West Yorkshire Combined Authority | Tracy Brabin Mayor of West Yorkshire

DTS Security Policy

Digital and Technology Services

Ian Towner / June 2024

Document Version Control

	Last Modified	Last Modified By	Document Changes
2.0	26/11/2018	David Gill	Document significantly updated
2.1	01/08/2021	Christopher Ndubuisi	Document updated
2.2	04/11/2022	Henry Kenyon	Document updated
2.3	09/01/2023	David Gill	Minor revisions pre SMT
2.4	01/03/2023	Henry Kenyon	Minor revisions pre SMT
2.5	23/05/2023	Henry Kenyon	Update to include agreed personal device access
2.6	26/10/2023	Henry Kenyon	Updated to meet PCI V4.0
2.7	01/11/2023	Zubair Rasib	Formatting
2.8	17/11/2023	Zubair Rasib	Moved document content to new template
2.9	26/04/2024	Ian Towner	Changed document classification from Internal to Public
2.10	17/06/2024	Ian Towner	Added sections on Ransomware and Extortion and foreign travel as well as updating ICT references and replaced with DTS.

Contents

1. Overview 4
2. Purpose 5
3. Policy Scope 5
4. Related Policies, Documents & Resources 5
5. Our Responsibilities 6
6. Access Control 8
7. Access to restricted data and copy/transfer activity 8
7.1 Data Transfer 9
8. Laptop & Desktop Computers 11
9. Corporate Mobile Phones and Smartphones 12
10. Removable Devices & Media 12
11. Networks & Cyber Security 13
12. Physical Security 17
13. System Permissions 18
14. Risk Assessment Process 19
14.1 Control Review 19
14.2 Governance and risk management 19
14.3 Internal and External Audit Reports 20
14.4 Legal and Regulatory Requirements 20
15. PCI Controls 20
16. Ransomware and Extortion 20
17. Foreign Travel 21
18. Exceptions 22
19. Formal Action 22
20. Equality Impact Assessment 22
21. Changes to Policy 22
22. Accessibility 22

1. Overview

The objective of this policy is to provide direction for the protection of systems and information owned by the Combined Authority, its customers, partners and suppliers. Of equal value is the trust of our partners and customers, that we will protect any information which they share with us.

High standards of security are required to safeguard access to data and information at a systems level which involves the effective operation of firewalls, access rights and technical solutions. Equally importantly, data, information and assets must be physically protected to ensure that brute force cannot be used to obtain unauthorised access within the organisation's buildings. Cyber Security is one of the Combined Authority's top corporate risks and the application of this policy is a key mitigation. The requirements detailed in this policy exist to help deliver the organisation's objectives and improved outcomes for the people of West Yorkshire, they mandate a proportional level of security in line with standards set by the UK Government through the National Cyber Security Centre (NCSC).

The Combined Authority's proprietary, customer, partner and supplier information and data must be protected from unauthorised access, use, modification, or destruction when it is created, stored, transmitted, or communicated. Consequently, all access to, and use of, this information and data, requires adherence to the following policy principles:

- Confidentiality - Appropriate measures must be taken to ensure that the Combined Authority's information and data is only accessible to those who are authorised to have access to it.

- Integrity - The accuracy and completeness of the Combined Authority's - information must be maintained and all changes or modifications affecting that information must be authorised, controlled, and validated.

- Availability – Information must be available to authorised individuals when required. In the event of a disaster or malicious attack, the Combined Authority's information, and the systems critical to the success of our business must be recoverable.

- Authentication - All persons and systems seeking access to information or to our networked computer resources must first establish their identity to the Combined Authority's satisfaction.

- Authorisation – Enforced by the Combined Authority authorisation policies which define what a user's profile is allowed to access and activities within the Combined Authority's IT estate.

- Access Control – Defines the methods used to enforce authentication and authorisation policies to view, or modify information, computer programs or the systems, on which the information resides, so as to be restricted to only those whose job functions absolutely require it.

- Auditing - User access and activity on the Combined Authority's computers, firewalls and networks must be recorded and maintained in compliance with all security, retention, and

regulatory requirements

This security policy must be reviewed by senior management, at a minimum once every 12 months or is updated as needed to reflect changes to business objectives or risks to the Combined Authority's environment.

All employees must have access to the policy, so it must be published on the Combined Authority's Intranet and communicated to all staff.

2. Purpose

This Digital Technology Service (DTS) Security Policy communicates the Combined Authority management's intent and objectives regarding the protection of its most valuable assets. It identifies the purpose, scope, accountability, and information that clearly defines the Combined Authority's position regarding cyber security. It also ties to and governs all other policies and procedures that define protection of the Combined Authority from cyber threats

This policy aims to make everyone aware of their responsibilities to:

- Ensure that computer equipment is not subjected to hazardous conditions.
- Ensure that systems, information and physical assets are protected from unauthorised access.
- Ensure the confidentiality of restricted information.
- Ensure the correctness of information.
- Meet the regulatory and legislative requirements in respect of information.
- Assist in the production, maintenance and testing of business continuity plans.
- Report any breaches of DTS security actual or suspected, to the DTS Service Desk.
- Securely store DTS equipment.

3. Policy Scope

The scope of this policy applies to all technology usage, including:

- Combined Authority applications and data which are accessed from using a device (desktop computer, laptop, tablet, mobile phone etc.) that is operated and utilised by the Combined Authority.
- Combined Authority applications and data which are accessed from equipment, which is not owned by the Combined Authority, but utilises the Combined Authority network, internet connection or cloud-based services.

Unless stated otherwise, the policy applies to Combined Authority working locations and all other working environments such as homes, partner offices and public environments.

4. Related Policies, Documents & Resources

- Data Systems Security Incident Policy
- Email, Internet & Telecoms Usage Policy
- Equipment Allocation Policy
- ICT Equipment Display and Returns Policy

- Bring your Own Device (BYOD) Policy
- Password Policy
- Acceptable Use Policy
- Data Protection & Confidentiality Policy
- Records Management and Data Quality Policy
- FOI-EIR Transparency Policy
- Disciplinary, Conduct and Capability Policy
- Data Security Incident Procedure
- DTS Major Incident Policy
- WYCA ICT Services Access Mgt High Level Design
- WYCA ICT Services Information Security Management Overview
- WYCA ICT Services Information Security Mgt Detailed Design
- WYCA ICT Services Information Security Mgt Protocol

5. Our Responsibilities

Information Security Policies, Procedures and Responsibilities

Ensure information security policies and procedures specify the following:

- All information security responsibilities shall be defined and allocated.
- The responsibility for technical security should be allocated to the Cyber Security Manager, who is a suitably security-knowledgeable member of staff with sufficient management support to perform his or her duties.
- The Senior Leadership Team will provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
- The Cyber Security Manager should be accountable for the implementation and day to day running of technology security
- The responsibility for establishing, documenting and distributing security policies and procedures is assigned to the Cyber Security Manager.
- The responsibility for monitoring and analysing security alerts is assigned to the DTS Services Team.
- Responsibility for establishing, documenting, and distributing security incident response and escalation procedures is assigned to the DTS Service Desk, in conjunction with the appropriate DTS and Information Governance team, as per the DTS Major Incident and Disaster recovery Policy and the Data & Cyber Security Incident Procedure.
- The Cyber Security Manager, in conjunction with the Information Governance team will perform periodic reviews to confirm Combined Authority personnel are following security policies and operational procedures. These may cover log reviews, firewall rule-set reviews, reviews of how configuration standards are applied to new systems and that they're being applied.
- Management information will be created to review how security alerts are responded to and issues remediated.
- The Cyber Security Manager will work with DTS Service Desk to ensure change management processes include information security requirements are considered.
- The Cyber Security Manager will work with the DTS 1st, 2nd and 3rd line support teams, the DTS Business Systems Team to ensure there is sufficient independence within the information security roles in order to provide adequate separation of duties for critical functions.

- The Cyber Security Manager is accountable to ensure cybersecurity controls and incident notification are addressed appropriately in contracts, nondisclosure agreements (NDAs) and service level agreements (SLAs) with critical vendors.
- The Cyber Security Manager will ensure:
  - the Combined Authority participates in information sharing and analysis groups.
  - the Combined Authority facilitates information sharing by enabling authorised users to share authorised information to sharing partners.

Security Operations Centre (SOC)

The Combined Authority have a managed service contract in place to provide a Security Operation Centre (SOC) service. The SOC has the following responsibilities:

- Monitoring systems for cyber security events 24/7/365
- Investigating phishing and other malicious emails
- Investigating and responding to cyber security incidents including:
  - Disabling accounts that are deemed a high risk
  - Isolating devices that may have been compromised
- Providing advice and guidance relating to cyber security event detection

The SOC work closely with the Cyber Security Manager and other DTS colleagues to investigate and respond to cyber security events and improving detection of such events.

The SOC service is provided by BrightSolid from 2024 until 2027.

Line Manager Responsibilities

It is every Line Manager's responsibility to ensure that both they and members of their team within their line management responsibility have read this policy and are adhering to it.

Line Managers must inform the DTS Service Desk at least 5 working days before any end user who they are responsible for commences or ends their employment with the Combined Authority, including those employed via agencies. New employee requests will be fulfilled as per the WYCA DTS Services Access Mgt High Level Design. Emails and personal data are retained for three months for all ex-employees unless the DTS Service Desk receives a line management request to vary this.

Employee Responsibilities

It is the responsibility of every Combined Authority employee to ensure that they comply with and do not abuse the policy.

When CA information is accessed or corporate IT equipment used, in public places, the user must take additional care. IT equipment must not be left unattended where it can be easily stolen. Users must take care that the equipment is not dropped or have liquids spilt on and must also avoid unauthorised people looking at the screen display. Further information regarding suitable use of equipment is specified in the Acceptable Use Policy.

Information Asset Owners

As defined in the Data Protection & Confidentiality Policy, Information Asset Owners (IAO) are Heads of Service (or sometimes Service Managers). IAOs must comply with the relevant Information Governance policies listed below:

- Data Protection & Confidentiality Policy
- Records Management and Data Quality Policy

- FOI-EIR Transparency Policy
- Data Security Incident Procedure

Human Resources

Human Resources must notify the DTS Service Desk within 24 working hours of the effective time of a staffing change, which includes employment termination, new employment, suspension, or a change of job function. This includes all employment contracts issued by the organisation

Similarly, accounts for suppliers, contractors or temporary staff must be set up with an expiration date that is appropriate to the expected duration the account is required and in use. It is the responsibility of the recruiting manager to inform the DTS Service Desk of changes for individuals who are not employed by the Combined Authority. They can be contacted on 01132517226 and/or ictservicedesk@westyorks-ca.gov.uk.

6. Access Control

Access to the Combined Authority's DTS systems and resources must follow the least privileged module, using roll based access (RBAC) where possible. Please see WYCA DTS Services Access Mgt High Level Design for further information.

All users must be assigned a unique ID before allowed access to the Combined Authority's DTS systems and resources. The purpose of this requirement is to make it possible to attribute all actions by all users to an individual.

Group, shared, or generic accounts, or other shared authentication credentials must only be used when necessary, on an exception basis, and are managed as follows:

- Account use is prevented unless needed for an exceptional circumstance.
- Use is limited to the time needed for the exceptional circumstance.
- Business justification for use is documented.
- Use is explicitly approved by management.
- Individual user identity is confirmed before access to an account is granted.
- Every action taken is attributable to an individual user.

7. Access to restricted data and copy/transfer activity

Restricted Data

All employees must be familiar with and comply with the relevant Information Governance and Data Protection policies to understand what is classed as Restricted Data.

Access to Restricted Data

Access to data is controlled by the relevant Information Asset Owner (IAO) and requests must be sent to the DTS Service Desk, documenting a business reason, and signed off by the IAO or a nominated deputy (typically an Information Asset Administrator – IAA) .

Automated monitoring of access will be performed by DTS Services or its IT third parties. The IAO will be responsible for periodic access review, often with the assistance of the DTS Services.

DTS Services will only grant access to data with the authorisation of the IAO, or their nominated deputy. Under exceptional circumstances, the IAO may grant access to a user of a sensitive system or data whose original role privileges may not have had such access before. This must be preceded by a documented business case. Also, there might be need for an IAO at a higher level to grant access to a user. This must only occur when there is a business critical need to access the data and the original IAO is not available to grant access. Irrespective of the business criticality of the request, every request must be logged with the DTS Service Desk.

Copying Restricted Data

Authorisation to copy restricted data must be obtained from the Information Asset Owner. The request might be for a specific authorisation (for example - to copy a specific set of data on a particular day), a regular authorisation (for example - to copy a specific set of data once a month) or a more general authorisation. A record of all authorisations will be documented and retained by the Information Asset Owner.

7.1 Data Transfer

Transfer of restricted data will only be permitted using secure methods that have been approved by DTS Services. DTS methods of data transfer include but are not limited to:

- Microsoft OneDrive: This is suitable for sharing single files or folders with a limited number of internal or agreed and vetted external parties. External file uploads are not permitted to OneDrive.
- Microsoft SharePoint. Where many files or folders need to be shared internally or externally with multiple people or organisations, a SharePoint site may be more appropriate. The relevant IAO can request the creation of a site via the DTS Service Desk. External file upload and collaboration may be allowed within SharePoint at the discretion of the IAO utilising Microsoft Teams secure collaboration, which works with SharePoint.
- Microsoft Teams. This is predominantly an internal sharing and collaboration tool, most suited for functional teams and projects. Team sites can be created by the appropriate IAO by submitting a request to the Marketing & Communications section. External file sharing via Teams, in integration with SharePoint can be configured at the discretion of the IAO, as above.
- Other authorised file sharing platforms authorised by DTS Services and Legal & Governance Services.
- Encrypted USB memory stick. Used for the physical transfer of data outside the Combined Authority where other means are not practical. This must be performed only on request to DTS Service Desk as per the Removable Devices and Media section below.

Prohibited Insecure Methods of Data Transfer:
This refers to Combined Authority data of any classification.

- Personal cloud storage services (e.g. iCloud Drive, Drop Box, Google Drive) must never be used within the Combined Authority without written permission from the Cyber Security Manager or Data Protection Officer (or their deputy). Requests to use such services should be submitted to the DTS Service Desk. It is strictly prohibited to upload Combined Authority data to External Cloud sites and Cloud Storage sites unless agreed and a NDA has been signed. These include but are not limited to:
  - Dropbox
  - Amazon S3 (Simple Storage Service)
  - Google Photos
  - Google Drive
  - Box
  - iCloud
  - Adobe Document Cloud
  - Altaro
  - Uploadcare
  - Nakivo
  - MediaFire
  - MultCloud
  - Backupify
  - Cyberduck

All requests for exception should be made to DTS Service Desk.

- Bulk data via normal email.
- CD/DVDs are not permitted media for transferring data.

Email: Normal email systems are not secure, and it is never acceptable to transfer bulk personal data or personal sensitive data via normal email services. Transfer of data via email must always be encrypted. Individuals must always contact the DTS Service Desk over matters relating to the transfer (or emailing) of data which may be of a sensitive nature.

Where data covered by the Data Protection Regulations has been transferred to a third party, the sender must check (and record) that the data has arrived.

Removable Media: The writing of data to removable media (including USB drives, CD/DVDs) should be requested from the DTS Service Desk. Employees outside DTS Services do not have the ability to create unencrypted copies of data on USB drives CDs and DVDs. All requests for data to be written to removable media will be recorded in the DTS Service Desk System.

Where restricted data is to be copied on to or processed on a laptop, the laptop hard drive must be encrypted by employees within DTS Services and recorded in the DTS Service Desk System.

Lost Media Devices and Mobile Devices: The loss of a CD/DVD containing restricted data, a USB memory stick, or a laptop must be immediately reported to the DTS Service Desk using the dedicated DTS Security Incident template.

In the event of a lost data:

- This must be reported to the DTS Service Desk as per the methods shown on the Intranet (see DTS Services - Home (sharepoint.com)
- If the loss occurs within DTS Service Desk hours, the loss must be reported within 1 hour.
- Out of hours or during weekends, the loss must be reported the next working day.

Common File Locations: Confidential data must not be copied into or stored in any common file locations such as Long/Short Term Share or SharePoint, Teams sites or other Office 365 locations which can be accessed by individuals not employed by the Combined Authority, unless through specific authorisation.

Downloading Combined Authority Data: Where a user wants to download the Combined Authority's data from the Combined Authority's Microsoft O365 domain to their BYOD device, the device must be enrolled in the Combined Authority's instance of Microsoft Endpoint Manager to manage the device, whether as a fully managed device or through mobile application management. Downloading covers copying and pasting, saving attachments, and directly downloading / copying from SharePoint amongst others.

8. Laptop & Desktop Computers

It is the responsibility of each user to take all reasonable precautions to safeguard the physical security of the computer. This includes protecting it from hazards such as spilling liquids or physical damage. It is not permitted to connect personal USB devices of any form to Combined Authority computers, unless for charging purposes, DTS Services enforce this. Exceptions to this may occur when relating to specialist devices, such as assistance devices for disabled colleagues. Where USB devices are required, contact the DTS Service Desk for assistance.

Laptop Computers

Users will be reminded of their extra responsibilities when they are issued with a laptop computer to use either on Combined Authority premises or remotely. No laptop device is permitted to leave Combined Authority premises without full hard disk encryption.

Most Combined Authority users will be issued with laptop computers as standard. Laptop computers must not be left logged in when unattended. If the user is to be away from the device, even for short periods they must lock the screen display using the CTL+ALT+DEL keys and clicking the "Lock Workstation" tab or use the Windows Key + L key shortcut. If users fail to do this the laptop computer will automatically lock out after no more than 5 minutes

When used in the office, laptop computers must not be left unattended for extended periods or overnight. Also, in the office, secure desk locks are not available, but personal lockers are provided across office locations to securely store the laptops.

When a user is due to leave a Combined Authority building for any reason, even if the laptop is to be left in a secure locker, the Windows operating system must be properly shut down and not simply locked or set to sleep. When simply locked or set to sleep, the full disk encryption (via the Microsoft Bitlocker feature) is less secure and could allow a stolen laptop to be accessed, therefore total shut down of the Windows operating system must be implemented.

When used in a public place it is not permitted to view or process restricted data. Care must be taken to ensure that the screen display cannot be overlooked when viewing or processing other data.

Laptop computers must never be left on view in a vehicle. They must always be stored in the boot. They must not be left in the vehicle overnight. Whilst in transit laptop computers must be placed in appropriate carrying case when transported. Please refer to the Acceptable Use Policy for further detail.

Laptops and Desktop computers must not be left logged in when unattended, either when located in or out of Combined Authority premises. If the user is away from the device, even for short periods they must lock the screen display using the CTL+ ALT+ DEL keys and clicking the “Lock Workstation” tab or use the Windows Key + L key shortcut.

9. Corporate Mobile Phones and Smartphones

It is the responsibility of each user to take all reasonable precautions to safeguard the physical security of the equipment. The equipment must only be used for the purposes for which it was provided.

DTS Services will issue equipment to individuals as per the Equipment Allocation Procedure.

If equipment used to access Combined Authority data and services is lost or stolen, it is the user’s responsibility to notify the DTS Service Desk as soon as possible via the incident template on the DTS Service Desk. Where necessary, DTS Services will remotely wipe data stored on the equipment such as emails. DTS Services will be responsible for ensuring that the SIM card is disabled, and the phone is locked by the service provider.

It is not permitted to store confidential data on any of this equipment which is not protected by an appropriate password.

Where available, it is best practice to use face/fingerprint recognition and any other kind of biometric authentication systems must be implemented / enabled to access corporate data.

The equipment must automatically lock following a period of 5 minutes of inactivity. The user must then be forced to enter a personal identification number (PIN) or password to enable further use of the device. When the equipment is returned to DTS Services the PIN or password will be removed.

No unauthorised applications must be installed on the device, via the Google Play Store or by any other method. If a new application is required, a request with associated business case can be submitted via the DTS Service Desk for approval.

For non Corporate Devices, please see the Bring Your Own Device policy which sets out how personal equipment should be managed for access to CA information and services.

10. Removable Devices & Media

Only removable devices and media supplied by the Combined Authority or an approved source can be connected to the organisation’s computers. When storing restricted data the devices/media will be encrypted.

Overnight storage of devices/media containing encrypted data must be within a locked DTS area with encryption keys only located in a private area of the company's SharePoint system, encryption keys must never be stored with the associated devices/media.

Users must request to borrow an encrypted USB stick from DTS Service Desk and DTS will enable the user to copy data from the laptop to the USB for an agreed timeframe.

Encrypted USB memory sticks can be allocated to individuals following authorisation by either the DTS Service Desk Manager or Live Services Manager. Requests must be submitted via the DTS Service Desk and DTS Services will retain a copy of the authorisation. The name of the requester will be recorded against the asset in the DTS Service Desk system. When employees leave the employment of the Combined Authority or to a post where an encrypted memory stick is not required, the memory stick must be returned to DTS Services.

The DTS Service Desk will maintain a record of users who have been allocated USB memory sticks. This will be audited on a periodic basis.

It is not permitted to store executable program files on these devices. Users will be reminded of their responsibilities when they are issued with a USB memory stick. The memory stick must always be removed from the computer when not in use and must be stored out of view.

The loss of any of the Combined Authority's USB memory sticks must be reported immediately via the DTS Service Desk using the DTS Security Incident template.

Personal removable devices and memory sticks must not be connected to the Combined Authority desktop or laptop computers to access data stored on them. Such devices include, but are not limited to, USB memory sticks, external hard drives, CD/DVDs, digital cameras and mobile phones.

By default, DTS Services will block all devices connected into the USB ports of the Combined Authority desktop and laptop computers except for USB memory sticks issued by DTS Services, mobile phones where there is a business reason for the connection and digital cameras or cards.

It is recognised that from time to time it might be necessary to connect a memory stick from another organisation to a Combined Authority computer in a meeting room, in order to load a presentation or file that is required for the meeting. A representative at the meeting must arrange this via the DTS Service Desk and give reasonable notice. In this case, any non Combined Authority memory stick must be initially scanned for viruses before use.

USB memory sticks that are no longer required by an individual must be returned to DTS Services who will ensure that all data is removed before reuse or disposal. Appropriate records will be maintained. The DTS Service Desk will maintain a list of staff issued memory sticks with their name and location. This list will be updated periodically to reflect the most recent status of the list.

11. Networks & Cyber Security

DTS Services are responsible for Identity Management. DTS Services will ensure sufficient safeguards are in place to prevent unauthorised persons from accessing the Combined Authority's IT systems. It is the user's responsibility to ensure the security of systems by ensuring their equipment and passwords are not compromised or accessible by malicious sources.

Where there is a need to connect with a third party's network or cloud domain, a firewall or secure network connection will be used.

Passwords

Staff are to revert to the password policy for the purpose and approved standard for the creation of strong passwords and their protection.

The Combined Authority's Password policy can be found on the intranet here.

Managing Remote Access

All remote access to the Combined Authority's internal network will be via virtual private network (VPN), or through closed communication channels (point to point leased lines).

The Combined Authorities small remote offices and bus stations will be connected via dedicated Multiprotocol Label Switching (MPLS) lines.

DTS Services may restrict access to personal devices accessing via these remote access mechanisms that exhibit unsecure behaviour, such as out of date operating systems or anti-virus.

The VPN solution is only available to corporate devices and will form a secure connection back to the Combined Authority network whenever an Internet connection is detected. Once connected to the VPN the device will appear as though it is physically located within the perimeter of a Combined Authority premise. No personal device will be permitted to access the VPN.

A large subset of Combined Authority data and systems can also be accessed via Microsoft 365 through the Internet. Similar to remote access via VPN, DTS Services restricts access for personal devices to Microsoft 365. Personal devices, including mobile phones and laptops are allowed read only access. This covers SharePoint, Teams and Outlook for emails. Users will be able to read and write emails, including viewing attachments but will not be able to download and upload documents and attachments.

Access to any Combined Authority systems by known 3rd parties should be requested via the DTS Service Desk to ensure due process is followed.

Cyber Security

All users must undergo annual cyber security training provided by iHasco. In conjunction with this DTS Security Policy, the cyber security awareness training defines information security roles and responsibilities for all personnel, making all personnel aware of their information security responsibilities.

Information security roles and responsibilities are coordinated and aligned with internal roles and external partners. This covers security devices like firewall monitoring in order to provide adequate separation of duties for critical functions. Contracts, nondisclosure agreements (NDAs) and service level agreements (SLAs) with critical vendors must ensure cybersecurity controls and incident notification are addressed appropriately.

It is important to ensure that the Combined Authority's policies and procedures relate to continually improving protection processes, thorough the consideration of the following:

- Ongoing audits, assessments and vulnerability scanning are conducted, reviewed and responded to.
- Plans, processes and policies are updated based on lessons learned from tests (e.g., business continuity, disaster recovery, incident response).
- Designated position and/or committee responsible for continuous evaluation of the organisation's information security needs and posture.
- Threat information gathering and responses to changes in the threat environment.

Combined Authority employees have a duty to ensure the integrity of systems and data by remaining vigilant to threats and questioning when unsure. Users must be familiar with the main forms of Cyber Security threats including but not limited to:

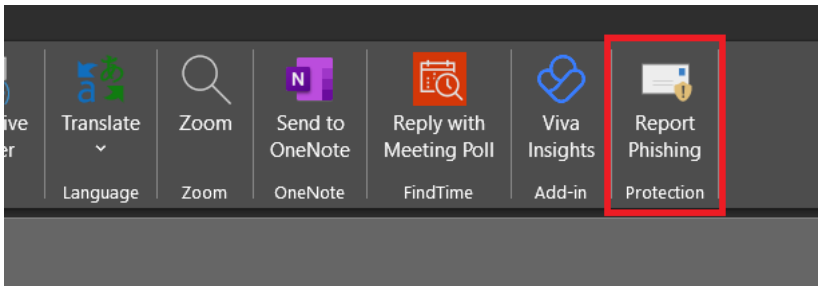
- Social Engineering. Attackers use various methods to obtain credentials or information needed to gain access to systems. This could be via email, phone calls, social media or impersonating a trusted source.

- Phishing. The act of sending an email that looks to have come from a legitimate source, requesting information or asking for money to be transferred. It may appear to come from a trusted source, but usually contains demands or tight timescales designed to exert pressure.

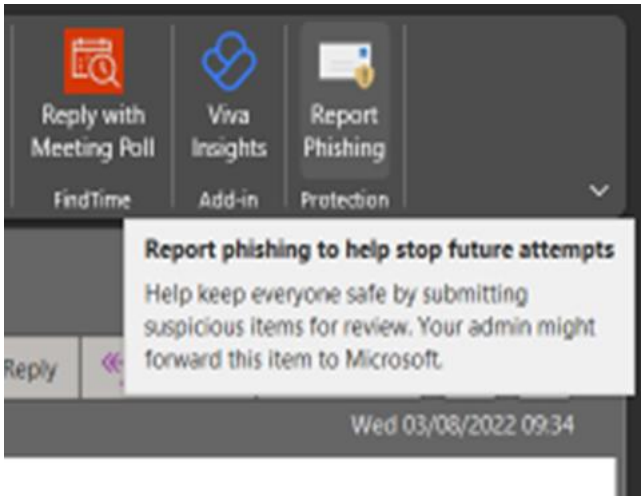
- Malware. Any software or program designed to cause harm or exploit security flaws. It can take many forms, but the most common threat is Ransomware, designed to lock users out of files until a ransom payment is made. Malware may arrive though various methods, but the main method of distribution is via emails designed to look interesting or intriguing, enticing the user to open them. Malware may also be distributed via malicious websites using pop-ups.

Although Cyber Security threats can come in many forms and are sometimes very difficult to spot, users must remain vigilant and never open emails, click on links or visit websites that are sent by a suspicious source.

If an employee is suspicious of any content or they think they have detected a threat, press the "Report Phishing" button immediately as below to report the mail to the Cyber Security team in DTS Services.



The button is purely to help stop future phishing attempts, as well as to cut down on SPAM. It deletes the email, updates Microsoft and notifies the Security Operations Centre (SOC) who can perform additional analysis. The mail can be reinstated on request to the DTS Service Desk.



12. Physical Security

The location of computer equipment will be planned in consideration of potential risks from fire, natural disasters and civil unrest. This will also consider potential risks associated with neighbouring buildings.

DTS Server Rooms and other DTS Areas

These are the responsibility of the Live Services Manager.

The organisation's DTS Server Room and other designated DTS areas must be closed and locked at all times, with restricted access limited to named individuals approved by the Live Services Manager. The DTS Server Room and Build Room must have CCTV installed.

Visitor access should be recorded in a visitor log and entry to the DTS Server rooms should be arranged and approved by one of the following, who should accompany the visitor or arrange for a member of their team to do so:

- Live Services Manager
- DTS Systems Engineer
- DTS Service Desk Manager
- Head of DTS Services or above

Door locks used on DTS Server Rooms must be significantly more robust than the standard used by internal offices, such as the magnetic ACS logs. The ACS logs should be augmented with a separate physical lock, so doors should be able to withstand a level of physical force that is likely to be exerted by those seeking to unlawfully gain entry.

DTS Server rooms must be neat, tidy with minimal dust. They should be highly clean environments with no rubbish, unkempt cabling and storage of items which are not essential to the provision of technology services. Food and drink is strictly not allowed in these areas.

Facilities must provide the ability for entrants to the Server Room to be able to disengage the HVAC system when entering. Server Room entrants must disengage on entry and re-engage when leaving the room.

Where room keys are used, these should either be combination locks or keys which are stored in a safe overnight. Combination lock codes used on server rooms, DTS storage areas or safes should be changed at least on a quarterly basis and these details recorded in a private SharePoint area. A strict key management procedure will be formulated and adhered to by all staff.

Safes used for DTS storage should be designed to meet European standards for safes EN 1143-1:2015 grade 2 or higher.

Storage & Security of DTS Equipment

In order to securely store DTS equipment (mostly end user devices such as laptops and desktop PCs) a Storage Facility will be provided by Facilities and Assets. The integrity of this facility is the responsibility of Head of Assets while the Head of DTS Services is responsible for its management and operational use.

Access controls to the Storage Facility as well as protocols for the security of assets within the facility are set by the Head of DTS Services and Head of Assets or their delegated team members.

Volumes of storage and deliveries are managed by ICT Services and Facilities & Assets to ensure stock levels can be maintained within the facility.

Electrical Protection

Key elements of the DTS systems will be protected against problems emanating from the power supply. These will include variations in power that may lead to failure in maintaining service and complete loss of power. All key systems, including servers and network equipment will be protected by an uninterruptible power supply.

Fire Protection

The main computer suite will be fitted with an automatic smoke detection system and an automatic fire suppression system. Appropriate fire extinguishers will be located immediately inside the access doors.

Flammable materials must not be stored inside the main computer suite.

Natural Disasters

Where possible, ICT installations will be located on a floor that is a reasonable distance above ground level to avoid flood damage. Installations should also avoid any internal plumbing systems.

Neighbouring Accommodation

Consideration will be given to the adjoining rooms and buildings when locating DTS installations. A risk analysis will be carried so that any risks can be mitigated.

Standby Services

Uninterruptible power supply systems will be provided to ensure that the service can be maintained to enable DTS systems to be closed down in a controlled fashion.

13. System Permissions

All changes which affect access to data, network folders and system software must be logged with the DTS Service Desk.

- Changes must be logged by the Information Asset Owner of the resource in question.
- Where changes are required which will affect a person who is no longer employed by the Combined Authority, the request must be submitted by either:
- The relevant Head of Service (if this person is of a higher grade than the ex-employee).
- A member of the Senior Leadership Team (if this person is of a higher or equivalent grade than the ex-employee).
- The appropriate Information Asset Owner
- The Managing Director.

For information governance reasons, personal assistants and others cannot independently speak on behalf of more senior staff. Where necessary, required changes can be set-out by employees and forwarded to ictservicedesk@westyorks-ca.gov.uk by the Information Asset Owner or a Senior Leadership Team member with “approved” written next to the requirements.

14. Risk Assessment Process

Ensure that a risk-assessment process is documented that:

- Is performed periodically, where possible annually and upon significant changes to the environment (for example, merger, relocation, etc.),
- Identifies critical assets, threats, and vulnerabilities
- Identifies the factors that contribute to the likelihood and/or impact of a threat being realised.
- Identifies the associated controls corresponding to those threats and vulnerabilities for the identified critical assets.
- The procedure must determine, and include justification for how frequently the control must be performed to minimize the likelihood of the threat being realised.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
- Performance of updated risk analyses when needed, as determined by the annual review.
- Results in a formal, documented analysis of risk, producing a formal risk assessment using either the ISO 27005 or NIST SP 800-30 risk assessment methodology

14.1 Control Review

A targeted risk analysis must be performed to review each control to include:

- Documented evidence detailing each element specified in the risk and associated control(s).
- Approval of documented evidence by senior management.
- Performance of the targeted analysis of risk at least once every 12 months.

Where a control is to be performed periodically, the frequency of how often it is performed is supported by a targeted risk analysis as per above.

The Cyber Security Manager is responsible for performing the control review.

14.2 Governance and risk management

The Senior Management Team and through the internal audit reporting procedures, must provide board oversight and understanding of cybersecurity, taking into account the following:

- Risk Management
- Governance Structures
- Security Oversight
- Training
- Accountability

- Reporting

14.3 Internal and External Audit Reports

Internal and external audit findings must be noted and responded to in a timely and managed way.

The Cyber Security Manager is responsible for responding to security finding from internal and external audits.

14.4 Legal and Regulatory Requirements

Changes in cybersecurity laws and regulations must be monitored and changes reviewed as required.

The Combined Authority will follow information security guidance from the NCSC, DLUHC and CPNI, as well as best practice covering standards including OWASP, NIST, CIS and ISO 27001. The Cyber Security Essentials is a standard which the Combined Authority is also focused on achieving. The Combined Authority takes card payments, so PCI controls are within scope which are identified below.

The Cyber Security Manager is responsible monitoring and reviewing changes to cyber security laws and regulations.

15. PCI Controls

The payment processing is performed by various 3rd parties, but because the process is performed under the Combined Authority's merchant IDs and the card data is transmitted in some form through the Combined Authority's network, the Combined Authority is in scope of Payment Card Industry.

The Combined Authority has the following payment channels:

1. Kiosks (Cammax) - SAQ P2PE
2. Website and mobile applications (MCard Write app with Moulton Mouse and MCard Mobile payments with YorCard) –SAQ A.
3. Tills (Haven) - SAQ P2PE

16. Ransomware and Extortion

Ransomware is a type of malware which encrypts data and then a payment is demanded to unencrypt the data. As well an encrypting data, attackers will often exfiltrate data as well to increase the pressure to pay the ransom demand, known as "double extortion".

The Combined Authority has mechanisms in place to prevent, detect and respond to ransomware attacks which minimise the risk of an attack occurring, and backups of data stored in immutable storage which would be used to recover systems in the event of a

successful ransomware attack. The DTS Major Incident Policy details how a major incident such as a ransomware event would be managed and DTS would restore services following documented and tested recovery procedures.

It is not illegal to pay a ransom in the UK, however it is strongly discouraged, with the International Counter Ransomware Task Force (ICRTF) of which the UK is a member, stating:

“We have reached consensus that relevant institutions under the authority of our national government should not pay ransomware extortion demands.”

Paying a ransom to ransomware actors:

- does not guarantee the end of an incident, or the removal of malicious software from your systems
- provides incentives for criminals to continue and expand their activities
- provides funds that criminal actors can use for illicit activity
- does not guarantee you will get your data back

It is the Combined Authority’s position not to pay a ransom demand in the event of ransomware encryption or data exfiltration.

Responsibilities

All Staff – Must report any suspicious activity or ransom demands to the DTS Service Desk immediately.

Cyber Security Manager – Determine the validity of any threat and invoke the DTS Major Incident process to perform the following steps:

- Detect and analyse
- Contain
- Eradicate
- Recover

Information Governance Manager – To investigate if a data breach has occurred, identify the severity of any breach and ensure our statutory obligations to report a breach within 72 hours is achieved.

17. Foreign Travel

To protect against cyber security threats which often originate from outside the UK, access to the Combined Authorities systems is restricted by default to the UK and Ireland. If access is required from other countries, a request for this to be enabled must be summited to the DTS service desk prior to travel, stating which countries access is required from and the period of travel.

18. Exceptions

Any exception to the policy must be approved and recorded by the Cyber Security Manager in advance and reported to the DTS Service Desk. The following exceptions have been noted:

- Combined Authority and Bring Your Own Device items currently do not enforce multifactor authentication when sometimes accessing the Combined Authority's O365 services. However, the Combined Authority will use Microsoft InTune to enforce biometric multifactor authentication to BYOD mobile devices when enrolled into InTune and Multi Factor Authentication will be enforced for all Combined Authority devices shortly.
- Certain legacy applications do not support multi factor authentication.
- There are also legacy applications which do not support sufficiently long passphrases and will have to continue to follow existing password complexity rules.

19. Formal Action

Employees should note that any breaches of this policy may be considered either misconduct or gross misconduct and may lead to action within the Combined Authority's Disciplinary, Conduct & Capability Policy and Procedure.

20. Equality Impact Assessment

In the creation of this policy, consideration has been given to any possible adverse equality impact for the following groups: disability; gender; gender reassignment; marital status (including civil partnerships); sexual orientation; race; religion or beliefs; age; pregnancy and maternity. The policy is considered to have little or no adverse equality impact.

21. Changes to Policy

The Combined Authority reserves the right to amend the details of this policy as required following consultation with recognised trade unions and other relevant parties.

This policy will be monitored and reviewed on an annual basis, as part of the continual improvement process to ensure that it meets the needs of the Combined Authority and ensure compliance with relevant legislation.

A written request can be made to review this policy at any time, by any of the signatories, giving appropriate reasons for requesting the review.

22. Accessibility

Accessibility has limited effect on this policy. Most systems and software can be amended to suit accessibility needs to allow all users to comply with password requirements.

Employees should contact the DTS Service Desk should they have accessibility needs which effects their adherence to this policy.

Find out more
westyorks-ca.gov.uk

West Yorkshire Combined Authority
Wellington House
40-50 Wellington Street
Leeds
LS1 2DE

West Yorkshire Combined Authority | Tracy Brabin Mayor of West Yorkshire

All information correct at time of writing