Resources

Isle of Wight Council

Information Security Policy

26th March 2026 / Final v5.4

Document Information

Title:	**Information Security Policy**
Status:	**Final**
Current Version:	**5.4**
Author:	Carl Moreira-Smith, Information Security Manager (Deputy SIRO) ICT & Digital, Corporate Services Carl.Moreira-Smith@iow.gov.uk (01983) 821000 x4654
Sponsor:	Roger Brown, Strategic Manager - ICT & Digital Services ICT & Digital, Corporate Services roger.brown@iow.gov.uk
Consultation:	(01983) 821000 x4694
Approved by:	Cyber Security Strategy Programme Board
Approved Date:	26th March 2026
Review Frequency:	Annually [In addition to Cyber Security Strategy Programme Board continuous review]
Next review:	2027

Version History

Version	Date	Description
1.0	26th June 2008	Final Approved Version
2.0	29th May 2014	Final
2.3	17th August 2015	Final Draft
3.0	11th January 2016	Final
4.0	7th September 2017	Final
4.1	18th October 2019	GDPR amendments
4.2	26th April 2020	Rewrite Draft
5.0	31st July 2020	Final
5.1	29th July 2021	Final
5.2	3rd March 2023`	Final
5.3	30th January 2025	Final
5.4	26th March 2026	Final

Document Status

This is a controlled document. While this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Contents

1 Introduction

1.1 The council holds and manages a great deal of personal and confidential data relating to clients, customers, the public and its employees as well as commercially sensitive information. With consistent changes to both technology and demands supporting ever-easier ways by which information can be accessed and shared it is important that a consistent approach is adopted to safeguard information as a vital asset within the council.

1.2 This policy sets the standards expected to maintain the security of information within the council. Its' implementation will ensure a safe and secure environment for information held both manually and electronically. Particularly that this information is handled in accordance with:

- Data Protection legislation including the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018,
- The PSN Code of Connection,
- Caldicott Guardian principles and related legislation, and
- The NHS Data Security & Protection Toolkit.

1.3 This policy aims to embed the concept of identifying, recording and managing information assets and associated risks within the wider risk management framework and to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the council by:

- Meeting contractual and legal requirements to maintain best practice in information security,
- Meeting standards set through the National Cyber Security Centre (NCSC),
- Introducing a consistent approach to security, by ensuring that all elected council members (hereafter referred to as members) and officers fully understand their own responsibilities and accountability,
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day-to-day business,
- Protecting information assets under the control of the organisation.

1.4 Information, whether in paper or digital form, is the lifeblood of the council because of its critical importance to providing services to the public effectively.

1.5 High quality information underpins the delivery of high-quality services and many other key service deliverables. Information has the greatest value when it is accurate, up to date and is accessible where and when it is needed.

1.6 Effective information security management ensures information is properly protected and is reliably available. Without effective security, the council's information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised parties.

1.7 Information security management is underpinned by robust information risk management. This requires the council to have a robust information risk management

structure in place that reduces the risks created by threats to information whilst retaining its confidentiality, integrity and availability.

1.8 The council is committed to ensuring that information in whatever its context, is held in accordance with current legislation and best practice. Compliance with all organisational policies is a condition of employment and a breach of policy may result in disciplinary action. In addition, a breach of this policy may be considered as a breach of the Computer Misuse Act and treated as a criminal offence.

1.9 This policy is managed in line with ISO|IEC27001, the international standard for Information Security.

2 Definitions

2.1 Throughout this policy the following terms will have the agreed definitions

	Definition
Data	Data is a factual output that is the result of measurements taken.
Information	Information is that data taken and interpreted in a way that it can be easily read, discussed, heard, and presented.
Must	This term is used to state a Mandatory requirement of this policy.
Should	This term is used to state a Recommended requirement of this policy.
May	This term is used to state an Optional requirement.
OFFICIAL	This refers to the protective making of documents. Please refer to the Protective Marking Policy for further information. The current version is available on the Intranet.

3 Scope

3.1 The Information Security Management System's (ISMS) scope covers all aspects of security when handling, obtaining, recording, using, sharing and disclosing data or information, whether held in physical, electronic or verbal form. This applies to all information held by the council.

4 Confidentiality, integrity and availability

4.1 The Policy is intended to achieve and maintain these Information Security objectives:

Confidentiality

Information must be protected to ensure that access to information is restricted so that only those with appropriate authority can access it.

Integrity

Information must be input correctly, completely and accurately and protected from unauthorised modification or deletion. All systems, assets and networks must operate correctly, according to specification.

Availability

Information must be protected to ensure that information is available to be delivered to the right person, at the time when it is needed.

4.2 It is important to ensure that information security is sufficient and effective across the council.

4.3 To do this we will ensure information is:

- Held securely and, where necessary, confidentially,
- Processed fairly and lawfully,
- Recorded accurately and reliably,
- Retained only and for as long as appropriate or required by law,
- Used effectively and ethically[1], and
- Shared and disclosed appropriately and lawfully.

4.4 Legal background

4.4.1 The Isle of Wight Council, ('the council'), as data controller, have responsibility under current data protection legislation to ensure that the way in which it processes information complies with current data protection regulation and its overriding principles, to deal fairly with information.

4.4.2 The council recognises that electronic communications e.g. emails, recordings, images, text messages etc. may contain, or indeed constitute, personal information and therefore are protected under current data protection legislation. Equally an e-mail address personal to an individual may be personal information held about that individual.

5 Roles and Responsibilities

5.1 Everyone

5.1.1 Information security is everybody's business and therefore it is everybody's responsibility to ensure information is secure. This section describes the expected responsibilities in relation to Information Security by persons processing information and data. It is noted that some individuals will hold more than one role.

5.2 Chief Executive

5.2.1 The Chief Executive must have ultimate accountability for actions and inactions in relation to this policy. On behalf of the Chief Executive, the Senior Information Risk Owner (SIRO), with support from the Information Security Manager (Deputy SIRO) and the Senior Information Management Officer, will be responsible for implementing, monitoring, documenting and communicating information security and management requirements throughout the council.

5.3 Senior Information Risk Officer (SIRO)

5.3.1 The SIRO must take ownership of council's information risk and information security management, act as advocate for information risk to the Corporate Management Team and provide assurance and advice in regard to information risk.

[1] Information is managed in a way that avoids activities or organisations that do harm to people or the environment.

5.4 Caldicott Guardian

5.4.1 The Caldicott Guardian has responsibility for ensuring that there are appropriate standards for protecting patient information and that all data transfers are undertaken in accordance with Caldicott principles.

5.5 Data Protection Officer

5.5.1 The Data Protection Officer is the officer at the council who has responsibility for ensuring legal compliance with the GDPR.

5.5.2 The DPO can be contacted at dpo@iow.gov.uk

5.6 The Cyber Security Strategy Programme Board (CSSPB)

5.6.1 The Cyber Security Strategy Programme Board (CSSPB) is responsible for the implementation and oversight of the Information Security Policy.

- Ensuring that the council complies with the Data Protection Act 2018 and that
- Information security standards are effectively managed and implemented throughout the council.

5.7 Information Asset Owners (IAOs)

5.7.1 IAOs are directly accountable to the SIRO and must:

- Identify, appoint and manage Information Asset Administrators (IAA's) to assist them with their duties, where this is appropriate and necessary,
- Document, understand, retention manage and monitor what information assets they "own" and for what purpose, how information is created, deleted, amended or added to, who has access to the information and why,
- Identify the information necessary to respond to incidents or recover from a disaster affecting their information assets,
- Take ownership via input to the council's Information Asset Register (IAR) of assets under their control, providing risk assessment and management processes for the information assets they own, including the identification, review and prioritisation of perceived risk and oversight of actions agreed to mitigate those risks,
- Provide support to the SIRO to maintain awareness of risks to all information assets, for the purpose of risk awareness, reporting requirements and management procedures,
- Ensure that relevant members and officers are aware of and comply with expected information governance working practices for the effective use of owned information assets.

5.7.2 IAOs operate as Data Custodians across their areas of responsibility.

5.8 Line managers

5.8.1 Line Managers must take responsibility for ensuring that their permanent, temporary and voluntary workers, suppliers and contractors are aware of:

- Information security policies applicable to their role,
- Personal responsibilities for information security,
- How to access advice on information security matters.

5.8.2 Line Managers must take responsibility for ensuring that their staff have received suitable information security training in accordance with council training requirements, including the provision of information security induction prior to the provision of access to OFFICIAL assets.

5.8.3 Line managers are responsible for the security of their physical environments where information is processed or stored.

5.9 All members and officers

5.9.1 Have a responsibility to follow the duties and expectations detailed in the council constitution.

5.9.2 Must ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard possible.

6 Information Security Principles

6.1 General security standards

6.1.1 This policy is part of a suite of policies and procedures supporting the council's risk management strategy, information governance strategy and information security management system. The key documents are listed in the Related Documents section of this policy. Other documents include the standard operating procedures applicable to your role.

6.1.2 The following sections set out the standards that those working for or on behalf of the council are expected to adhere to in relation to information security.

6.2 Information security

6.2.1 Information security is the responsibility of all members and officers, who are always expected to act in a professional and responsible manner whilst conducting council business.

6.2.2 All information processed for council business is considered OFFICIAL information regardless of what device is used e.g. personal devices and must be treated accordingly.

6.2.3 All members and officers are responsible for their actions in relation to council information and government information systems.

6.2.4 Members and officers shall ensure that they understand their responsibilities, and that failure to comply with this policy may result in disciplinary action.

6.2.5 This policy will be reinforced by mandatory, annual, information security training.

6.3 Information risk management environment

6.3.1 The council assesses the risks to information security with the same vigour as for legal, regulatory, financial or operational risk.

6.3.2 All members and officers must read and understand the IWC Risk Management Framework and apply that guidance across the workplace to ensure that employees, contractors and suppliers are aware of the council's risk management boundaries.

6.4 Secure configuration

6.4.1 This is the use of corporate policies and processes to develop secure baseline builds and manage the configuration and use of your ICT systems. This is enabled, by removing or disabling unnecessary functionality and keeping devices patched against known vulnerabilities, as failing to do this would expose the council to threats and increase the risk to the confidentiality, integrity and availability of systems and information.

6.5 Network security

6.5.1 ICT must follow recognised network design principles when configuring perimeter and internal network segments and ensure all network devices are configured to a secure baseline build.

6.5.2 ICT must filter all traffic at the network perimeter so that only traffic required to support business is allowed and monitor traffic for unusual or malicious incoming and outgoing activity that could indicate an attack (or attempted attack).

6.6 Change Management

6.6.1 All changes to ICT equipment must be made via ICT's change management process. This is to ensure that changes are appropriately managed, recorded and documented.

6.6.2 All moves of static ICT equipment must be made via ICT's change management process. This is to ensure that changes are appropriately managed, recorded and documented.

6.7 Purchasing electronics devices

6.7.1 Members and officers must not purchase electronic devices as the council procures all electronic devices such as cameras, mobile phones, tablet devices, computers, peripheral devices, servers etc. centrally via the ICT department, who procure, manage and track these council assets.

6.8 Moving equipment inc. desks, PC's, cabinets, printers etc.

6.8.1 Members and officers must submit a move request. This is to allow moves to be:

- Approved and documented
- Planned and resourced
- Floor plans to be updated
- Asset registers to be updated

6.8.2 Team or departmental moves must not be carried out without formal approval.

6.9 Managing user privileges

6.9.1 Information asset owners (IAOs) must ensure that all users of ICT systems are only provided with the user privileges that they must have in order to carry out their duties, carrying out audit checks at interval against the assets under their ownership to ensure that users only hold appropriate permissions.

6.9.2 ICT must control the number of privileged accounts for roles such as system or database administrators, and ensure this type of account is not used for high risk or day-to-day user activities, and

6.9.3 ICT must monitor user activity, particularly all access to sensitive information and privileged account actions, such as creating or amending or deleting documents, user accounts, user passwords and audit logs.

6.10 Training for social care systems

6.10.1 Line Managers must ensure that all staff using social care systems have completed mandatory introductory application training prior to providing access to the live system.

6.11 Disaster recovery and business continuity management

6.11.1 All departments at the council must maintain a Business Continuity Management (BCM) plan that addresses the full range of incidents that can occur if information becomes unavailable.

6.11.2 BCM plans must be shared with and understood by all staff, so that all staff understand what to do when computer systems become unavailable.

6.11.3 The ICT department must maintain a Disaster Recovery (DR) plan for the council's ICT systems that addresses the full range of incidents that can occur.

6.11.4 All DR and BCM plans must be regularly tested (at least annually) and improved.

6.12 Monitoring

6.12.1 The council has established a monitoring strategy and developed supporting processes that consider known security incidents and attacks.

6.12.2 The council's ICT systems continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate attacks or the compromise of data. Alerting ICT managers where appropriate.

6.12.3 This includes monitoring all ICT systems using Security Information Event Management (SIEM) and intrusion detection systems.

6.13 Mobile & Home Working

6.13.1 The council's Mobile and Home Working Policy advises security policy for the use of portable devices e.g. laptops, when working at locations remote to the council's network. The current version is available on the Intranet.

6.14 Protective Marking

6.14.1 All Information must be managed in accordance with the Protective Marking Policy; the latest version is available on the Intranet.

6.15 Portable File Storage Media

6.15.1 This includes, but is not limited to:

- USB memory drives and storage keys,
- Smart cards,
- Memory cards e.g. Compact Flash, SSD, SD, Memory Stick etc.
- External connected portable hard drives/solid state drives,
- Mobile telephones,
- CD/DVD/Blu Ray disks, including writable disks.

6.15.2 These devices can help people in the council manage information more efficiently, especially when they are outside their normal office environment e.g. when travelling between sites, off-site or working from home.

6.16 Acceptable use of portable file storage media devices

6.16.1 Only devices supplied by the ICT department or devices checked and approved by the ICT Security Team should be connected to council owned ICT equipment.

6.16.2 Council provided devices are only to be used to transport data in the course of council business.

6.16.3 Information or data should only be stored on the device as a temporary mechanism to transfer encrypted files that users are working on, from one ICT device to another, and the information should be deleted once the transfer is complete.

6.16.4 All OFFICIAL information or data must be encrypted in transit. Please speak to your line manager if you have any questions about how to ensure this.

6.16.5 All mobile phones issued by the council to service users must be locked using a PIN code, passphrase or biometric e.g. Fingerprints, retina etc. when not actively being used.

6.16.6 Unless information or data is being exchanged with a third-party organisation where the correct information sharing and governance controls have been signed off and are in place, information or data, should not be copied from a council device onto devices that are not owned by the council.

6.16.7 All users of portable file storage media devices must ensure that before connecting to systems other than those operated and maintained by the council's ICT department, the system has anti-virus and anti-spam software which has been updated to the latest available version to reduce the risk of contamination by virus or malware.

6.16.8 All lost or stolen devices containing council information should be immediately reported to line management and the ICT Security Department (ICTSecurity@iow.gov.uk). If the loss is likely to cause a security breach, it should also

be immediately reported as per the guidance in the Data Breach Incident Reporting Policy, which is available on the intranet.

6.17 Email

6.17.1 It is important to be aware that the email system is not a case management system. Therefore, it must not be used to manage case file documents, as to do so would be a breach of the General Data Protection Regulations (GDPR).

6.18 The Information Asset Register

6.18.1 Information assets, as with any other assets at the council, are recorded.

6.18.2 The key assets that Information Asset Owners (IAOs) are protecting are listed within their service's information asset register. A central copy of all Information Asset Registers is held by the Corporate Information Unit (CIU).

6.18.3 As new information assets are identified, the relevant Information Asset Owner must log it on their Information Asset Register and identify any associated assets along with the risks and corresponding controls to mitigate to the level required to meet business continuity plans. Any updates to a service's Information Asset Register should be notified to CIU.

6.18.4 ICT software and hardware assets are recorded by the ICT Dept and human assets are recorded by Human Resources.

6.19 Information security incident investigation

6.19.1 Any data breach incident identified must be formally reported as per guidance in the council's Data Breach Incident Reporting Policy.

6.19.2 The council's Data Breach Incident Reporting Policy is available on the Intranet and all members and officers must understand how to manage data breach incidents as per its guidance.

6.20 Managing information risk

6.20.1 Any failure to effectively manage information risk could lead to the following:

Term	Definition
Reputational Damage	Making decisions based on inaccurate information could undermine decisions made and could affect organisational reputation.
Financial Loss	Loss of information could lead to financial penalties. Inefficient use of information may lead to duplication and wasted time.
Failure to comply with legal, regulatory, local, or central government requirements	There are a number of lawful requirements to manage information such as: The Data Protection Act 2018, Freedom of Information Act, Public Records Act & General Data Protection Regulations which, if contravened, could lead to prosecution and/or reputational and/or financial loss.

6.20.2 Information Asset Owners (IAOs) must ensure that information assets are assessed for risk annually or, as changes that impact the asset's risk are made. Results of risk assessments should be placed on asset registers and escalated as per the Risk Management Policy and Guidance.

6.20.3 Any member or officer that does not understand risk management to a level appropriate to their role must arrange for appropriate guidance or training via their line manager.

6.21 Requirements for safe sharing of personal data or information

6.21.1 The transfer of any personal information must:

- Be reviewed and a lawful basis established to transfer it,
- A data protection impact assessment (DPIA) must be completed if appropriate,
- Follow the protective marking principles and underpinning policy guidance to maintain the security of the information in transit.

6.22 Data flow mapping

6.22.1 Routine transfers of personal information must be logged, regardless of size to allow review of security procedures in place and compliance with information governance requirements. IAOs are required to identify and log the routine transfers of data that will take place using the council approved flow mapping tool, including:

- Lawful basis,
- Use of approved method,
- Volume,
- Frequency,
- Risks,
- Compensating controls.

6.23 Recruitment and contracts of employment

6.23.1 The council has put in place recruitment and selection processes that ensure:

- Proof of identity,
- Availability to work within the UK, the organisation and with relevant sensitive data,
- By signing a contract of employment members and officers agree to maintain the confidentiality, availability and integrity of data in line with this and all other council policies,
- A clear disciplinary process for breach of policies.

6.24 Members and officers' changes (leavers and movers)

6.24.1 Line managers are responsible for notification of members and officers' changes in role which affect access rights to any ICT Systems.

6.24.2 Line managers are responsible to ensure access rights are removed from effective dates.

6.25 Preservation of data held in archival storage

6.25.1 Processes must ensure that sensitive, critical or valuable information stored for prolonged periods are not lost due to deterioration of the storage media (e.g. magnetic media, thermal paper, etc.).

6.26 Protection of security log files

6.26.1 Security log files, detailing user activity are collected by the council's Security Information Event Management (SIEM) system and are protected and stored for a minimum of 6 months to allow user audits to be completed when required.

7 Electronic information security

7.1 Business continuity & disaster recovery

7.1.1 As outlined in the council's business continuity plans (BCP's), all critical systems, applications and data must be backed up such that they may be recovered to alternative hardware.

7.1.2 Back-up management in place must allow for a recovery point and recovery time that does not adversely affect the council ability to maintain services.

7.2 PCs and laptops

7.2.1 Laptops obtained via the council's ICT are encrypted. This means that when the device is switched off, the data at rest is protected. A logged in laptop is no longer encrypted, so additional care must be taken to ensure that data is protected. Please refer to the ICT Mobile and Remote Working Policy for additional guidance.

7.3 Networks

7.3.1 The council recognises the need for a secure, scalable and reliable system to transfer electronic data and information securely and efficiently as a critical system to enable the delivery of business.

7.3.2 The ICT department must make provisions to ensure the network is secure in line with the requirements set out within this policy and in accordance with National Cyber Security Centre (NCSC) guidance.

7.4 Remote access to electronic information

7.4.1 Any equipment provided will remain the property of the council and items such as Laptops, mobile phones and any other equipment provided by the organisation should only be used by the allocated member or officer for business purposes or pre-approved personal use, in line with council policy.

7.4.2 Only remote access methods configured or managed by the council's ICT department are permitted to remotely access council information and data.

7.5 Supplier remote access to electronic information

7.5.1 New 3rd party access requests are enabled by completing the "ICT 3rd Party VIA Initial Setup Request" form and once setup, an "ICT 3rd Party VIA Session Request" must be

completed for each access. There must be a sponsor within the council who will submit both of these forms and be aware of the supplier's access. Both of these forms are available on the intranet.

7.6 Wireless communication

7.6.1 This policy prohibits access to council networks via unapproved wireless devices.

7.6.2 With the exception of the guest wireless network, only wireless devices that have council ICT approval are allowed to connect to council networks.

7.6.3 The guest wireless network is provided for the use of visitors and contractors, working on behalf of the council, to allow access to online services whilst visiting IOW sites.

7.6.4 Staff should not connect smart phones/tablets or similar devices to the guest wireless network whilst at work.

7.6.5 All visitors/contractors should disconnect their devices from the guest wireless network when finished.

7.6.6 The guest wireless network is monitored, and persistent connections will be identified, removed and notified to the appropriate line manager.

7.7 Use and Installation of software

7.7.1 Any use of or installation of software must meet the requirements of the council's ICT Software policy.

7.7.2 The current version of the council's ICT Software policy is available on the Intranet.

7.7.3 Where a new information asset is to be created by the installation of software, an Information Asset Owner (IAO) must be assigned to manage and protect the asset.

7.8 Personal use of ICT systems

7.8.1 All ICT systems, software and hardware provided by the council to its members and officers and other users are for direct business use only. Any personal use of ICT systems and services is strictly restricted by the council and members and officers may only use equipment and services provided by the council for personal use when approved by an authorised manager.

7.9 Patching and remedial updating of ICT systems

7.9.1 All vendor patches and remedial updates must be installed in a timescale that ensures that critical issues are addressed within 72 hours and that all vendor patches and remedial updates have been installed within four weeks of release.

7.9.2 Exceptions are permitted where vendor patches and remedial updates are identified as high risk due to known issues where other organisations have installed them and discovered that they cause errors. Exceptions must be approved by the Strategic Manager for ICT & Digital Services.

7.9.3 An audit log of uninstalled vendor patches and remedial update approvals must be maintained.

7.10 Electronic information storage

7.10.1 Information must be always stored securely. The specific controls will vary depending on the nature of the device. All electronic information is stored on networked systems with access restricted not only to only those that require access, but also to restrict users to the appropriate level of access. On some occasions it may be required that data is stored elsewhere e.g. an encrypted portable drive, on a short-term basis, this should be risk assessed and transferred back to a secure location on the council's network as soon as is practicably possible.

7.11 Encryption

7.11.1 Protection of OFFICIAL and OFFICIAL - SENSITIVE electronic information held or transferred outside of the council is a key area where encryption (of electronic information) must be used to provide an additional layer of protection. To this end, an evaluation of risk should be undertaken when considering holding or transferring confidential data.

7.11.2 All confidential electronic information held or transferred by council members or officers must be encrypted to the minimum standard specified by the ICT department. Sending confidential information without adequate encryption will be deemed as a negligent action and may be subject to disciplinary action.

7.11.3 Passwords for encryption must meet those defined within the password section of this policy and must not be sent with the information.

7.12 End of life software

7.12.1 When software is approaching end of life, it means that it is approaching the end of manufacturers support.

7.12.2 The council is prohibited from running software that is not supported by its manufacturer. The only exception to this, is where an alternative provider can provide extended support, while the end of life software replacement project is completed. Any extended support option must be reviewed and approved by the council's SIRO before contracts are put in place.

7.12.3 The manager that is responsible for the software contract must ensure that continuity of systems is maintained, by ensuring that when software is approaching end of life, they liaise with ICT, to plan that suitable replacement software is put in place in a timely manner.

7.12.4 The manager that is responsible for the end of life software must ensure that appropriate budgets are in place to support procurement of the replacement solution.

7.13 New ICT devices

7.13.1 New ICT devices are any new electronic device that creates, uses or stores information.

7.13.2 All new ICT devices must only be procured after ICT approval of the device.

7.13.3 ICT approval of the device takes place once ICT have ensured that:

- the device can keep information created, used or stored by the device secure to

government approved standards.

- The device is compatible with existing council systems

8 ICT asset disposal

8.1 To ensure that the authority gains best use of its computer infrastructure and to ensure that the authority meets its legal requirements all ICT equipment must be returned to ICT Support if it is replaced by a new machine.

8.2 To ensure that the authority gains best value from its computer infrastructure all departments must return spare ICT equipment to ICT Support if it is not actively being used, as this will allow reuse of the equipment elsewhere within the Authority.

8.3 When disposing of ICT equipment which has reached the end of its useful life, ICT will attempt to recycle the component parts of the equipment where possible and where recycling is not an option, dispose through appropriate waste disposal processes.

8.3.1 Where goods are to be re-used elsewhere within the Authority ICT Support will ensure that any old information cannot be retrieved by using data recovery tools and that all disposals are formally recorded.

8.4 The ICT department manages the disposal of ICT electronic devices, ensuring that disposal processes meet current government and legislative requirements.

8.4.1 ICT take responsibility for disposal at the point they take possession of the equipment.

8.4.2 ICT will process the computers in the following manner:

- Once the device has been handed over to ICT, it will be labelled with the ex-user's name and date of receipt,
- The devices may be subjected to a search for unsuitable information such as pictures or other data files that breach council policy or legislation,
- The devices will be retained for 2 weeks to allow any retrospective access to information held on the equipment should needs arise,
- The devices will then have all data irrecoverably erased to an approved government standard,
- Each device will be examined to ensure that it meets the current minimum specification for use. If it does, then it will be configured and stored ready for redeployment,
- When a request for this type of device is received, it will be redeployed,
- If it does not meet the current specification, it will be disposed of.

8.4.3 Under no circumstances is a device to be re-used before all data is irrecoverably erased to an approved government standard and re-installed with a new image.

8.4.4 The ICT department will examine the records of all equipment being stored on a quarterly basis to ensure that it still meets the minimum specification. This will ensure that we do not store obsolete equipment.

8.5 Recycle the component parts where possible.

8.5.1 Where it is not possible to re-use ICT equipment, which is otherwise still functional, the ICT department will take a view as to whether the equipment can be recycled.

8.5.2 The council cannot accept the risks and cost of disposal direct to officers, elected members or the public.

8.5.3 Due to the council's significant liability from selling or donating unsafe equipment, this will apply even where a third party could potentially repair equipment.

8.6 Authorisation for disposal of equipment

8.6.1 To comply with internal governance arrangements for asset disposal, the disposal of any ICT asset must be authorised by the Strategic Manager- ICT & Digital Services.

8.7 Method of Disposal

8.7.1 As a lot of ICT equipment contains high levels of lead and other heavy metals which can seriously damage the environment, the council will ensure it complies with the Waste Electrical and Electronic Equipment Directive (WEEE Directive) by contracting ICT waste disposals to a WEEE conformant company, to dispose of the equipment and to provide a certificate of secure data destruction for electronic media and data storage devices.

8.8 To ensure continued compliance with the Public Services Network (PSN) Code of Connection (CoCo) ICT Support will only install the current minimum specification of Operating System (or other software) as specified in the ICT Standards Policy.

Also Note:

8.9 Equipment should only be procured in accordance with the ICT Standards Policy.

8.10 New desktop, laptops and tablet computers do not need to be wiped before installation.

9 Password policy

9.1 Central Government's National Cyber Security Centre (NCSC), the advisory body for information security, now recognises that regular password changing can harm, rather than improve security and now recommends that users choose a "Three random words" password that is 17 or more characters and never change it again.

9.1.1 The Isle of Wight council has adopted this as the current password policy for Microsoft Windows logons.

9.1.2 This standard should also be used where possible for creating encryption passwords e.g. with WinZip or for encrypted portable electronic devices.

9.2 **IMPORTANT**: The "never change it again" only applies if your password is a secret known only to you. Users must change their passwords immediately if there is any reason to suspect that their password has been compromised. See section 9.6

9.3 The only rules when choosing your three random words password are:

- The password MUST contain 17 or more characters
- Do not choose words that relate specifically to you, e.g. Children's names, Street names etc.
- Keep it Random. Only choose words that have no connection to the other words chosen, e.g. Road, Stairs, Apple rather than My, Favourite, Colour

PASSWORD EXAMPLES
COLOURED FOR EASE OF READING
superbouncytoilet
peppercloudbanana
fastesttreetriangles
longershelterslower

9.4 **Please be aware:** You do not have to use numbers, capital letters or special characters in your password, though you can if you want to.

9.5 Legitimate password sharing

9.5.1 When sending information from one place to another in an encrypted form (e.g. a zip file), the recipient must also have the password (key) to open the relevant files. In this circumstance you should still maintain the advice for strong passwords. The password must be sent by an alternate means e.g. verbally, encrypted messaging app, etc.

9.6 Password reset service

9.6.1 The council provides a password reset self-service portal for all staff. This allows you to change your password should you ever forget it, or if you believe it has been compromised by someone else discovering it.

9.6.2 You must first register with this service at a time while you can remember your password. The password reset service can be found here: https://passwordreset.microsoftonline.com/

9.6.3 You can access this service online from any internet connected device. Even via your mobile phone.

10 Cyber security controls

10.1 Overriding access controls

10.1.1 Access to an individual's files, folders and systems will be granted to a line manager or investigating officer. This will only be authorised upon written/email request to a senior member of ICT and may, at ICT's discretion, be referred to the SIRO, Caldicott Guardian (or nominated deputy) or HR for approval. ICT will retain copies of requests. This will ensure that proper auditing of access made can be maintained and that the security of the user account is not compromised.

10.2 Antivirus & malware

10.2.1 As Viruses, Worms, Trojan horses and hoaxes can potentially cause major disruption to council services. They can also prove costly to recover from. The following measures are designed to manage these risks:

- Automatic virus detection software must be installed and kept up to date on every council server, PC and laptop,
- Members and officers are responsible for immediately reporting any problems with their anti-virus software to the ICT department,
- Members and officers are responsible for immediately reporting all incidents where viruses are detected to the ICT department. In addition, suspected breaches/incidents should be reported to the Corporate Information Unit (ciu@iow.gov.uk) immediately,
- The ICT department is responsible for ensuring that updates to anti-virus and anti-malware software is made promptly available,
- Members and officers must not install or run unauthorised software (including games and screen savers) on any ICT equipment owned by the council,
- All files received or distributed via portable media from external sources must be scanned with anti-virus software prior to use. If you require assistance with this, please contact the ICT Service desk,
- All servers connected to the live infrastructure must be protected by anti-virus and anti-malware software,
- Any client or third-party equipment that may occasionally be permitted to connect to the network must be checked prior to connecting to ensure it is free from viruses.

11 Protective Controls

11.1 Transactional monitoring (TxM)

11.1.1 Transaction monitoring is the process of reviewing, analysing and administering the transactions processed on a business application or information system. It is an ICT management and security process that evaluates each or selected transactions performed on a given application or system.

11.1.2 Proposals for the design, specification or procurement of new digital services that may be attractive to cyber criminals for the purposes of fraud, e.g. Internet accessed transaction systems, must implement transactional monitoring techniques (TxM) from the outset. Examples of transactional monitoring techniques include:

- Typing text from a picture to prove that you are “not a robot”
- Identifying which squares of an image contain a specific item,
- Monitoring activity for suspicious behaviours such as multiple failed login attempts.

11.2 Systems administrators

11.2.1 Systems administrators by nature of their role have elevated rights compared to a normal user. Normal user access can be restricted to a role and limited to what is needed to do to perform that role, thus protecting the organisation and themselves.

11.2.2 Conversely, administrators do not have the same level of role limiting protection, so it falls to the individual. System administrators therefore have a great deal of system power and with that great power comes considerable responsibility. The system administrator must uphold the highest level of integrity in terms of respect of the confidentiality, integrity or availability of the systems they support.

11.2.3 All activity of systems administrators is logged for audit purposes.

11.3 Firewall policy

11.3.1 Network security and network boundary protection are essential in protecting the confidentiality, integrity and availability of council information and ensuring normal operations that are free from disruption. Council firewalls provide critical network protection and shall therefore be configured, managed and monitored to ensure the highest levels of security.

11.3.2 **Boundary protection** - Firewalls must be implemented between the council’s internal network and the internet and other external connections. The type, size and performance of the firewalls to be implemented shall be determined according to the defined business requirements.

11.3.3 **Secure configuration and hardening** - Firewalls must be configured so that the minimum number of externally accessible services ports are enabled, and only those that have a documented business case and risk assessment will be enabled. Firewalls must be hardened at time of installation in line with vendor hardening guidelines and good industry practice and default passwords shall be changed and replaced with complex passwords before any firewall is added to the council’s network.

- Firewall failover implementations must meet business requirements and be

regularly tested to ensure effective resilience,

- Administration of firewalls must only be permitted from a secure environment and administrator access shall require two-factor authentication as a minimum,
- The physical locations of firewalls must be resistant to unauthorised access and tampering,
- Firewall configurations must be formally documented.

11.3.4 **Firewall logs** - Logging shall be enabled on all firewalls and all firewall logs will be stored securely off the host device, be backed up on a regular basis, be accessible by authorised personnel only and be protected against unauthorised access and tampering.

11.3.5 **Firewall change management** - Firewall configuration and rules shall only be changed in line with strict change control approval. When firewall configuration or rule changes are made, change details will always be recorded in the relevant firewall rule description to include:

- Ticket reference,
- Description of the changes,
- Date the changes were made,
- Name of the person making the changes.

11.3.6 A firewall port scan must be performed after every rule change to verify the amended rule set.

11.3.7 **Firewall auditing** – Each firewall's configuration and rules must be audited and tested regularly, and at least annually, to ensure that rule sets are effective.

11.3.8 Every firewall audit shall include a review of:

- Operating system updates,
- Admin ports,
- Firewall rules.

11.3.9 **Firewall configuration backup** - Firewall configurations shall be securely backed up before and after every configuration and rule change and at the time of every firewall audit.

11.4 Penetration testing

11.4.1 The council must commission penetration testing annually, via an approved supplier, to ensure ICT infrastructure is appropriately secure, to provide the relevant assurance to the council regarding infrastructure and any other key systems it manages.

11.4.2 Systems hosted by a 3rd party, will be arbitrarily selected for inclusion in the annual penetration test.

11.5 Application security

11.5.1 An application, which processes sensitive data, must be afforded protection appropriate to that sensitivity. The following are the minimum controls to be applied to sensitive applications, i.e. systems that hold sensitive data:

- Security requirements and specifications will be approved by ICT Management, prior to acquiring or starting development of applications, or prior to making a substantial change in existing applications,
- New or substantially modified applications shall be thoroughly tested prior to implementation to verify that the user functions and the required administrative, technical and physical safeguards are present and are operationally acceptable,
- Live sensitive data or files must not be used to test applications software until software integrity has been reasonably assured by testing with non-sensitive data or files,
- Application software will not be made live until the system tests have been successfully completed,
- Any sensitive software documentation should be provided the same degree of protection as that provided for the software.

11.6 Change Control

11.6.1 Changes to information systems, applications, hardware or networks shall be reviewed and approved by the ICT Change Advisory Board (ICT CAB) or when appropriate, the Cyber Security Strategy Programme Board (CSSPB) or Internal Information Governance Group (IIG), to ensure that the requirements of this policy have been applied.

11.7 General physical and environmental security controls

11.7.1 It is the responsibility of all council members and officers to make their area of work as secure as is reasonably possible.

11.7.2 All council premises must be appropriately secured to prevent unauthorised access.

11.7.3 All members and officers must observe and adhere to the security arrangements of the building in which they are working or visiting, and personal identity cards should be worn at all times whilst on site.

11.7.4 If you have access to secure areas within council premises or your areas of responsibility, you should ensure that only yourself, approved members and officers and accompanied visitors have access to these areas.

11.7.5 Do not allow non-council staff to follow you through secure doors unless they are with you.

11.7.6 Do not allow anyone to watch you typing in a door code.

11.8 The ICT datacentre and ICT equipment rooms

11.8.1 All ICT server and equipment rooms must remain locked and only accessible by controlled access.

11.8.2 All members and officers working at the ICT datacentre must be trained in the fire suppression systems in use.

11.8.3 Unrestricted access to the ICT datacentre and network equipment rooms is limited only to those who regularly need it, and that access is reviewed on a regular basis.

11.8.4 All non-ICT personnel must be accompanied at all times, by an authorised member of the ICT department while conducting work in the ICT datacentre and network equipment rooms.

11.8.5 ICT equipment is housed in a controlled and secure environment. Critical or sensitive equipment must be housed in an environment that is monitored for temperature, humidity and power supply quality.

11.8.6 Critical and sensitive ICT equipment is protected from power supply failures and is protected by intruder alarms and fire suppression systems where appropriate.

11.9 Deliveries (equipment security)

11.9.1 All deliveries of ICT equipment must be signed for and the ICT Asset registers updated accordingly.

11.9.2 ICT equipment must be securely stored when delivered. With all loading/unloading areas secured for planned deliveries.

11.10 Removal of equipment

11.10.1 When ICT equipment has been removed, the ICT Asset register must be updated accordingly. Removal is only permitted by ICT authorised personnel.

11.11 Returning of borrowed equipment

11.11.1 When borrowed equipment is returned to the ICT department, members and officers must notify a member of ICT, to allow the ICT Asset register to be updated accordingly.

11.12 Network security

11.12.1 The council uses authentication on its network and if unauthorised devices are connected, network ports are shut down and the network team is alerted.

11.13 Secure disposal of data

11.13.1 All council information held on any ICT equipment must be securely destroyed prior to disposal or re-use of the equipment.

11.13.2 Hard drives must be wiped to current standards by the ICT department using a suitable security product.

11.14 Clear desk and clear screen policy

11.14.1 All members and officers are required to operate a clear desk and clear screen approach to ensure that information is not inappropriately on display. This includes ensuring that no OFFICIAL or OFFICIAL - SENSITIVE information, regardless of format (paper, electronic etc.) is left unattended at any time. Indeed, all sensitive, commercial or personal information must be placed out of sight when left unattended and access by unauthorised persons must be prevented via locked cabinets or drawers when not in use.

11.14.2 In addition, all members and officers are required to lock their PC/Laptop when not in use or prior to leaving it unattended. This can be achieved by simultaneously pressing Ctrl + Alt + Delete, and then pressing Enter

12 Acceptable use of council assets

12.1.1 Council resources may not be used for any unlawful or prohibited purpose.

12.1.2 You are responsible for the security of information and data, accounts, systems and assets under your control. Providing access either deliberately or through failure to secure access is a violation of this policy.

12.1.3 Using council resources for the following is strictly prohibited:

- Causing a security breach to either council or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorised,
- Circumventing user authentication on any device or intercepting network traffic,
- Causing a malicious disruption of service to either council or other network resources,
- Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software,
- Intentionally introducing malicious code,
- Port scanning or security scanning on a production network unless authorised in advance by ICT Security,
- Inappropriate use of communication equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates council policies against harassment or the safeguarding of confidential or proprietary information,
- Sending Spam via e-mail, text messages, instant messaging, voice mail, or other forms of electronic communication,
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender,
- Use of a council e-mail to engage in conduct that violates council policies or guidelines,
- Posting anything to a social networking site as a representative of the council, unless authorised to do so.
- Copying or removing council information from any source, and taking it with you or sharing it, without your managers approval, with anyone outside the council when employed by the council, or when leaving council employment.

12.1.4 All information created or accessed on council systems or created by yourself during the course of your employment remains the property of the council when you leave.

13 Non-compliance with this Policy

13.1.1 Should it not be possible to meet the requirements within this policy and associated guidelines this must be brought to the attention of the relevant Information Asset Owner or the SIRO. Any issues will need to be documented as a risk and either:

- Tolerated and reviewed in line with this policy,
- Accepted with a view to implementing an action plan to reduce the risk,
- Not accepted and the practice will stop until such time as the risk can be reduced.

13.1.2 Failure to comply with the standards and appropriate governance of information as detailed in this policy and supporting protocols and procedures, can result in disciplinary action. All members and officers are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible for. Failure to maintain these standards can result in criminal proceedings against the individual. Legally binding regulations include but are not limited to:

- Data Protection legislation including The UK General Data Protection Regulation and the Data Protection Act 2018
- Common Law Duty of Confidentiality
- Computer Misuse Act
- Freedom of Information Act
- Human Rights Act
- Public Records Act
- Defamation Act
- Disability Discrimination Act
- Equality Act
- Obscene Publications Act
- Regulation of Investigatory Powers Act
- Criminal Justice and Public Order Act
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations
- Environmental Information Regulations

14 Related Documents

- Electronic Communications Policy
- Mobile and Home Working Policy
- ICT Hardware Policy
- ICT Software Policy
- ICT Standards Policy
- Telecommunication Policy
- Protective Marking Policy
- Disciplinary Procedure Policy
- Corporate Retention Policy
- Data Breach Incident Reporting Policy

15 Appendices

15.1 Appendix A – Information security policy overview

15.2 Appendix B – Virus, worm, trojan horse, virus hoax, email spoofing & phishing explained

15.3 Appendix C - Access control requirements

15.4 Appendix D – Software development requirements

Appendix A – Information Security Policy Overview

DO'S!	DONT'S
✓ Keep your passwords secret. If you suspect that a password has been revealed to anyone. Please change it immediately.	• Do not use the council's computer equipment for personal use unless authorised to do so.
✓ Highlight security risks such as broken locks to your Line Manager.	• Do not write your passwords down!
✓ Ensure that people passing by do not have the opportunity to read documents left open on your desk or screen.	• Do not disclose your passwords to anyone, including ICT officers.
✓ If you receive an on-screen virus warning do not respond, instead, contact ICT while it is still on-screen.	• Do not ignore damaged or worn security devices. Get them replaced.
✓ Protect information by ensuring that it is kept confidential, accurate and available for use.	• Do not leave windows open at the end of the day.
✓ Lock your system or log out when leaving your desk, unless you are taking your laptop to somewhere in the same building.	• Do not allow anyone to use a device that is logged in under your credentials or share your login details.
✓ When transporting a laptop outside of office buildings, ensure it stays in the case provided when not stationary, it will protect the equipment.	• Do not allow visitors into secure areas without first checking their ID.
✓ Be careful who you allow to follow you through security doors.	• You are not authorised to purchase any ICT equipment, USB devices or accessories, including cameras, tablets, phones etc. All such purchases must be centrally purchased via the ICT department.
✓ Consider the risks of eating or drinking near computer equipment.	• Do not loan ICT equipment or disclose passwords to anyone outside of the council.
✓ Ensure that cabinets and rooms containing confidential data and/or information are kept locked when not in use.	• Do not allow anyone to connect non-approved ICT equipment to council ICT equipment. Contact the ICT Service Desk if there is a requirement.
✓ Be aware of suspicious activity and report it.	• Do not dispose of any sensitive - personal or confidential – material, including CD, DVD, Blu Ray disks and USB sticks in the waste bins, if in doubt take it to the ICT department for appropriate disposal.

Appendix B – Virus, worm, trojan horse, virus hoax, email spoofing & phishing explained

15.5 What is a virus?

15.5.1 A virus is a computer programme that changes the way a computer behaves usually without the user's knowledge or permission it often copies itself to other computers. Viruses can steal, destroy or deny access to data and can use your computer to attack other computers.

15.5.2 Indications of a possible virus infection include:

- Files or programs become corrupted or lost
- Files increase dramatically in size
- Sudden unexplained slowing of the computer
- Unexpected text, visual or audio messages
- Unexplained computer failure

15.6 Computer worms

15.6.1 Worms are similar to viruses. They spread by attaching themselves to files such as Word or Excel documents and screensavers. They move between computers when the file is transferred to another computer.

15.7 Trojan horses

15.7.1 A Trojan Horse is a file that mimics the method used in the tale of the Trojan horse. It appears or claims to be useful or desirable but contains malicious code which, when opened or triggered, can:

- cause loss and theft of data,
- pass the control of the computer to remote users,
- use the host computer to attack other computers.

15.8 Virus hoaxes

15.8.1 Virus hoaxes are usually email messages that work in a similar way to chain letters. They warn of a new virus threat that does not exist. By forwarding the 'warning' to other users the hoax spreads misinformation and confusion. It may also increase email traffic as users email the warning to others.

15.8.2 If you receive an email advising, you of a new computer virus do not forward the email on. Check with the ICT department who will advise whether it is a hoax or not.

15.8.3 Members and officers must be alert to computer virus related messages and contact the ICT Service Desk if a message appears.

15.9 Email spoofing

15.9.1 Email spoofing is the forgery of the displayed email address so that the message appears to have originated from someone or somewhere familiar to you. Email spoofing is a popular tactic used in phishing campaigns because you are more likely to open an email if you think it has been sent by a legitimate business or friendly source. The goal of email spoofing is to get recipients to open and possibly even respond to links within the message.

15.10 Phishing

15.10.1 Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing, it often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

15.10.2 Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or ICT administrators.

Appendix C – Access control requirements

1 Aim

1.1 The aim of access control is to ensure appropriate access control rules are in place across Isle of Wight Council's ICT, including the network and associated information systems, to ensure the confidentiality, integrity, and availability of systems and information.

1.2 It ensures the actions or operations that a legitimate user can perform are those authorised for their role and ensures that the risks associated with unauthorised access are mitigated.

1.3 Access control must be in place to protect the interests of the council by providing a secure and readily accessible environment.

1.4 Access control applies to the council's network, its resources, and associated information systems and applications.

1.5 Access control applies to individuals requesting access to council ICT and the ongoing management of that access. This includes, but is not limited to, employees, elected members, contractors, consultants, volunteers, and third-party organisations.

2 Access Control Principles

2.1 Access must be strictly controlled to maintain the confidentiality, integrity and availability of information and systems.

2.2 The overall security of the infrastructure, systems, applications and information must take precedence over any individual requirement for access.

2.3 Access rights must be based on a clear business need and must be afforded in line with the principles of need to know and need to access.

2.4 The allocation and use of privileged access rights must be strictly controlled.

2.5 Access to the council network must be through the provision of a unique User ID which must be assigned to an individual user to enable an audit of specific activity and to ensure accountability of actions.

2.6 Generic user accounts must not be permitted unless exceptional circumstances exist and only when there is a clearly defined and documented business reason to do so.

2.7 Account holders must conform to the council's Information Security Policy, Electronic Communications Policy and Protective Marking Policy.

2.8 Access provided to non-council staff must be supported by a relevant information sharing agreement and/or contract which sets out appropriate information assurance requirements. Services must be the minimum necessary.

2.9 Access to council email must be strictly limited to council staff or in very limited circumstances those representing the council.

3 Access Authorisation

3.1 Before access is authorised a formal process must be followed which requires that:

3.1.1 An agreed business need is identified.

3.1.2 Authority is provided by a relevant line manager.

3.1.3 The identity of the User is verified.

3.1.4 The provision of privileged access is via formal change control.

3.2 The level of access provided must be commensurate with the tasks the User is expected to perform.

3.3 Users must change their passwords at the first log on and enrol for multi factor authentication (MFA).

4 Adjustment of Access Rights

4.1 Adjustments to access rights must be based on the criteria set out at Para 4.

4.2 Access rights to systems used by staff when changing roles must be reviewed by managers and updated where necessary e.g. removal of unnecessary access permissions.

4.3 Suspension of access rights must be requested by the relevant Line Manager for lengthy periods of planned inactivity e.g. secondment; suspension; maternity leave; long term sick leave.

5 Disabling of User Accounts

5.1 Once a business requirement ceases to be relevant e.g. due to contract termination, staff transfer, resignation, or retirement, access to the council network and to systems previously required to complete a role must be revoked and the users account disabled or modified.

5.2 Line Managers are responsible for notifying the IT Service Desk of the need to disable the User account and to disable any access permissions the user had to systems used as part of their role.

5.3 ICT assets must be recovered from employees once a business requirement has ceased and returned to the council's ICT department.

6 Allocation of Privileged Access Rights

6.1 The allocation of privileged access rights must be strictly controlled and must follow the access authorisation process.

6.2 Privileged access rights must be consistent with an individual's role.

6.3 Privileged access rights must be subject to formal change control process.

6.4 Privileged access rights must be assigned to a User ID different from those used for regular business activities.

6.5 When privileged access rights are no longer justifiable, they must be removed as soon as practicable.

6.6 A regular review of privileged access rights must be undertaken (not less than annually).

6.7 Users requiring administrative privileges (for example, users who can reconfigure the network or system administrators) must be subject to the Baseline Personnel Security Standard.

Appendix D - Software development requirements

1 Code Quality and Readability

1.1 Adhere to established style guidelines (e.g., PEP 8 for Python, Java Code Conventions) to ensure code is readable and maintainable.

1.2 Choose descriptive names for variables, functions, and classes to make the code self-explanatory.

1.3 Write clear comments and use documentation to explain the purpose and usage of code segments.

1.4 Break down code into reusable functions and modules to enhance readability and maintainability.

2 Version Control

2.1 Implement version control using council hosted tools to track changes and manage code versions effectively.

2.2 Make frequent commits with meaningful messages to document the development process.

3 Security Best Practices

3.1 Always validate and sanitise user inputs to prevent injection attacks and other vulnerabilities.

3.2 Rely on well-maintained and secure libraries for cryptographic functions and other security-related tasks.

3.3 Store sensitive information like API keys and passwords in environment variables, not in the codebase.

3.4 Keep your development environment and libraries up to date to protect against known vulnerabilities.

4 Error Handling

4.1 Implement robust error handling to ensure the application can handle unexpected situations without crashing.

4.2 Use logging to record errors and important events, which aids in debugging and monitoring.

5 Publicly Shared Code

5.1 Public code repositories often contain unpatched vulnerabilities. Attackers can exploit these weaknesses to gain unauthorised access or cause damage.

5.2 Open source projects can be targeted by malicious actors who introduce harmful code, leading to security breaches or data loss.

5.3 Never include sensitive information, such as credentials or private keys, in public repositories, as this can be exploited by attackers for further attacks.

5.4 Public code often relies on other open source components, which may themselves have vulnerabilities or be poorly maintained. Avoid using code written in the public domain where possible.

5.5 Thoroughly vet any publicly shared code before integrating it into your projects and regularly update and patch all dependencies.

6 Testing

6.1 Write unit tests and use frameworks like JUnit, pytest, or similar to automate testing and ensure code reliability.

6.2 Integrate automated testing into the development pipeline to catch issues early.

7 Code Reviews

7.1 Conduct regular code reviews to catch potential issues, share knowledge, and improve code quality.

7.2 Use tools like pylint, flake8, or similar to automatically check for coding standard violations and potential errors.

8 Data Protection

8.1 If plaintext credentials are stored in databases or files, they can be exposed during data breaches. Attackers gaining access to these credentials can compromise user accounts and systems.

8.2 PCI-DSS, mandates the use of encryption for sensitive data, including credentials. Encrypt sensitive data both in transit and at rest to protect it from unauthorised access.

8.3 Use current cryptographic standards, such as TLS, and ensure encryption is updated to newer standards before deprecation dates.

8.4 Implement strict access controls to ensure only authorised users can access sensitive information.