Information Security Policy

1. Introduction

Information security and management is an integral part of IT governance, which in turn is a keystone of corporate governance. Information is an asset, and like other important business assets, it has a value and consequently needs to be suitably protected. A comprehensive information security management system protects information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

This is the British Library's high level **Information Security Policy**, part of the Library's **Information Risk Management Framework**. The principles described in this policy provide direction for the more detailed processes, procedures and guidelines that are referenced.

1.1 Objectives

The overarching purpose of this policy is to protect British Library information and systems from risks and associated threats and vulnerabilities, whether internal or external, malicious or accidental.

This policy, its sub policies and associated procedures define how the Library will manage information security. It is intended to ensure that all security risks to the Library's information, and information others entrust to it, are identified, analysed and managed so that they are maintained at acceptable levels. This includes risks to the confidentiality, integrity and availability of Library information.

The core objectives of this policy are to ensure:

- business continuity through the prevention, control, and minimisation of the impact of information security incidents;
- the confidentiality, integrity, and availability of Library information by documenting, implementing, and measuring information security controls against defined policies;
- that Library business units comply with legal, regulatory, and contractual requirements relating to the security of information.

In support of these objectives, the Library maintains a formal information governance programme which provides oversight of the **Information Risk Management Framework**. This programme is administered by the Corporate Information Governance Group (CIGG).

This policy will provide management support for information security principles, and unambiguously demonstrate management's commitment to information security.

2. Definitions

- **Authorised User –** Any individual who is permitted access to British Library buildings and systems during the course of their work for the British Library. This includes:
    - Permanent staff employed directly by the British Library and on the British Library Payroll and recruited by Human Resources;
    - Third party staff hired indirectly through a third party listed on the British Library's preferred supplier list. This includes agency staff;
    - Consultants, contractors and other temporary workers engaged indirectly through procurement contracts;
    - Voluntary staff and interns.
- **Electronic Media** – Any device that stores British Library information in digital form. This includes, but is not limited to:
    - Magnetic Media - Hard disk drives (both internal and external), floppy discs, magnetic tapes (reel, digital, back-up tape etc.);
    - Optical Media - CDs and DVDs;
    - Solid state memory devices (e.g. Flash media, USB drives, EEPROM etc.);
    - Personal digital assistants (PDAs);
    - Mobile devices / Tablets.
- **Hard Copy Media –** Any non digital storage medium on which information is physically recorded in a format suitable for direct use by a human being. This may include, but is not limited to:
    - Paper;
    - Microfiche;
    - Microfilm.
- **Information Asset –** An Information Asset is a collection of information that has *value* to the business of the Library, is *organised* in some form of structure and is managed as a single unit, and tends to *grow or change over time*. Any organised collection of information containing personal data should automatically be considered to be an Information Asset. An Information Asset may be stored in the form of a database, a discrete collection of electronic files, or hard-copy.
- **Information Asset Owner –** Managers held responsible for ensuring that specific Information Assets are handled and managed appropriately. This means making sure that Information Assets are properly protected and that their value to the organisation is fully exploited.
- **Mobile Device –** Smart Phones (e.g. iPhone, Blackberry, Android, Windows Mobile), Tablets (e.g. iPad, Nexus), PDA's, mobile phones, and other mobile technology (excluding laptops) that store, transmit, or process British Library and/or British Library customer information.
- **Removable Media –** Any easily portable Electronic Media in which information can be recorded separately from its network or system
- **Sensitive Information –** All Personal Data (as defined by the Data Protection Act 1998), financial data or information which is likely to be exempt from disclosure under the Freedom of Information Act 2000
- **Third Party -** Any external organisation or individual who is not a member of the Library staff, for example service providers, external IT maintenance and support staff, contractors or consultants. This includes external individuals and agencies not working under the instruction or on behalf of the Library, such as regulatory authorities and law enforcement agencies.
- **Visitor –** Any member of the general public who visits the Library premises as a Reader, customer or guest.

3. Scope

This policy applies throughout the British Library. All Authorised Users are expected to comply with information security policy and its associated processes, controls and guidelines.

4. Information Security Policy

The following sections are numbered in accordance with the relevant sections of ISO27002:2013 for ease of use.

Introductory Statement

The British Library will identify and manage information security risks that endanger the achievement of its strategic and operational aims.

The Library will embed information security into business processes and functions by means of approved procedures, processes, and controls.

The Library will make all reasonable efforts to discharge any security related obligations arising from legislation, regulation or voluntary agreement, drawing on best practice and recognised standards where appropriate.

The Library will publish sub-polices, mandatory procedures and optional guidelines in support of this policy.

In instances where the Library is unable to meet the requirements of this Information Security Policy the exception shall be formally evaluated, logged and periodically reviewed.

There are seven fundamental information security principles that guide the British Library's approach to information security:

- Our approach to information security management aims to align with accepted best practice as defined by the ISO/IEC 27000-series and other relevant information security standards.
- Information is a critical business asset and must be protected to a level appropriate to its vulnerability, importance and value to the Library.
- Information security controls are necessary to protect information against unacceptable risks to its confidentiality (*e.g*. preventing unauthorised disclosure of sensitive corporate or personal information), integrity (*e.g*. ensuring that human errors and programming bugs do not reduce the completeness or accuracy of our data) and availability (*e.g*. minimizing unplanned system downtime consequent interruption of critical business processes).
- We aim to invest wisely in proven information security controls. This is on the basis of lifecycle cost-benefit assessment and risk analysis. The goal is not to completely eliminate information security risks, but to reduce and manage them in the most cost-effective manner, offsetting the cost of controls against the anticipated reduction in losses due to avoiding or mitigating security incidents.
- Information security should be pervasive throughout the entire organisation. It is an inherent part of our IT architecture and a component of our operational and management processes. In short, we are *all* responsible for information security.
- Information security is a core element of corporate governance. It is closely related to aspects such as IT management, physical site security, risk management, legal and regulatory compliance and business continuity. It supports various obligations to our employees, business partners and to the community at large.

- Information security is a business enabler that allows us to enter more confidently into and maintain business relationships, markets and situations that would otherwise be too risky. By minimizing net losses resulting from information security incidents, it supports our financial bottom line. It also enhances our image as a trustworthy, open, honest and ethical organisation.

5. Information Security Policies

Core Objectives

- To define a clear and consistent direction for the management of Information Security within the British Library.

5.1 Management Direction for Information Security

The British Library shall determine and maintain a suitable **Information Security Policy** approved by Senior Management. This policy shall be communicated to all Authorised Users.

The **Information Security Policy** (and its supporting sub-policies, user manual, procedures and guidelines) shall be reviewed and evaluated periodically to ensure the content remains effective.

6. Organisation of Information Security

Core Objectives

- To define the management framework established to control the implementation of information governance and on-going management of security within the British Library.

6.1 Internal Organisation

The British Library Board has overall responsibility for the implementation of information security as a whole within the British Library. The Board delegates responsibility for all operational matters to the Executive Leadership Team, which in turn delegates responsibility for information security matters to the Senior Information Risk Officer (SIRO), a government-mandated responsible person of Executive level. The SIRO is responsible for coordinating the work of the Corporate Information Governance Group (CIGG). The responsibilities of this group include, but are not limited to:

a. Monitoring of the British Library's **Information Asset Register**;
b. Overseeing development of high level security policy documentation and associated procedural documentation;
c. Endorsing the main information risks faced by the Library, to be incorporated into the **Divisional/Strategic Risk Registers**;
d. Undertaking an organization wide information risk assessment on an annual basis, and, where required, on a risk triggered basis;
e. Understanding what information risks the Library is exposed to and ensuring that these are addressed;
f. Ensuring there is a process in place for reporting and managing information security breaches;
g. Reviewing the outcomes of information management/compliance/security audits.

Further details can be found in the **CIGG Terms of Reference**.

Security risk management accountabilities and responsibilities shall be clearly defined and allocated by direction of the CIGG. These will cover all aspects of the **Information Security Policy** and be commensurate to the risk appetite of the British Library.

Duties and areas of responsibility must be segregated between individuals to reduce opportunities for unauthorised or unintentional modification or misuse of British Library business networks, Systems or applications.

Tasks involved in critical information systems and processes must be performed by separate individuals (e.g. by segregating the initiation and authorisation responsibilities for a task).

If there is a danger of primary controls being bypassed (e.g. through collusion) on Systems containing Sensitive Information, additional controls must be designed and implemented. These may include but are not limited to:

a. Secure logs/records of transactions;
b. Regular review of controls and processes;
c. Alarms/alerts on significant security events.

Individuals performing checks such as security audits and system acceptance tests must be independent of the management and operation of the systems and processes being reviewed.

It is recognized that operational constraints may necessitate exceptions to the principle of segregation of duties in particular. In all cases these exceptions must be evaluated, logged, escalated to Divisional Risk Registers where appropriate, and periodically reviewed by the Information Security Officer.

Contact with regulators or other authorities in relation to information security matters shall be coordinated by CIGG.

6.2 Mobile Devices & Teleworking

Only Mobile Devices or laptops owned and managed by the British Library, or personal devices explicitly approved by the IT department, shall be connected to Library networks and systems.

All laptops owned and managed by the British Library shall have full disk encryption installed.

All Mobile Devices that connect to the British Library internal network shall be encrypted.

Mobile Devices that have the ability to access and store British Library emails shall not retain emails for longer than 30 days.

Where possible, Mobile Devices shall be configured to require a password for authentication in line with the following requirements:

a. Passwords shall be a minimum of five (5) characters in length;
b. At a minimum, the previous 7 passwords shall not be reused;
c. Passwords shall expire, or manually changed after ninety (90) days.

Where possible, Mobile Devices shall be configured to automatically lock after five (5) minutes of inactivity

Where possible, Mobile Devices shall be configured to wipe (delete data) and return to factory defaults after ten (10) unsuccessful login attempts.

Line managers shall only authorise remote working where the business benefit outweighs the costs and information security risks.

Authorised remote workers shall gain remote access using a British Library approved method as per the **Network Access and Management Standard** and shall follow guidance set out in the documented **Portable Computing Security Guidelines**.

Data shall be stored on the Library network wherever possible and not held on Mobile Devices or laptops. Where data is stored on Mobile Devices or laptops when working remotely, it must be backed up onto the Library network at a frequency commensurate with the sensitivity of the data.

Remote workers using Mobile Devices or laptops shall keep equipment, files and media locked out of sight during transit and when unattended in a fixed location. Particular care must be taken when Mobile Devices or laptops are taken on to public transport.

7. Human Resource Security

Core Objectives

- All British Library authorised users undergo appropriate screening prior to engagement.
- All British Library authorised users understand their security roles and responsibilities, and this is included in appropriate recruitment documentation and contracts.
- Any change of role is subject to system access, permission and asset possession review.
- System access is revoked and British Library assets shall be returned upon termination of employment.

7.1 Prior to Engagement / Appointment

In accordance with the **Recruitment Policy** and the **Guidelines for Hiring and Engaging of Temporary staff,** security roles and responsibilities for all Authorised Users shall be described in appropriate recruitment documentation and contracts.

All successful Authorised Users shall undergo screening commensurate to their role and grade. This may include but is not limited to:

a. Taking up references;
b. Checking career history/qualifications;
c. Confirming identity;
d. Other security or background checks required by role

7.2 During Engagement / appointment

As part of induction training, Authorised Users shall receive training and information regarding their role and responsibilities in relation to the protection of British Library information, including information that has been entrusted to them by others. The Corporate Information Governance Group is responsible for the content and adequacy of this training.

The Corporate Information Governance Group is responsible for ensuring that all Authorised Users receive periodic security risk awareness materials and updates on relevant business policies and procedures.

In accordance with the **Electronic Communications Security Policy**, access to all computers, systems, software and networks requests shall be granted commensurate to user role and responsibilities. Access to specific information or Systems shall be granted by the IT Helpdesk at the request of the relevant line manager, Information Asset Owner, or other appropriate business owner. Further information can be found in Section 4.7 (Identity and Access Management) of this Policy.

Line Managers, in consultation with Human Resources, are responsible for keeping role profiles up to date, including role specific responsibilities for Information Security or Information Asset Management.

Any material breach of this **Information Security Policy** (and its associated manual, sub-policies, standards and mandatory procedures) may be dealt with as a disciplinary issue under the Library's normal **Disciplinary policy**.

7.3 Termination or Change of Engagement / Appointment

In accordance with documented staff change procedures, Authorised User system access, permissions and asset possession shall be reviewed and amended as commensurate to their new role and/or grade.

Authorised Users on long term leave such as sabbatical, sickness, maternity or under a relevant investigation process shall have their system access, permissions and asset possession reviewed and amended accordingly in line with business risk appetite and relevant legislation.

All changes to the engagement or appointment of an Authorised Used shall be communicated to IT Operations as soon as possible by the relevant Line Manager or HR Representative so that the appropriate changes can be made.

On the last contractual day of their service the Library shall remove all Authorised User access, including remote access to Library buildings and systems.

8. Asset Management

Core Objectives

- To achieve and maintain appropriate protection of British Library information assets.
- To ensure all information assets are accounted for and have a nominated owner.

8.1 Responsibility for Information assets

In accordance with the **Information Asset Management Policy**, the British Library shall maintain an inventory of Information Assets. This includes but is not limited to:

a. the Library's System assets, including any underlying and associated technologies;
b. the Library's Servers and the Utility Services that support them;
c. the Library's physical IT assets such as desktop computers, laptops, printers and mobile telephony devices;
d. Library owned or licensed software.

In accordance with the **Information Asset Management Policy**, all information and physical assets associated with Sensitive Information shall be "owned" by a designated responsible individual. The responsibilities of the designated owner shall include but are not limited to the following:

a. Knowing what information the asset contains and what information is transferred in or out of it;
b. Appropriately classifying and (where necessary) labelling the asset;
c. Knowing who has access to the asset and why, and ensuring that access and use of the asset is properly monitored;
d. Identifying and addressing risks to the Information Asset assigned to them
e. Ensuring that appropriate arrangements are made through the Central Procurement Team to include relevant confidentiality, data protection and data security clauses in contracts that permit external contractors and consultants access to Library Information Assets.

In accordance with the **Information Asset Management Policy** and Section 4.9 of this Policy (Information Security Event Management), should a physical IT asset be lost , stolen or damaged then the Authorised User to whom it is assigned to must immediately report the event to the Security Control Room at St Pancras as soon as practically possible.
All British Library authorised users are responsible for the acceptable use of information assets and physical IT assets to which they have access to in the course of their employment, and in particular they shall comply with all elements of the Library's **Electronic Communications Security Policy.**

Where a non-routine use of a System or Information Asset may be required for business purposes the member of staff requiring the non-routine use shall contact the appropriate Information Asset Owner for permission.

In accordance with documented exit management procedures, all Authorised Users shall return to their line managers all British Library assets (including all passes and other security tokens) on the last day of their employment.

8.2 Information Classification

Where appropriate, Sensitive Information and Sensitive Information processing facilities must be clearly labelled, named or otherwise identified by the relevant asset owner so as to maintain its confidentiality, integrity or availability in accordance with regulatory, legal and business requirements.

8.3 Media Handling

Removable Media shall be managed in accordance with the **Media Handling Policy** and the **Electronic Communications Security Policy**. In particular:

a. Removable Media shall only be used where there is a justified business need;
b. All Removable Media shall be stored in an environment which affords a level of protection commensurate with the value of the data stored on the media.

USB ports and other removable media interfaces on British Library infrastructure devices, servers and PCs shall be controlled commensurate to the sensitivity of the information stored and accessed by the device.

When no longer required, Electronic Media shall be disposed of in accordance with the **Disposal of Media Process.**

Hard Copy Media containing Sensitive Information shall be shredded on Library premises using the shredders provided. Other Hard Copy Media may be disposed of in one of the lockable paper bins provided by the British Library Estates team.

Sensitive Information in British Library business Systems, networks and Mobile Devices shall be managed and protected in accordance with the **Media Handling Policy**.

9. Identity & Access Management

Core Objective

- To ensure that only authorised individuals gain appropriate and attributable access and privileges to British Library business networks, systems and applications.

9.1 Access Control Policy

Access to Information Assets must only be granted to Authorised Users based on defined business and security requirements. IT systems must be administered in accordance with the Library's documented **Access Control Policy**.

9.2 User Access Management

User accounts shall be created based upon the concept of least privilege and requests for similar levels of access to other user accounts must not result in excessive and potentially toxic privileges being granted.

User accounts shall be created using a unique identifier (User ID) which shall be linked to the Authorised User's British Library employee number.

Information Asset Owners must ensure that access and privileges for business networks, systems and applications accessing Information Assets under their ownership are clearly documented and maintained. These may include but are not limited to:

a. Defined business roles and the associated access and privileges;
b. Types of user account and associated default access and privileges;
c. System, generic and shared accounts and their associated access and privileges.

Line Managers shall determine appropriate access and privileges for new joiners and shall notify the IT Help Desk in order to initiate and authorise the request.

When an employee moves department or changes roles (including promotion or demotion), Line Managers shall review access and privileges to ensure they are still appropriate. Line Managers shall contact the IT Help Desk in order to initiate and authorise any changes.

When a user leaves the British Library, their Line Manager shall ensure that employee access to British Library buildings and systems, including remote access and access to third party systems, is removed on the last contractual day of employment, in accordance with documented **Exit Management Procedures.**

Authorised User accounts with special privileges that allow the creation, modification and deletion of accounts and data must be restricted to individuals responsible for the management or

maintenance of business networks, systems and applications. A record of these privileges shall be maintained.

Each Authorised User who requires special privileges shall have their own administrator level account which shall only be used for system administrative purposes. This shall be kept separate from their standard user level account.

System Owners shall ensure that there is a documented process in place to periodically review user access to business networks, systems and applications under their ownership. The process shall confirm that access and permissions are appropriate and that there are no breaches of segregation of duty rules.

The frequency of the review and number of accounts reviewed shall be commensurate with the risk of unauthorised or inappropriate access.

Technical Owners shall ensure that there is a documented process in place to maintain user account administration information and audit logs. The process must ensure that:

a. An audit trail of all user account creations, modifications and deletions together with the relevant authorised request (unless pre-approved) shall be retained;
b. Individual user account information (including system, generic and shared accounts) relating to ownership, access rights, privileges and permissions shall be available upon request.

9.3 User Responsibilities

Authorised Users must follow good security practices in the selection and use of passwords on IT systems and mobile devices as detailed in the **Choosing & Using Passwords Guidance** issued by the IT Security Officer. In particular:

a. Passwords shall not be shared with, used by or disclosed to other users;
b. Passwords must be kept secure and not written down;
c. Passwords shall be changed at least every 90 days;
d. At a minimum, the previous 7 passwords shall not be reused.

PCs, terminals and mobile computing devices shall not be left unattended during working hours while any user is logged-in, unless they are first locked by a suitable mechanism such as a password-protected screensaver, key lock or token lock, as detailed in the Library's documented **Clear Screen Guidelines**.

Outside office hours, laptops that are left in the office must be stored in a suitable locked cabinet, or secured with an approved cable lock.

9.4 System and Application Access Control

Access to Operating Systems, British Library applications and information held in these applications shall be restricted to Authorised Users in accordance with the **Operating System Access Control Policy** and **Application and Information Access Control Policy**.

10. Cryptography

Core Objective

- To ensure that British Library business networks, systems, applications and data are properly protected by cryptographic controls when not adequately protected by other means

10.1 Policy on the Use of Cryptographic Controls

Cryptographic techniques for file encryption, user authentication and preserving the integrity of British Library information shall be considered using a risk-based approach taking into account the sensitivity of the information and business requirements.

11. Physical & Environmental Security

Core Objectives

- Provide a secure environment for all staff and visitors to British Library sites.
- Protect British Library assets, buildings, equipment, IT infrastructure and collections against theft, damage or loss.
- Ensure the confidentiality, integrity and availability of British Library services.

11.1 Secure Areas

Risk assessments relating to physical security controls shall be carried out on at least an annual basis in accordance with the Library's overarching risk management approach.

All sites shall be protected using proportional security controls based on the level of risk and in accordance with the Library's documented **Physical Security Policies and Procedures**. In terms of information security these controls will include, but not be limited to:

a. CCTV monitoring of publicly accessible areas;
b. Physical security measures to protect strong rooms, secure storage cabinets and high risk information storage / processing areas;
c. Physical barriers designed in accordance with British government standards.

Access to all operational areas shall be restricted to those who have an operational or service need, and in accordance with section 4.7 (Identity and Access Management) of this Policy.

All Authorised Users shall be issued with individual identity passes, which must be worn at all times.

All Visitors authorised to enter British Library operational areas shall be logged in and out, and provided with temporary individual identity passes for the duration of their visit.

Organisers of events being held on British Library sites shall consult the IRM Security Team to ensure that appropriate levels of [information] security are maintained throughout.

Lost or stolen identity passes or keys shall be reported immediately to a member of the IRM Security Team.

11.2 Equipment

Processes and procedures shall be put in place to protect the confidentiality, availability and integrity of the British Library's physical IT assets and the Systems they support, based on their assessed criticality and/or value. Examples of these measures include but are not limited to:

a. Regular back-up generator and uninterruptible power supply (UPS) load tests;
b. Regular fire detection system tests;
c. Segregation of data cabling in accordance with industry wiring regulations.

All IT equipment and supporting infrastructure shall be maintained in accordance with manufacturer's recommendations and or documented procedures, in order to ensure the on-going confidentiality, integrity and availability of the Library's information.

Valuable and/or attractive assets containing Sensitive Information shall not be taken off British Library premises without prior authorisation. Such assets must be protected in line with the Library's documented risk appetite and relevant physical security policies and procedures.

All Library storage media must, at the end of its useful life, be securely disposed of in accordance with the **Media Disposal Process**.

All desks and working areas shall be cleared of papers and removable computer storage media containing Sensitive Information when not in use, whether during or outside normal working hours.

12. Operations Security

Core Objectives
To ensure the correct and secure operation of British Library business networks, systems and information processing facilities to preserve their confidentiality, integrity and availability.

12.1 Operational Procedures & Responsibilities

All procedures for the operation and administration of British Library business networks, Systems, applications and activities shall be properly documented and regularly reviewed and maintained. These documented procedures may include but are not limited to:

a. Processing and handling of information;
b. Information backup and media handling;
c. Computer start-up and shutdown, including restart and recovery procedures for use in the event of system failure;
d. Management of system, security and audit logs.

Documented **Operating Procedures** relating to critical systems and administrative utilities shall be held securely and access restricted on a need to know basis.

Where feasible, Systems and networks shall be managed consistently using similar procedures, tools and utilities.

Changes to British Library processing facilities, business networks, systems, applications and procedures shall be controlled through formal management responsibilities and procedures in proportion to the risks involved.

All proposed changes shall be risk assessed to determine their significance, and the associated management decisions and approvals must be recorded.

All significant changes shall be managed in accordance with the documented **Change Management Process.**

British Library capacity demands shall be monitored using appropriate network and System monitoring tools and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

New demands from users shall be identified and the effects on the Systems assessed before being accepted. Quota management shall be implemented for all users wherever possible.

Pre-production / staging environments (including the Systems, networks and data associated with specification, design, development and testing of applications) shall be logically isolated from production environments to ensure their respective integrity.

Where appropriate, development and test environments shall be isolated from each other using physically different Systems, processors, domains, directories or networks.

The introduction of new or modified software into production must be controlled in accordance with the documented **Change Management Process**.

Test systems shall emulate production environments as closely as possible except that:

a. Testers and developers shall not have root access on production systems;
b. Production data shall only be available on production systems;
c. Development and testing should use dummy data wherever possible. If production data must be used, fields containing Sensitive Information (such as credit card numbers and personal data) must first be obfuscated;
d. No personal data shall be used for the purpose of system testing without the express and prior authorisation of the Data Protection Manager;
e. Where possible, on-screen messages, screen colours etc. shall clearly indicate whether a system is in test or production to minimise the risk of accidental submission of test transactions on production system.

Compilers, editors, auditing tools and similar system utilities shall not be installed on production systems unless absolutely necessary. In this instance they shall only be used by specifically Authorised Users for legitimate purposes in accordance with the **Change Management Process**.

It is recognized that operational constraints may necessitate exceptions to this section of the **Information Security Policy** in particular. In all cases these exceptions must be evaluated, logged, escalated to Divisional Risk Registers where appropriate, and periodically reviewed by the Information Security Officer.

New British Library business Systems, or significant changes to existing Systems, shall be authorised by the relevant Information Asset Owner and/or the project sponsor in accordance with the **System Acceptance Process**.

Acceptance criteria for new Library business Systems, or significant changes to existing Systems, shall be established and suitable testing of the system carried out prior to migration to operational status, in accordance with the **System Acceptance Process**.

All business Systems developed for or by the Library shall follow an appropriate formal project management methodology.

12.2 Protection From Malware

All British Library business systems, including servers, desktops and Mobile Devices shall be protected against malicious and mobile code in accordance with the **Malicious and Mobile Code Protection Standard**.

12.3 Back-Up

British Library data shall be protected in accordance with the documented **Information Backup Process** and at a frequency commensurate with the sensitivity of the data.

All users shall ensure that Library data on Mobile Devices, laptops and Removable Media is backed up onto the Library network at a frequency commensurate with the sensitivity of the data, and by methods established as part of normal operating procedures.

12.4 Logging & Monitoring

All British Library business Systems, networks, applications and Mobile Devices shall be routinely monitored, and audit trails kept, in accordance with the **Security Monitoring Standard**.

All Library information logs shall be protected to ensure their confidentiality, integrity and availability.

A single “master” British Library network firewall shall synchronise with the external Janet Network Time Service. All other British Library network infrastructure devices, servers and desktop PCs with the capability to operate a real-time clock shall synchronise with this device.

All Library infrastructure devices, servers and desktop PCs shall be reviewed on an annual basis to ensure their internal system clocks are synchronised to the appropriate network device.

12.5 Control of Operational Software

The installation of software on operational systems shall be controlled in accordance with documented procedures in order to minimise the risk of corruption to operational systems. In particular, the updating of all operational software, applications, and program libraries shall only be performed by authorised individuals in accordance with Sections 4.7 (Identity and Access Management) of this Policy.

12.6 Technical Vulnerability Management

British Library business networks, Systems and applications shall be evaluated for technical vulnerabilities in accordance with the **Technical Vulnerability Management Policy**.

Penetration tests of Library business networks, Systems and applications shall be carried out using a risk-based approach. Any penetration tests shall be conducted in accordance with the **Internal Penetration Testing Policy** or **External Penetration Testing Policy** as applicable.

12.7 Information Systems Audit Controls

British Library Authorised Users are required to fully cooperate with all approved audit activity.

Audit activities shall be risk-based and carefully planned and agreed to minimise the risk of disruption to the business.

Access to information systems audit tools shall be controlled to prevent any possible misuse or compromise.

13. Communications Security

Core Objectives
To ensure the correct and secure operation of British Library business networks, systems and information processing facilities to preserve their confidentiality, integrity and availability.

13.1 Network Security Management

British Library business networks shall be managed and controlled in accordance with the **Network Access and Management Standard** in order to safeguard the confidentiality and integrity of data passing over Third Party networks and to protect the integrity of Library networks and computer systems against internal and external threats.

Access and changes to both internal and external British Library networked services shall be controlled in accordance with the **Network Access and Management Standard**.

Security features, arrangements, service levels and management requirements of all network services (e.g. the provision of private network services) shall be identified and documented in a **Network Services Agreement**.

Network Services Agreements shall be reviewed at a frequency commensurate with the criticality of the service.

13.2 Information Transfer

The exchange of Sensitive Information between the British Library and any Third Party shall be in accordance with documented **Data Sharing Guidance** and **Sharing Personal Information Policy**.

All media containing Library information shall be protected during transportation between Library sites and off-site locations in accordance with documented **Data Sharing Guidance** and **Sharing Personal Information Policy**.

.

Information exchanged in electronic messaging and between Library business systems and networks shall be appropriately protected commensurate with the sensitivity of the information, and adhere to all requirements of the **Electronic Communications Security Policy**, the **Records Management Policy**, and the **Personal Information Policy**.

14. Systems Acquisition, Development & Maintenance

Core Objectives

- To ensure that security is an integral part of British Library business systems and applications.
- To prevent error, loss, unauthorised modification or misuse of information in British Library applications.

14.1 Security Requirements of Information Systems

Business requirements for new or significant changes to existing British Library business Systems and applications shall include requirements for security controls. These requirements may include but are not limited to authentication, authorisation, access, and auditing controls as well as requirements for vulnerability and penetration testing, patch management, business continuity and disaster recovery.

Security requirements that are identified shall be justified, agreed and documented as part of the overall business case, and included as a formal part of the systems development life cycle.

14.2 Security in Development and Support Processes

Software changes to British Library business Systems and applications shall be strictly controlled in accordance with the documented **Change Management Process**.

Library applications shall be reviewed and tested when operating system changes occur to ensure security controls and integrity procedures have not been compromised by the changes.

The purchase of any new IT System shall follow the authorisation requirements as defined in the **Authorisation of Information Processing Facilities Policy**. This includes the identification of defined Business Owners and Information Asset Owners.

Where there is a specific business need to outsource software development, approval shall be sought from IT Development and the following controls shall be implemented:

a. Licensing agreements reviewed by the Corporate Procurement Unit;
b. Escrow agreements in the event of the third party liquidation;
c. Requirements for the quality and rights of access to audit the source code to be included in contractual agreements;
d. Testing of software in a segregated environment prior to installation on British Library business networks and systems.

15. Supplier Relationships

Core Objectives
To ensure that British Library IT contracts properly address all relevant risks through the implementation of appropriate security controls and operating procedures.

15.1 Information Security in Supplier Relationships

[Proposed] Business owners shall ensure that Third Party information security risk is assessed prior to contracting, managed within the contract and actively monitored during the life of the contract. This may include but is not limited to:

a. Enforcing Non-Disclosure agreements commensurate to information being exchanged with the third party;
b. Governing the provision of third party access to the Library's IT Infrastructure in accordance with the **Third Party Supplier and Contract Management Standard**;
c. Ensuring that information security requirements as detailed in the Library's documented **IT Technical Standards** are addressed in the contract.

15.2 Supplier Service Delivery Management

Business owners shall ensure that Third Party IT service delivery is managed in accordance with the **Third Party Supplier and Contract Management Standard**. In particular:

a. Security controls, service definitions and delivery levels must be included in a Third Party service delivery agreement;
b. The agreement should be monitored and reviewed regularly by the relevant business owner or contract manager based on the information security risk to the British Library;
c. Any changes, or exit of the agreement, shall be managed in accordance with the **Third Party Supplier and Contract Management Standard** and CPU Exit Management processes.

16. Information Security Incident Management

Core Objectives

- All information security incidents shall be reported, classified, handled, reviewed and documented using British Library security incident management processes.
- Minimise the business impact of security incidents on British Library.
- Reduce the likelihood of similar information security incidents re-occurring.

16.1 Management of Information Security Incidents and Improvements

Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents both during and out of office hours. This includes but is not limited to:

a. Assessing the potential impact of an information incident, its prioritisation and presenting options for remediation;
b. Prioritising the response according to the criticality of the affected information and/or reporting obligations for specific categories of data e.g. personal data;
c. Seeking expert advice/guidance from an established list of internal contacts;
d. Establishing mechanisms to enable the frequency, types and costs of information security incidents and other issues to be quantified and monitored.

Please refer to the **Information Breach Management Process** for specific responsibilities and procedures with regards to information security breaches or events involving or suspected to involve, personal data.

Regular reviews, at least annually, of all information security incidents must be carried out by IT Operations and/or the Data Protection Officer in order to identify whether patterns reveal any control weaknesses, and to take steps to close any identified control gaps. .

Investigations into the activities of staff and customers may only be carried out in accordance with the **Digital Investigation Policy** and its associated procedures.

Information security incidents or suspected security weaknesses shall be reported as follows:

a. All information security breaches (or other incidents involving (or suspected to involve) personal data, including 'near misses') must be reported to the Security Control Room at St Pancras as soon as practically possible;
b. Where the breach or incident is in relation to a System disruption the IT Helpdesk shall be notified as soon as practically possible by calling extension 2020, 01937 882 020 (external), or emailing ITHelpDesk@bl.uk between 8am and 5pm.

The Corporate Information Governance Group is responsible for ensuring that all Authorised Users receive periodic awareness training on how to quickly report an information security incident, risk event or security weakness.

For further information on the management of system related incidents, please refer to the **IT Incident Management Process.**

For further information on the management of incidents involving personal information, including, loss or theft of data storage equipment or paper files, please refer to the **Information Breach Management Process.**

17. Information Security Aspects of Business Continuity Management

Core Objectives

- To ensure that Systems are sufficiently resilient to ensure the continuity of critical business processes despite minor incidents, and have proven disaster recovery arrangements in place to minimise the business impact of serious incidents

17.1 & 17.2 Information Security Continuity

The British Library's **Business Continuity Management Policy** must ensure that information security controls are taken into account in the business continuity and disaster recovery processes.

All Authorised Users must comply with the requirements of the **Business Continuity Management Policy** and its associated plans and processes.

18. Compliance

Core Objectives

- To avoid breaches of legal, statutory, regulatory or contractual obligations in relation to Information Security.
- To ensure systems comply with British Library Information Security policies and processes.

18.1 Compliance with legal, regulatory and contractual requirements

All Information Security processes and policies must take into account all relevant legal, regulatory and contractual requirements.

In particular, special care should be taken to ensure compliance with the **Personal Information Policy** and its associated sub-policies and procedures.

IT Operations shall manage distribution and use of software licenses within the British Library.

The Intellectual Property & Licensing team are responsible for the management and licensing of all intellectual property belonging to the British Library Board.

In accordance with the **Records Management Policy**, important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

Cryptographic controls may only be used in accordance with all relevant legal, regulatory and contractual requirements.

British Library managed business systems and applications that are involved in electronic commerce information passing over public networks shall be managed in accordance with the **Payment Card Industry Data Security Standard (PCI DSS) Policy**.

18.2 Independent Review of Information Security

Managers shall ensure that all information security procedures within their area of responsibility are carried out correctly.

Critical information Systems must be checked by the relevant System or Technical Owner at risk-based intervals to ensure they comply with British Library security standards. For details on System Penetration Testing, please refer to the **Internal Penetration Testing Policy** and **External Penetration Testing Policy** as appropriate. For details on System Vulnerability Assessments, please refer to the **Technical Vulnerability Management Policy**.

CIGG are responsible for carrying out annual information risk assessments in relation to all Information Assets. Additional risk assessments will be carried out at other times in accordance with the level of risk identified as set out in the **Information Risk Management Policy**.

Where a Library department is unable to meet the requirements of the Information Security policy, the exception shall be evaluated and logged by the Information Security Officer, and escalated to the relevant Divisional Risk Register if appropriate. All exceptions to the Information Security policy shall be subject to regular review by the Information Security Officer.

19. Ownership & Review

This policy will be reviewed every year by the Corporate Information Governance Group; major changes will be referred to the Executive Leadership Team for authorisation.