Minimum IT Standards Every UK Business Should Meet

Executive Summary

- A basic level of IT security, as well as governance, is required by any and all businesses in the UK, regardless of their size.
- The majority of cyber-attack incidents in SMEs are the result of simple vulnerabilities such as weak passwords, lacking MFA, poor backup maintenance, or systems not being updated.
- When we talk about ‘minimum standards’ we do not mean expensive enterprise software; we mean common-sense, logical security controls.
- The UK GDPR mentions the need for businesses to implement "appropriate technical and organisational measures", and therefore the basic IT security standards form part of that requirement.
- The Cyber Essentials Grant Scheme provides a practical measurement scale for assessing your security level and demonstrating how small firms can protect themselves at low cost with readily available, easy to understand policy procedures.
- A 10 person company could easily achieve a very good level of protection against cyber threats by using very inexpensive tools to implement a set of documented policies that enhance their security.
- Implementing a 30-day structured, low-impact plan would make a significant reduction in your exposure to cyber threats.
- Making small, consistent improvements to IT Security is much more successful than making large one-off fixes.

Who this guide is for

- All UK businesses with staff of 1–50 people
- Owner-managed companies
- Directors, operations managers and office managers
- Decision makers who are non-technical feeling responsible for the security and/or privacy of IT/data.

Why Minimum IT Standards Matter

Most of the cyber incidents that affect SMEs in the UK have not been sophisticated attacks, but are entirely preventable incidents, such as:

- A laptop with sensitive information being stolen and no encryption.
- A Microsoft 365 account being breached because no multi-factor authentication (MFA) was enabled.
- Ransomware attacks encrypting files when there is no available backup of the files.
- Invoice fraud as a result of clicking on a phishing email.

The UK General Data Protection Regulation (GDPR) requires businesses who are Data Controllers to have in place, “the appropriate technical and organisational measures,” as required by Article 32 of the regulation. The Information Commissioner’s Office (ICO) does not expect small businesses to be working towards the same standards as Banks; however, they do expect small businesses to have proportionate controls in place.

In addition, there are many factors working against you if you do not have minimum IT Standards in place:

- Many of the Cyber Insurance Policies require MFA and certain minimum security requirements.
- More and More larger businesses expect their supply chain to be compliant with standards such as Cyber Essentials.
- The impact of any amount of downtime on your small business cash flow or reputation can be immense.
- Minimum IT Standards are primarily about reducing the obvious risk and not adding unnecessarily to the level of complexity.

Core IT Standards

Every single standard outlines: the standard, what's the importance of it, the minimum compliance level that you should be compliant with to be in compliance by 2026, a better than minimum compliance level, the mistakes that are regularly made, and ways you can achieve those standards quickly.

1. Multi-Factor Authentication (MFA):

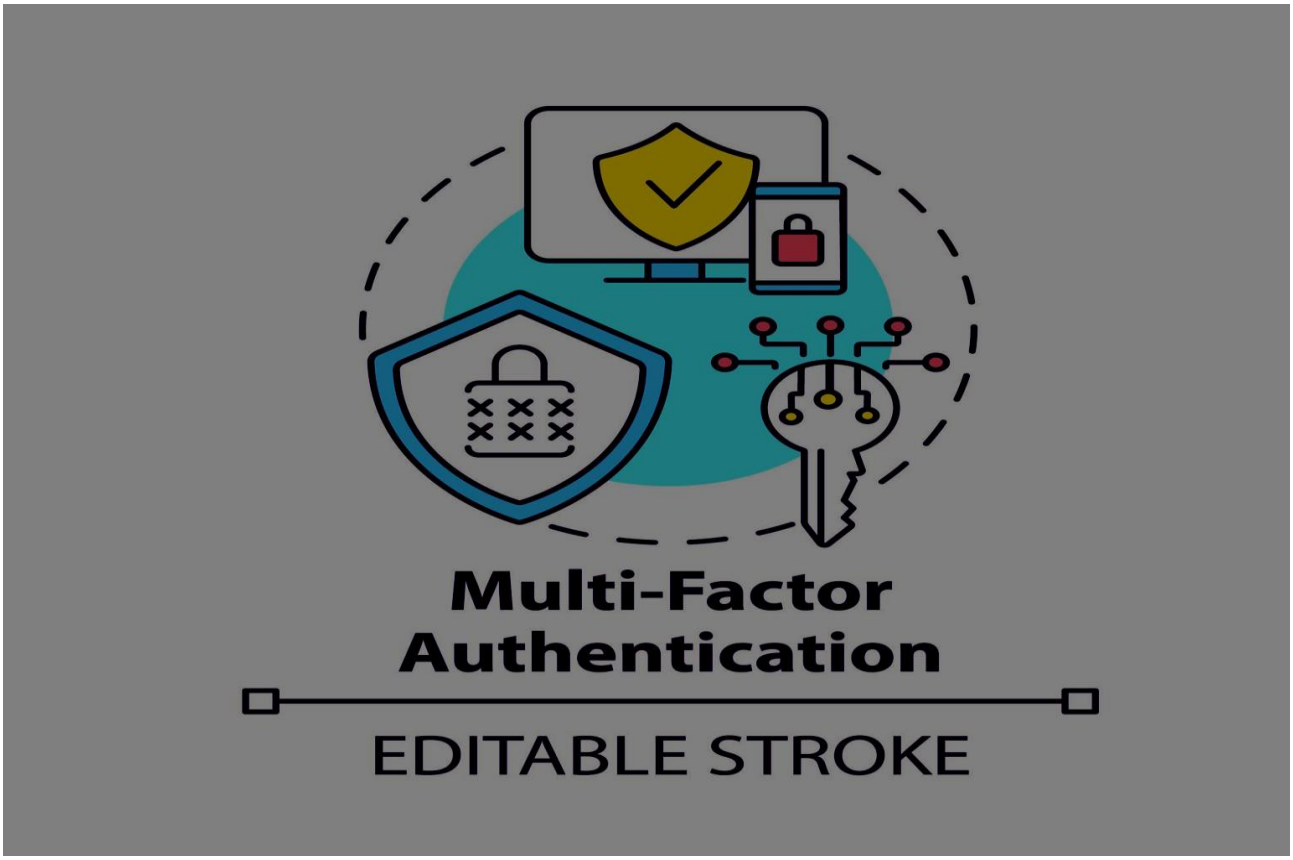
MFA is a second form of authentication that comes after you enter your password (using a code sent via your phone, or obtaining a code from an authenticator app). MFA reduces the likelihood of your credentials being stolen via bot attacks by 99.9% according to Microsoft.

Minimum Level: Use MFA on all emails, cloud storage, accounting, and CRM accounts.

Best Level: Use MFA on every login you have + use methods of MFA that resist phishing such as using Microsoft Authenticator for push notifications and/or using FIDO2 keys.

Common Mistakes: Only enabling MFA for admins, allowing SMS as an MFA authentication method (note that SMS is highly vulnerable to SIM-swap).

Quick Win: Enable MFA for the entirety of your organisation by using Microsoft 365 or Google Workspace (this should take less than 20 minutes).



2. Device Security and Patching:

This means protecting (via updating) your laptops, phones, and tablets.

Why is it important? Unpatched devices are the second-largest entry point to your business after phishing attacks.

Minimum Level: Automatic updates enabled for both your operating system and apps; have antivirus software that is built into your operating system running at all times.

Best Level: Central management is enabled for your devices (using Intune or Google Endpoint Management); have endpoint detection and response (EDR) software such as Microsoft Defender for Business running on your devices ($3 - $5/user/month).

Common Mistakes: You will disable updates to avoid disruption to your business, you will not put controls around personal devices used in your organisation.

Quick Win: Go check currently used company devices to ensure that they are both using automatic updates and run Windows Update (or macOS Software Update) immediately.

3. Antivirus/Endpoint Protection

This software recognises and removes malware.

Importance: It protects against ransomware, viruses, and spyware that have bypassed other security measures.

Minimum Requirement: Microsoft Defender (a built-in, free antivirus with Windows 10/11) or something similar.

Preferred Option: Defender for Business (or similar EDR solution that provides behavioural detection) = £3-8/user/month.

Common Errors: Free consumer antivirus software without central management.

Quick Wins: Verify that Defender is active and updated on every computer.

4. Backups

Regular duplication of key files and systems.

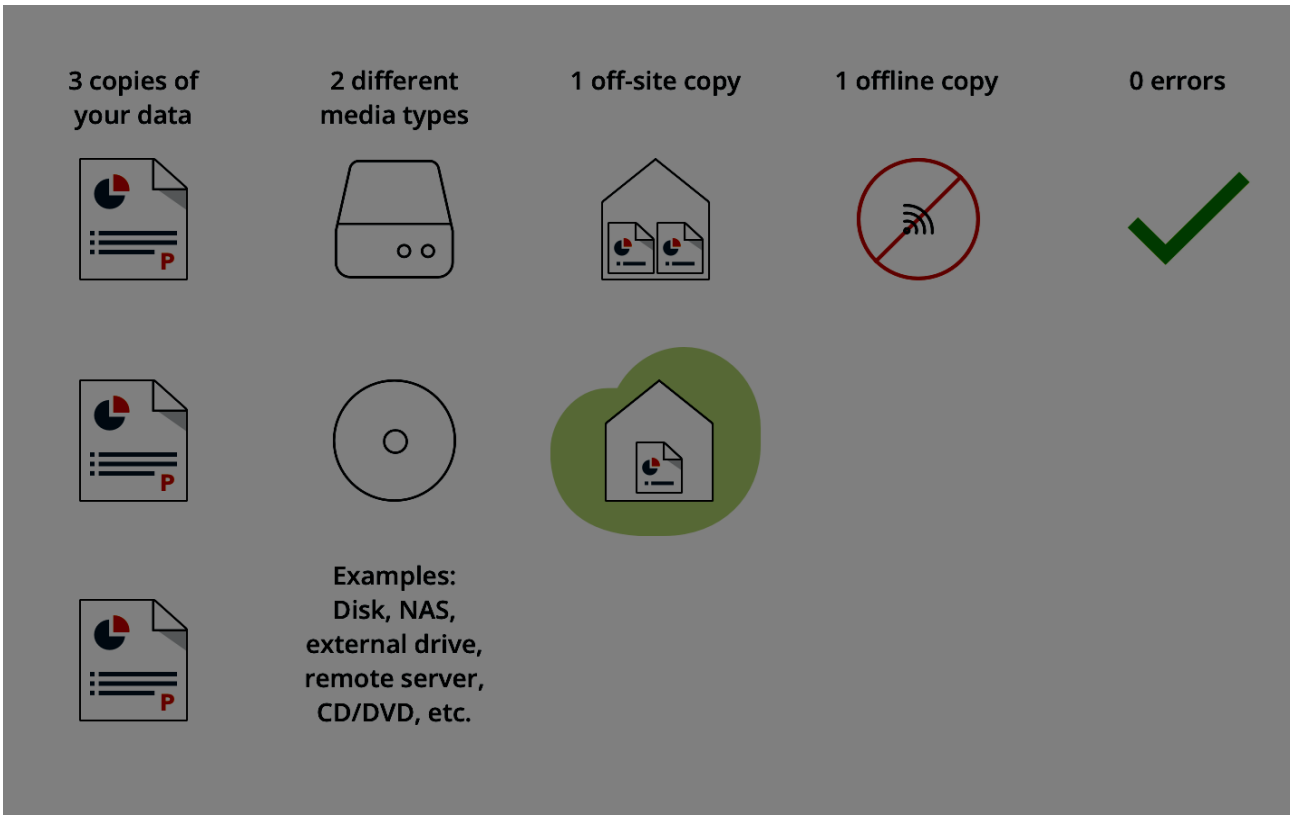
Importance: Allows recovery from ransomware, accidental deletion, or hardware crash.

Minimum Requirement: 3 copies; each copy on a different media type; at least 1 off-site (e.g., OneDrive + external storage).

Preferred Option: Automated daily backups to cloud storage (e.g., OneDrive Known Folder Move; Google Backup & Sync); at least one immutable copy of data (e.g., through use of retention policy).

Common Errors: No testing of restorability; only 1 backup located on-site.

Quick Wins: Turn on OneDrive folder backup for Documents/Desktop; test restore process on at least 1 file this week.



5. Email Protection and Phishing Protection

What this is: Filtering spam/phishing, and raising staff awareness.

Why this is important: Email is still #1 attack vector

Minimum: Basic Microsoft Defender Office 365 or Gmail spam filters and a staff briefing.

Better: Advanced threat protection and quarterly phishing simulations (at a cost of £2 - 5 per user per month).

Common Mistakes: Clicking on links without checking the sender or not reporting them if you suspect them to be phishing.

Quick Win: Hold a 15 minute team talk to raise awareness of phishing signs and enable tagging of external emails.

6. Access Control and Password Policy

What this is: Rules for access to information resources and how passwords should be used.

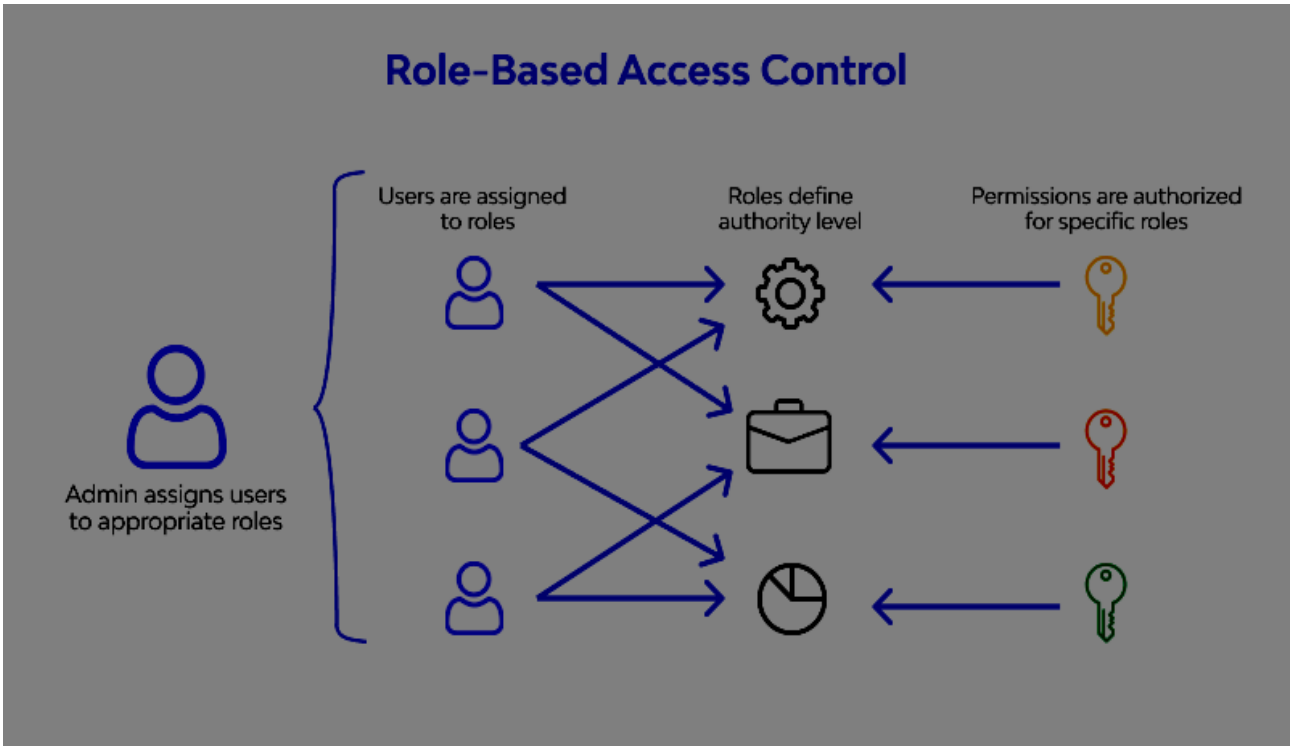
Why this is important: It prevents the potential damage caused by a compromised account

Minimum: Use of unique passwords (14 characters) and no use of shared accounts. Use of MFA

Better: Use of a password manager and role-based access (e.g. finance seeing accounting only).

Common mistakes: Admin accounts having weak passwords and the reuse of passwords.

Quick win: Ban shared logins and require the use of a password manager.



7. Firewall and Network Security

What this is: Prevents unwanted incoming and outgoing traffic from your network.

Why this is important: Prevents many automated attacks against your network.

Minimum: Windows Firewall enabled, and router firewall enabled.

Better: Cloud-based firewall (like Cloud-flare free) and VPN access for remote users.

Common mistakes: Port forwarding without necessity and using a default router password.

Quick win: Change the router admin password and block RDP unless absolutely necessary.

8. Basics for GDPR and Data Protection

What is it: Protecting personal information through the organisation's way of working.

Why is it important: Failure to keep information safe could incur fines from the ICO.

Minimum compliance: You must have a privacy notice on your website, data map (explanation of what you have and where you keep it), a way to report if you have had a breach.

Best practice: Obtaining Cyber Essentials certification, developing a data protection policy.

Common errors: Not keeping a record of breaches; assuming that the cloud is safe.

Quick win: Download the ICO's small business checklist; set up a basic register of breaches.

30-Day Implementation Checklist

Quick Security Foundations (Days 1-10)
• Enable MFA on all company email and cloud accounts • Ensure auto-update is enabled on all company devices • Run full AV scan on all devices • Change the router administration password
Cloud Backups & Email (Days 11-20)
• Enable daily cloud backup (OneDrive or Google) on all company computers • Test deleting one file/folder and restoring it from backup • Enable external sender tags in emails • Train all employees on how to recognise and respond to phishing emails
Access & Documentation (Days 21-30)
• Eliminate shared accounts and review all company administrator user accounts • Document the basic structure of your data and how to respond to a data breach • Add a "Privacy Notice" link to your company website and email footer • Schedule the next quarterly review of security policies and procedures

FAQ

- **Is Cyber Essentials certification necessary?**

It is not required but highly recommended as many public sector tenders and insurance providers ask for this certification.

- **Is free antivirus adequate?**

For small businesses, Microsoft Defender should be fine as long as it remains current.

- **How frequently do we perform backup tests?**

Regularly, at least once every three months.

- **For passwords, how long do they have to be now?**

14 characters, however, passphrases are better than highly complex, short passwords.

- **Do we need a password manager?**

It is highly recommended if you have more than five staff members, there are free versions for one-person teams.

- **If we have strong passwords, do we need multi-factor authentication (MFA)?**

You will need MFA even with strong passwords by 2026.

- **Should we block USB drives?**

For high-risk teams, you may want to block USB, for others, simply ensure that your antivirus scans the USB device.

- **How do we deal with staff using their own devices?**

You need a BYOD policy and MFA, however, you should not allow personal devices to do sensitive work.

- **What can we do if we don't have the extra tools to protect our data?**

Start out with built-ins through Microsoft or Google; they help cover 80 percent of what the minimum standards are.

- **How do we show our clients/insurers compliant with Cyber Essentials?**

Get your Cyber Essentials Certificate, plan for documented processes and document MFA rollout.

About This Guide

“Minimum IT Standards Every UK Business Should Meet” has been developed by **Computer Support Centre**, a UK IT and cybersecurity consultancy that helps small and medium-sized businesses improve their security, resilience, and compliance with UK GDPR and Cyber Essentials. The guide draws upon real-life experience of working with UK SMEs to improve their IT security, IT resilience, and overall risk profile.

The guide aims to provide straightforward, clear guidance that is easy for non-technical business owner(s) and manager(s) to understand and implement, without the burden of additional complexity. The document is intended to provide a foundation for businesses to implement practical actions that will result in a safer, more reliable IT environment.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:

☞ **https://computersupportcentre.com**

Conclusion

In summary, minimum IT standards do not require investment in expensive technology or complex systems. The criticality of the minimum IT standard is the ability to implement the right foundation. By ensuring that businesses implement at least the five minimum IT standards, such as MFA, strong passwords, secured devices, regular updates, and reliable backups, all businesses can significantly reduce their exposure to cyber risk. Any small, ongoing improvement implementation will help mitigate against business interruptions over the long term. If you begin this week with one practical action, over the next 30 days you will have built momentum toward having a stronger, more resilient IT environment to run your business from.