SAMPLE CYBERSECURITY REPORT CARD

Essential

Client Winterby Town Council
Date 5 November 2024

4N6

Technology Resilience for the Cyber Age

This report has been compiled by 4N6 Limited, a company registered in England and Wales No. 15477135.

Tel 0300 1880 365
Email hi@4n6.io
Web www.4n6.io

Registered Office: 5th Floor,
167-169 Great Portland Street,
London,
W1W 5PF.

Table of Contents

Date	Author	Description
4 Nov 2024	Jamie Taylor	Initial version
4 Nov 2024	Sean Howell	QA check
5 Nov 2024	Jamie Taylor	Action Plan agreed with client

Summary

The IT systems are of low complexity. Staff use laptops with local logins then access Microsoft 365 (Email and cloud storage) using their council login. The website is hosted externally.

Many of the IT security and physical security measures in place are appropriate for an organisation of this size, although there are areas of improvement some of which should be implemented as soon as possible.

High Priority Actions

- **URGENT:** Update router firmware and/or close port 22.
- Update outdated software on all devices.
- Remove administrative privileges from all users.

Medium-Term Actions

- Implement a password policy.
- Change the router's password from the default.
- Perform security upgrades to Email and the Website.
- Consider upgrading Windows 10 devices to Windows 11 where possible. Some devices may not be able to support Windows 11 so new devices may need to be purchased.
- Put in place a process to regularly check whether software and operating system updates are available and have been installed.

Long-Term Actions

- Apply all controls required for Cyber Essentials and optionally consider applying for Cyber Essentials certification. Please see www.4n6.io/cyber-essentials for more information.

Cyber Risk

Cyber Risk Profile

Winterby Town Council is a local council covering Winterby and the surrounding area (population 7,234) in South Havenshire. They provide services to the community including:

- Promoting and developing a busy programme of recreational and social activities,
- Maintenance and leasing of the community centre and the allotments,
- Provision and maintenance of the cemetery,
- Grounds maintenance and general gardening related to public spaces including the town centre park,
- Representation via town councillors, and
- The creation and adoption of the Winterby Local Plan.

The Council has one office, on Winterby High Street, which is used by the Town Clerk, two full-time staff and two part-time assistants. The office has an intruder alarm with a contracted monitoring service, a composite door to the front and uPVC double glazed windows that are internally lockable. The rear door, used as an emergency exit, is solid wood but also has a high security metal shutter that is locked when the building is not in use. The front of the office is covered by CCTV and is well lit after dark, but the rear is not covered by either CCTV or lighting.

The office has a router, 5 laptops and a multifunction printer. There are 5 telephones which have external calling via a traditional PABX to a single external line. The council have a website running on Wordpress, which is hosted externally. Email and cloud storage are also hosted externally using Microsoft 365. The council have in place a support contract for IT services, but the provider does not have expertise in Cybersecurity.

Much of the information handled by the council is not sensitive in nature, and in many cases can be made public via the Freedom of Information Act 2000. The Council invites tenders for external services, which are commercially sensitive. The Council has access to the electoral roll for the local area, including those who have opted out of appearing on the public register for a variety of reasons. It holds sensitive personal data in relation to its staff. The Council occasionally receive correspondence from the public that contains sensitive personal data.

Short disruptions to IT systems are tolerable but longer-term disruptions would significantly affect the Council's ability to carry out the services it provides to the community. The impact of unauthorised disclosure of information would depend on the sensitivity of the data. Much of the information held is routine, but there is some sensitive data of both a personal and a commercial nature. The effect of incorrect or manipulated data would depend on what the data is. The most obvious area of a potential error with damaging effects is in financial records, but these are checked for accuracy and independently audited annually.

Whilst Winterby Town Council is considered part of government, it does not face the same threats as central government, unitary authorities, county councils, borough councils or district councils. The threats it faces are similar to a small business but could attract greater media attention in the local area should there be a disruption to services or loss of control of sensitive data.

Adversaries and Attack Methods

Not included in this report

Technical Checks

Email Security Check

Check	Description	Comment
SPF	SPF is an email authentication technique used to prevent unauthorised sending of emails pretending to emanate from your domain.	✅ SPF record in place.
PTR	PTR works with SPF to ensure the server sending the email is in your allowed list of senders.	✅ Test email's PTR record ok.
DKIM	DKIM is another email authentication technique to prevent unauthorised sending of emails pretending to emanate from your domain.	✅ Test email's DKIM record ok.
DMARC	DMARC is an important anti-spoofing control. It tells recipient email services what to do with emails that do not pass SPF or DKIM checks.	❌ No DMARC record in place.
TLS	TLS allows for messages to be encrypted when sent to you. If the other party's email servers also support TLS, you will be able to send them encrypted emails.	✅ TLSv1.3
MTA-STS	Emails are now usually encrypted using TLS when being sent or received but it is possible for adversaries to force this to be downgraded which means the message will no longer be encrypted. MTA-STS is a standard designed to address this vulnerability.	❌ No MTA-STS record in place.
BIMI	BIMI is a new standard allowing the display of your organisation's logo in users' inboxes when the DMARC, SPF and DKIM checks are passed. This standard is not yet widely recognised and can be costly to implement and maintain so we cannot recommend proactive adoption.	💡 No BIMI record in place.

Recommended Actions

DMARC

- Sign up to a DMARC reporting service
- Establish a basic DMARC policy (p=none)
- Monitor the results using your DMARC reporting tool
- Move to a strong DMARC policy (p=quarantine or p=reject)

We can assist and guide you through the process of implementing DMARC.

MTA-STS

- Create an MTA-STS file and have it hosted at https://mta-sts.winterbytowncouncil.gov.uk/.well-known/mta-sts.txt
- Create an MTA-STS DNS record

We can assist and guide you through the process of implementing MTA-STS.

Website Security Check

Check	Description	Comment
HTTPS	HTTPS ensures there is a secure encrypted connection to your website.	✅ HTTPS available
HTTP Redirect	Insecure HTTP connections should be redirected to HTTPS unless there is a good reason not to.	✅ HTTP redirect in place
TLS	There are different versions of the protocols that HTTPS uses. We recommend you only use TLS1.2 and TLS1.3.	❌ TLS1.0, TLS1.1 and TLS1.2
HSTS	HSTS means that once a browser has accessed your website it will only attempt to connect to it over HTTPS in the future.	❌ No HSTS
HSTS Preload	Browser manufacturers can include your domain in a list that will always apply HSTS.	❌ No HSTS Preload
Certificate	To allow connections over HTTPS your website needs a certificate, from a reputable vendor, that is renewed periodically.	✅ OK Expires 21 Jan 2025.
CAA	This prevents a certificate supplied by a vendor you do not trust from being recognised by web browsers.	❌ No CAA record in place.

Recommended Actions

TLS

- Remove TLS1.0 and TLS 1.1 support
- Investigate adding TLS1.3 support
- Ensure the cypher suites used give an adequate level of protection

We can assist and guide you through the process of resolving the TLS issues.

HSTS

- Investigate whether you can support HSTS on your website and whether this can be extended to your whole domain
- If it can, put in place the appropriate HTTP headers on your website.
- If you have applied HSTS to your whole domain, and want this to be preloaded.

We can assist and guide you through the process of implementing HSTS.

Website Vulnerability Scan

Not included in this report

Device Security Check

The device selected for the security check is the Windows 10 laptop used by Julie Duncan, the Town Clerk.

Check	Description	Comment
Operating System	The operating system controls the software and how it interacts with the hardware making up your computer. The operating system must be regularly updated to ensure security vulnerabilities are patched.	💡 Windows 10 22H2 installed and activated. Support ends 14 Oct 2025 unless you purchase extended support.
Malware Protection	Protection against malware has traditionally been called an 'antivirus' although there are newer and more complex approaches to stopping malware. You should ensure the computer has malware protection that is regularly updated and set to scan regularly.	✅ Windows Defender is up to date and set to scan regularly
Software	Software on a computer must be regularly updated to ensure vulnerabilities are patched.	❌ Old software with known vulnerabilities - 7-zip, Zoom
Encryption	Encryption prevents someone from accessing the data on your device unless they know the password.	✅ BitLocker is activated
Admin Rights	Malware can use administrative privileges to cause much greater damage than if it was run using a normal user account. For this reason, general computer use should not take place using an admin account. A separate admin account may be created.	❌ User account has administrative privileges

Recommended Actions

- Update the software that has known vulnerabilities (i.e. 7-zip and Zoom).
- Remove administrative rights from user accounts.

External IP Address Scan

The Town Council has a router for their office which they selected for a scan. The external IP address is 172.29.218.189. A full scan of all TCP and UDP ports was undertaken.

Open Port	Description	Comment
22 TCP	SSH – This is used to allow remote access to manage the router.	❌ OpenSSH 6.6.0 has multiple vulnerabilities.

Recommended Actions

SSH on port 22

- Check why the port is open and if it does not need to be left open, close it.
- Investigate whether the router has new firmware available that does not have this vulnerability. If it does, install it as soon as possible.

We can assist and guide you through the process of remedying this issue, including contacting the router vendor about the identified vulnerabilities.

Internal Network Vulnerability Scan

Not included in this report

Policy Review

IT services are provided on request by the external IT support company, but there is little to no proactive management of IT. Staff are aware they must install updates when the systems request it, but this does not cover all installed software leading to some software with vulnerabilities being present on devices. The router uses the default 8-character password as supplied by the ISP.

Office staff are trained in the security of information, including GDPR, via their induction training and annually thereafter. There are good internal processes for ensuring sensitive and personal data in handled securely. There is a good awareness of traditional risk management in relation to health and safety and in relation to business continuity. There are strong financial management procedures.

There is no password policy in place, so staff are free to choose any password they would like.

When staff leave the council, they are required to return their allocated laptop and their Microsoft 365 account is then deactivated by the external IT support company.

Recommended Actions

- Put in place procedures for regularly checking and updating software. The IT support company may need to take a more proactive approach including by using a Remote Monitoring and Management solution.
- Implement a password policy with the following guidance:
    - Minimum length of 8 characters when multifactor authentication is used
    - Minimum length of 12 characters when multifactor authentication is not used
    - Consider using three random words that are not logically connected to each other e.g. dinosaurpentriangle
    - Do not re-use passwords, particularly from non-work accounts.
    - Do not require regular password changes.
- Change the router's password from the default.