



Microsoft 365 Security for Charities

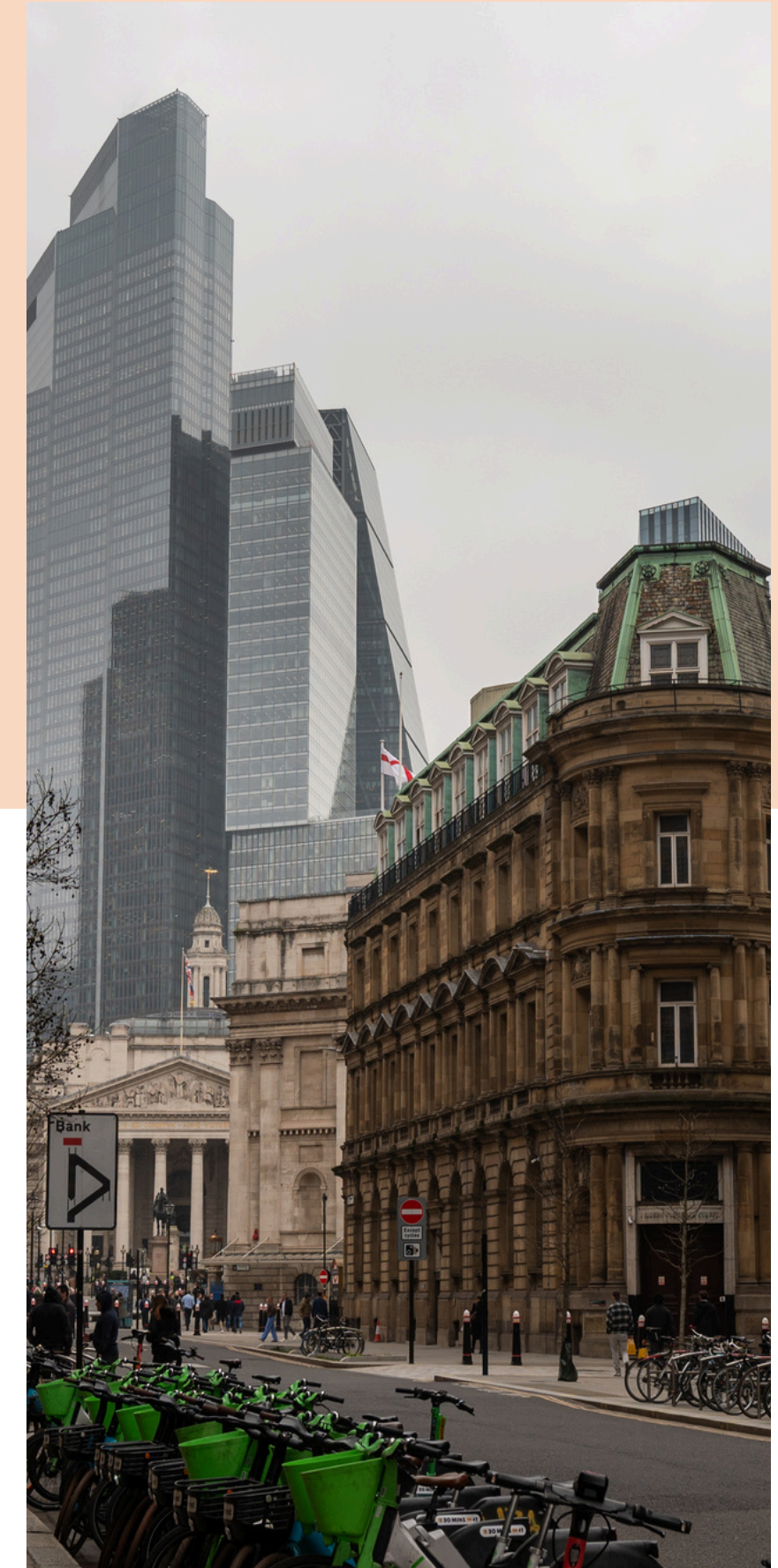
10 CONTROLS EVERY CHARITY SHOULD CONSIDER
Executive Guide

Why this matters

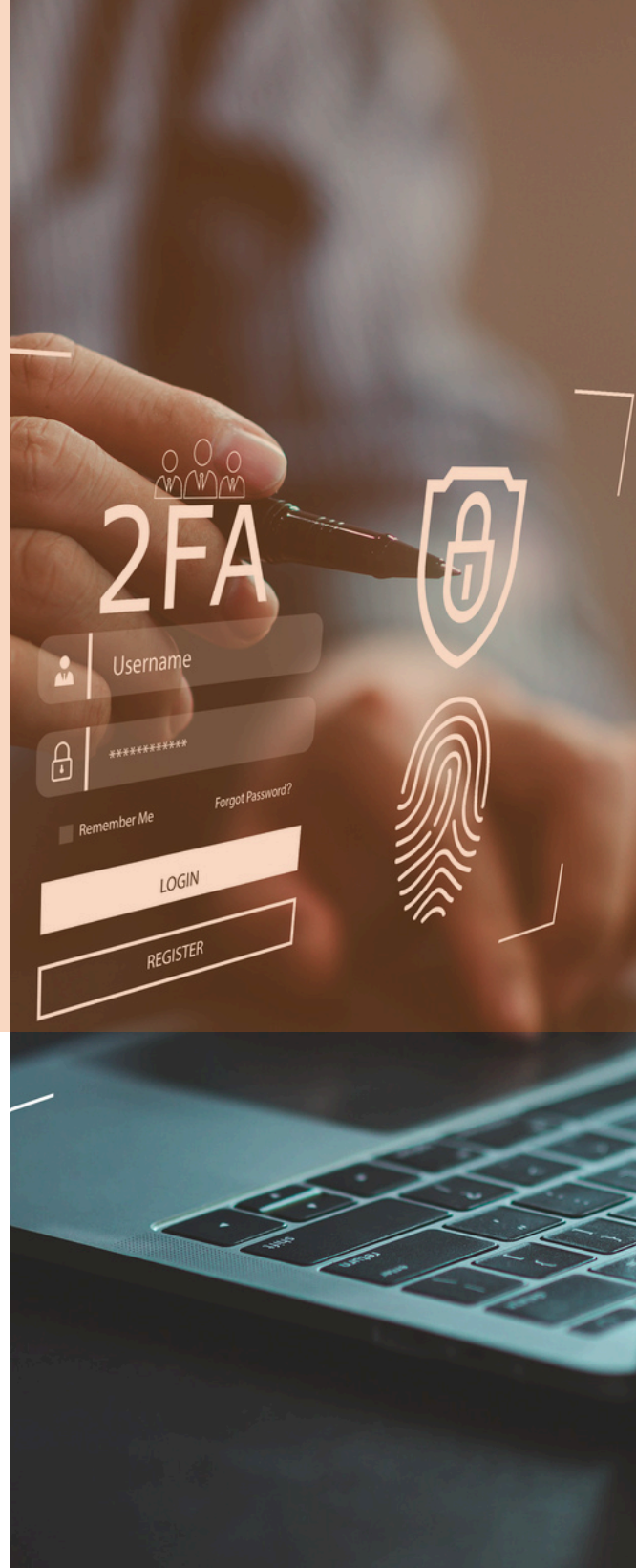
While Microsoft 365 provides a secure and feature-rich platform, achieving a strong security posture requires each organisation's environment to be properly configured, protected, and actively managed.

For charities handling sensitive donor, employee, and operational data, implementing the right security controls, access policies, and data protection measures is essential to minimise risk, maintain compliance, and safeguard critical information.

Cyber threats continue to evolve, and charities are increasingly being targeted due to the sensitive personal data they hold and often limited in-house IT resources. While Microsoft 365 includes a powerful range of security tools to help reduce cyber risk, many organisations face the challenge of understanding which controls to prioritise and how to implement them effectively as part of a cohesive security strategy.



The 10 Controls



01



Multi-Factor
Authentication
(MFA)

MULTI-FACTOR AUTHENTICATION (MFA)

Multi-Factor Authentication (MFA) is a security measure that requires users to provide two or more forms of verification before accessing an account or system. MFA significantly reduces the risk of unauthorised access, as attackers would need more than just a stolen password to gain entry to an account.

02



Conditional
Access

CONDITIONAL ACCESS

Conditional Access is a Microsoft 365 security feature that controls who can access company resources and under what conditions. Every sign-in is evaluated against a set of predefined rules before access is granted. For example, access can be restricted to authorised devices, trusted locations, or accounts using multi-factor authentication, helping to protect sensitive business data from unauthorised access.

03



Microsoft
Defender

MICROSOFT DEFENDER

Microsoft Defender is Microsoft's integrated security platform that helps protect users, devices, email, applications, and data from cyber threats. Built into Microsoft 365, it uses advanced threat detection, automation, and real-time monitoring to identify and respond to suspicious activity before it can impact the organisation.

04



Microsoft
Secure Score

MICROSOFT SECURE SCORE

Microsoft Secure Score is a security measurement tool within Microsoft 365 that helps organisations understand their current security posture and identify opportunities to improve it. It provides a score based on how many recommended security controls and best practices have been implemented across the Microsoft 365 environment.

05



Identity
Protection

IDENTITY PROTECTION

Microsoft Entra ID Protection continuously monitors user accounts and sign-in activity for indicators of identity compromise. It can detect risks such as leaked credentials, unfamiliar sign-in activity, anonymous IP addresses and suspicious travel patterns. Based on these risk signals, organisations can automatically require Multi-Factor Authentication, block access or require a password reset.



The 10 Controls



06



Email
Security

EMAIL SECURITY

Email security refers to the technologies, policies, and controls used to protect an organisation's email system from threats such as phishing, malware, spam, business email compromise, and unauthorised access.

07



Endpoint
Protection

ENDPOINT PROTECTION

Endpoint Protection is a cybersecurity solution designed to protect devices such as laptops, desktops, and mobile devices from cyber threats including malware, ransomware, viruses, and other malicious activity. For charities handling sensitive information, Endpoint Protection forms a critical layer of defence by securing every device that accesses company data and systems.

08



Data Backup
& Recovery

MICROSOFT 365 BACKUP & RECOVERY

While Microsoft 365 provides data retention and recycle bin capabilities, a dedicated backup and recovery solution offers additional protection by creating separate, recoverable copies of business-critical data and enabling faster restoration when needed. This is in the event of accidental deletion, data corruption, cyber attacks, or ransomware incidents.

09



Data Loss
Prevention

DATA LOSS PREVENTION (DLP)

DLP works by identifying and monitoring sensitive data, such as financial information, personal data, or confidential business documents, and applying policies that control how that data can be used. For example, DLP can block users from emailing confidential files externally, uploading sensitive data to unauthorised websites, or copying information to personal devices.

10



Sharepoint &
Teams Governance

SHAREPOINT & TEAMS GOVERNANCE

SharePoint & Teams Governance is the set of policies, processes, and controls used to manage how Microsoft Teams and SharePoint are created, used, shared, and secured across an organisation. It helps charities to maintain a well-organised and secure collaboration environment.



How does your charity compare?



Microsoft 365 includes a wide range of security capabilities, but many charities only utilise a portion of what is available. The checklist below provides a simple way to assess your organisation's current security posture across key areas.

Security Control	In Place	Partial	Not Sure
MFA for every user			
Conditional Access			
Defender configured			
Secure Score regularly reviewed			
Identity Protection			
Email security			
Endpoint management			
Independent M365 backup			
DLP / information protection			
SharePoint & Teams governance			

If you answered "Partial" or "Not Sure" to several of these controls, there may be opportunities to strengthen your Microsoft 365 environment, reduce cyber risk, and better protect sensitive charity data. Reviewing these areas regularly helps ensure your organisation remains secure, compliant, and resilient against evolving cyber threats.



Get the Complete Framework



ACCESS THE COMPLETE FRAMEWORK



Explore all 10 Microsoft 365 security controls in more detail, including the risks, recommendations and practical steps your charity can take to strengthen its security.

[VIEW THE COMPLETE FRAMEWORK](#)

PUBLISHED
2026

PRODUCED BY
BUNKER TECHNICAL SOLUTIONS

Microsoft 365 Security Framework

A PRACTICAL GUIDE FOR UK CHARITIES

Helping charity leaders build a secure, compliant and resilient Microsoft 365 environment.



01 MULTI-FACTOR AUTHENTICATION (MFA)



IMPLEMENTATION DIFFICULTY
LOW



WHAT IT IS

Multi-Factor Authentication (MFA) adds an extra layer of security by requiring users to verify their identity using a second factor, such as the Microsoft Authenticator app.

WHY IT MATTERS

MFA blocks **99.9%** of automated attacks, even if passwords are stolen through phishing or reused elsewhere.

WHO IT AFFECTS

All users with access to Microsoft 365 accounts, including admins and trustees.

LICENSING

Included in Microsoft 365. No additional licence required.

RECOMMENDATIONS

We recommend to enable MFA for every user, prioritise Microsoft Authenticator over SMS and regularly review any account exclusions.

RELATED CONTROLS

- Conditional Access
- Microsoft Defender
- Identity Protection

RISKS WITHOUT MFA



Stolen Credentials
Attackers use leaked or stolen passwords to sign in.



Phishing Attacks
Fake users and sites trick users into giving up their passwords.



Account Takeover
Once inside, attackers can access sensitive data and apps.



Data Breaches
Compromised accounts can lead to costly breaches.



Business Disruption
Downtime, lost productivity and damage to reputation.

BUSINESS IMPACT



HIGH
Security Improvement
Risk Reduction



LOW
Operational Impact