Harrow Council

Information Governance and Security Policy

Final 2.0

Version and Review Summary

Revision	Date	Author	Revision description
1.00	March 2016	Reena Parmar (Information Governance Manager) Samji Patel (Security and Compliance Manager) Mene Menelaou (Enterprise Architect) Bernie Harrison (Service Manager IT Strategy and Change)	Formal Review Ratified by the Information Governance Board March 2016
1.1	December 2017	Reena Parmar (Information Governance Manager) and Samji Patel (Security and Compliance Manager)	Reviewed and updated Draft distributed to: Rahim St John (Head of Transformation and Technology) Catherine Little (Service Manager Service Delivery)
1.2	December 2017	Reena Parmar (Information Governance Manager Samji Patel – Security and Compliance Manager	Includes comments from Catherine Little (Service Manager Service Delivery) Updated draft distributed to Information Governance Board members for final review
2.0	January 2018	Reena Parmar – Information Governance Manager Samji Patel – Security and Compliance Manager	Formal Review Ratified by the Information Governance Board 22 January 2018

Related Documents

Related Documents Name
Information Technology and Systems Acceptable Use Policy
Architectural Standards Document

POLICY / TARGET AUDIENCE	ALL STAFF	MANAGERS / PROJECT LEADS	THIRD PARTY SUPPLIERS / SHARED SERVICES
INTRODUCTION AND PURPOSE	✓	✓	✓
INFORMATION, TECHLOLOGY AND SYSTEMS ACCEPTABLE USE POLICY	✓	✓	✓
INFORMATION ASSET MANAGEMENT	✓	✓	✓
INFORMATION RETENTION AND DISPOSAL	✓	✓	✓
SECURITY CLASSIFICATION AND HANDLING	✓	✓	✓
FREEDOM OF INFORMATION ACT 2000 POLICY AND ENVIRONMENTAL REGULATION	✓	✓	✓
DATA PROTECTION	✓	✓	✓
PRIVACY IMPACT ASSESSMENT	✓	✓	✓
PSEUDONYMISATION AND ANONYMISATION	✓	✓	✓
CLOUD SECURITY	✓	✓	✓
THIRD PARTY CODE OF CONNECTION	✓	✓	✓
INFORMATION SHARING	✓	✓	✓
SECURITY INCIDENT RESPONSE	✓	✓	✓
PASSWORD SECURITY	✓	✓	✓
REMOVABLE MEDIA	✓	✓	✓
PERSONNEL SECURITY		✓	✓
RISK MANAGEMENT		✓	✓
DIASTER RECOVERY AND BUSINESS CONTINUITY		✓	✓
ENCRYPTION POLICY (SECURE TRANSMISSION OF DATA)		✓	✓
APPLICATION DEVELOPMENT		✓	✓
IT INFRASTRUCTURE			✓
LOGICAL ACCESS CONTROL			✓
NETWORK SECURITY MANAGEMENT			✓
REMOTE ACCESS SECURITY			✓
ANTI-VIRUS AND MALWARE			✓
FIREWALL SECURITY			✓
SECURITY TESTING			✓
BACKUP AND ARCHIVING			✓
SECURITY AUDIT AND MONITORING			✓

Contents

1. Introduction and Purpose

1.1 Harrow Council (hereafter referred to as ‘the Council’) holds information in many forms such as electronic records, paper files, audio recordings, photographs, videos, images all known as Information Assets (IA). It is important that these IA are protected for the following reasons:

- Assure our residents, staff and other stakeholders that their information is secure
- Satisfy legal requirements and avoid monetary penalties
- Avoid reputational damage

1.2 The purpose of this document is to describe the Council's policies and approach to the governance, management and security of Information Assets. It covers the definition of Information Security and describes policies and how they must be applied. This document must be read in conjunction with the Information Technology and Systems Acceptable Use Policy and the Architectural Standards Document.

1.3 Services Areas across the Council will also need to hold local policies and procedures relating to the management and handling of their specific IA, based on this document and must be able to demonstrate accountability, transparency and governance of their IA.

Information Security Definition

1.4 Information Security is anything that affects the confidentiality, integrity and availability of the Council’s Information Assets. It is about protecting information and systems from unauthorised access, use, disclosure, disruption, modification, or destruction.

1.5 Standards for information security cover three areas:

- Confidentiality: Information is only available to those that are authorised to have access.
- Integrity: Safeguarding the accuracy and completeness of information and processing methods.
- Availability: The assurance that authorised users have access to Information Assets when required.

Scope

1.6 This policy applies to all Council:

- Employees, partners, 3rd party suppliers, contractors, elected members, site visitors or anyone working for or on behalf of the Council.
- IA held, stored or processed by or on behalf of the Council.
- Equipment (owned, operated or leased) and includes both online and off line backup technologies.
- Networks, firewalls and infrastructure managed by the Council or on its behalf, and IA connected to it.
- Production, development and test systems used to store, process and transmit data, which may be considered personal or sensitive or would otherwise financially affect the organisation or its clients should its confidentiality, integrity or availability be compromised.

Roles and Responsibilities

1.7 Everyone working for or on behalf of the Council:

- is responsible and accountable for information governance and security within his or her respective service areas;
- must sign up to the Information Technology and Systems Acceptable Use Policy;
- must undertake the online information governance and security awareness training on an annual basis.

Policy Compliance

1.8 It is the responsibility of all employees, partners, elected members, contractors, 3rd party suppliers, site visitors or anyone working for or on behalf of the Council to comply with this policy.

1.9 Failure to comply with this policy may result in disciplinary action being taken, which could result in dismissal or for 3rd parties' breach of contract.

1.10 If you suspect that someone has breached this policy, please follow the Security Incident Response policy and procedure.

Policy Review

1.11 This policy will be reviewed every two years or as and when required.

Exceptions

1.12 Exceptions to this policy must be requested in writing to the ICT Service Desk, in the first instance and will be based on consideration of the business risk.

2. Information Asset Management

2.1 Information Assets (IA) are those that are central to the efficient running of departments within the Council, for example, service user information, social care information, card holder data, health information, commercial documents, finance information, staff files etc.

2.2 Physical assets include the computer systems, network hardware and software, which are used to store and process this data. It also includes physical assets, such as, infrastructure, equipment and accommodation used for data processing.

2.3 The Information Asset Register (IAR) must be used to record information assets and the Configuration Management Database (CMDB) to record physical assets.

2.4 Information Assets must have an Information Asset Owner (IAO). Responsibility for the day-to-day management may be delegated to the Information Asset Controller (IAC), although accountability must remain with the nominated IAO of the IA. This must be recorded in the IAR.

Information Governance Assurance Roles

2.5 The following table summarises the Information Governance structure:

Structural Model	Harrow Council
Accounting Officer	Chief Executive
Senior Information Risk Owner (SIRO)	Corporate Director of Resources and Commercial
Caldicott Guardian	Head of Safeguarding Assurance and Quality Services
Information Asset Owners	Corporate Directors / Divisional Directors
Information Asset Controllers	Head of Service / Service Managers

2.6 As well as the designated roles defined below, the governance and safeguarding of Information Assets is the responsibility of all employees and 3rd parties.

Role	Key Responsibilities
Accounting Officer (Chief Executive)	• Has overall responsibility to ensure that information risks are assessed and mitigated to an acceptable level.
Senior Information Risk Owner (SIRO)	• The SIRO is the Information Governance Lead with delegated authority from the Chief Executive. The SIRO provides assurances to the Chief Executive on the controls and procedures for assessment and management of information risk within the Council. The SIRO chairs the Council’s Information Governance Board (IGB).
Information Governance Board (IGB)	• IGB is represented by senior management across the Council to provide support and clear direction for information governance and security at the mangement level.

Role	Key Responsibilities
Caldicott Guardian	• Has specific responsibility for protecting and defining the circumstances in which social care and patient identifiable data can be legitimately shared with other Council departments and outside agencies.
Information Asset Owner (IAO)	• The IAO is responsible for ensuring that information risk is managed appropriately and for providing assurance to the IGB and the SIRO. This will include business continuity plans for information that is deemed critical. • Ensure compliance with the Information Governance and Security Policy.
Information Asset Controller (IAC)	• Provide support to the IAO and are responsible for managing risks to information assets within their respective service area.
Service Delivery Team	• Act as the focus for all information security issues, suggesting policies to mitigate risk, and assisting with their interpretation into team procedures and standards, whilst implementing those aspects affecting the operational security of the Council's information and IT infrastructure.

Information Management

2.7 The management of information will be in accordance with the Information Governance and Security policy and comply with legal requirements.

2.8 All users of Council IA must manage; the creation, storage, amendment, copying, deletion and destruction of information to ensure confidentiality, integrity and availability.

2.9 All users must:

- Create and maintain full and accurate records of all council activities and transactions;
- Organise information by function at point of creation;
- Store and manage information in the relevant centralised service area filing system (such as SharePoint or business systems). Team specific information must not be stored on personal drives, e.g. H: drive or MyFiles;
- Ensure information is accurate and kept up to date;
- Carry out regular reviews and only hold information for as long as necessary and where there is a justified business need to, taking into account requirements or retention, specified legislation, governing regulations and evidential requirements;
- Clearly label the sensitivity of information created and handle information in alignment with the Security Classification, Labelling and Handling guidance.

- Securely dispose of information no longer required,
- Keep information safe, secure and protect against unauthorised access;
- Only use email as means of communication and not for storage;
- Where practicable, make information and records accessible to all Council staff and members of the public, unless there is an explicit business reason for access to be limited.
- When appropriate, carry a Data Protection Impact Assessment (also known as Privacy Impact Assessment) to identify and manage privacy risks related to the collection and handling of personal information for new projects or processes to ensure that it is compliant with privacy, confidentiality and data protection requirements.
- Take precautionary measures to prevent unauthorised disclosure of data through “shoulder surfing” i.e. someone looking over the shoulder to view information that they have no right to read.
- Keep council computers, laptops or any other devices secure and must not leave them unattended or in such a state as to risk unauthorised viewing of information displayed on it.
- Collect personal and sensitive information straightaway when printing. Place any papers found on a printer in the secure waste paper bins.
- Ensure personal and sensitive information is sent by secure email.
- Ensure personal and sensitive information sent via conventional post, is sent by registered or recorded delivery.
- Ensure if personal or sensitive information is sent by fax the ‘Safe Haven’ process is followed.
- Ensure that all individuals are notified in advance whenever voice conversations are being recorded.
- Ensure that only material that is publically available should be published on the Harrow website. Ensure information that forms part of a document, which contains personal and sensitive information, is redacted prior to publication.
- Ensure that if information has been redacted, it cannot be reversed.

3. Information Retention and Disposal

3.1 Information and records must only be kept for as long as there is a justified business need, taking into account any retention restrictions or requirements specified by legislation, governing regulations or evidential requirements.

3.2 The length of time information must be kept for before disposal must be documented in an information retention and disposal schedule.

3.3 Information Asset Owners will be responsible for ensuring compliance with the information retention and disposal schedule and ensure that documented procedures for the disposal of information are in place.

3.4 Automated tools should be employed, where possible, to purge or archive information as necessary. Where this is not possible, manual procedures must be in place.

3.5 Purging of information must be carried out in accordance with HMG IA Standard No.5 and must be authorised by the Information Asset Owner, Information Asset Controller or delegated Officer(s).

3.6 All electronic storage media information must be destroyed in accordance with HMG IA Standard No.5.

3.7 All paper documents that contain personal and sensitive information must be destroyed in line with EN15713:2009 standards for secure destruction and in line with appropriate security shredding standards. The Council provides secure paper waste bins for the disposal of all paper documents.

3.8 Information that is of short-term value and has no operational or evidential value can be disposed of in the normal course of the day-to-day business once they have served their primary purpose. Authorisation for this type of information is not required.

3.9 Any Partner or 3rd Party providing a service for the disposal and destruction of information (electronic or paper) or any obsolete equipment must be able to demonstrate compliance with Harrow Information Governance and Security Policies. A Service Level Agreement must be in place, prior to commencement of the service and must meet defined standards.

3.10 Further guidance on information retention and disposal schedules can be found on the hub.

4. Security Classification and Handling

4.1 Security classifications indicate the sensitivity of Information Assets (in terms of the likely impact resulting from compromise, loss or misuse) and the need to ensure they are appropriately protected against possible threats.

4.2 Security classifications must be applied to any asset that has value to the Council.

4.3 There are three levels of classification provided by the Cabinet Office, OFFICIAL, SECRET, and TOP SECRET. However, the Council will only use OFFICIAL.

OFFICIAL Classification

4.4 The Council will classify all information as OFFICIAL, which includes information in any form that has intrinsic value and requires an appropriate degree of protection, which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened security threat profile.

4.5 There is no requirement to mark routine OFFICIAL information.

4.6 In addition, the Council will adopt two caveats, PUBLIC and SENSITIVE, to be used as handling guidance with the OFFICIAL classification.

OFFICIAL-PUBLIC Caveat

4.7 The PUBLIC caveat should be used if the information is fit for public consumption i.e. any information that could reasonably be made available to the public.

OFFICIAL-SENSITIVE Caveat

4.8 A subset of OFFICIAL information, which could have more damaging consequences (for the individual and/or the Council) if it were lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification tier, but may attract the additional SENSITIVE caveat to reinforce the ‘need to know’.

4.9 The SENSITIVE caveat should be used if the information contains sensitive information (personal or commercial) that would cause threat or significant harm or distress to an individual or the organisation, if disclosed inappropriately.

Examples of this type of information include:

- Sexual abuse cases, domestic violence cases, social care cases, disciplinary files etc.
- Borough or wider civil contingency plans or information obtained in relation to anti-terrorist activity and/or planning but excluding general emergency plans or strategies.
- Commercially sensitive documents where the release of the information could significantly prejudice the Council or 3rd party commercial interests.
- Information about 1000 or more identifiable individuals (other than information sourced from the public domain).
- Configuration details relating to the controls of networks and/or network defences that may facilitate further attack.

4.10 In such cases where there is a clear and justifiable requirement to reinforce the ‘need to know’, information assets should be conspicuously marked: ‘OFFICIAL–SENSITIVE’.

4.11 All individuals are responsible for identifying any sensitive information within this category and marking the information appropriately.

4.12 Information Asset Owners and Information Asset Controllers must ensure that appropriate processes and procedures are in place to it is securely handled, reflecting the potential impact from compromise or loss and in line with any specific statutory requirements and the Council's Information Governance and Security policies.

4.13 Access to OFFICIAL-SENSITIVE information must ONLY be granted based on a genuine, 'need to know' basis and must have the appropriate security clearance to handle that type of data. .

4.14 If there is any doubt about providing access to OFFICIAL–SENSITIVE assets, individuals should consult their managers or contact the Council's Information Governance Manager before doing so.

Document/Asset Handling and Marking

4.15 All information must be safeguarded and protected, irrespective of whether it is labelled or not. OFFICIAL-SENSITIVE information will require additional security controls and protection.

4.16 A collection of sensitive documents or assets must carry the highest marking contained within it. For example, a case file or an e-mail string containing OFFICIAL and OFFICIAL–SENSITIVE material must be covered by the higher marking (i.e. OFFICIAL–SENSITIVE).

4.17 When creating documents with OFFICIAL–SENSITIVE information, the classification must be in CAPITALS at the top and/or bottom of each page. Consider separating the sensitive information into appendices, so the main body can be distributed widely with fewer restrictions.

4.18 Sensitive material published on the Council's intranet must also be clearly marked.

4.19 Where practicable, time-expiry limits should be considered so that protective controls do not apply for longer than necessary, this is particularly the case for embargoed material intended for general release and only sensitive until it is published, e.g. official statistics.

4.20 Whilst the presence or absence of a classification marking is not in itself a deciding factor as to whether an exemption is engaged, it may be a helpful indicator that one is applied.

4.21 Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOIA) may apply. However, it must be noted that each FOI request must be considered on its own merits and the classification in itself is not a justifiable reason for exemption.

4.22 Information Assets received from or exchanged with external partners must be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

4.23 Further guidance on security classification and how to handle information can be found on the hub.

5. Freedom of Information Act 2000 and Environmental Information Regulations 2004

5.1 Harrow Council is fully committed to the requirements of both the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR). The legislation promotes a culture of openness and accountability across the public sector, but also sets out exemptions from that right.

5.2 The legislation gives individuals a right to request any recorded information held by, or on behalf of, the Council. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. It does not apply to information, which the Council only holds on behalf of another person or organisation.

5.3 The FOIA does not give people access to their own personal data (information about themselves). If an individual wants to see information held about themselves, they should make a subject access request under the Data Protection regulation.

5.4 The Council aims to respond to requests promptly and in any event, within the statutory response period of 20 working days following receipt of a valid request. To ensure that the Council can fulfil its obligations individuals should respond to internal requests for information within the timescales given. Responding to information requests is a corporate and shared responsibility.

A valid request for information under the FOIA must:

- be in writing,
- include the requesters real name,
- include address for correspondence (postal or email) and
- describe the information requested.

5.5 The Council is obliged to disclose information requested under the FOIA, unless an exemption applies. Exemptions will be applied, where appropriate to ensure information that is not suitable for publication, is protected.

5.6 The Council can charge a fee in accordance with the Fees Regulations for FOIA requests.

5.7 The EIR allow public authorities to charge for making environmental information available, but any such charge must be reasonable. EIR requests can be made verbally or in writing, but the Council should maintain a record of all requests made.

FOIA and EIR Roles and Responsibilities

5.8 The designated FOIA and EIR roles are defined below:

Role	Key Responsibilities
Director of Legal and Governance Services (Monitoring Officer)	• Overall responsibility and accountability for ensuring compliance with the FOIA and EIR and escalating issues to the Corporate Strategic Board (CSB).
Corporate/Divisional Directors (Information Asset Owners)	• Responsibility and accountability for ensuring compliance with the FOIA and EIR within their Directorate. • Approval of responses.
Business Support Team (Resources and Commercial FOIA and EIR Champions)	• Allocation of FOIA requests to the relevant Service Area. • Responsible FOIA and EIR system support (liaising with the 3rd Party on current issues including system upgrades). • Housekeeping of the system (including starters/leavers/training). Providing management information and performance reports (checking overdue cases and unassigned cases).
All FOIA and EIR Champions	• Management and co-ordination of responses for their directorate to ensure the request is satisfied within 20 working days (including Subject Access Requests made under the Data Protection regulation). • Providing management information and performance reports related to their directorate. • Publication of responses to the Disclosure Log. Personal details (e.g. requester name and contact details) must be redacted before information is published. • Co-coordinating and responding to internal reviews and complaints from the ICO.
All Employees	• All employees are responsible for ensuring that any internal requests for information they receive are responded to within the timescale given. • Requests for information received should be sent to harrow@icaseworkmail.com, for processing by the FOIA and EIR champions.

Internal Reviews

5.9 Applicants wishing to ask for an internal review must do so within 40 working days of the date of the Council's response to their request.

5.10 Internal reviews should be sent to the Council's FOIA Champion. The FOIA Champion will be responsible for managing and co-ordinating the internal review. The review should be handled by a Senior Manager who was not involved with the original decision to assess whether or not the request was handled appropriately, in line with the requirement of the FOIA.

5.11 The Council aims to respond to internal reviews within 20 working days of receipt. All internal reviews and responses must be recorded in the FOIA logging system.

5.12 Complaints from the ICO should be sent to the Council's FOIA Champion, who will be responsible for managing and co-ordinating the response. The Information Governance Manager should be informed of any complaints from the ICO.

Complaints from the ICO

5.13 Complaints from the ICO should be handled by a Senior Manager who was not involved with the original decision to assess whether or not the request was handled appropriately, in line with the requirement of the FOIA.

5.14 The Council must respond within the timescales given by the ICO. All ICO complaints must be logged in the ICO Complaints Register.

ICO Publication Scheme

5.15 The Council will maintain a comprehensive ICO Publication Scheme that provides information, which is readily accessible. The Council aims to publish as much information as it can, both proactively and in response to requests under the FOIA.

5.16 Harrow Council's ICO Publication Scheme is available via the Council's website and is reviewed and updated on an annual basis to ensure the information contained within it is adequate, relevant and up to date.

Copyright and Re-Use of Public Sector Information (RPSI)

5.17 Where documents are created or modified require copyright protection or distribution restriction under the Freedom of Information Act, they will be marked as 'Copyright Protected'.

5.18 Where information and datasets are made available in response to a FOIA, in the ICO Publication Scheme or under the Open Data and Transparency initiative, the Council must, so far as is reasonably practicable, make it available in a re-usable, electronic form and permit the re-use of information, under the Open Government Licence (OGL).

Open Data and Transparency Code

5.19 The Council has an obligation to publish a range of information and is committed to complying with the Open Data and Transparency initiative.

5.20 The Council will be open and transparent and will continuously review the data sets made available, with a view to increasing the amount of information made available and the frequency with which it is published. Data set owners across the Council will be responsible for ensuring that data sets are up to date and published according to the guidelines and frequency set.

6. Data Protection

6.1 The Council is fully committed to compliance with the requirements of data protection laws and regulation.

6.2 The Council will follow procedures to ensure that all employees, partners, 3rd party suppliers, contractors, elected members, site visitors or anyone working for or on behalf of the Council, who have access to any personal data held by, or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under these laws and regulation.

6.3 The Council will:

- Observe fully conditions regarding the fair collection and use of personal information;
- Specify the purpose for which the Council will use personal information;
- Collect and process personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure that the personal information it processes is accurate and up to date;
- Apply checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of the individuals (Data Subjects) about whom the information is held can be fully exercised under the data protection regulation (this includes responding to Subject Access Requests within 30 calendar days);
- Ensure there is an officer with specific responsibility for data protection within the Council and identify designated officers (Information Asset Owners) within all Directorates;
- Ensure that the Council is registered with the Information Commissioner's Office (ICO) as a Data Controller and must notify the ICO to renew the registration on an annual basis.

6.4 All partners, 3rd parties or contractors of the Council must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities. Any breach will be deemed as being a breach of contract between the council and that individual, company, partner or organisation;
- Allow data protection audits by the Council of data held on its behalf (if requested);
- Indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages.

6.5 All employees will take steps to ensure that personal information is kept secure at all times against unauthorised disclosure and all breaches of the data protection laws and regulation must be reported. See Security Incident Response Policy.

7. Privacy Impact Assessment (Data Protection Impact Assessment)

7.1 A Privacy Impact Assessment (PIA), also known as Data Protection Impact Assessment (DPIA) should be conducted to identify and manage privacy risks related to the collection, handling and storage of personal information to ensure that it is compliant with privacy, confidentiality and data protection requirements.

7.2 A privacy risk is the risk of potential harm, damage or distress to an individual arising through the use or misuse of personal information. The risk can arise through personal information being:

- Inaccurate
- Excessive or irrelevant
- Kept for too long
- Disclosed to unauthorised person(s)
- Used in ways that are unacceptable to or unexpected by the person it is about
- Not kept securely

7.3 The PIA should be conducted for a new project or any change to an existing system or process regarding the handling of personal information; it includes obtaining, recording, holding/storing, disclosing, transmitting or disseminating personal information.

7.4 A PIA should be started at the initiation stage and before any systems or applications have been procured, or before any new processes are implemented or existing processes changed. This is to ensure that privacy risks can be identified and appreciated before they are executed into the project design. Privacy implications should be considered at each phase of the project life cycle.

7.5 The Project Manager (or delegated officer) should conduct the PIA with involvement from other team members.

7.6 Further guidance on completing a PIA can be found on the hub.

8. Pseudonymisation and Anonymisation

8.1 Personal data should be pseudonymised or anonymised, where possible.

8.2 Pseudonymisation is the processing of personal data which can no longer be attributed to a specific data subject without the use of additional data (which must be kept separately with appropriate security controls in place) to ensure that personal data is not attributed to an identified or identifiable person.

8.3 Anonymous data is information that is not related to living person and cannot be traced back to an individual.

8.4 Further information can be found on the ICO website.

9. Cloud Security

9.1 The use of cloud based services, must comply with this policy.

9.2 Services Areas responsible for engaging Partners and/or 3rd Party to provide cloud hosted/managed services must ensure that they conform to the NCSC cloud principles and the Council's Architectural Standards document.

10. Third Party Code of Connection

10.1 Employees responsible for engaging Partners and 3rd Party Data Processors/Controllers must ensure that the services provided by the 3rd Party are from reputable and appropriately assessed companies. These companies must operate in accordance with quality standards, which should include a suitable Service Level Agreement.

10.2 Only authorised persons may engage Partners and 3rd Parties, following the implementation of appropriate information security and commercial controls.

10.3 Partner and 3rd Party connection to Harrow Council network is only permitted where the proper authentication and authorisation controls have been applied and the risk posed by the 3rd Party has been assessed, using the 3rd Party Minimum Security Standards Code of Connection document. A Code of Connection agreement is required between the Council and the 3rd Party before any access is permitted to the Council network.

11. Information Sharing

11.1 When sharing information with Partners and 3rd Parties a non-disclosure, Information Processing or Information Sharing Agreements must be used in all situations where the confidentiality, sensitivity or value of the Council data being disclosed or shared contains personal information.

11.2 Where there is a business reason for granting a Partner or 3rd Party access to Council systems or data a formal risk assessment should be carried out, to determine the security implications and control requirements.

11.3 The security controls determined from all risk assessments of Partners and 3rd Parties will be incorporated within any contractual agreement, with relevant penalties for breaches of these controls and requirements.

11.4 All Partners and 3rd Parties engaged will be expected to adhere to the Harrow Council Information Governance and Security Policies.

11.5 An appropriate summary of, or copy of, the relevant Information Governance and Security Policies must be formally delivered to 3rd Parties and updated periodically to the 3rd Parties.

11.6 Prior to sending information to 3rd Parties, not only must the intended recipient be authorised to receive this information, but the procedures and information security measures adopted by the 3rd Party, must be seen to continue to assure the confidentiality and integrity of the information to at least the same level applied within the Council.

11.7 Personal and/or sensitive information shared must always be transmitted using an approved encrypted process.

11.8 Information sent by employees to 3rd Parties must be approved by authorised persons. Email addresses and faxes sent by employees must be checked carefully prior to dispatch, especially where the information is considered to be of a personal and sensitive nature.

11.9 Further guidance on information sharing can be found on the hub.

12. Security Incident Response

12.1 Managers are responsible for controlling employee access to the Council's network and systems as well as for ensuring that staff are aware of the threats, and trained in the safeguards, to reduce the risk of security incidents and breaches.

12.2 A security incident is an alert to the possibility that a breach of security may be taking, or may have taken place. A security breach is where a system, service, organisational policy, legal requirement or policy regarding information security has been contravened. However, any incident that suggests that the Confidentiality, Integrity and/or Availability of the information have been inappropriately changed can be considered a security incident. Every suspected security breach will be treated as a security incident, only if confirmed does it become a security breach.

12.3 Any information security incidents or breaches must be reported immediately to the ICT Service Desk on ext. 2000, direct dial, 020 8424 1000, or by emailing ICT Service Desk (ssc.harrow.servicedesk@soprasteria.com). Any personal and sensitive information related to the security incident or breach must not be given to the ICT Service Desk. The Security Incident Reporting form will be sent to be completed.

12.4 The line manager is responsible for investigating and resolving any suspected or actual security breaches. They must respond rapidly but calmly to the information security incident and should:

- Liaise and coordinate with colleagues to gather information and offer advice to contain the incident or breach.
- Ensure that the service area has identified all those affected by unauthorised access / data loss and a course of action agreed and noted on the reporting form. Where no further action is taken, this should also be indicated.
- ensure that specific risks associated with an incident are noted and actions planned recorded so that all identified risks are thoroughly addressed.
- ensure that the impact of each incident is recorded and follow on actions planned so that all individuals/ teams/ systems affected are dealt with accordingly.
- take action that will avoid, or reduce the impact or probability of a further similar occurrence.
- provide sufficient evidence to confirm that actions agreed upon have been completed.

12.5 The completed form and evidence must be sent to the informationgovernance@harrow.gov.uk email account.

12.6 Incidents and Breaches will be recorded in the Security Incidents and Breaches Register and quarterly reports will be provided to the Senior Information Risk Owner (SIRO), via the Information Governance Board (IGB).

12.7 Internal Audit will provide assurance to the Information Governance Manager to ensure that the incidents have been satisfactorily processed and investigated. The Senior Information Risk Owner (SIRO) will approve closure and sign off resolved incidents.

12.8 All information security incidents must be evaluated according to their particular circumstances, and this may require various departments to be involved, such as IT, Human Resources, Legal and the owners of information. If it appears that disciplinary action against a member of staff is required, this must be handled with the assistance of HR.

12.9 Any complaints should be sent to the Council's Corporate Complaints Manager (complaints.eforms@harrow.gov.uk) who will be responsible for managing and co-ordinating the response, within the ICO timescale and logged in the ICO Complaints Register.

12.10 Security breaches caused knowingly, by reckless behaviour, or non-compliance with information governance and security polices including the non-reporting of an incident, may result in disciplinary action.

13. Password Security

13.1 Passwords are an essential part of authentication to systems and services. The selection of passwords, their use and management as a means to control access to systems must strictly adhere to security best practice guidelines.

13.2 To prevent unauthorised access to systems and accountability is maintained, passwords (including PIN numbers and tokens) must not be shared between staff under any circumstances. This includes IT staff, managers, partners and 3rd parties.

13.3 Passwords must never be written down, on paper or in electronic form and must not be re-used between work and home.

13.4 Where passwords need to be recorded, specialist password management software must be used that facilitate password protected encrypted storage. All storage files from such tools must be appropriately backed up.

13.5 User passwords must be changed at regular intervals, and should be chosen privately by the individual users.

13.6 Any one time passwords (for initial logon) issued by system administrators should not be common or include easily guessed dictionary words. When the user initially logs on they should be prompted to change this one time password immediately.

13.7 Password changes must be forced by implementing an expiry period after which a user’s password will not be accepted, and the next attempt to log on by that user will result in a security message displayed to the user.

13.8 All user accounts and passwords must be disabled by system administrators after 30 days of continuous inactivity, and failing the production of business justification for the period of inactivity.

13.9 All default passwords must be changed before deployment of equipment, applications and software, paying particular attention to essential infrastructure devices. Regular checks must be carried out to check for default passwords.

13.10 Information systems must be resistant to automated brute force attacks and account lockout mechanism must be activated after five failed attempts or a fixed amount of time.

13.11 Users must not use easily guessable dictionary passwords to access systems. Where technically feasible systems must contain a list of such prohibited passwords and prevent their use for all users.

13.12 Following any systems or communication failure, users must be prompted to re-authenticate.

13.13 The possession and use of password sniffing tools and other hacking tools are forbidden on unless they are used during a legitimate security scan/testing exercise. Such use must have the prior approval of the Council’s Security and Compliance Manager and have been recorded as part of a Change Request for approval by Harrow Council.

13.14 Any password transmitted over any communication channel must be encrypted. Passwords must be stored in cryptographically hashed (irreversibly encrypted) form.

13.15 System passwords must conform to the following standards:

Passwords

- Minimum password length of 8 characters
- Use a combination of three random words
- Must contain at least one of each of the following:
  - Numeric character – (0-9)
  - Uppercase character – (A-Z)
  - Lowercase character – (a-z)
  - Special character (?, @, #, %, !, £, $)
- The password characters must not be visible when entered
- Must be stored in irreversibly encrypted form: Unix systems must use password shadowing
- Password cannot be the same as or derivation of username
- System forces a minimum password age of 1 day
- System does not allow re-use of last 10 passwords
- Time of last logon will be displayed to the user when they logon
- All user-level passwords must be changed at least every 90 days

In addition, for Administrator passwords

- Minimum length of 15 characters
- Must use different passwords for their administrative and non-administrative accounts
- Administrator privileges must not be granted routinely to standard users
- All administration-level passwords (e.g. root, Windows admin, database admin, application admin etc.) must be changed every 30 days
- System does not allow re-use of last 24 passwords

Technical Controls

- Where technically possible, account lockout duration is 30 minutes.
- Where technically possible, account lockout threshold is 5 invalid logon attempts or less.
- Where technically possible, reset account lockout counter after 30 minutes
- Devices must auto lock after 10 minutes or less of user inactivity.

13.16 Passwords should be changed immediately whenever they have been compromised or on an indication or suspicion of a compromise. Any password compromises should be logged as a security incident as per the Security Incident Response Policy.

13.17 Any failure or technical inability to meet the above standards must be reported to the Council's Security and Compliance Manager for risk assessment.

14. Removable Media

14.1 Only authorised removable media devices will be permitted to be attached to Council endpoint devices.

14.2 All removable media must be encrypted prior to any data or information being stored.

14.3 Bulk transfer of any highly personal or/and sensitive data (regardless of encryption controls) must not be transferred on to any removable media unless there has been written approval from the Information Asset Owner.

14.4 Requests for access to use removable media devices must be made via the ICT Service Desk.

14.5 All removable media must be disposed of securely using the Council's approved secure disposal service.

14.6 Staff must make every effort to protect any removable device from loss, theft, damage.

14.7 The following data is not permitted to be transferred onto Harrow systems from a removable media device:

- Data not related to the Council's business purposes
- Illegally sourced copyrighted material and any copyrighted material, which is prohibited from being copied
- Non approved applications or programs, or not covered by an appropriate licence

14.8 When an employee becomes aware that a removable device has become lost or stolen, they must follow the Security Incident Response Policy.

15. Personnel Security

15.1 There must be a secure procedure for screening and verification of new employees and a vetting procedure for more sensitive job positions.

15.2 In addition, employees (including Partners and 3rd Parties) may be required by the Council to undergo a background check e.g. Baseline Personnel Security Standard (BPSS) check.

15.3 Further vetting of employees is required where they will be employed in positions where they:

- Work or be exposed to child protection systems and data
- Have access to secure areas (e.g. server rooms, servers, mailroom etc.)
- Come into contact with bulk amounts of sensitive financial information (i.e. payment card details) or negotiable items.
- Require access to secure Public Sector Network (PSN systems/services and PSN derived data, N3 network, GCSx mail etc.)

15.4 Upon notification of staff resignations, or movements, the line manager responsible for the staff member resigning, must notify the appropriate personnel, this will include:

- Human resources and/or recruitment agency, local site security (if staff member is office-based and has been granted staff access to Harrow buildings)
- The ICT Service Desk for removal of systems accounts

16. Risk Management

16.1 A risk methodology, aligned to the ISO/IEC 27001 standards must be defined, documented and implemented to manage business information security risks. This risk methodology should not be seen as a replacement for the existing Harrow Council ISMS and risk management methodology but should be complimentary.

16.2 The supplier and Council's Security and Compliance Manager must produce the following information security risk management documentation and keep it up to date:

- Information Security Risk Register
- Information Security Risk Treatment Plan and methodology commensurate to ISO27001 standards

16.3 The information security risk methodology must incorporate the following elements:

- Identification of critical business assets
- Identification of threats
- Identification of vulnerabilities
- Business impact assessment
- Estimation of probabilities of threat agents exploiting vulnerabilities
- Determination of business security risk levels
- Recommendation of suitable business security controls
- Comparison with existing controls to identify areas of remedial risk

16.4 The supplier and Council's Security and Compliance Manager will commission or carry out information security risk assessments on an annual basis. This will enable the business to review the information security strategy and update policy where necessary.

17. Disaster Recovery and Business Continuity

17.1 The Council's Senior Management Team must initiate Disaster Recovery (DR) and/or Business Continuity (BC) plans, including Emergency Response plans. The DR or BC must be initiated and formally approved and committed to by the Council.

17.2 The Head of Emergency Planning and Business Continuity is responsible for preparation, maintenance and regular testing of BC plans to ensure that damage done by possible internal or external attacks can be minimised and that restoration takes place as quickly and efficiently as possible.

17.3 The Head of Emergency Planning and Business Continuity must undertake an annual formal risk assessment through a business impact analysis in order to determine the requirements for the BC plan.

17.4 The DR Service and BC plans must be periodically tested to ensure that the management and staff understand how it is to be executed.

17.5 All staff must be made aware of the DR and BC mechanisms for their respective roles.

Further information can be found in the Business Continuity Management Strategy and Policy.

18. Encryption Policy (Secure Transmission of Data)

18.1 Data that contains personal and/or sensitive information must be transmitted in encrypted form using current encryption technologies. Prior to transmission, consideration should be given to the procedures to be used between the sender and recipient.

18.2 Proprietary encryption algorithms must never be used to protect personal and sensitive data.

18.3 All encryption keys must be protected against both disclosure and misuse and key management procedures must be fully documented and implemented, where applicable.

Encryption of data in Transit

18.4 Cryptographic controls should be applied to data transmitted over networks in accordance to its security classification. The level of security controls applied to the network must at least match the highest level of classification of the data being transmitted.

18.5 Cryptographic controls such as Transport Layer Security (TLS) and Internet Protocol Security (IPSEC) must be used to safeguard personal and sensitive data during transmission over un-trusted or non-dedicated communications channels. A minimum key length of 128-bits will be used and a current secure version of the protocol must be used (i.e. HTTPS, SSL, TLS, etc.).

18.6 Any password transmitted over a network must be encrypted or one way hashed.

Encryption of data at rest

18.7 All managed mobile endpoint devices must have an approved full disk encryption product installed to prevent the compromise of confidentiality, in case of device theft or loss.

18.8 The confidentiality of encrypted data must be assured wherever it is copied or transferred to other storage media. Data backups will maintain at least the same level of encryption applied to the original source.

18.9 Where payment card information is used, only the minimum elements of the cardholder data should be stored. This data should also be encrypted where required under the PCI DSS standards.

19. Application Development

19.1 Application security requirements should be formally defined at the requirements gathering phase for all application development. A Privacy Impact Assessment (also known as Data Protection Impact Assessment) should be carried out if the application will collect or store personal data.

19.2 Best practice should be applied to any application development processes and supporting tools, this applies to both internal and 3rd Party application development.

19.3 Applications must be developed based on industry best practices and include information security throughout the software development life cycle. Development must confirm to NCSC Application Development guidance.

20. IT Infrastructure

20.1 Where the risks associated with a project or major installation warrant it, information security requirements and associated testing plans shall be defined and agreed with responsible personnel, formally included in any project plan and circulated to all interested parties, well in advance of installation. The security requirements shall be a formal element of the operational acceptance criteria.

20.2 Access to the infrastructure resources shall be controlled under the Principle of Least Privilege with privileges allocated specific to business need in accordance with Logical Access Control Policy.

20.3 All business-critical and payment card infrastructure systems shall record system events and reviewed in accordance with Security Audit and Monitoring Policy.

20.4 Systems shall have anti-virus protection in accordance with Anti-virus and Malware Policy.

20.5 Documentation shall be provided sufficient to recreate the functionality of any infrastructure system; this shall include references to relevant technology security standards.

20.6 Prior to being loaded with live data or being deployed into production, systems shall:

- Have all development tools and utilities removed that may pose a security risk.
- Be hardened with only those services enabled, that are required for system to function correctly with all other associated communication protocols and logical ports disabled.
- Have any unnecessary physical external interfaces controlled by security software and configuration settings, or devices disabled wherever they pose a security risk (e.g., CD/DVD drive, USB port, Firewire port, Infrared, Wireless Networking and Bluetooth etc.).
- Be configured in accordance with all relevant technology security standards in line with industry best practice. Partners and 3rd Party suppliers shall be expected to meet these standards or adopt and maintain equivalent documented security standards for the systems they manage on behalf of the service.

20.7 The IT infrastructure shall be designed and configured to deliver the availability and reliability needs as defined by the business in accordance with Disaster Recovery and Business Continuity Policy.

20.8 There shall be a formal process whereby the supplier's and Council's Security Managers receives and instructs BAU teams to act upon new security update (patches) notifications. An assessment will be made on all patches and communicated to the relevant teams as necessary.

Patch installation deadlines shall be firstly governed by the below table but also directed by the Council's Security and Compliance Manager based upon the criticality rating of the patch (e.g. emergency) and the relevance and business risk of the associated vulnerability. The installation timetable for relevant patches is defined in the table below. Where this is not achievable compensating controls will need to be agreed with Council's Security and Compliance Manager.

20.9 Patches should be tested in non-production environments where possible before being deployed into production.

Type of Patch	Patch Deployment Targets (after notification)		
	Critical	Moderate / Important	Low / Other
All Public Facing Operating Systems and Applications (this includes but is not limited to databases, servers, switches, routers and all other network infrastructure).	14 days	30 days	60 days
3rd Party Staging Infrastructure Operating Systems and Applications (this includes but is not limited to servers, switches, routers and all other network infrastructure).	14 days	30 days	60 days
All other operating systems, applications and databases (this includes but is not limited to servers, switches, routers and all other network infrastructure).	14 days	30 days	60 days
Antivirus signature updates	immediately	immediately	immediately

20.10 All system security configuration changes shall be under formal change control and give consideration to testing and fall-back procedures. To ensure associated security risks can be identified and planned for, all changes shall be assessed by the supplier's and Council's Security Managers.

20.11 System security housekeeping schedules shall be formally planned, approved and documented.

20.12 All business-critical data on IT systems shall be backed up to meet the continuity requirements as defined by the business and in accordance with Backup and Archiving Policy.

20.13 The physical location of sensitive or critical infrastructure systems shall be resistant to unauthorised access and tampering in accordance with Backup and Archiving Policy.

20.14 Systems shall be securely purged of all stored data before they are removed from service.

Server-specific Security

20.15 Systems should implement only one primary function per server (e.g., web, database, and DNS should be implemented on separate servers).

20.16 Servers shall encrypt stored data based on its sensitivity in accordance with Encryption Policy.

Personal Computing-specific Security

20.17 Unless a genuine business reason exists for doing so, Council data shall not be stored on the local fixed location workstation hard drives; instead such data shall be committed to an appropriate network location or line of business system.

20.18 All mobile computing systems shall employ storage encryption in accordance with Encryption Policy.

20.19 Personal endpoint devices (unmanaged devices) are not permitted to connect to any part of the Council network.

Network Infrastructure-specific Security

20.20 The network topology shall be documented in at least a diagram, which shall be kept up to date by the supplier.

20.21 All Firewall rule sets shall be documented including the business justification (reason) for each rule as noted in the change record.

20.22 Cryptographic controls shall be applied to personal and sensitive data transmitted over all networks in accordance with Encryption Policy.

20.23 Routing Design shall enable, so far as is feasible, to limit personal and sensitive information to the sections of the infrastructure which are authorised to carry them.

20.24 Precautions shall be taken to limit the effectiveness of unauthorised password and network ‘sniffers’.

20.25 The security risks associated with network cable/port exposure and inappropriate cable routing shall be reviewed during any installations, moves or changes to premises.

20.26 Network cabling infrastructure shall be labelled and recorded to aid its identification and purpose.

21. Logical Access Control

21.1 Access controls shall be designed into systems in accordance with the Principle of Least Privilege and enforce separation of duties.

21.2 In order to strike an appropriate balance between the need to minimise risk and allow business activities to be carried out without undue hindrance, system access controls shall be designed in accordance with the value and classification of the information assets being protected.

21.3 Data directories, file structures and application functions shall be established in consultation with the Information Asset Owner or Controller of the information system. User's access shall be restricted and controlled to limit the potential for unauthorised information disclosure (confidentiality) or modification (integrity).

21.4 Systems should enforce the automatic closure of administrative user sessions after 15 minutes of inactivity, this includes local console access.

21.5 Systems shall enforce role based access control model. User permissions shall be based on pre- approved role templates from which a minimum set of permissions necessary to perform the related business function, are inherited. In order to ensure the permissions for each role are set at a level that is fit for purpose, they shall be designed in consultation with the business owner of the system and be documented in an access control matrix.

21.6 Personal identification and authentication credentials (User IDs and passwords) shall not be shared or disclosed to others (including staff members).

21.7 Partner and 3rd Parties with remote access must inform the Council's system owner whenever a member of their staff leave their employment, where that employee was previously authorised and issued with access credentials to a Council system. Accordingly, the Council's system owner must maintain appropriate procedures to cover Partner and 3rd Party access arrangements including account and credential resetting.

21.8 All employees (including Partners and 3rd Parties) must treat authentication credentials (Passwords, SNMP Community Strings, Personal Identification Numbers (PIN's) and Tokens etc.) as private assets and not disclose these assets to any other personnel.

21.9 System owners must, at the earliest opportunity, change default passwords, including any SNMP Community Strings, installed by vendors at the initial delivery of equipment and software.

21.10 New log in passwords for new users must only be given to that user or in a secure manner to the nominated person. The new log on password must only be allowed to be used once, and must be changed immediately upon first use of the system known only to the receiving user.

22. Network Security Management

22.1 All access to the Council’s network will only be permitted through authorised and approved access points.

22.2 The Council’s network should only permit access to and from authorised sources and must be documented.

22.3 The Council’s network should be segregated where applicable in support of the Council’s regulatory and legislative compliance efforts.

22.4 Design and support teams must maintain an up to date network diagram for the Council and share this with the Council.

22.5 Business critical networks must be designed with appropriate resilience to ensure the availability of the Council’s network

22.6 Network designs must include appropriate controls to ensure the confidentiality, integrity and availability of all the Council’s data.

22.7 Connection of 3rd Party equipment to the Council’s network is prohibited without the prior approval by the Council.

22.8 Network device and firewall logs for the Council’s network should be retained for a minimum of 3 months online and 12 months offline or archived. The minimum details to be logged include user identification, type of event, date and time, event disposition (success/failure), origination of the event, and identity of the name of the affected data, system component, or resource. See Security Audit and Monitoring Policy.

22.9 Access to the Council’s assets must be strictly controlled in accordance with the Principle of Least Privilege and documented accordingly.

22.10 System hardware, operating and application software, the networks and communication systems within the Council’s infrastructure should be adequately configured, patched and safeguarded against both physical attack and unauthorised network intrusion.

22.11 Out-of-band administrative console access should be provided over a secure channel wherever possible.

22.12 All systems and network devices must have system clocks time synchronised using a primary and secondary NTP time source.

22.13 Network devices and firewalls must run current stable operating system IOS versions and a patch routine must be in place to address vulnerabilities in a timely fashion.

22.14 Network and System Administrators must be fully trained and have adequate experience in the wide range of systems and platforms used. In addition, they must be knowledgeable and conversant with the range of Information Security risks, which need to be managed.

22.15 The security of the Council’s network cabling must be reviewed during any upgrades or changes to hardware or premises.

22.16 The Council’s network cabling infrastructure must be actively managed following security best practice, for example:

- Cables must be labelled at each entry and exit point to a riser
- Cables must be labelled on each side of a wall, sleeve or fire break
- Cables must be labelled during installation
- Cables must be laid out in a logical order

- Cabling diagrams must be maintained and up-to-date
- Formal change control must be applied to cabling
- Any unused network wall sockets should be sealed-off and their status formally noted

22.17 Only the Council's Wireless Networks using strong WPA2 network keys are permitted to connect to the corporate LAN, based on NCSC best practice guidance. Wireless networks are not permitted connectivity to any network segments with PCI DSS or GCSx security compliance requirements. All other Wireless Network devices in any guise are not permitted on the Council's estate, without prior review and approval by the Council.

22.18 Switches and Routers will be built, hardened and configured in line with the industry best practice, all unnecessary administrative interfaces and legacy administration protocols must be disabled, including any unused ports. Remote support must be via an encrypted channel.

22.19 All changes to network device and firewall configuration settings must be subject to the formal Change Control procedures.

23. Remote Access Security

23.1 Remote access systems and remote access control procedures should provide adequate safeguards through robust implementation of identification, authentication and encryption controls.

23.2 Remote access to the Council systems, network and resources will only be permitted providing that authorised users are authenticated using 2 Factor Authentication (2FA), data is encrypted across the network, that the remote device is a Council owned/managed device and that privileges are restricted.

23.3 All remote access connections to the Council's network must be logged and log must be kept for 3 months online, with 12 months available offline or archived.

23.4 Remote access authentication credentials and tokens must not be shared or given to anyone else but the named party they were issued to. This includes family members and other staff members. Issued authentication tokens must be made to a single individual and are not intended to be shared resources.

23.5 All devices connecting remotely must be managed. Managed devices connecting to the network remotely must have up to date antivirus software and virus signatures installed and enabled, in addition a personal firewall and end point data control software must be installed.

23.6 Employees (including Partner and 3rd Party contractors) with remote access privileges are only allowed to connect using business owned/managed endpoint devices. 3rd Parties must have a signed Code of Connection (CoCo) in place; remote access must be controlled and only allowed when required.

23.7 Remote access to Council systems by non IT support partners / 3rd Parties must use a Council managed device, for example, housing repairs, clinician access to Frameworki etc.

23.8 Non-business endpoint devices are not allowed to connect to the network and systems.

24. Anti-Virus and Malware

24.1 A centrally managed anti-virus and anti-malware solution must be installed on all endpoint devices (laptops, work stations, servers and other endpoint devices where supported) that connect to the Council's network.

24.2 Anti-virus and anti-malware software must be included in the secure builds for all Council endpoint devices that connect to the Council's network, where this is not possible for example on some UNIX based systems, other compensating controls must be applied.

24.3 All new software must be scanned for viruses and malware before being moved into production or being transmitted or stored on the Council's network.

24.4 Virus and malware signature updates must be obtained from the anti-virus software vendor as soon as available, tested to ensure that a new signature does not negatively impact system infrastructure and must be automatically pushed out to endpoint devices from a centrally managed point in the Council's infrastructure.

24.5 Anti-virus and anti-malware software must be enabled and configured so that it cannot be tampered with on endpoint devices that connect to the Council's network.

24.6 A virus and malware incident response procedure must be in place to facilitate the removal of any infection with minimal disruption. Such procedures must be regularly reviewed and tested.

24.7 System users must take great care when downloading information and files from the Internet to safeguard against both malicious code and also inappropriate material

24.8 Employees, including Partner and 3rd Parties, are not permitted to load non-approved screen savers or software that is not required by the business onto the Council's desktops, laptops and workstations.

24.9 All anti-virus and malware mechanisms current, and actively running, must be capable of generating audit logs and the logging must be effectively configured.

24.10 Anti-virus and malware logs must be retained for a minimum period of 3 months online and 12 months off line or archived.

24.11 All client devices must at a minimum be configured for "On access virus scanning" and all server devices configured for "scheduled virus scanning" with at least weekly scans scheduled on servers.

25. Firewall Security

25.1 Firewall type, size and performance must be chosen according to business requirements in order to ensure they meet availability, integrity and confidentiality business needs. The firewalls must meet the common criteria scheme.

25.2 The physical location of Firewalls must be resistant to unauthorised access and tampering.

25.3 Failover implementations must meet business requirements and be tested to ensure effective resilience.

25.4 Firewalls must have minimal protocols, services running and ports open. Any unnecessary protocols not required by the business must be disabled.

25.5 Firewalls must be security hardened to industry best practice.

25.6 Firewalls must apply state-ful ingress (inbound) and egress (outbound) filtering, applied to control traffic to and from the Harrow network.

25.7 Firewall configurations must be formally documented, securely backed up and be under strict change control. Requests regarding changes to the firewall configuration must be approved by the suppliers Security Manager.

25.8 Firewall logging must be enabled and logs must record 3 months of online event data and 12 months offline or archived. There must be a formal process for secure back up of firewall logs.

25.9 All systems, firewalls and network devices must have system clocks time synchronised using a primary and secondary NTP time source.

25.10 Firewall management should be restricted to the internal Harrow Council network. Management interfaces should also apply secure management protocols and authentication resistant to brute-force attacks. This should be limited to firewall administrators via authentication and firewall administration devices via Access Control List.

25.11 There must be a defined formal process for notification of new patches, secure download and patch testing and implementation.

25.12 The Firewall must have a "warning banner" stating that it is unlawful to enter or attempt to enter the Council's network without proper authorisation.

25.13 The Firewall implementation and rule-set must be reviewed at least annually, in line with industry best practice and any compliance and regulatory standard. Where applicable the Firewall implementation and rule-set must be reviewed every six months to ensure that the rules are implemented and effective in line with PCI DSS requirements.

25.14 Firewall logs must be protected against unauthorised access and tampering.

25.15 Source routing must be disabled to prevent attackers from bypassing the Firewall.

25.16 Firewalls protecting the Council's infrastructure, services and data must be configured and under formal Change Control procedures.

25.17 Where the Firewall is part of the Harrow PCI DSS, PSN or N3 security compliance effort the requirements of the specific standards must be taken into consideration.

26. Security Testing

26.1 Any security testing and the results must be formally documented in a Terms of Reference. The supplier's and Council's Security and Compliance Manager must be included in the sign-off.

26.2 Security testing must only be performed by reputable and trained security professionals who hold relevant qualifications and indemnity insurance.

26.3 The Council's Security and Compliance Manager should be involved in the review of all prospected 3rd Parties to carry out testing. Planned security tests should be accompanied by a proposal document which outlines what tests will be carried out, what data will be used and who will be carrying out the tests. Testing must always be conducted in a controlled manner and must never subvert any business process or business operations.

Operational Systems

26.4 The effectiveness of the Council's security controls should be tested internally at least every 12 months, preferably by an independent party to the Partner or 3rd Party.

26.5 This review must include at least;

- Testing of IT security management
- IT Health Check for the Council's estate (including Penetration Testing)
- Regular internal and external vulnerability scanning
- PCI DSS ASV testing (quarterly)
- Testing must support the Councils PSN, PCI DSS, N3 and other compliance

System Development

26.6 Formal change control procedures must be employed for all amendments to systems. All key system and configuration changes to programs must be properly authorised and tested before moving to the live environment. Such procedures must include provision for backing-out any system amendments should they prove to be detrimental.

New Systems

26.7 Information systems must be fully tested for business logic and processing, prior to operational usage. Where such systems contain information of a personal and sensitive nature, or specific HMG compliance requirements, procedures and access controls must ensure compliance with necessary legislation.

26.8 All equipment and software must be tested and formally accepted by users before being transferred to the live environment. Procedures must be defined for backing-out any equipment or software change should they prove to be detrimental.

26.9 The use of live data for testing new systems or system changes should not be performed. Using live data for testing can compromise its confidentiality, possibly even leading to legal action. Separate realistic test data, expressly created for the purpose must be used for system testing. In particular, personal identifiable data, real bank account and credit card numbers are not to be used for testing or the development of software. Where this is not possible, a risk assessment must be carried out by the Information Asset Owner in conjunction with the supplier.

26.10 All test data and accounts must be removed before new production systems go live.

26.11 All default application accounts, usernames, and passwords must be removed before applications go live.

26.12 There should be a formal review of custom code prior to release to production, to identify any potential coding vulnerability.

26.13 All new internet facing applications should have all custom application code reviewed for common vulnerabilities, or utilise a tool to carry out the secure code review.

26.14 Non production environments should never be accessible or visible from public networks.

26.15 All equipment should be subject to a formal security testing schedule as defined in the following table. All such tests shall be commissioned by or with the approval of the Council's Security and Compliance Manager.

Type Of System	Independent Application and Network Penetration Test	Independent External Vulnerability Assessment	Internal Vulnerability Assessment
Internet facing payment card applications and infrastructure	1 per year plus following any significant functional code change	Every 3 months	-
Internal payment card systems	-	-	Every 3 months
Harrow Infrastructure	1 per year plus following any significant infrastructure change	Every 3 months	Every 3 months

27. Backup and Archiving

27.1 Backups must be selectively tested regularly on a minimum of an annual basis to ensure that the recovery process works properly.

27.2 The frequency of backup operations for business data files and the procedures for their recovery must meet the needs of the business and ensure Disaster Recovery and Business Continuity capability, be fit for purpose, documented and recovery procedures tested on annual basis.

27.3 Safeguards must be in place to protect the integrity of data files during the recovery and restoration of data files, in particular where such files may replace more recent files.

27.4 On site and remote locations where backup data is stored must provide access controls and protection, which reduce the risk of loss or damage to an acceptable level.

27.5 The archiving of information must take place with due consideration for legal, regulatory and business issues with liaison between both the technical and business staff.

27.6 The storage media used for the archiving of information must be appropriate to its expected longevity.

27.7 Storage media must be transported using secure methods.

27.8 Backups should be encrypted where technically feasible.

27.9 Backup retention:

- All backups must follow a 31 day rolling cycle with retention of 31 days. Enabling any file no older than one month to be recovered to a specific day.

- The following systems must also follow a monthly cycle with retention of 1 year. Enabling files over one month old to be recovered to a specific end of month.

    - Network Drives
    - SharePoint
    - Email
    - Security and System Logs

28. Security Audit and Monitoring

28.1 Operating systems must be regularly monitored and all required 'housekeeping' procedures must be performed, in line with NCSC Good Practice Guide (GPG) 13 baseline controls.

28.2 Information systems and business applications must be monitored regularly with all unexpected events recorded and investigated.

28.3 These systems and business applications must be periodically audited with the combined results and history strengthening the integrity of the systems and improving the results of any subsequent investigations.

28.4 All reports must be kept for a minimum of 3 months online and 12 months offline or archived, for all systems.

28.5 All critical systems and equipment must be monitored for security incidents, where applicable.

Audit Logs

28.6 All business critical system audit logs must be sized appropriately and their contents reviewed regularly by appropriately trained personnel, with suspected security discrepancies being reported to the Council's Security and Compliance Manager.

28.7 Under no circumstances must a user deliberately remove, deactivate, clear down or otherwise render system audit logs inoperative in order to conceal present or future unauthorised systems activities.

28.8 All critical system clocks shall be synchronised at least daily from a trusted time source. A single time source should be used.

28.9 Manipulating 'system time' in the system is not allowed, since it may invalidate log contents, which might compromise investigation of security incidents.

28.10 System audit tables (and logs) shall be safeguarded using a combination of automated system access controls and robust procedures.

28.11 The system shall record in an audit table (or log) which will be available for analysis, all significant configuration changes including privileged administrator activities.

28.12 The system shall record in an audit table (or log) which will be available for analysis, all business sensitive system events where available this shall include:

- Actions taken by an individual with root or administrative privileges
- Access to audit trails on systems storing, processing or transmitting payment card data
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialisation and clear down of audit logs
- Creation and deletion of system-level objects
- Transaction Start and end times for transactions that have a financial implication.
- Instances when processes are halted because of security or privilege breaches
- System start-up and stop
- All individual access to cardholder data (if relevant)

28.13 The system shall include the following information for each entry recorded in the audit table (or log):

- User name who performed the action

- Date the action was performed
- Access to and alteration of critical or security data
- Type of event
- Success or failure indication of event
- Origin of event
- Identity or name of affected data system component or resource

28.14 Notwithstanding any legal restrictions to the contrary, system logs should be retained for a minimum of 3 months online, with 12 months available offline or archived.

28.15 System administrators' activities and the use of powerful system utility tools must be audited by independent internal auditors on a regular basis.

28.16 The use of information systems must be monitored regularly with all unexpected events recorded and investigated.

28.17 Each layer within the IT system (Physical, Operating System, Middleware, and Application) must host appropriate monitoring to ensure suitable warnings are generated if their Security Access Structures fail.

28.18 System access and password reset records shall be monitored regularly to thwart attempts at unauthorised access and to confirm that access control standards are effective.

28.19 The log output from infrastructure components will be analysed to detect any abnormal or suspicious activity, which should be reported.

Automated security monitoring technology

28.20 Infrastructure components within the Council's PCI DSS card processing environment, where applicable, will be continuously monitored for suspected or actual information security incidents using a combination of automated Intrusion Detection/Prevention (IDS) and Log Correlation technologies; in accordance with the requirements of the Council and PCI DSS.

28.21 All automated security monitoring technology deployed on systems shall be authorised by the Council's Security and Compliance Manager prior to installation. Where Intrusion Prevention systems are used, consideration shall also be given to ensure they do not introduce a denial of service to the business infrastructure. Systems must be vulnerability tested to ensure they do not create a denial of service situation when under attack.

28.22 The physical location of automated security monitoring technologies shall be resistant to unauthorised access and tampering.

28.23 There must be a formal process for the timely notification and escalation of security alerts.

Expectation of Privacy

28.24 All monitoring is carried out in accordance with all relevant laws and regulations.

28.25 In particular the following should be noted. Interception and recording of information systems (including telephony systems) is permitted for lawful business purposes under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and must take into consideration the Privacy and Electronic Communications (EC Directive) Regulations 2003.

28.26 Lawful business purposes include:

- prevention or detection of crime (including crimes such as fraud as well as infringement of IT-related legislation such as the Computer Misuse Act 1990 or the Data Protection regulation)
- staff training and quality control
- systems maintenance, including ensuring the effective operation of the system (e.g. to protect against viruses or other threats such as hacking or denial of service attacks, to monitor traffic levels, to forward e-mails to correct destinations)
- protection of the organisation's resources
- establishing the existence of facts (for example, to obtain evidence of a business transaction)
- ascertaining compliance with regulatory or self-regulatory practices or procedures relevant to the business (to ascertain whether the business is abiding by its own policies). This includes the investigation or detection of unauthorised use of systems e.g. inappropriate or excessive use contrary to policy
- checking whether or not communications are relevant to the business (e.g. checking email accounts when staff are absent on holiday or sick leave to access business communications)

28.27 Information systems may be monitored and audit logs which record activity are maintained for legal, regulatory and policy compliance as well as system maintenance purposes. Inevitably personal communications may be recorded and monitored as part of this process.

28.28 Conversations where telephony systems are used may often be recorded for lawful business purposes.

28.29 Systems records will be retained in accordance with the Council's Information Retention and Disposal Schedules and where applicable be governed by the Data Protection regulation.