Cyngor Abertawe
Swansea Council

Swansea Council

Cyber Security Strategy

V2.0 Sept 2023

Contents

Cyber security means
working together to PROTECT the Council

1. Foreword by Head of Service

As we move with the digital world, it is more important than ever for Swansea Council staff to protect themselves and the Council from cyber threats.

The Council holds large amounts of data to help make decisions and provide a service to the public. It is held on networks and in software programs.

Some criminals will try anything to steal this data to inflict financial and/or reputational damage, or to hold us to ransom.

Part of my responsibility is to ensure Swansea Council has the ability to defend itself against attacks by criminals, and recover from incidents like hard drive failures or power outages. I can only do this with the help of **all** of our staff.

Even with our strong security controls that we will put in place, we will always experience cyber-attacks. An attacker is always one-step ahead and will exploit the weakest links, but many attacks are easily preventable by staff performing basic security tasks.

We all have a duty to perform these tasks such as maintaining strong passwords and authentication practices and not storing sensitive data where it is openly accessible.

With regard to the General Data Protection Regulation (GDPR), should we fail to protect our data then the Council can risk the safety of individuals, loss of financial information, breach of commercial confidentiality and subsequent financial penalties from the regulator, the Information Commissioner.

This cyber security strategy sets out our plan to help make Swansea Council more resilient in a fast moving digital world. This is no longer an issue for Digital services but for the whole workforce.

Thank you

Sarah Lackenby

Head of Digital and Customer Services

2. What is cyber security?

Cyber security refers to the preventative techniques used to protect the integrity of our networks, programs and data from attack, damage or unauthorized access.

Cyber criminals use a variety of malware (MALicious softWARE) to attack the Council. Their motivation can vary, from demonstrating their technical digital skills for personal kudos, to general disruption, financial gain, commercial advantage or political protest.

As a Council, we have no control over their capabilities and motivations, but we can make it harder for attackers by reducing our vulnerabilities. The impact (and therefore the harm) on the Council will depend on the opportunities we as staff present to an attacker.

3. Our vision

Cyber security is important because we collect, process, and store large amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences.

Our vision is to:

- defend the Council against evolving cyber threats
- respond effectively to incidents
- ensure our data and systems are protected and resilient
- ensure staff have the knowledge to protect themselves
- work with the National Cyber Security to help provide a national response to cyber threats.

A question for you

In your personal life, would you:

- **make yourself vulnerable by leaving your front door open when you go out?**
- **put your bank statement by the window in clear view of people walking by?**

Probably not. So let's bring your home life skills into the workplace and protect the Council's data and network as best you can.

4. Cyber threats

As an ever present threat, cyber-attacks must be understood and defended against. This will ensure our systems retain their integrity and will protect us from data breaches and cyber theft. The types of threats include:

4.1 Malicious software

Cyber criminals will use embedded links in emails and websites to upload malware onto your digital device. Digital and Transformation Service deal with these on a daily basis and has the relevant staff skills and anti-virus software in place to lower the risk of the attacks penetrating our networks. Some examples of attacks are as follows:

- Ransomware blocks the victim's access to their files, images and videos etc. and inserts a warning message on their screen. The only way to regain access to the files is to pay a ransom.

- A **computer virus**, much like a flu virus, has the ability to replicate itself and is designed to spread via computers. It's a type of malicious code or program written to alter the way a computer operates. A virus operates by attaching itself to a software program or document that sits on your device.

- Spyware is installed on a device without the knowledge of the owner in order to collect the owner's private information and send it back to the attacker. Spyware is often hidden from the user in order to gather information about their internet interaction, keystrokes (also known as keylogging), passwords, and other valuable data. It can also turn your camera on.

- A **Trojan horse** is often disguised as legitimate software. Users are tricked into loading and executing Trojans on their systems by thinking they are uploading free software but in fact are uploading malware onto their device. Once activated, Trojans can enable criminals to spy on you, steal your data and gain backdoor access to your system providing remote access to everything including emails.

4.2 Phishing

Phishing threats means criminals are trying to steal data from you so they can commit identity theft. This could be through fraudulent email messages appearing to come from legitimate enterprises (e.g. Amazon, your internet service provider, your bank) or someone pretending to be your friend on social media. It can also happen over the phone.

These messages usually get you to divulge private information (e.g. passphrase, credit card, or other account updates). Remember, companies like your bank or Microsoft will never email or ring you to gather your private information.

4.3 The insider

Anyone who has legitimate access to our systems as an employee or a contractor must also be considered as part of our security regime. Managers are responsible to ensure they monitor their employee's daily activities and understand who has access to our sensitive data.

Threats from staff may be accidental due to the fact they have clicked on that malicious link in an email (attackers are just waiting for employees to slip up). However, staff may also be motivated by personal gain or redress against grievances. An insider could simply use their normal access to compromise our data by taking advantage of their permissions, unlocked computers or guessable passwords.

Staff can also be negligent. These are the inside threats where employees try to avoid the policies and procedures we have put in place to protect valuable data just to make life easier for themselves. For example, staff may download data from a secure platform and email the data to their unsecure home PC to work on in the house. NOTE: Council data must only be stored in emails or on corporate servers/cloud.

4.4 Weak passwords

Passwords are an integral part of information security but are frequently targeted by criminals when trying to break into a system. If your password is compromised, then anything your user account is able to do or access is at risk.

Good passwords need to be both memorable and difficult for an attacker to guess or figure out. As a minimum, the council require a number of controls aimed at making the job of the criminal as time consuming and difficult as possible. Systems must be configured to enforce these rules where possible.

4.5 USB memory sticks (portable media)

Humans are curious creatures. The cyber-criminal will leave a device such as a USB stick that is infected with malware out in the open in a public place. Someone will pick up that device and plug it into their computer to see what's on it. The malware will then inject itself onto the computer and the trouble starts!

USB sticks are one of the highest risk areas and the main routes of data loss. Even though they are convenient, portable and easy to use, they are also easy to lose or mislay. Staff need to be made aware that the Information Commissioner's Office (ICO) is taking a tough line with local authorities over data security breaches and the loss of USB memory devices. They should only be used when absolutely necessary.

5. Setting our goals

5.1 Email filtering

The Council will use an externally hosted email filtering service to prevent the sending and receiving of emails which contain known and suspected virus infections and inappropriate key words (including racist vocabulary). It will also block emails from known SPAM mail originators. **NOTE**: Users still need to be highly vigilant, even suspicious as filtering has limits.

5.2 Firewalls

Firewalls and filtering software will be our first line of defence to monitor incoming and outgoing network traffic. It will decide whether to allow or block specific traffic based on a defined set of security rules. These will be constantly reviewed by the 3rd party suppliers as new threats are discovered.

As a minimum, these rules will block material which is of a sexual or violent nature including child abuse or adult pornography, online gaming, extremist websites etc.

5.3 Software patching

Council staff use a variety of software to undertake duties. Digital Services will use a patch management process that helps acquire, test and install multiple patches on existing applications and software tools, enabling systems to stay updated and secure from weaknesses and unauthorised access.

5.4 Encryption

Encryption will be used on mobile devices as a security measure that makes data unreadable if it's stolen. Transferring data online via emails opens the Council up to possible data loss, so email encryption will be available to help protect the content from being disclosed to unauthorised recipients. Staff must purchase encrypted USB portable media to transfer data securely out of the office.

5.5 Antivirus software

Up-to-date anti-virus software will be installed on all Council PC's and laptops to detect and remove malicious software.

These tools are critical for staff to have, because a PC or laptop without anti-virus software installed will be infected within minutes of connecting to the internet. The bombardment is constant. Anti-virus software will also be installed on all our servers to protect the data we store on our shared drives.

In your personal life, you must ensure you protect your own ICT devices. Further details are on staffnet:
https://staffnet.swansea.gov.uk/protectingyourpersonaldevices

5.6 Council policies and procedures

The Council will have ICT policies and procedures to ensure staff are responsible for their actions when using technology. These policies will outline the acceptable use of all Council ICT equipment and facilities.

NOTE: All Council staff members will be required to use the ICT equipment and facilities in an appropriate and professional manner.

5.7 Social media access

Staff will only granted access to social media / networking for specific business reasons in a work-related professional capacity. Outside the Council, staff can freely access social media sites but this must be handled in a sensible and considered way in line with the Councils code of conduct so that neither the individual nor the Council is put at potential risk of embarrassment, loss, disciplinary action or criminal proceedings.

5.8 Data backup

The data the Council holds on its servers will be backed up every night and taken off-site. In the event of a disaster, data can be restored from the previous day.

5.9 Mobile working and remote access

Mobile working and remote access offers great business benefits to the Council. Staff will have the facilities to work outside their office and still have the same secure setup as if they were sitting at their desks.

5.10 Cloud Storage

Digital Services will provide access to approved cloud facilities which has advanced security and sharing capabilities for staff to transfer data securely across the internet via a username and password.

To conform to data protection regulations, staff must not use non-corporate Cloud storage facilities for sharing confidential, sensitive or classified information unless approved by Digital Services. E.g. dropbox, google docs etc.

5.11 Penetration testing

The Council will undergo an annual ICT penetration test designed to evaluate the effectiveness of our security controls and to highlight any vulnerabilities that could impact our networks.

The Council is connected to the Public Services Network (PSN), which is the government's high-performance network helping public sector organisations work together, reduce duplication and share data/resources.

To maintain our connection to the PSN, we must ensure our security connections are compliant with a code of connection framework set by the Cabinet Office.

If we fail this audit, we risk being cut off from the network and unable to access critical services which will have a huge impact on service delivery. Exchange of benefits data with the Department for Work and Pensions is an example. This audit will be performed by a third party and internal testing will also be undertaken on a quarterly basis by Digital Services.

5.12 Training and development

Various webpages will be available to staff to improve their awareness of security. This includes the use of encrypted memory sticks and external hard drives and storing them securely.

Mandatory Data protection and cyber-security eLearning will be available via learningpool. Passwords are an integral part of ICT security so we will encourage staff to select a good, complex and memorable password.

Key messages will be sent from the ICT Service Desk to inform staff of potential issues including cyber-attacks. To help staff keep their personal information safe online, we will put together useful tips to help avoid them becoming a victim of fraud:
https://staffnet.swansea.gov.uk/befraudsmart

6. Protect yourself and the Council

This strategy is intended to shape the way the council and staff are protected from cyber threats. Staff must ensure this strategy is implemented in all parts of the Council to continually increase our cyber security levels.

All staff must be part of our vision to defend the Council against evolving cyber threats. It will never be possible to stop every cyber-attack; however, working together can build layers of defence that will significantly reduce our exposure to cyber incidents.

Data protection is a key responsibility to all staff. Digital Services has an Information Asset Register (IAR) that identifies all software systems that hold data. If you process data electronically within your service then you must identify the system on the IAR. See Staffnet for details:
https://staffnet.swansea.gov.uk/ropa

Digital Services evaluates the entries in the IAR to ensure the correct permissions and protection has been assigned. By identifying your assets, you are protecting your service against the impact of a data breach due to the fact, fines will be much heavier from the ICO if your system has not been identified on the IAR and data is lost from that system.

Finally, the Council will measure its success to cyber security by the number of successful cyber-attacks that have penetrated our business. It will also be measured against an improved security culture across the organisation. Some **top tips** for cyber security can be found in appendix 1.

7. Report any threats or concerns

A key priority for staff is to ensure they know the ***two simple steps*** required to report a cyber security incident once it has been recognised.

Details of the incident must be provided to ensure quick response. Details can then be logged and a security incident report (appendix 2) completed by Digital Services. This includes your name, affected area and a brief description of where the incident was discovered.

STEP1. Report the incident to the ICT Security Officer using
Cybersecurity@swansea.gov.uk

STEP 2: Alert the ICT Service Desk
ICT.servicedesk@swansea.gov.uk

The Council strive to create a non-blame culture where staff can be confident in reporting any cyber incidents without worrying about personal consequences.

Appendix 1 - Cyber security top tip

Don't become a victim of cyber crime

- ✓ Criminals want you to act first and think later. If the email conveys a sense of urgency, or uses high-pressure tactics; never let it influence you.
- ✓ Research the facts. Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research before replying.
- ✓ Don't let a link control where you land. Stay in control by finding the website yourself using a search engine to be sure you land where intended.
- ✓ Curiosity leads to careless clicking – if you don't know what the email is about, clicking links is a poor choice. Similarly, never use phone numbers from the email as it's easy for a scammer to pretend you're talking to a bank.
- ✓ Email hijacking is rampant. Once they control someone's email account they will prey on the trust of all the person's contacts.
- ✓ Beware of any download. If you don't know the sender personally AND you are not expecting a file from them, downloading anything is a mistake.
- ✓ Foreign offers are fake. If you receive email offers from a foreign lottery or from an unknown relative it is guaranteed to be a scam.
- ✓ Watch those USB devices – they could be dangerous! If you find any, report them to the ICT service desk or the Council's security officer at cybersecurity@swansea.gov.uk. NEVER plug them in!

Discuss cyber bullying with children

- ✓ Set parental controls to ensure privacy settings are at their highest. See Internet Matters for information www.internetmatters.org/parental-controls
- ✓ The internet never sleeps - online bullying can reach children anytime especially when the adults are asleep. Make sure your children are not on their devices past a certain time at night
- ✓ It's easy to do - even children who have never been involved in bullying can post or share something without thinking. Make sure children are aware of cyber bullying and the impact it can have.
- ✓ It can be anonymous - even though you can keep the evidence, it's hard to identify who's behind it
- ✓ Talk about it - if children you know use social media, don't wait for bullying to happen. Talk about it now.
- ✓ Beware when they share - Discuss what children should and should not share online and how this could invite bullies.
- ✓ Take it seriously - Check in with children and be mindful of signs that they may be getting bullied.
- ✓ Block and report - Teach children what to do if they want to report or prevent abusive messages because sometimes they don't want to discuss it with you.

Don’t fall for text message scams

A text might not be from who you think – this is when criminals pretend a message is from your bank or another organisation you trust.

They will usually tell you there has been fraud on your account and will ask you to deal with it by calling a number or visiting a fake website to update your personal details. Please take a moment to stop and think and realise this is the fraud.

3 signs a text message might not be genuine:

- ✓ It asks you to provide sensitive personal or financial information, passwords, or to make transactions by following a link in the message.
- ✓ It asks you to call a certain number but that number is unknown to you. In this case, call your bank on a number that you trust to check the number and that the message is authentic e.g. ring the number on the back of your bank card.
- ✓ The sender uses an urgent tone, urging you to ‘act now’.

Appendix 2 – Security incident report

Cyngor Abertawe Swansea Council	Swansea Council Security incident report			
	Affected area:			
	Date identified:		**ID No.**	**SI.**

Section 1 – Identification and assessment

1. Discovery
(Detail how and where the infection was discovered. Include staff names where applicable)

2. Incident process
(Detail the actions taken to communicate the incident and assign responsibilities)

3. Affected areas
(Detail what servers/drives/users were affected)

4. Investigation and actions
(Provide a full assessment on the scope of the infection and the actions taken to mitigate)

Section 2 – Impact and prevention

5. Clean up
(Identify what was put in place to recover from the incident)

6. Suspected cause of the infection
(Following investigations, identify the cause of the incident)

7. Impact to the Council
(Details how services were disrupted following the infection)

8. Future activities
(Identify any outcomes, concerns, lessons learned and long term resolution plans and strategies)