SITE survey. APP

SITE SURVEY REPORT

IT Security Audit Checklist

Prepared for	Marlow Design Studio Ltd
Date	26 Sep 2026
Site	Marlow Design Studio, Reading
Prepared by	E. Barker

FORM

IT Security Audit Checklist

1. Details

Project	Marlow Design Studio, Reading: security audit
Customer	Marlow Design Studio Ltd
Site	Marlow Design Studio, first floor
Site address	Kings Yard, Reading RG1
Date of audit	26 Sep 2026
Auditor	E. Barker
What is in scope?	Office laptops and desktops, company phones, the firewall and the studio's Microsoft 365 tenant
Number of users in scope	14
Number of devices in scope	31
How was this checked?	Seen on devices, Checked in admin consoles, Told by staff

How this checklist is built. Pages 2 to 6 follow the five technical controls of Cyber Essentials, the minimum standard of cyber security the UK government recommends for organisations of all sizes: firewalls, secure configuration, security update management, user access control and malware protection. The questions follow the NCSC document Cyber Essentials: Requirements for IT Infrastructure v3.3 (April 2026). This is a readiness check, not a Cyber Essentials assessment or certificate.

2. Firewalls

Is every device protected by a firewall, at the network edge or on the device?	Yes
Has the default administrator password on every firewall and router been changed?	Yes
Can the firewall admin page be reached from the internet?	No
Is every inbound rule approved, documented and still needed?	Partly
Is a software firewall switched on for laptops used on other networks, such as home or public Wi-Fi?	Yes
Notes	Two inbound rules for an old CCTV viewer are still open. Nobody knows if they are needed.

Checks met in this section	4
Partly	1
Not met	0
Not known	0

3. Secure configuration

Have unused and guest accounts been removed or disabled?	Partly
Have default and guessable passwords been changed?	Yes
Has software that is not needed been removed or disabled?	Partly
Is auto-run switched off, so files do not run without the user agreeing?	Yes
Do devices need a PIN, password or biometric to unlock?	Yes

> Where a device unlocks with a PIN or password, Cyber Essentials requires protection against guessing: no more than 10 guesses in 5 minutes, or locking after no more than 10 failed attempts.

Notes	Trial software left on three laptops. One former freelancer account still enabled.
Checks met in this section	3
Partly	2
Not met	0
Not known	0

4. Security update management

Is all software licensed and still supported by its maker?	Partly
What is unsupported, and on which devices?	Two design desktops on an operating system version that has reached end of support. An old PDF editor on four laptops.

> Unsupported software. Cyber Essentials requires software to be licensed and supported, and removed from devices when it becomes unsupported.

Are automatic updates switched on where they can be?	Yes
Are critical and high risk updates installed within 14 days?	Partly

> Updates. Cyber Essentials requires updates that fix critical or high risk vulnerabilities (a CVSS v3 base score of 7 or above) to be installed within 14 days of release.

What evidence did you see?	Device management update report, 26 September 2026: 3 of 31 devices more than 14 days behind
Checks met in this section	1
Partly	2
Not met	0
Not known	0

5. User access control

Is there a process to approve new accounts?	Partly
Does everyone sign in with their own account?	Yes
Are accounts removed or disabled when someone leaves or changes role?	No
Are administrator accounts separate, and not used for email or browsing?	No
Multi-factor authentication	Administrators and internet-facing accounts
Where a password is used, which protection is in place?	Multi-factor authentication
Notes	New accounts are asked for by email to the director. No leaver checklist.
Checks met in this section	1
Partly	2
Not met	2
Not known	0

6. Malware protection

How are devices protected?	Anti-malware software
Is anti-malware kept up to date in line with the maker's recommendations?	Yes
Does it stop connections to malicious websites?	Yes
Is every device in scope covered, including phones and tablets?	Partly

Notes	Two company phones are not enrolled in device management.
Checks met in this section	3
Partly	1
Not met	0
Not known	0

7. Backups, premises and incidents

Is important data backed up?	Yes
Has a restore been tested in the last year?	No
Are servers and network equipment locked away?	No
Do screens lock when left?	Yes
Are visitors signed in and accompanied?	Partly
Do staff know how to report a security incident, and to whom?	Partly
Is there a record of security incidents and personal data breaches?	No

> Personal data breaches. The ICO says a notifiable breach must be reported to it without undue delay, and not later than 72 hours after becoming aware of it. Staff need to know who to tell straight away.

Have staff had security awareness training in the last year?	No
Checks met in this section	2
Partly	2
Not met	4
Not known	0

8. Findings and recommendations

Findings 1: User access control

Area	User access control
Risk	High
What did you find?	A freelancer who left in June still has an enabled account with access to client files.

What do you recommend?	Disable it today. Add a leaver checklist that IT signs off.
Who should act on it?	J. Hart, studio director
By when?	26 Sep 2026

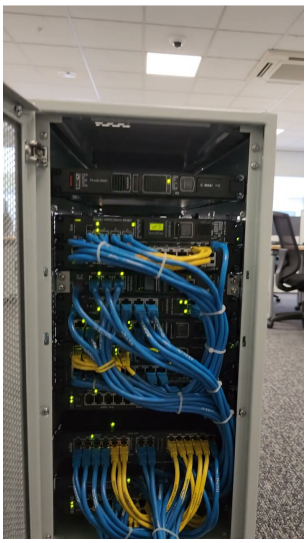
Findings 2: User access control

Area	User access control
Risk	Medium
What did you find?	Both administrators use their admin accounts for everyday email and browsing.
What do you recommend?	Give each a separate admin account used only for admin work.
Who should act on it?	E. Barker
By when?	16 Oct 2026

Findings 3: Physical security

Area	Physical security
Risk	Medium
What did you find?	The network cabinet stands in the open office with its door open. The lock is not used.
What do you recommend?	Keep it locked and give the key to the office manager.
Who should act on it?	Office manager
By when?	2 Oct 2026

Photos or screenshots



Findings 4: Firewalls

Area	Firewalls
Risk	Medium
What did you find?	Two inbound firewall rules for an old CCTV viewer are still open. They are not documented and nobody knows if they are needed.
What do you recommend?	Remove both unless the director confirms a business need, then record it.
Who should act on it?	E. Barker
By when?	9 Oct 2026

Findings 5: Security updates

Area	Security updates
Risk	Medium
What did you find?	Two design desktops run an unsupported operating system version, and four laptops still have an old PDF editor that no longer gets updates.
What do you recommend?	Upgrade both desktops, or replace them if the hardware cannot run a supported version. Remove the old PDF editor.
Who should act on it?	E. Barker
By when?	31 Oct 2026

Findings 6: Backups

Area	Backups
Risk	Low
What did you find?	Files are backed up, but nobody has tried restoring from the backup.
What do you recommend?	Restore a sample project folder to a spare laptop and note how long it took.
Who should act on it?	E. Barker
By when?	13 Nov 2026

Findings 7: Incident readiness

Area	Incident readiness
Risk	Low

What did you find?	No record is kept of security incidents or personal data breaches. Staff remembered a misdirected client email in the spring, but nothing was written down.
What do you recommend?	Start a simple incident and breach log, and record every personal data breach in it, whether or not it is reported to the ICO.
Who should act on it?	E. Barker
By when?	30 Oct 2026
Findings	7
High risk findings	1
Medium risk findings	4
Low risk findings	2

9. Summary and sign-off

Checks met	14
Partly met	10
Not met	6
Not known	0
Share of answered checks fully met (%)	47
Firewalls score (%)	90
Secure configuration score (%)	80
Security updates score (%)	67
User access control score (%)	40
Malware protection score (%)	88
Backups, premises and incidents score (%)	38
Overall score (%)	63
RAG band	Red
Cyber Essentials sections (pages 2 to 6) with every check met	0
Overall	Needs attention

Summary for the customer	Multi-factor authentication and malware protection on computers are in good shape. The main gaps are in accounts: a leaver still has access, and admin accounts are used for everyday work. Before applying for Cyber Essentials, also remove the old CCTV firewall rules, deal with the unsupported desktops and PDF editor, and bring the three devices that are behind on updates up to date.
The three things to do first	1. Disable the former freelancer's account and start a leaver checklist. 2. Separate admin accounts. 3. Upgrade or replace the two unsupported desktops.
Auditor name	E. Barker
Auditor signature	
Customer name	J. Hart, studio director
Customer signature	