IT and Digital Transformation Service

IT Security Policy

Author	Andy Griffiths
Date	April 2019
Status	Current
Version	1.2
Protective Marking	OFFICIAL
Review Date	February 2020
Policy Renewal	December 2020

Document Control Information

Organisation	Conwy County Borough Council
Title	Information Technology Security Policy
Author	Andy Griffiths
Filename	IT Security Policy.doc
Owner	IT Security Officer
Subject	IT Security
Protective Marking	OFFICIAL
Review Date	January 2020

Revision History

Document Version	Revision Date	Revised by	Description of Revision
1.0	November 2017	Andy Griffiths	New format of policy
1.1	February 2018	Andy Griffiths	Changes requested by audit to strengthen processes around AD account updates and privilege reviews.
1.2	February 2019	Andy Griffiths	

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Signed	Date
Head of IT & Digital Transformation	Huw McKee		

Policy Consultation

This Policy has been created with consultation from SMT and Head of Audit & Procurement Services.

Contributors

Development of this policy was assisted through information provided by the following organisations:

Devon County Council	Sefton Metropolitan Borough Council
Dudley Metropolitan Borough Council	Staffordshire Connects
Herefordshire County Council	West Midlands Local Government Association
Plymouth City Council	Worcestershire County Council
Sandwell Metropolitan Borough Council	

Contents

Policy Overview

1.1. Policy Statement

1.1.1. The Chief Executive and the Senior Management Team of Conwy County Borough Council are committed to preserving the confidentiality, integrity and availability of the IT Systems, electronic assets and information throughout their organisation in order to maintain the successful achievement of the Council's Corporate Objectives.

1.1.2. All employees, elected members and approved partners who access any IT system provided by Conwy County Borough Council are required to comply with this policy, supporting policies and legislative requirements.

1.1.3. This Policy will be reviewed at least annually with any updates circulated to all staff who use IT via the appropriate available means.

1.1.4. This Policy will be updated by the designated IT Security Officer with input from IT Management Team, Internal Audit, the Senior Information Risk Officer (SIRO) and other Service Heads as appropriate.

1.2. Introduction

1.2.1. Any loss of electronic data can have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide services to the public.

1.2.2. In order to provide connection to Government IT systems, the Council is required to comply with a number of governing bodies and regulations. As such, this policy is reflective of the requirements of all necessary regulations and legislation including data protection regulations.

1.3. Scope

1.3.1. The IT Security Policy applies to, but is not limited to, all Conwy County Borough Council Members, elected or otherwise, Committees, Services, Partners, Employees of the Council, Schools, employees of partner organisations engaged in collaborative work with Conwy, contractual third parties and agents of the Council who access the Councils IT systems and IT equipment. This collection will from now on be referred to as 'users'.

1.3.2. This Policy is applicable to different sections of IT Security and affected users. However, the entire Policy should be read and understood by all within the Scope.

1.3.3. This Policy relates to all personal data held or processed by the Council in any form and all data classified following the guidance of Government Classification Scheme and Impact Levels 1, 2 and 3. This Policy refers to IT equipment as devices which include, but are not limited to, desktop PC's, laptops, tablets, mobile phones, smart phones, servers, network switches, access points and all other Conwy owned IT asset.

2. All IT Users

2.1. IT Access

2.1.1. All users of IT systems and equipment require a unique identifying account (Corporate Log-in) with password details only known to themselves.

2.1.2. Subsequent IT systems access may require further usernames or passwords which should be treated in the same manner.

2.1.3. Under no circumstances should any IT account details be written down unless with the prior approval of the Head of IT and Digital Transformation.

2.1.4. At first log in these details will be provided to the new user by the IT Service Desk and not to any other user.

2.1.5. Any additional system access can be requested via a user's Line Manager or Service Senior Manager to the IT Service Desk.

2.1.6. All users must ensure any PC or Laptop in use is locked or logged out while unattended.

2.1.7. Computer screens will be locked after 10 minutes of inactivity and require a password to resume.

2.1.8. Users are required to inform IT Service Desk of any threat and/or concerns regarding the IT systems or hardware they use as soon as possible.

2.1.9. Any activity on CCBC IT systems or equipment may be logged by IT and used by Service management and/or Internal Audit if required.

2.1.10. All users must read and understand the associated ICT & Digital Services Policies as located on the intranet before using that technology.

2.1.11. Any usernames and passwords used by IT & Digital Transformation Officers to carry out their duties which are held outside of the corporate Active Directory or AS400 (such as but not limited to software as a service accounts, web based portals, infrastructure, network and support related administrator accounts or management system accounts) must be stored in the service's chosen secure password safe system. The secure password account should be protected by a password set in accordance with Conwy standards and shared with each officer's line manager to ensure that access can be achieved by appropriate colleagues in the event of an emergency, unplanned or prolonged period of absence from work.

2.2. Restrictions

2.2.1. Non-Council owned devices are not permitted to access the corporate network or IT Systems unless provisioned by the IT and Digital Transformation Service through the Council's chosen mobile device management and secure remote access solutions.

2.2.2. All users are required to abide by the Corporate Password Policy.

2.2.3. All users are required to abide by the Acceptable Usage Policies for Internet and Email.

2.2.4. Users must not enter corporate log-in details to non-Council IT equipment in an attempt to access corporate data. Users must never use corporate log-in details for access to systems outside of the Council.

2.2.5. Users must not take corporate data outside Council premises or email information to their home or other personal account without the written approval of their senior manager.

2.2.6. Any user actions on IT systems may be recorded by the IT and Digital Transformation Service for security purposes but only monitored with express permission from Head of Audit and Procurement or Service Senior Management.

2.2.7. Non-Conwy employees are not permitted to access or use Conwy IT equipment or systems without prior approval from the Head of IT and Digital Transformation.

2.2.8. Staff must not record any conversations, meetings, events, discussions or any other communications using phones or other devices without prior agreement.

2.3. Access Control

2.3.1. Only designated IT and Digital Transformation Service officers are permitted to access IT secure areas (e.g., Data Centres, equipment rooms).

2.3.2. IT Equipment should be located in designated areas, secure from public access. If in public areas, IT equipment should be sufficiently secured to fixed structures.

2.3.3. The IT and Digital Transformation Service reserves the right to remove any account and associated data from IT systems which has not been used for a period of 2 years. If a user is on Long Term Absence then a section manager must notify the IT Service Desk by logging a call to prevent this account and associated data (e.g. my documents or e-mail content) being deleted.

2.4. IT Equipment & Systems

2.4.1. All IT equipment owned by Conwy should have a clearly marked Inventory Label which must not been tampered with or removed and where the value exceeds the asset inventory level should be marked as belonging to the council.

2.4.2. Use of IT equipment must be formally approved by Senior Managers in each Service.

2.4.3. No personal or sensitive data should be stored on the local hard drive of any workstation or laptop.

2.4.4. All Conwy laptops are encrypted with a unique passcode which provides protection to the content stored on that device only. This passcode should not be shared with anyone outside of the Authority.

2.4.5. Conwy IT equipment should not be tampered with, damaged or destroyed/disposed of by anyone but the IT and Digital Transformation Service.

2.4.6. Maintenance work on Conwy IT equipment should only be carried out by the IT and Digital Transformation Service or with express consent from the IT and Digital Transformation Service.

2.4.7. Users are responsible for the safety and physical security including concealment of any Conwy-issued device when inside and outside of Council premises.

2.4.8. Users are responsible for ensuring data on CCBC devices are concealed from view to any unauthorised individual.

2.4.9. Users should take due care to limit risks of environmental hazards to any Conwy County Borough Council IT equipment.

2.4.10. In exceptional circumstances use of corporate IT equipment may be granted to support work carried out for partner organisations subject to protocols for such use being in place or where permissions in such instances has been granted by the Head of IT and Digital Transformation.

2.4.11. Any work for or on behalf of the Authority must be done from an authorised or Council-provisioned system

2.5. Software

2.5.1. Under no circumstances should personal or unsolicited software be installed onto a Council machine.

2.5.2. All software used by Conwy County Borough Council must be registered in that name and with the Service in which it will be used.

2.5.3. All software used by Conwy County Borough Council is required to have a valid license covering its use.

2.5.4. All software owned and in use by the Council must be kept in a register maintained by the IT and Digital Transformation Service and is for use on CCBC devices only.

2.5.5. All software installed on the network must be fully patched and in-support from the software vendor. Failing to do so may result in the software being removed from the network.

2.6. Procurement and installation of IT equipment and systems

2.6.1. All IT hardware and software acquired for use by Conwy County Borough Council must be purchased through the IT and Digital Transformation Service.

2.6.2. The procurement of IT equipment and systems must be formally approved by a Departmental Senior Manager and must be approved by the Head of IT and Digital Transformation to ensure compliance with IT strategic standards.

2.6.3. Software and hardware may not be purchased outside of IT and Digital Transformation procurement processes through user corporate credit cards, petty cash, and travel or entertainment budgets.

2.6.4. The Head of IT and Digital Transformation reserves the right to decline implementation or support for any IT product or service (including systems, software or hardware) purchased outside of the IT and Digital Transformation Service.

2.6.5. Software and hardware must only be installed by the IT and Digital Transformation Service. Schools may have a nominated, agreed member of staff with access to an administrator-level account for their school machines only. Access to this account is upon request to the IT Service Desk and will expire at the end of every day unless otherwise agreed between the school and IT Security Officer.

2.6.6. Sensitive information/data should be saved in compliance with data protection rules to secure folders within the relevant Service file structure.

2.7. Software Development

2.7.1. All software, systems and data development tools owned by the Council are to be used only for the purpose of the Council's business and Services.

2.7.2. Software must not be changed or altered by any user unless there is a clear business need.

2.7.3. IT and Digital Transformation Service must be made aware when a change to an IT system or software has been made so that it can be registered into the IT Changelog or IT Service Desk software.

2.8. Removable Media

2.8.1. All removable media devices are set to Read-Only by default unless there is a business requirement with authorisation from a senior manager.

2.8.2. Any removable media which requires corporate data to be saved to it must be encrypted and the password kept securely and separately.

2.8.3. USB data drives must be purchased through the IT and Digital Transformation Service.

2.8.4. Removable media should not be used as the sole location to store any data.

2.8.5. Non-Council owned removable media devices must not be connected or used to store or transmit any information from the Councillor to conduct official Council business.

2.8.6. Removable media should be stored in a safe, secure location at all times.

2.8.7. Requests for removable media to not have encryption must be made by the users department with a full explanation with express consent from the relevant Head of Service and Head of Audit and Procurement. Internal Audit and/or the IT Security Officer reserve the right to refuse this request if the risk to the Council outweighs the requirement.

2.8.8. All removable media must be returned to the user's Service when employment ends.

2.9. Cloud Storage Platforms

2.9.1. To maintain the security of Council data, access to internet-based Cloud storage websites and platforms (including but not limited to Dropbox, ICloud, azure, google drive etc.). is blocked by default.

2.9.2. Requests to access such sites should be made to the IT Service Desk with details of why and exception has been requested from a Service's Senior Manager or Head of Service.

2.9.3. Data stored on any cloud storage platform must not contain Personal or Official-Sensitive classification.

2.9.4. Data sent and received on any cloud storage platform is the responsibility of the department user and department Head of Service.

2.10. Incident Reporting

2.10.1. All IT Security events (or suspicions of) must be **reported immediately** to the IT Service Desk (see Appendix 2).

2.10.2. Security incident reports will remain confidential unless an investigation dictates.

2.10.3. Examples of IT Security Incident types can be seen in Appendix 1 and the Procedure for Incident Handling in Appendix 2.

2.11. IT Equipment and Software Misuse

2.11.1. Users must not attempt to disable or reconfigure any software, system or hardware either on the Conwy Corporate network or to any Conwy-owned system or device.

2.11.2. Any attempt to reproduce, copy or distribute data or IT system from the Conwy network is not permitted under the Copyright, Designs and Patents Act (1988).

2.11.3. Disposal of all IT equipment and software/data is to undertaken by the IT and Digital Transformation Service only in line with the Disposal of Obsolete Hardware policy.

2.11.4. The misuse of CCBC IT equipment, including telephony, is considered to be potential gross misconduct and may result in disciplinary action including dismissal.

2.11.5. Officers must not use any CCBC IT system or asset in a manner which could have a negative effect on the reputation of the Council or any associated body. Systems should always be used in accordance with data protection legislation.

2.11.6. Failing to adhere to any or all parts of this Policy may result in disciplinary procedures.

3. Service Managers

3.1. Scope

3.1.1. Service Senior Managers (SSM) are those users defined by a department with permission to make certain administrative IT decisions.

3.1.2. IT will provide updates to SSM in respect of process and policy compliance via their nominated IT Business Partner.

3.1.3. SSM must be aware of IT Security threats and their responsibilities to mitigate threats. They should also ensure their own officers within a service are informed and aware of the same.

3.1.4. A Head of Service (who may be part of SSM for a Service) is the recognised data owner for that Service with responsibility for the safeguarding of personal and sensitive data.

3.2. Account Access

3.2.1. SSM are responsible for ensuring all users who access any IT system or data have read and understood the IT Security policy before using any IT systems or equipment.

3.2.2. SSM are responsible for ensuring all officers are familiar with the IT Security Policy updates at least annually.

3.2.3. It is the responsibility of the SSM to ensure users are adequately trained and equipped to carry out their role on an IT system efficiently and securely.

3.2.4. It is the responsibility of the SSM to ensure enrolments for new users or any changes in role are correct by following the IT Enrolment Guidelines

3.2.5. It is the responsibility of the SSM to ensure their users are allocated only the access rights and privileges required to undertake their role. These privileges should be reviewed regularly so that they reflect the requirements of a user's specific role and where appropriate changed to ensure data and system protection remains the Council's main priority.

3.2.6. Staff will only be provided with access to IT systems or data listed on the new users enrolment form.

3.2.7. Request for access to additional or reduced systems or data must be made via a user's Line Manager or SSM.

3.2.8. Request for temporary users or access must include a valid expiry/review date for the account.

3.2.9. Request for enrolments, change of access or access to be withdrawn from any system or data for a user must be made via the IT Service Desk by SSM.

3.2.10. In exceptional circumstances, requests for user access may be referred to the Head of IT & Digital Transformation or Head of Audit & Procurement for approval.

3.2.11. SSM must complete a withdrawal for any user leaving the Council's employment or changing role with a valid end date for the account in a timely manner so that access is withdrawn at close of business of the last working day or role change of the employee.

SSM must ensure all IT Assets are recovered by any user leaving the Council's employment before the final day.

3.2.12. Generic Accounts may be requested but are subject to the following restrictions:

- No internet access from the generic account.
- No generic mailbox associated with the account.
- Specific requirements for the generic account must be provided by the Senior Manager within the section.
- IT Security Officer sign-off on generic account requests.

3.3. Authorisation

3.3.1. IT Purchases for a Service must be made via a SSM

3.3.2. IT Asset management for each Service is the responsibility of a SSM.

3.3.3. Requests for disposals of IT Equipment must be made to the IT Service Desk by a user with approval of their SSM.

3.3.4. Any requests for available user activity logs must come from a SSM and/or Head of Service and will be referred to Internal Audit.

3.3.5. Where users require Removable Media to be created without Encryption, a SSM or Head of Service (as Data Owner) must provide explicit authorisation. IT Security Officer and/or Audit reserve the right to decline this if there is a risk to the Council.

3.3.6. SSM (or other nominated person within each department) are required to provide authorisation for remote access where third party support companies are required to have IT access (via the IT Service Desk) as per the Third Party Support Agreements.

4. IT and Digital Transformation Service Officers / Service System Administrators

4.1. Access rights

4.1.1. Default accounts/passwords must be changed before being introduced to the Corporate Network.

4.1.2. System Administration access to supported technologies by technical specialists within the IT and Digital Transformation team should be allocated only where the requirement is essential. Where possible access should be granted for an agreed time period for work to be undertaken. Where it is deemed permanent access is appropriate then the allocation of these privileges should be reviewed on a monthly basis to ensure they remain essential. Full systems administration access rights to the Council's systems and infrastructure should be tightly controlled in consultation with the Head of IT and Digital Transformation. All permissions and access methods for external users (including suppliers) must be controlled by IT and Digital Transformation Service through a nominated technical specialist officer.

4.1.3. External remote contractor access must be logged.

4.1.4. Supplier AD accounts must be disabled when not in use and should only be active until the end of the current working day.

4.1.5. System Administrators must have individual administrator accounts that will be logged and audited and must not be used to access websites or the internet.

4.1.6. System Administrators should only provide access to systems based on least privilege to the requirements of the user with reviews undertaken regularly.

4.1.7. To reduce the potential for damage to systems, system administrator accounts must not be used by individuals for normal activities – they should be signed in to only to carry out specific tasks which require the higher level access.

4.1.8. Visitors to IT secure areas must be accompanied at all times.

4.1.9. All IT Infrastructure areas (including, but not limited to, Data Centres, Network Cabinets, Stores, Test laboratories etc.) must be secured with appropriate security measures which is reviewed on a cyclical basis.

4.1.10. Test and Train environments must have separate appropriate account controls in place from the live systems.

4.1.11. Any access change requests completed by Services for users must be recorded on the IT Service Desk for auditing purposes.

4.2. Equipment Security

4.2.1. All IT equipment being received by the Council must follow the policies and processes in place in the IT Stores function.

4.2.2. All IT equipment procured with a value in excess of £50 must be security marked and recorded on the IT inventory.

4.2.3. No IT Equipment should be left unsecured in the IT Lab when Council offices are closed.

4.2.4. Network cables must be protected by conduit and avoid routes through public areas where possible.

4.2.5. Access to Network switch cabinets should be secure with access provided to designated IT and Digital Transformation officers only.

4.2.6. IT Infrastructure (including but not limited to Servers, Switches, and Drives etc.) should be properly assessed to ensure they can operate effectively in the environment factors prior to any installation.

4.2.7. Equipment that is to be reused or destroyed must have all data erased/destroyed in accordance with the Obsolete Hardware Policy.

4.2.8. All Mobile phones (and associated SIM/memory cards) must be disposed of/erased/destroyed in accordance with the Mobile Telephone policy.

4.2.9. All ‘current’ IT Equipment should be up to date and secured with Anti-Virus and Encryption where applicable.

4.2.10. All default passwords on equipment or systems must be changed before introduced to the Corporate Network.

4.2.11. Disposal of all IT assets must be done in accordance with the Disposal of Obsolete IT Hardware policy.

4.2.12. Any IT hardware leaving the Council temporarily (e.g. for repair or return) must have all data appropriately removed either by a secure format or destruction of disk before being sent. However, where possible, any drives containing Council data should be retained.

4.3. Software

4.3.1. IT and Digital Transformation Service must keep a register of licenses for all software owned by the Council with details including software publisher, asset owner, and date of purchase and, where available, version and serial number(s).

4.3.2. Software should be scanned for Viruses before being installed on to any corporate device or the corporate network,

4.3.3. Software can only be installed by the IT and Digital Transformation Service. Wherever possible IT officers should use the central software repository to install software.

4.3.4. Only software which is licensed and certified by the publisher as secure is permitted to be installed and used on the corporate network by Services.

4.3.5. Software containing vulnerabilities will be detected upon quarterly IT scans performed by the IT Security Officer. These scans will identify software which is no longer within support and must be removed from all CCBC devices within a timely manner.

4.3.6. Disposal of all software media should be undertaken in line with the Disposal of Obsolete and Redundant IT Hardware Policy. Any digital software should be deleted from CCBC network(s) and devices when required.

4.4. Operations

4.4.1. Changes to any system or infrastructure including maintenance work or upgrades must be logged in detail on the IT Change Log.

4.4.2. Changes to any system or new technologies must be tested in isolation wherever possible, with an appropriate testing plan followed before being introduced to the corporate network.

4.4.3. All operational data should be removed from a system for testing or working with suppliers pre-contract, in line with data protection legislation.

4.4.4. All Hardware devices must have appropriate critical security patches applied within thirty days of release.

4.4.5. All Software packages, including but not limited to, Applications and Operating Systems, must have appropriate critical security patches applied within thirty days of release.

4.4.6. Regular backups of essential business information must be taken to ensure that the Council can recover from a disaster, media failure or error with an appropriate backup cycle must be fully documented and implemented.

4.4.7. Backup media must be retained offsite in a designated secure location and maintained to recognised good practice.

4.4.8. Backup media must be encrypted and test restores carried out on a monthly basis with evidence of the test recorded on the IT Service Desk. A full Disaster Recovery exercise should be undertaken on an annual basis by the IT and Digital Transformation Service.

4.4.9. Backup media should only be transported by designated couriers within a locked container and protected against unauthorised access, misuse or corruption.

4.4.10. All Backup Media should be disposed of in accordance with the Disposal of Obsolete and Redundant IT Hardware Policy.

4.4.11. Where audit logs are in use, they must be backed up and stored for a minimum of 1 year consisting of 6 months on tape and 6 months immediate (subject to compliance with data protection regulations).

4.4.12. All IT Equipment on the corporate network must have the time synchronised to the Conwy NTP time source.

4.4.13. Wireless networks must be WPA2 as a minimum.

4.4.14. Internal Vulnerability scans of the network and devices must take place every 3 months.

4.4.15. Results of the Internal Vulnerability scan must be resolved within 30 days of detection.

4.4.16. A full PSN-scope IT Health Check must take place every 12 months by a recognised third party specialist and remediation actions completed within 3 months.

4.4.17. Operating procedures and system documentation must be readily available to the appropriate IT and Digital Transformation officers and updated whenever changes are made.

4.4.18. IT and Digital Transformation must undertake regular reviews of the Network Architecture to ensure the best and most suitable safeguard technologies are in place including, but not limited to, 6 monthly Firewall rule reviews.

4.4.19. All laptops, desktops and server devices must be built from a secure standard image controlled by restricted administrators.

4.5. Security Incidents

4.5.1. All Security Incidents must be correctly logged in the IT Service Desk system.

4.5.2. All Security Incidents must be logged as Critical with IT and Digital Transformation management team and the designated IT Security Officer informed. In the absence of the IT Security Officer, the Head of IT and Digital Transformation or nominated deputy should be informed.

4.5.3. The designated IT Security Officer must take ownership of all logged Security Incidents.

4.5.4. The designated IT Security Officer is responsible for contacting the Senior Information Risk Officer (SIRO), Head of IT and Digital Transformation, Head of Audit and Procurement and any other required internal person(s) as required.

4.5.5. IT and Digital Transformation Officers are not required to divulge information on any Security Incident to any persons within or outside of the Council without permission from the Head of IT and Digital Transformation.

4.5.6. All Cyber Security Incidents reported to IT must be logged and escalated appropriately with the IT Security Officer (and wider team in any absence) notified immediately.

4.5.7. All Cyber Security Incidents must be collated by the IT Security Officer to be reported to Senior Management Team on a quarterly basis.

4.5.8. All Cyber Security Breaches must be reported to the Head of IT and Digital Transformation Service upon discovery of a breach. A full report of each breach must be submitted to Senior Management Team including all details on actions and any consequences to the Authority.

5. Appendix 1 – Examples of IT Security Incidents

5.1. Information Asset Management

5.1.1. Examples of the most common IT Security Incidents are listed below. It should be noted that this list is not exhaustive.

5.1.2. Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a Virus or other malware.
- Sending a sensitive e-mail to the wrong person(s) by mistake either other CCBC officers or external.
- Receiving unsolicited mail of an offensive nature.
- Receiving unsolicited mail which requires you to enter personal data.
- Finding data that has been changed by an unauthorised person.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

5.1.3. Misuse

- Use of unapproved or unlicensed software on Conwy County Borough Council equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

- Any other behaviour on IT deemed unprofessional or irresponsible.

5.1.4. Theft / Loss

- Theft / loss of any Conwy County Borough Council computer equipment

6. Appendix 2 – Procedure for Incident Handling

6.1. Reporting Security Events or Weaknesses

6.1.1. The following sections detail how users and IT Support officers must report IT security events or weaknesses.

6.1.2. Reporting IT Security Events for all Employees

- Security events, for example a virus infection, could quickly spread and cause data loss across the organisation. All users must understand, and be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users **must**:
  - Note the symptoms and any error messages on screen.
  - Disconnect the workstation from the network if an infection is suspected (with assistance from IT Service Desk officers).
  - Not use any removable media (for example USB memory sticks) that may also have been infected.
- All suspected security events should be reported immediately to the IT Service Desk on 01492 57 6033.
- If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to Senior Management and the Information Governance Unit for the impact to be assessed.
- The Information Governance Unit will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:
  - Contact name and number of person reporting the incident.
  - The type of data, information or equipment involved.
  - Whether the loss of the data puts any person or other data at risk.
  - Location of the incident.
  - Inventory numbers of any equipment affected.
  - Date and time the security incident occurred.
  - Location of data or equipment affected.
  - Type and circumstances of the incident.

6.1.3. Reporting Information Security Weaknesses for all Employees

- Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.
- Weaknesses reported to application and service providers by employees must also be reported internally to the IT Service Desk. The service provider's response must be monitored and the effectiveness of its action to

repair the weakness must be recorded by the IT and Digital Transformation Service.

6.1.4. Reporting Information Security Events for IT Officers

- Information security events and weaknesses must be reported to the IT Security Officer within IT as quickly as possible, recorded on to the IT Service Desk and the incident response and escalation procedure must be followed.
- Security events can include:
    - Uncontrolled system changes.
    - Access violations – e.g. password sharing.
    - Breaches of physical security
    - Non-compliance with policies
    - Systems being hacked or manipulated
- Security weaknesses can include:
    - Inadequate firewall or antivirus protection
    - System malfunctions or overloads
    - Malfunctions of software applications
    - Human errors
- An escalation procedure must be incorporated into the response process so that users and support staff are aware who else to report the event to if there is not an appropriate response within a defined period.
- Incidents must be reported to senior management should the incident become service affecting.

6.2. Management of Security Incidents and Improvements

6.2.1. A consistent approach to dealing with all security events must be maintained across the Council. The events must be analysed and the IT Security Officer must be consulted to establish when security events become escalated to an incident. The incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the Council on continuing operation during the incident.

6.2.2. Collection of Evidence

- If an incident may require information to be collected for an investigation strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. Internal Audit must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt about a situation, for example concerning computer misuse, contact the IT Security Officer on, 01492 57 5988 or Internal Audit on 01492 57 6212 for advice.

6.2.3. Responsibilities and Procedures

- Management responsibilities and appropriate procedures must be established to ensure an effective response against security events. The IT Security Officer will decide when events are classified as an incident and determine the most appropriate response.

- An incident management process must be logged and include details of:

  - Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
  - Limiting or restricting further impact of the incident.
  - Tactics for containing the incident.
  - Corrective action to repair and prevent reoccurrence.
  - Communication across the Council to those affected.

- The process must also include a section referring to the collection of any evidence that might be required for analysis as forensic evidence. The specialist procedure for preserving evidence must be carefully followed.

- The actions required to recover from the security incident must be under formal control. Only identified and authorised staff should have access to the affected systems during the incident and all of the remedial actions should be documented in as much detail as possible.

6.2.4. Learning from Information Security Incidents

- To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

  - Types of incidents.
  - Volumes of incidents and malfunctions.
  - Costs incurred during the incidents.

- The information must be collated and reviewed on a regular basis by IT and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.

- The information, where appropriate, should be shared with the Warning, Advice and Reporting Point (WARP) to aid the alert process for the region.

7. Appendix 3 – Saving Data

7.1. Where to save data

7.1.1. As an employee in Conwy County Borough Council, you have the ability to save files in lots of different locations and some locations are better than others. The whole question of where you save your files depends on what you want to do with them. Our best advice is to always save information to your department's S: drive.

- S: drive data is available to you on any Conwy workstation you log into.
- Your colleagues are also able to access the files
- Your files are backed up, so if you accidentally delete them, or make a mistake we can restore them
- You can request a secure shared folder to share data with a subset of colleagues
- Snap shots of data are taken through the day – at 10am, 12pm, 2pm, and 4pm, this will provide you with the ability to perform quick restores to recover files without having to contact the IT Service Desk
- If required, information in your department's S: drive can be shared with other people in different departments

7.1.2. Our next best practice advice on saving data is to save in your 'My Documents'. This location is also on the server, so you still have the ability to use the self-restore snap shots, or contact IT for other restores but the main difference in saving in My Docs is…

- All files save in My Documents are private to you and no other employee can access this area
- For laptop users, your 'My Documents' are synchronised with your laptop so you can take it with you when you go off-site

7.1.3. Many people save to My Documents because of the benefit of keeping data private and taking data with you, however, these benefits can sometimes be a curse. For example, If you are working on a project and you have saved information relating to this project in your 'My Documents' and unfortunately, you go off sick, nobody else is able to access this information without contacting IT. This happens more often that you realise!

7.2. Where *not* to save data

7.2.1. As mentioned earlier, there are other locations you can save data, but these locations are **not backed up** and not managed by IT. These locations include:

- Your desktop - **never save documents to your desktop**. If your workstation fails or is stolen, all your documents on your desktop are lost. Instead, you should create a shortcut to the document and save the document to your S: drive or My Documents
- A Pen drive/external removable media - these are handy for transporting info, but it should only have a copy of the data with the original file held on

a Conwy server (S drive or My Docs) and not the original file. No sensitive information should be saved to a pen drive unless it has been encrypted.