are reasonably necessary to enable the Supplier to comply with the requirements set out in this Call Off Schedule. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the termination or expiry of this Call Off Contract and all matters connected with this Call Off Schedule and each Party's compliance with it.

4. OBLIGATIONS TO ASSIST ON RE-TENDERING OF SERVICES

4.1 On reasonable notice at any point during the Call Off Contract Period, the Supplier shall provide to the Customer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), the following material and information in order to facilitate the preparation by the Customer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence:

4.1.1 detailed descriptions of the Service(s);

4.1.2 a copy of the Registers, updated by the Supplier up to the date of delivery of such Registers;

4.1.3 an inventory of Customer Data in the Supplier's possession or control;

4.1.4 details of any key terms of any third party contracts and licences, particularly as regards charges, termination, assignment and novation;

4.1.5 a list of on-going and/or threatened disputes in relation to the provision of the Services;

4.1.6 all information relating to Transferring Supplier Employees required to be provided by the Supplier under this Call Off Contract; and

4.1.7 such other material and information as the Customer shall reasonably require,

(together, the "**Exit Information**").

4.2 The Supplier shall:

4.2.1 notify the Customer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon

the provision of any Services and shall consult with the Customer regarding such proposed material changes; and

4.2.2 provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and in any event within ten (10) Working Days of a request in writing from the Customer.

4.3 The Exit Information shall be accurate and complete in all material respects and the level of detail to be provided by the Supplier shall be such as would be reasonably necessary to enable a third party to:

4.3.1 prepare an informed offer for those Services; and

4.3.2 not be disadvantaged in any subsequent procurement process compared to the Supplier (if the Supplier is invited to participate).

5. EXIT PLAN

5.1 The Supplier shall, within three (3) months after the Call Off Commencement Date, deliver to the Customer an Exit Plan which:

5.1.1 sets out the Supplier's proposed methodology for achieving an orderly transition of the Services from the Supplier to the Customer and/or its Replacement Supplier on the expiry or termination of this Call Off Contract;

5.1.2 complies with the requirements set out in paragraph 5.3 of this Call Off Schedule;

5.1.3 is otherwise reasonably satisfactory to the Customer.

5.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

5.3 Unless otherwise specified by the Customer or Approved, the Exit Plan shall set out, as a minimum:

5.3.1 how the Exit Information is obtained;

5.3.2 the management structure to be employed during both transfer and cessation of the Services;

5.3.3 the management structure to be employed during the Termination Assistance Period;

5.3.4 a detailed description of both the transfer and cessation processes, including a timetable;

5.3.5 how the service provision will transfer to the Replacement Supplier and/or the Customer, including details of the processes, documentation, data transfer, systems migration, security and the segregation of the Customer's technology components from any technology components operated by the Supplier or its Sub-Contractors (where applicable);

5.3.6 details of contracts (if any) which will be available for transfer to the Customer and/or the Replacement Supplier upon the Call Off Expiry Date together with any reasonable costs required to effect such transfer (and the Supplier agrees that all Transferable Assets and Transferable Contracts will be available for such transfer);

5.3.7 proposals for the training of key members of the Replacement Supplier's personnel in connection with the continuation of the provision of the Replacement Services following the Call Off Expiry Date charged at rates agreed between the Parties at that time;

5.3.8 proposals for the process of handing over to the Customer or a Replacement Supplier copies of all documentation:

(a) used in the provision of the Services and necessarily required for the continued use thereof, in which the Intellectual Property Rights are owned by the Supplier; and

(b) relating to the use and operation of the Services;

5.3.9 proposals for the assignment or novation of the provision of all services, leases, maintenance agreements and support agreements utilised by the Supplier in connection with the performance of the supply of the Services;

5.3.10 proposals for the identification and return of all Customer Property in the possession of and/or control of the Supplier or any third party (including any Sub-Contractor);

5.3.11 proposals for the disposal of any redundant Services and materials;

5.3.12 how each of the issues set out in this Call Off Schedule will be addressed to facilitate the transition of the service provision from the Supplier to the Replacement Supplier and/or the Customer with the aim of ensuring that there is no disruption to or degradation of the provision of service to the Customer during the Termination Assistance Period; and

5.3.13 proposals for the supply of any other information or assistance reasonably required by the Customer or a Replacement Supplier in order to effect an orderly handover of the provision of the Services.

6. TERMINATION ASSISTANCE

6.1 The Customer shall be entitled to require the provision of Termination Assistance at any time during the Call Off Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least six (6) months prior to the Call Off Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

6.1.1 the date from which Termination Assistance is required;

6.1.2 the nature of the Termination Assistance required; and

6.1.3 the period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) months after the date that the Supplier ceases to provide the Services.

6.2 The Customer shall have an option to extend the Termination Assistance Period beyond the period specified in the Termination Assistance Notice provided that such extension shall not extend for more than six (6) months after the date the Supplier ceases to provide the Services or, if applicable, beyond

the end of the Termination Assistance Period and provided that it shall notify the Supplier to such effect no later than twenty (20) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Customer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier to such effect.

7. TERMINATION ASSISTANCE PERIOD

7.1 Throughout the Termination Assistance Period, or such shorter period as the Customer may require, the Supplier shall:

7.1.1 continue to provide the Services (as applicable) and, if required by the Customer pursuant to paragraph 6.1 of this Call Off Schedule, provide the Termination Assistance;

7.1.2 in addition to providing the Services and the Termination Assistance, provide to the Customer any reasonable assistance requested by the Customer to allow the Services to continue without interruption following the termination or expiry of this Call Off Contract and to facilitate the orderly transfer of responsibility for and conduct of the Services to the Customer and/or its Replacement Supplier;

7.1.3 use all reasonable endeavours to reallocate resources to provide such assistance as is referred to in paragraph 7.1.2 of this Call Off Schedule without additional costs to the Customer;

7.1.4 provide the Services and the Termination Assistance at no detriment to the Service Level Thresholds, save to the extent that the Parties agree otherwise in accordance with paragraph 7.3; and

7.1.5 at the Customer's request and on reasonable notice, deliver up-to-date Registers to the Customer.

7.2 Without prejudice to the Supplier's obligations under paragraph 7.1.3 of this Call Off Schedule, if it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in paragraph 7.1.2 of this Call Off Schedule without additional costs to the Customer, any additional costs incurred by the Supplier in providing such reasonable assistance which is not already in the scope of the Termination Assistance or the Exit Plan shall be subject to the Change Control Procedure.

7.3 If the Supplier demonstrates to the Customer's reasonable satisfaction that transition of the Services and provision of the Termination Assist during the Termination Assistance Period will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Level Threshold(s), the Parties shall vary the relevant Service Level Threshold(s) and/or the applicable Service Credits to take account of such adverse effect.

8. TERMINATION OBLIGATIONS

8.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

8.2 Upon termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Services and the Termination Assistance and its compliance with the other provisions of this Call Off Schedule), the Supplier shall:

8.2.1 cease to use the Customer Data;

8.2.2 provide the Customer and/or the Replacement Supplier with a complete and uncorrupted version of the Customer Data in electronic form (or such other format as reasonably required by the Customer);

8.2.3 erase from any computers, storage devices and storage media that are to be retained by the Supplier after the end of the Termination Assistance Period all Customer Data and promptly certify to the Customer that it has completed such deletion;

8.2.4 return to the Customer such of the following as is in the Supplier's possession or control:

(a) all copies of the Customer Software and any other software licensed by the Customer to the Supplier under this Call Off Contract;

(b) all materials created by the Supplier under this Call Off Contract in which the IPRs are owned by the Customer;

(c) any parts of the IT Environment and any other equipment which belongs to the Customer;

(d) any items that have been on-charged to the Customer, such as consumables; and

(e) all Customer Property issued to the Supplier under Clause 28 of this Call Off Contract (Customer Property). Such Customer Property shall be handed back to the Customer in good working order (allowance shall be made only for reasonable wear and tear);

(f) any sums prepaid by the Customer in respect of Services not Delivered by the Call Off Expiry Date;

8.2.5 vacate any Customer Premises;

8.2.6 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Services and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier and/or any Supplier Personnel;

8.2.7 provide access during normal working hours to the Customer and/or the Replacement Supplier for up to twelve (12) months after expiry or termination to:

(a) such information relating to the Services as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Personnel as have been involved in the design, development and provision of the Services and who are still employed by the Supplier, provided that the Customer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to requests for access under this paragraph.

8.3 Upon termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the

Supplier's performance of the Services and the Termination Assistance and its compliance with the other provisions of this Call Off Schedule), each Party shall return to the other Party (or if requested, destroy or delete) all Confidential Information of the other Party and shall certify that it does not retain the other Party's Confidential Information save to the extent (and for the limited period) that such information needs to be retained by the Party in question for the purposes of providing or receiving any Services or Termination Services or for statutory compliance purposes.

8.4 Except where this Call Off Contract provides otherwise, all licences, leases and authorisations granted by the Customer to the Supplier in relation to the Services shall be terminated with effect from the end of the Termination Assistance Period.

9. ASSETS, SUB-CONTRACTS AND SOFTWARE

9.1 Following notice of termination of this Call Off Contract and during the Termination Assistance Period, the Supplier shall not, without the Customer's prior written consent:

9.1.1 terminate, enter into or vary any Sub-Contract;

9.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets; or

9.1.3 terminate, enter into or vary any licence for software in connection with the provision of Services.

9.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier pursuant to paragraph 7.1.5 of this Call Off Schedule, the Customer shall provide written notice to the Supplier setting out:

9.2.1 which, if any, of the Transferable Assets the Customer requires to be transferred to the Customer and/or the Replacement Supplier ("**Transferring Assets**");

9.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets,

the Customer and/or the Replacement Supplier requires the continued use of; and

9.2.3 which, if any, of Transferable Contracts the Customer requires to be assigned or novated to the Customer and/or the Replacement Supplier (the **"Transferring Contracts"**) in order for the Customer and/or its Replacement Supplier to provide the Replacement Services from the expiry of the Termination Assistance Period. Where requested by the Customer and/or its Replacement Supplier, the Supplier shall provide all reasonable assistance to the Customer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts the Customer and/or its Replacement Supplier requires to provide the Services or the Replacement Services.

9.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Customer and/or its nominated Replacement Supplier for a consideration equal to their Net Book Value, except where the cost of the Transferring Asset has been partially or fully paid for through the Call Off Contract Charges at the Call Off expiry Date, in which case the Customer shall pay the Supplier the Net Book Value of the Transferring Asset less the amount already paid through the Call Off Contract Charges.

9.4 Risk in the Transferring Assets shall pass to the Customer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title to the Transferring Assets shall pass to the Customer or the Replacement Supplier (as appropriate) on payment for the same.

9.5 Where the Supplier is notified in accordance with paragraph 9.2.2 of this Call Off Schedule that the Customer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

9.5.1 procure a non-exclusive, perpetual, royalty-free licence (or licence on such other terms that have been agreed by the Customer) for the Customer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

9.5.2 procure a suitable alternative to such assets and the Customer or the Replacement Supplier shall bear the reasonable proven costs of procuring the same.

9.6 The Supplier shall as soon as reasonably practicable assign or procure the novation to the Customer and/or the Replacement Supplier of the Transferring Contracts. The Supplier shall execute such documents and provide such other assistance as the Customer reasonably requires to effect this novation or assignment.

9.7 The Customer shall:

9.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

9.7.2 once a Transferring Contract is novated or assigned to the Customer and/or the Replacement Supplier, carry out, perform and discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

9.8 The Supplier shall hold any Transferring Contracts on trust for the Customer until such time as the transfer of the relevant Transferring Contract to the Customer and/or the Replacement Supplier has been effected.

9.9 The Supplier shall indemnify the Customer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Customer (and/or Replacement Supplier) pursuant to paragraph 9.6 of this Call Off Schedule in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract.

10. SUPPLIER PERSONNEL

10.1 [NOT USED]

10.2 The Supplier shall not take any step (expressly or implicitly and directly or indirectly by itself or through any other person) to dissuade or discourage any employees engaged in the provision of the Services from transferring their employment to the Customer and/or the Replacement Supplier.

10.3 During the Termination Assistance Period, the Supplier shall give the Customer and/or the Replacement Supplier reasonable access to the Supplier's personnel to present the case for transferring their employment to the Customer and/or the Replacement Supplier.

10.4 The Supplier shall immediately notify the Customer or, at the direction of the Customer, the Replacement Supplier of any period of notice given by the Supplier or received from any person referred to in the Staffing Information, regardless of when such notice takes effect.

10.5 The Supplier shall not for a period of twelve (12) months from the date of transfer re-employ or re-engage or entice any employees, Suppliers or Sub-Contractors whose employment or engagement is transferred to the Customer and/or the Replacement Supplier.

11. CHARGES

11.1 Except as otherwise expressly specified in this Call Off Contract, the Supplier shall not make any charges for the Services provided by the Supplier pursuant to, and the Customer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with, this Call Off Schedule including the preparation and implementation of the Exit Plan, the Termination Assistance and any activities mutually agreed between the Parties to carry on after the expiry of the Termination Assistance Period.

12. APPORTIONMENTS

12.1 All outgoings and expenses (including any remuneration due) and all rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Customer and the Supplier and/or the Replacement Supplier and the Supplier (as applicable) as follows:

12.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

12.1.2 the Customer shall be responsible for (or shall procure that the Replacement Supplier shall be responsible for) or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

12.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

12.2 Each Party shall pay (and/or the Customer shall procure that the Replacement Supplier shall pay) any monies due under paragraph 12.1 of this Call Off Schedule as soon as reasonably practicable.

CALL OFF SCHEDULE 10: AGENCY AGREEMENT

CALL OFF SCHEDULE 11: DISPUTE RESOLUTION PROCEDURE

1. DEFINITIONS

1.1 In this Call Off Schedule 11, the following definitions shall apply:

"CEDR"	the Centre for Effective Dispute Resolution of International Dispute Resolution Centre, 70 Fleet Street, London, EC4Y 1EU;
"Counter Notice"	has the meaning given to it in paragraph 6.2 of this Call Off Schedule;
"Exception"	a deviation of project tolerances in accordance with PRINCE2 methodology in respect of this Call Off Contract or in the supply of the Services;
"Expert"	the person appointed by the Parties in accordance with paragraph 5.2 of this Call Off Schedule 13; and
"Mediation Notice"	has the meaning given to it in paragraph 3.2 of this Call Off Schedule;
"Mediator"	the independent third party appointed in accordance with paragraph 4.2 of this Call Off Schedule 13.

2. INTRODUCTION

2.1 If a Dispute arises then:

2.1.1 the representative of the Customer and the Supplier Representative shall attempt in good faith to resolve the Dispute; and

2.1.2 if such attempts are not successful within a reasonable time either Party may give to the other a Dispute Notice.

2.2 The Dispute Notice shall set out:

2.2.1 the material particulars of the Dispute;

2.2.2 the reasons why the Party serving the Dispute Notice believes that the Dispute has arisen; and

2.2.3 if the Party serving the Dispute Notice believes that the Dispute should be dealt with under the Expedited Dispute Timetable as set out in paragraph 2.6 of this Call Off Schedule, the reason why.

2.3 Unless agreed otherwise in writing, the Parties shall continue to comply with their respective obligations under this Call Off Contract regardless of the nature of the Dispute and notwithstanding the referral of the Dispute to the Dispute Resolution Procedure.

2.4 Subject to paragraph 3.2 of this Call Off Schedule, the Parties shall seek to resolve Disputes:

2.4.1 first by commercial negotiation (as prescribed in paragraph 3 of this Call Off Schedule);

2.4.2 then by mediation (as prescribed in paragraph 4 of this Call Off Schedule); and

2.4.3 lastly by recourse to arbitration (as prescribed in paragraph 6 of this Call Off Schedule) or litigation (in accordance with Clause 55 of this Call Off Contract (Governing Law and Jurisdiction)).

2.5 Specific issues shall be referred to Expert Determination (as prescribed in paragraph 5 of this Call Off Schedule) where specified under the provisions of this Call Off Contract and may also be referred to Expert Determination where otherwise appropriate as specified in paragraph 5 of this Call Off Schedule.

2.6 In exceptional circumstances where the use of the times in this Call Off Schedule would be unreasonable, including (by way of example) where one Party would be materially disadvantaged by a delay in resolving the Dispute, the Parties may agree to use the Expedited Dispute Timetable. If the Parties are unable to reach agreement on whether to use of the Expedited Dispute Timetable within five (5) Working Days of the issue of the Dispute Notice, the use of the Expedited Dispute Timetable shall be at the sole discretion of the Customer.

2.7 If the use of the Expedited Dispute Timetable is determined in accordance with paragraph 2.5 or is otherwise specified under the provisions of this Call Off Contract, then the following periods of time shall apply in lieu of the time periods specified in the applicable paragraphs:

2.7.1 in paragraph 3.2.3, ten (10) Working Days;

2.7.2 in paragraph 4.2, ten (10) Working Days;

2.7.3 in paragraph 5.2, five (5) Working Days; and

2.7.4 in paragraph 6.2, ten (10) Working Days.

2.8 If at any point it becomes clear that an applicable deadline cannot be met or has passed, the Parties may (but shall be under no obligation to) agree in writing to extend the deadline. Any agreed extension shall have the effect of delaying the start of the subsequent stages by the period agreed in the extension.

3. COMMERCIAL NEGOTIATIONS

3.1 Following the service of a Dispute Notice, the Customer and the Supplier shall use reasonable endeavours to resolve the Dispute as soon as possible, by discussion between the Customer's Representative and the Supplier's Commercial Manager.

3.2 If:

3.2.1 either Party is of the reasonable opinion that the resolution of a Dispute by commercial negotiation, or the continuance of commercial negotiations, will not result in an appropriate solution;

3.2.2 the Parties have already held discussions of a nature and intent (or otherwise were conducted in the spirit) that would equate to the conduct of commercial negotiations in accordance with this paragraph 3 of this Call Off Schedule; or

3.2.3 the Parties have not settled the Dispute in accordance with paragraph 3.1 of this Call Off Schedule within thirty (30) Working Days of service of the Dispute Notice,

either Party may serve a written notice to proceed to mediation (a "**Mediation Notice**") in accordance with paragraph 4 of this Call Off Schedule.

4. MEDIATION

4.1 If a Mediation Notice is served, the Parties shall attempt to resolve the dispute in accordance with CEDR's Model Mediation Agreement which shall be deemed to be incorporated by reference into this Call Off Contract.

4.2 If the Parties are unable to agree on the joint appointment of a Mediator within thirty (30) Working Days from service of the Mediation Notice then either Party may apply to CEDR to nominate the Mediator.

4.3 If the Parties are unable to reach a settlement in the negotiations at the mediation, and only if the Parties so request and the Mediator agrees, the Mediator shall produce for the Parties a non-binding recommendation on terms of settlement. This shall not attempt to anticipate what a court might order but shall set out what the Mediator suggests are appropriate settlement terms in all of the circumstances.

4.4 Any settlement reached in the mediation shall not be legally binding until it has been reduced to writing and signed by, or on behalf of, the Parties (in accordance with the Variation Procedure where appropriate). The Mediator shall assist the Parties in recording the outcome of the mediation.

5. EXPERT DETERMINATION

5.1 If a Dispute relates to any aspect of the technology underlying the provision of the Services or otherwise relates to an ICT technical, financial technical or other aspect of a technical nature (as the Parties may agree) and the Dispute has not been resolved by discussion or mediation, then either Party may request (which request will not be unreasonably withheld or delayed) by written notice to the other that the Dispute is referred to an Expert for determination.

5.2 The Expert shall be appointed by agreement in writing between the Parties, but in the event of a failure to agree within ten (10) Working Days, or if the person appointed is unable or unwilling to act, the Expert shall be appointed on the instructions of the President of the British Computer Society (or any other association that has replaced the British Computer Society).

5.3 The Expert shall act on the following basis:

5.3.1 he/she shall act as an expert and not as an arbitrator and shall act fairly and impartially;

5.3.2 the Expert's determination shall (in the absence of a material failure to follow the agreed procedures) be final and binding on the Parties;

5.3.3 the Expert shall decide the procedure to be followed in the determination and shall be requested to make his/her determination within thirty (30) Working Days of his appointment or as soon as reasonably practicable thereafter and the Parties shall assist and provide the documentation that the Expert requires for the purpose of the determination;

5.3.4 any amount payable by one Party to another as a result of the Expert's determination shall be due and payable within twenty (20) Working Days of the Expert's determination being notified to the Parties;

5.3.5 the process shall be conducted in private and shall be confidential; and

5.3.6 the Expert shall determine how and by whom the costs of the determination, including his/her fees and expenses, are to be paid.

6. ARBITRATION

6.1 The Customer may at any time before court proceedings are commenced refer the Dispute to arbitration in accordance with the provisions of paragraph 6.4 of this Call Off Schedule.

6.2 Before the Supplier commences court proceedings or arbitration, it shall serve written notice on the Customer of its intentions and the Customer shall have fifteen (15) Working Days following receipt of such notice to serve a reply (a "**Counter Notice**") on the Supplier requiring the Dispute to be referred to and resolved by arbitration in accordance with paragraph 6.4 of this Call Off Schedule or be subject to the jurisdiction of the courts in accordance with Clause 55 of this Call Off Contract (Governing Law and Jurisdiction). The Supplier shall not commence any court proceedings or arbitration until the expiry of such fifteen (15) Working Day period.

6.3 If:

6.3.1 the Counter Notice requires the Dispute to be referred to arbitration, the provisions of paragraph 6.4 of this Call Off Schedule shall apply;

6.3.2 the Counter Notice requires the Dispute to be subject to the exclusive jurisdiction of the courts in accordance with Clause 61 of this Call Off Contract (Governing Law and Jurisdiction), the Dispute shall be so referred to the courts and the Supplier shall not commence arbitration proceedings;

6.3.3 the Customer does not serve a Counter Notice within the fifteen (15) Working Days period referred to in paragraph 6.2 of this Call Off Schedule, the Supplier may either commence arbitration proceedings in accordance with paragraph 6.4 of this Call Off Schedule or commence court proceedings in the courts in accordance with Clause 55 of this Call Off Contract (Governing Law and Jurisdiction) which shall (in those circumstances) have exclusive jurisdiction.

6.4 In the event that any arbitration proceedings are commenced pursuant to paragraphs 6.1 to 6.3 of this Call Off Schedule, the Parties hereby confirm that:

6.4.1 all disputes, issues or claims arising out of or in connection with this Call Off Contract (including as to its existence, validity or performance) shall be referred to and finally resolved by arbitration under the Rules of the London Court of International Arbitration ("**LCIA**") (subject to paragraphs 6.4.5 to 6.4.7 of this Call Off Schedule);

6.4.2 the arbitration shall be administered by the LCIA;

6.4.3 the LCIA procedural rules in force at the date that the Dispute was referred to arbitration shall be applied and are deemed to be incorporated by reference into this Call Off Contract and the decision of the arbitrator shall be binding on the Parties in the absence of any material failure to comply with such rules;

6.4.4 if the Parties fail to agree the appointment of the arbitrator within ten (10) days from the date on which arbitration proceedings are

commenced or if the person appointed is unable or unwilling to act, the arbitrator shall be appointed by the LCIA;

6.4.5 the chair of the arbitral tribunal shall be British;

6.4.6 the arbitration proceedings shall take place in London and in the English language; and

6.4.7 the seat of the arbitration shall be London.

7. URGENT RELIEF

7.1 Either Party may at any time take proceedings or seek remedies before any court or tribunal of competent jurisdiction:

7.1.1 for interim or interlocutory remedies in relation to this Call Off Contract or infringement by the other Party of that Party's Intellectual Property Rights; and/or

7.1.2 where compliance with paragraph 2.1 of this Call Off Schedule and/or referring the Dispute to mediation may leave insufficient time for that Party to commence proceedings before the expiry of the limitation period.

CALL OFF SCHEDULE 12: VARIATION FORM

No of Order Form being varied:

.....

Variation Form No:

.....

BETWEEN:

[insert name of Customer] ("**the Customer**")

and

[insert name of Supplier] ("**the Supplier**")

1. This Call Off Contract is varied as follows and shall take effect on the date signed by both Parties:

[Guidance Note: Insert details of the Variation]

2. Words and expressions in this Variation shall have the meanings given to them in this Call Off Contract.

3. This Call Off Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Customer

Signature

Date

Name (in Capitals)

Address

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature

Date

Name (in Capitals)

Address

CALL OFF SCHEDULE 13: ALTERNATIVE AND/OR ADDITIONAL CLAUSES

1. INTRODUCTION

1.1 This Call Off Schedule 12 specifies the range of Alternative Clauses and Additional Clauses that may be requested in the Order Form and, if requested in the Order Form, shall apply to this Call Off Contract.

2. CLAUSES SELECTED

2.1 The Customer may, in the Order Form, request the following Alternative Clauses:

2.1.1 Scots Law (see paragraph 4.1 of this Call Off Schedule);

2.1.2 Northern Ireland Law (see paragraph 4.2 of this Call Off Schedule)

2.1.3 Non-Crown Bodies (see paragraph 4.3 of this Call Off Schedule); or

2.1.4 Non-FOIA Public Bodies (see paragraph 4.4 of this Call Off Schedule).

2.2 The Customer may, in the Order Form, request the following Additional Clauses should apply:

2.2.1 Security Measures (see paragraph 5 of this Call Off Schedule);

2.2.2 Access to MoD Sites (see paragraph 6 of this Call Off Schedule);

3. IMPLEMENTATION

3.1 The appropriate changes have been made in this Call Off Contract to implement the Alternative Clauses specified in paragraph 2.1 of this Call Off Schedule and the Additional Clauses specified in paragraphs 2.2 of this Call Off Schedule shall be deemed to be incorporated into this Call Off Contract.

4. ALTERNATIVE CLAUSES

4.1 SCOTS LAW

Law and Jurisdiction (Clause 55)

References to "England and Wales" in the original Clause 55 of this Call Off Contract (Law and Jurisdiction) shall be replaced with "Scotland".

4.2 NORTHERN IRELAND LAW

Law and Jurisdiction (Clause 55)

References to "England and Wales" in the original Clause 55 of this Call Off Contract (Law and Jurisdiction) shall be replaced with "Northern Ireland".

Insolvency Event

In Call Off Schedule 1 (Definitions), reference to "section 123 of the Insolvency Act 1986" in limb f) of the definition of Insolvency Event shall be replaced with "Article 103 of the Insolvency (NI) Order 1989".

4.3 NON-CROWN BODIES

Clause 43.3.1(a) of this Call Off Contract (Official Secrets Act and Finance Act) shall be deleted.

4.4 NON-FOIA PUBLIC BODIES

Replace Clause 31.6 of this Call Off Contract (Freedom of Information) with "The Customer has notified the Supplier that the Customer is exempt from the provisions of FOIA and EIR."

5. ADDITIONAL CLAUSE: SECURITY MEASURES

5.1 The following definitions to be added to Call Off Schedule 1 (Definitions) to the Call Off Form and the Call Off Terms:

"Document" includes specifications, plans, drawings, photographs and books;

"Secret Matter" means any matter connected with or arising out of the performance of this Call Off Contract which has been, or may hereafter be, by a notice in writing given by the Customer to the Supplier be designated 'top secret', 'secret', or 'confidential';

"Servant" where the Supplier is a body corporate shall include a director of that body and any person occupying in relation to that body the position of director by whatever name called.

5.2 The following new Clause [58] shall apply:

[Guidance Note: the intention is for this clause to follow immediately after the final clause in the T&Cs]

58. SECURITY MEASURES

58.1. The Supplier shall not, either before or after the completion or termination of this Call Off Contract, do or permit to be done anything which it knows or ought reasonably to know may result in information about a secret matter being:

58.1.1. without the prior consent in writing of the Customer, disclosed to or acquired by a person who is an alien or who is a British subject by virtue only of a certificate of naturalisation in which his name was included;

58.1.2. disclosed to or acquired by a person as respects whom the Customer has given to the Supplier a notice in writing which has not been cancelled stating that the Customer requires that secret matters shall not be disclosed to that person;

58.1.3. without the prior consent in writing of the Customer, disclosed to or acquired by any person who is not a servant of the Supplier; or

58.1.4. disclosed to or acquired by a person who is an employee of the Supplier except in a case where it is necessary for the proper performance of this Call Off Contract that such person shall have the information.

58.2. Without prejudice to the provisions of Clause 58.1, the Supplier shall, both before and after the completion or termination of this Call Off Contract, take all reasonable steps to ensure:

58.2.1. no such person as is mentioned in Clauses 58.1, 58.1.1 or 58.1.2 hereof shall have access to any item or document under the control of the Supplier containing information about a secret matter except with the prior consent in writing of the Customer;

58.2.2. that no visitor to any premises in which there is any item to be supplied under this Call Off Contract or where Services are being supplied shall see or discuss with the Supplier or any person employed by him any secret matter unless the visitor is authorised in writing by the Customer so to do;

58.2.3. that no photograph of any item to be supplied under this Call Off Contract or any portions of the Services shall be taken except insofar as may be necessary for the proper performance of this Call Off Contract or with the prior consent in writing of the Customer, and that no such photograph shall, without such consent, be published or otherwise circulated;

58.2.4. that all information about any secret matter and every document model or other item which contains or may reveal any such information is at all times strictly safeguarded, and that, except insofar as may be necessary for the proper performance of this Call Off Contract or with the prior consent in writing of the Customer, no copies of or extracts from any such document, model or item shall be made or used and no designation of description which may reveal information about the nature or contents of any such document, model or item shall be placed thereon; and

58.2.5. that if the Customer gives notice in writing to the Supplier at any time requiring the delivery to the Customer of any such document, model or item as is mentioned in Clause 58.2.3, that document, model or item (including all copies of or extracts therefrom) shall forthwith be delivered to the Customer who shall be deemed to be the owner thereof and accordingly entitled to retain the same.

58.3. The decision of the Customer on the question whether the Supplier has taken or is taking all reasonable steps as required by the foregoing provisions of this Clause 58 shall be final and conclusive.

58.4. If and when directed by the Customer, the Supplier shall furnish full particulars of all people who are at any time concerned with any secret matter.

58.5. If and when directed by the Customer, the Supplier shall secure that any person employed by it who is specified in the direction, or is one of a class of people who may be so specified, shall sign a statement that he understands that the Official Secrets Act, 1911 to 1989 and, where applicable, the Atomic Energy Act 1946, apply to the person signing the statement both during the carrying out and after expiry or termination of a Call Off Contract.

58.6. If, at any time either before or after the expiry or termination of this Call Off Contract, it comes to the notice of the Supplier that any person acting without lawful authority is seeking or has sought to obtain information concerning this Call Off Contract or anything done or to be done in pursuance thereof, the matter shall be forthwith reported by the Supplier to the Customer and the report shall, in each case, be accompanied by a statement of the facts, including, if possible, the name, address and occupation of that person, and the Supplier shall be responsible for making all such arrangements as it may consider appropriate to ensure that if any such occurrence comes to the knowledge of any person employed by it, that person shall forthwith report the matter to the Supplier with a statement of the facts as aforesaid.

58.7. The Supplier shall place every person employed by it, other than a Sub-Contractor, who in its opinion has or will have such knowledge of any secret matter as to appreciate its significance, under a duty to the Supplier to observe the same obligations in relation to that matter as are imposed on the Supplier by Clauses 58.1and 58.2 and shall, if directed by the Customer, place every person who is specified in the direction or is one of a class of people so specified, under the like duty in relation to any secret matter which may be specified in the direction, and shall at all times use its best endeavours to ensure that every person upon whom obligations are imposed by virtue of this Clause 58 observes the said obligations, and the Supplier shall give such instructions and information to every such person as may be necessary for that purpose, and shall, immediately upon becoming aware of any act or omission which is or would be a breach of the said obligations, report the facts to the Supplier with all necessary particulars.

58.8. The Supplier shall, if directed by the Customer, include in the Sub-Contract provisions in such terms as the Customer may consider appropriate for placing the Sub-Contractor under obligations in relation to secrecy and security corresponding to those placed on the Supplier by this Clause 58, but with such variations (if any) as the Customer may consider necessary. Further the Supplier shall:

58.8.1. give such notices, directions, requirements and decisions to its Sub-Contractors as may be necessary to bring the provisions relating to secrecy and security which are included in Sub-Contracts under this Clause58 into operation in such cases and to such extent as the Customer may direct;

58.8.2. if there comes to its notice any breach by the Sub-Contractor of the obligations of secrecy and security included in their Sub-Contracts in pursuance of this Clause 58, notify such breach forthwith to the Customer; and

58.8.3. if and when so required by the Customer, exercise its power to determine the Sub-Contract under the provision in that Sub-Contract which corresponds to Clause 58.11.

58.9. The Supplier shall give the Customer such information and particulars as the Customer may from time to time require for the purposes of satisfying the Customer that the obligations imposed by or under the foregoing provisions of this Clause 58 have been and are being observed and as to what the Supplier has done or is doing or proposes to do to secure the observance of those obligations and to prevent any breach thereof, and the Supplier shall secure that a representative of the Customer duly authorised in writing shall be entitled at reasonable times to enter and inspect any premises in which anything is being done or is to be done under this Call Off Contract or in which there is or will be any item to be supplied under this Call Off Contract, and also to inspect any document or item in any such premises or which is being made or used for the purposes of this Call Off Contract and that any such representative shall be given all such information as he may require on the occasion of, or arising out of, any such inspection.

58.10. Nothing in this Clause 58 shall prevent any person from giving any information or doing anything on any occasion when it is, by virtue of any enactment, the duty of that person to give that information or do that thing.

58.11. If the Customer shall consider that any of the following events has occurred:

58.11.1. that the Supplier has committed a breach of, or failed to comply with any of, the foregoing provisions of this Clause 58; or

58.11.2. that the Supplier has committed a breach of any obligations in relation to secrecy or security imposed upon it by any other contract with the Customer, or with any department or person acting on behalf of the Crown; or

58.11.3. that by reason of an act or omission on the part of the Supplier, or of a person employed by the Supplier, which does not constitute such a breach or failure as is mentioned in 58.11.2, information about a secret matter has been or is likely to be acquired by a person who, in the opinion of the Customer, ought not to have such information;

and shall also decide that the interests of the State require the termination of this Call Off Contract, the Customer may by notice in writing terminate this Call Off Contract forthwith.

58.12. A decision of the Customer to terminate this Call Off Contract in accordance with the provisions of Clause 58.11 shall be final and conclusive and it shall not be necessary for any notice of such termination to specify or refer in any way to the event or considerations upon which the Customer's decision is based.

58.13. Supplier's notice

58.13.1. The Supplier may within five (5) Working Days of the termination of this Call Off Contract in accordance with the provisions of Clause 58.11, give the Customer notice in writing requesting the Customer to state whether the event upon which the Customer's decision to terminate was based is an event mentioned in Clauses 58.11, 58.11.1 or 58.11.2 and to give particulars of that event; and

58.13.2. the Customer shall within ten (10) Working Days of the receipt of such a request give notice in writing to the Supplier containing such a statement and particulars as are required by the request.

58.14. Matters pursuant to termination

58.14.1. The termination of this Call Off Contract pursuant to Clause 58.11 shall be without prejudice to any rights of either party which shall have accrued before the date of such termination;

58.14.2. The Supplier shall be entitled to be paid for any work or thing done under this Call Off Contract and accepted but not paid for by the Customer at the date of such termination either at the price which would have been payable under this Call Off Contract if this Call Off Contract had not been terminated, or at a reasonable price;

58.14.3. The Customer may take over any work or thing done or made under this Call Off Contract (whether completed or not) and not accepted at the date of such termination which the Customer may by notice in writing to the Supplier given within thirty (30) Working Days from the time when the provisions of this Clause 58 shall have effect, elect to take over, and the Supplier shall be entitled to be paid for any work or thing so taken over a price which, having regard to the stage which that work or thing has reached and its condition at the time it is taken over, is reasonable. The Supplier shall in accordance with directions given by the Customer, deliver any work or thing taken over under this Clause, and take all such other steps as may be reasonably necessary to enable the Customer to have the full benefit of any work or thing taken over under this Clause; and

58.14.4. Save as aforesaid, the Supplier shall not be entitled to any payment from the Customer after the termination of this Call Off Contract

58.15. If, after notice of termination of this Call Off Contract pursuant to the provisions of 58.11:

58.15.1. the Customer shall not within ten (10) Working Days of the receipt of a request from the Supplier, furnish such a statement and particulars as are detailed in Clause 58.13.1; or

58.15.2. the Customer shall state in the statement and particulars detailed in Clause 58.13.2. that the event upon which the Customer's decision to terminate this Call Off Contract was based is an event mentioned in Clause 58.11.3,

the respective rights and obligations of the Supplier and the Customer shall be terminated in accordance with the following provisions:

58.15.3. the Customer shall take over from the Supplier at a fair and reasonable price all unused and undamaged materials, bought-out parts and components and articles in course of manufacture in the possession of the Supplier upon the termination of this Call Off Contract under the provisions of Clause 58.11 and properly provided by or supplied to the Supplier for the performance of this Call Off Contract, except such materials, bought-out parts and components and articles in course of manufacture as the Supplier shall, with the concurrence of the Customer, elect to retain;

58.15.4. the Supplier shall prepare and deliver to the Customer within an agreed period or in default of agreement within such period as the Customer may specify, a list of all such unused and undamaged materials, bought-out parts and components and articles in course of manufacture liable to be taken over by or previously belonging to the Customer and shall deliver such materials and items in accordance with the directions of the Customer who shall pay to the Supplier fair and reasonable handling and delivery charges incurred in complying with such directions;

58.15.5. the Customer shall indemnify the Supplier against any commitments, liabilities or expenditure which are reasonably and properly chargeable by the Supplier in connection with this Call Off Contract to the extent to which the said commitments, liabilities or expenditure would otherwise represent an unavoidable loss by the Supplier by reason of the termination of this Call Off Contract;

58.15.6. if hardship to the Supplier should arise from the operation of this Clause 58.15 it shall be open to the Supplier to refer the circumstances to the Customer who, on being satisfied that such hardship exists shall make such allowance, if any, as in its opinion is reasonable and the decision of the Customer on any matter arising out of this Clause shall be final and conclusive; and

subject to the operation of Clauses 58.15.3, 58.15.4, 58.15.5 and 58.15.6 termination of this Call Off Contract shall be without prejudice to any rights of either party that may have accrued before the date of such termination.

6. ACCESS TO MOD SITES

6.1 The definition of Call Off Contract in Call Off Schedule 1 (Definitions) to the Call Off Terms shall be replaced with the following:

6.1.1 **"Call Off Contract"** means this written agreement between the Customer and the Supplier consisting of the Order Form and the Call Off Terms and the MoD Terms and Conditions.

6.2 The following definitions shall be inserted into in Call Off Schedule 1 (Definitions) to the Call Off Terms:

6.2.1 **"MoD Terms and Conditions"** means the contractual terms and conditions listed in Schedule [...] which form part of the Call Off Terms ***[Guidance Note: read with the Guidance Note below]***

6.2.2 **"Site"** shall include any of Her Majesty's Ships or Vessels and Service Stations.

6.2.3 **"Officer in charge"** shall include Officers Commanding Service Stations, Ships' Masters or Senior Officers, and Officers superintending Government Establishments.

6.3 The following clauses shall be inserted into Clause 2 of this Call Off Contract (Due Diligence):

6.3.1 The Supplier confirms that it has had the opportunity to review the MoD Terms and Conditions and has raised all due diligence questions in relation to those documents with the Customer prior to the Commencement Date.

6.3.2 Where required by the Customer, the Supplier shall take such actions as are necessary to ensure that the MoD Terms and Conditions constitute legal, valid, binding and enforceable obligations on the Supplier.

6.4 The following new Clause [59] shall apply:

[Guidance Note: the intention is for this clause to follow after the final clause in the T&Cs and/or the Additional Clause "Security Measures"]

59. ACCESS TO MOD SITES

59.1. In this Clause 59:

59.1.1. The Customer shall issue passes for those representatives of the Supplier who are approved for admission to the Site and a representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Customer and shall be surrendered on demand or on completion of the supply of the Services.

59.1.2. The Supplier's representatives when employed within the boundaries of a Site, shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force for the time being for the conduct of personnel at that Site. When on board ship, compliance shall be with the Ship's Regulations as interpreted by the Officer in charge. Details

of such rules, regulations and requirements shall be provided, on request, by the Officer in charge.

59.1.3. The Supplier shall be responsible for the living accommodation and maintenance of its representatives while they are employed at a Site. Sleeping accommodation and messing facilities, if required, may be provided by the Customer wherever possible, at the discretion of the Officer in charge, at a cost fixed in accordance with current Ministry of Defence regulations. At Sites overseas, accommodation and messing facilities, if required, shall be provided wherever possible. The status to be accorded to the Supplier's personnel for messing purposes shall be at the discretion of the Officer in charge who shall, wherever possible give his decision before the commencement of this Call Off Contract where so asked by the Supplier. When sleeping accommodation and messing facilities are not available, a certificate to this effect may be required by the Customer and shall be obtained by the Supplier from the Officer in charge. Such certificate shall be presented to the Customer with other evidence relating to the costs of this Call Off Contract.

59.1.4. Where the Supplier's representatives are required by this Call Off Contract to join or visit a Site overseas, transport between the United Kingdom and the place of duty (but excluding transport within the United Kingdom) shall be provided for them free of charge by the Ministry of Defence whenever possible, normally by Royal Air Force or by MOD chartered aircraft. The Supplier shall make such arrangements through the Technical Branch named for this purpose in this Call Off Contract. When such transport is not available within a reasonable time, or in circumstances where the Supplier wishes its representatives to accompany material for installation which it is to arrange to be delivered, the Supplier shall make its own transport arrangements. The Customer shall reimburse the Supplier's reasonable costs for such transport of its representatives on presentation of evidence supporting the use of alternative transport and of the costs involved. Transport of the Supplier's representatives locally overseas which is necessary for the purpose of this Call Off Contract shall be provided wherever possible by the Ministry of Defence, or by the Officer in charge and, where so provided, shall be free of charge.

59.1.5. Out-patient medical treatment given to the Supplier's representatives by a Service Medical Officer or other Government Medical Officer at a Site overseas shall be free of charge. Treatment in a Service hospital or medical centre, dental treatment, the provision of dentures or spectacles, conveyance to and from a hospital, medical centre or surgery not within the Site and transportation of the Supplier's representatives back to the United Kingdom,

or elsewhere, for medical reasons, shall be charged to the Supplier at rates fixed in accordance with current Ministry of Defence regulations.

59.1.6. Accidents to the Supplier's representatives which ordinarily require to be reported in accordance with Health and Safety at Work etc Act 1974, shall be reported to the Officer in charge so that the Inspector of Factories may be informed.

59.1.7. No assistance from public funds, and no messing facilities, accommodation or transport overseas shall be provided for dependants or members of the families of the Supplier's representatives. Medical or necessary dental treatment may, however, be provided for dependants or members of families on repayment at current Ministry of Defence rates.

59.1.8. The Supplier shall, wherever possible, arrange for funds to be provided to its representatives overseas through normal banking channels (e.g. by travellers' cheques). If banking or other suitable facilities are not available, the Customer shall, upon request by the Supplier and subject to any limitation required by the Supplier, make arrangements for payments, converted at the prevailing rate of exchange (where applicable), to be made at the Site to which the Supplier's representatives are attached. All such advances made by the Customer shall be recovered from the Supplier.

6.5 Ministry of Defence (MoD) DEFCON 129J shall apply and will form part of this Call Off Contract.

6.6 The following new Call Off Schedule [15] shall apply:

CALL OFF SCHEDULE [15]: MOD DEFCONS AND DEFFORMS

The following MOD DEFCONs and DEFFORMs form part of this Call Off Contract:

DEFCONs

DEFCON No	Version	Description

DEFFORMs (Ministry of Defence Forms)

DEFFORM No	Version	Description

[Guidance Note: the above documents can be found at http://www.aof.mod.uk/]

[Guidance Note for the Ministry of Defence: Upon placing of an Order the Ministry of Defence shall select and refine the DEFCONs or DEFFORMs from the tables above, in accordance with the DEFCONs and DEFFORMs which are appropriate to the specific Call Off Contract, and set them out in Call Off Schedule [11].]

CALL OFF SCHEDULE 14: BENCHMARKING

1. DEFINITIONS

In this Call Off Schedule the following definitions shall apply:

"Benchmark Review"	a review of the Services carried out in accordance with Paragraph 6 of this Call Off Schedule to determine whether any or all of the Services represent Good Value;
"Benchmarked Services"	the Services that the Customer elects to include in a Benchmark Review under Paragraph 3.1 of this Call Off Schedule, and where a sub-set of Services is selected, such Services shall be related;
"Benchmarker"	the independent third party appointed under Paragraph 5.1 of this Call Off Schedule;
"Benchmarking Report"	the report produced by the Benchmarker following the Benchmark Review as further described in Paragraph 7 of this Call Off Schedule;
"Benchmark Review"	a review of the Services carried out in accordance with Paragraph 6 of this Call Off Schedule to determine whether any or all of the Services represent Good Value;
"Good Value"	that: (a) the Charges attributable to a Benchmarked Service are, having taken into account the Service Level Thresholds less than or equal to the Average Price or within the Upper Quartile (as specified in the Order Form); and (b) any Service Levels Performance Measure attributable to Benchmarked Services are, having taken into account the Charges, equal to or greater than the median or mean average (as specified in the Order Form) service levels for Comparable Services as adjusted using Equivalent Services Data;
"Average Price"	in relation to the Comparable Services provided by the Comparison Group(s), the mean average of prices for those Comparable Services as adjusted to produce Equivalent Services Data over the previous twelve (12) month period or other period as agreed in writing between the Parties. The **"mean average price"** shall be calculated by aggregating the prices derived from Equivalent Services Data for each of the services and dividing the same by the number instances of Comparable Services;
"Comparable Services"	services that are identical or materially similar to the Benchmarked Services (including in terms of scope, specification, volume and quality of performance) provided that if no identical or materially similar services exist in the market, the Benchmarker shall propose an approach for developing a comparable service benchmark;

"Equivalent Services Data"	data (including price data) derived from an analysis of the Comparable Services provided by the Comparison Group(s) as adjusted in accordance with Paragraph 6.8.1 of this Call Off Schedule;
"Comparison Group(s)"	a sample group or groups of organisations providing Comparable Services identified by the Benchmarker under Paragraph 6.8 of this Call Off Schedule which consist(s) of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be (in the Benchmarker's professional opinion) fair comparators with the Supplier or which, in the professional opinion of the Benchmarker, are best practice organisations;
"Upper Quartile"	that based on an analysis of Equivalent Services Data, the Charges for the Benchmarked Services, as compared to the range of prices for Comparable Services, are within the top twenty five percent (25%) in terms of best value for money or the recipients of Comparable Services;

2. INTRODUCTION

2.1 The purpose of this Schedule is to enable the Customer to ensure that the provision of Services and payment of Charges continues to represent value for money for the Customer throughout the Term.

3. FREQUENCY OF BENCHMARK REVIEW

3.1 The Customer may, by written notice to the Supplier (with a copy being simultaneously sent to the Authority), require a Benchmark Review of any or all of the Services.

3.2 The Customer shall not be entitled to carry out a Benchmark Review during the twelve (12) month period from the Call Off Commencement Date nor at intervals of less than twelve (12) months after any previous Benchmark Review.

3.3 The Benchmarking Review may be undertaken by or on behalf of the Customer. If the Customer wishes the Authority to carry out a Benchmarking Review on its behalf, the Customer shall approach the Authority but the Authority shall not be obliged to carry out such Benchmarking Review. The costs and expenses of the Authority shall be borne by the Parties in accordance with Paragraph 5.3 below. The Authority shall have no liability for any costs or expenses of the Benchmarker and the Benchmark Review if it agrees to undertake the Benchmarking Review on behalf of the Customer.

4. PURPOSE AND SCOPE OF BENCHMARK REVIEW

4.1 The purpose of a Benchmark Review shall be to establish whether a Benchmarked Service is and/or the Benchmarked Services as a whole are, Good Value.

4.2 The Services that are to be the Benchmarked Services shall be identified by the Customer in the written request given under Paragraph 3.1 above.

5. APPOINTMENT OF BENCHMARKER

5.1 The Parties shall appoint the Benchmarker to carry out the Benchmark Review from the list of organisations set out in the Order Form. The terms under which the Benchmarker is engaged shall be:

5.1.1 consistent with the relevant provisions set out in this Schedule; and

5.1.2 determined and agreed solely by the Customer (unless otherwise advised by the Customer). The Customer may consult with the Supplier on the terms under which the Benchmarker is engaged but the Supplier agrees that such terms shall be determined and agreed solely by the Customer.

5.2 The Customer will, at the written request of the Supplier, require the Benchmarker to enter into an appropriate confidentiality undertaking with the Supplier provided that nothing shall prevent the Benchmarker from using anonymised data about the Services in future benchmarks for its other clients.

5.3 The costs and expenses of the Benchmarker and the Benchmark Review (including any costs and expenses incurred by the Authority pursuant to Paragraph 3.3 above) shall be shared equally between the Parties provided that each Party shall bear its own internal costs of the Benchmark Review.

5.4 In order to enable the Benchmarker to be in a position to effectively and efficiently conduct Benchmark Reviews, the Parties acknowledge that a newly appointed Benchmarker will need to be given a sufficient opportunity, prior to its initial Benchmark Review, to:

5.4.1 become familiar with the requirements of this Schedule and the information that will be required from the Parties to facilitate any Benchmark Review; and

5.4.2 determine that its methodology is not ineffective or inadequate to any material extent and make any changes that it deems appropriate.

5.5 Where the Authority carries out a Benchmark Review on behalf of the Customer, the Authority will require the Benchmarker to enter into an appropriate confidentiality undertaking with the Supplier, provided that nothing shall prevent the Benchmarker from using anonymised data about the Services in future benchmarks for its other clients.

6. BENCHMARKING PROCESS

6.1 The Customer shall require the Benchmarker to produce, and to send to each Party for approval, a draft plan for the Benchmark Review (a copy of the plan shall be provided to the Authority upon request) within eight (8) Working Days (or such other period as the Parties agree in writing) after the date of the appointment of the Benchmarker, or such longer period as the Benchmarker shall reasonably request in all the circumstances. The plan must include:

6.1.1 the scope, proposed timetable and description of Services for the Benchmark Review;

6.1.2 a description of the information that the Benchmarker requires each Party to provide;

6.1.3 a description of the benchmarking methodology to be used and the means by which Good Value will be established;

6.1.4 a description that demonstrates objectively and transparently that the benchmarking methodology to be used is capable of fulfilling the benchmarking objectives;

6.1.5 an estimate of the resources required from each Party to underpin the delivery of the plan;

6.1.6 a description of how the Benchmarker will scope and identify the Comparison Group(s) and the minimum number of samples required to establish each Comparison Group; and

6.1.7 details of any entities which the Benchmarker proposes to include within the Comparison Group(s) including a description of the methodology which the Benchmarker may use to normalise or otherwise adjust the results from the Comparison Group(s).

6.2 Each Party must give notice in writing to the Benchmarker and to the other Party within eight (8) Working Days (or such other period as the Parties agree in writing) after receiving the draft plan, advising whether it approves the draft plan or, if it does not approve the draft plan, suggesting amendments to that plan. Neither Party may unreasonably withhold or delay its approval of the draft plan nor suggest any amendments which are unreasonable.

6.3 Where a Party suggests amendments to the draft plan in accordance with Paragraph 6.2 above, the Benchmarker must, if it believes the amendments are reasonable, produce an amended draft plan. In making a determination as to whether or not to accept amendments put forward by either Party, the Benchmarker must act reasonably and in accordance with the terms under which it has been engaged by the Customer. Paragraph 6.2 above shall apply to any amended draft plan.

6.4 Failure by a Party to give notice under Paragraph 6.2 above shall be treated as approval of the draft plan by that Party.

6.5 Once the plan is approved by both Parties (a copy of the approved plan shall be provided to the Authority upon request), the Benchmarker shall carry out the Benchmark Review in accordance with the plan. Each Party shall procure that all the information described in the plan, together with any additional information reasonably required by the Benchmarker is provided to the Benchmarker without undue delay. If the Supplier fails to provide any material information requested from it by the Benchmarker and does not promptly remedy such failure once such omission has been identified such failure shall constitute a material Default for the purposes of Clause 38.2.1.

6.6 Each Party shall cooperate fully with the Benchmarker including by providing access to records, technical documentation, premises, equipment, systems and personnel at times reasonably requested by the Benchmarker, provided that the Benchmarker shall be instructed to minimise any disruption to the Benchmarked Services.

6.7 Either Party may provide additional material to the Benchmarker to assist the Benchmarker in conducting the Benchmark Review.

6.8 Once it has received the information it requires, the Benchmarker shall finalise a sample of entities constituting the Comparison Group(s) and collect data relating to Comparable Services. The selection of the Comparison Group(s) (both in terms of number and identity of entities) and Comparable Services shall be a matter for the Benchmarker's professional judgment by:

6.8.1 applying the adjustment factors listed in Paragraph 6.10 below and from an analysis of the Comparable Services derive the Equivalent Services Data;

6.8.2 using the Equivalent Services Data calculate (as set out in of the Order Form) the Average Price or the Upper Quartile and/or the mean or median Service Levels;

6.8.3 comparing the Charges attributable to the Benchmarked Services (having regard in particular to the Service Level Thresholds and Service Credits regime) with (as set out in the Order Form) the Average Price or Upper Quartile using the Equivalent Services Data;

6.8.4 comparing the Service Level Thresholds attributable to the Benchmarked Services (having regard to the Charges and Service Credits) with (as set out in the Order Form) the median or mean average service levels using the Equivalent Services Data; and

6.8.5 determining whether or not each Benchmarked Service is and/or the Benchmarked Services as a whole are, Good Value.

6.9 Members of the Comparison Group(s) with unusually high or low prices due, for example, to loss-leading prices or cross-subsidised prices, will be identified by the Benchmarker and removed from the Comparison Group(s) with the agreement of the Parties (not to be unreasonably withheld or delayed). The Benchmarker shall ensure that both Parties have full visibility of such Comparison Group(s) before and after the elimination of the identified members. No other organisations shall be removed from the Comparison Group(s).

6.10 In carrying out the benchmarking analysis the Benchmarker shall have regard to the following matters when performing a comparative assessment of the Benchmarked Services and the Comparable Services in order to derive Equivalent Services Data:

6.10.1 the contractual and business environment under which the Benchmarked Services are being provided (including the scope, scale, complexity and geographical spread of the Benchmarked Services);

6.10.2 any front-end investment and development costs of the Supplier;

6.10.3 the Supplier's risk profile including the financial, performance or liability risks associated with the provision of the Benchmarked Services as a whole;

6.10.4 the extent of the Supplier's management and contract governance responsibilities; and

6.10.5 any other factors reasonably identified by the Supplier which, if not taken into consideration, could unfairly cause the Supplier's pricing to appear non-competitive (such as erroneous costing or over-aggressive pricing).

6.11 The Benchmarker shall maintain an audit trail which is sufficiently detailed for any Expert appointed pursuant to Paragraph 7.10 below to understand all work conducted by the Benchmarker, including, so far as is reasonably practicable, details of the relevant information referred to in

Paragraphs 6.8 to 6.10 (inclusive) above, calculations, cost base information, source data, analyses, normalisation and adjustment.

7. BENCHMARKER'S REPORT

7.1 The Customer shall be entitled to disclose the Benchmarking Report to the Authority and any Contracting Body (subject to the Contracting Body entering into reasonable confidentiality undertakings).

7.2 The Benchmarker shall be required to prepare a Benchmarking Report and deliver it simultaneously to both Parties (a copy of the Benchmarking Report shall be provided to the Authority upon request), at the time specified in the plan approved under Paragraph 6 above, setting out its findings. Those findings shall be required to:

7.2.1 identify whether or not each Benchmarked Service is and/or whether the Benchmarked Services as a whole are, Good Value;

7.2.2 address the quality and competitiveness or otherwise of those Benchmarked Services; and

7.2.3 if any Benchmarked Service is not Good Value, or the Benchmarked Services as a whole are not Good Value, specify the changes that would be required to the Charges or Service Level Thresholds, that would be required to make that Benchmarked Service or those Benchmarked Services as a whole Good Value.

7.3 The Benchmarker shall act as an expert and not as an arbitrator.

7.4 Benchmark Reviews shall not result in any increase to the Charges or any decrease in the performance of any Services or Service Level Thresholds.

7.5 If the Benchmarking Report states that any Benchmarked Service is not Good Value, or that the Benchmarked Services as a whole are not Good Value, then the Supplier shall (subject to Paragraph 7.7 below) implement the changes set out in the Benchmarking Report as soon as reasonably practicable within a timescale agreed in writing with the Customer but (in the case only of a reduction in the Charges) in any event within no more than one (1) month of receipt of the Benchmarking Report and otherwise no more than three (3) months of receipt of the Benchmark Report.

7.6 Subject to the Supplier's right to dispute or reject the Benchmarking Report under Paragraph 7.8 below, if the Benchmarking Report determines that any or all of the Benchmarked Services are not Good Value, any failure by the Supplier to reduce the Charges in accordance with such timescales agreed between the Parties under Paragraph 7.5 above shall, without prejudice to any other rights or remedies of the Customer, constitute a material Default for the purposes of Clause 38.2.1.

7.7 The Supplier shall not be obliged to:

7.7.1 reduce any Charges which relate to a Service which has a service term specified in this Call Off Contract and such service term has not expired. In such instance and notwithstanding anything to the contrary in this Call Off Contract, the Customer shall be entitled to terminate such Service for convenience (and pay the early service termination charge (if any) relating to such Service stated in this Call Off Contract (or the Supplier's Pricing Catalogue where such

is required by the Customer)) and re-order such Service from the Supplier (at the reduced price) or another Supplier; or

7.7.2 implement any Benchmarking Report to the extent this would cause the Supplier to provide the Benchmarked Services at a loss or to the extent the Supplier cannot technically implement the recommended changes.

7.8 If the Supplier believes that implementation of any changes set out in the Benchmarking Report would cause the Supplier to provide the Services at a loss, it shall be entitled to provide a written submission to the Customer explaining why it believes this. Any such submission must be made to the Customer within ten (10) Working Days of receipt of the Benchmarking Report and must demonstrate clearly:

7.8.1 how specific elements of the Supplier's profit and profit margin would be impacted by implementation of the proposed changes; and

7.8.2 that it has taken full account of the financial impact of the change on all other Services due to be performed under this Agreement.

7.9 If the Customer receives a written submission from the Contactor pursuant to Paragraph 7.8 above, it shall review the evidence provided by the Supplier and shall, acting reasonably and in good faith, within ten (10) Working Days, either:

7.9.1 accept the Supplier's submission that implementation of the changes set out in the Benchmarking Report would cause the Supplier to provide the Services at a loss, in which case the Supplier shall implement the changes set out in the Benchmarking Report only to the extent that such changes could be implemented without the Supplier incurring a loss in respect of performance of the Services; or

7.9.2 reject the Supplier's submission, in which case the Customer shall provide a written explanation of its rationale for rejecting the Supplier's submission; and the Supplier shall implement the changes set out in the Benchmarking Report.

7.10 In the event of a Dispute or rejection of the Benchmarking Report under Paragraph 7.9 above, the matter shall be referred to an Expert for determination in accordance with Schedule 11 (Dispute Resolution). In the event of a Dispute between the Parties, the Customer shall continue to pay the Charges to the Supplier in accordance with the terms of this Call Off Agreement pending the conclusion of the Expert determination process.

On conclusion of the Expert determination process, if the Expert determines that all or any part of the Benchmarking Report recommendations regarding any reduction in the Charges shall be implemented by the Supplier, the Supplier shall, within four (4) Working Days, repay to the Customer the difference between the Charges paid by the Customer up to and including the date of the Expert's determination and the date upon which the recommended reduction in Charges should have originally taken effect.