



PRACTICAL GUIDE · 7IT CYBERSECURITY

Securing Microsoft 365

The essential checklist to protect your accounts, emails and data

● SECURE

Microsoft 365 holds most of a company's daily life: email, documents, meetings, shared files. A single compromised account can expose years of conversations. This checklist brings together the measures that truly protect you, grouped by theme. Some depend on your licences: we say so where relevant.

1. Accounts and identities

- ☐ Multi-factor authentication (MFA) is enabled for every user, including management.
- ☐ Administrators use a dedicated admin account, separate from their everyday work account.
- ☐ The number of global administrators is limited to a few clearly identified people.
- ☐ Legacy authentication protocols, which do not support MFA, are disabled.
- ☐ Accounts of people leaving the company are blocked on their last day.
- ☐ A password manager is provided to the teams.

2. Email

- ☐ SPF, DKIM and DMARC records are configured for your domain name: they limit spoofing of your addresses.
- ☐ Automatic forwarding of emails to external addresses is blocked.
- ☐ A warning flags messages coming from outside the company.
- ☐ Protection against phishing and dangerous attachments is enabled (Microsoft Defender for Office 365, depending on your licences).

3. Data and sharing

- ☐ "Anyone with the link" sharing is disabled or time-limited.
- ☐ External shares are reviewed regularly and removed when no longer needed.
- ☐ Important documents are saved in OneDrive, SharePoint or Teams, not on local computers.
- ☐ Sensitive documents are identified and protected with sensitivity labels (depending on your licences).

4. Devices

- ☐ Computers are encrypted (BitLocker) and receive updates automatically.
- ☐ Devices are managed with Microsoft Intune: they can be locked or wiped remotely if lost.
- ☐ Data access is restricted to compliant devices through conditional access (Microsoft Entra ID P1, included in Microsoft 365 Business Premium).

5. Backup and recovery

- ☐ An independent backup covers mailboxes, OneDrive, SharePoint and Teams.
- ☐ A restore is tested at least twice a year.
- ☐ An incident response plan sets out who does what in the event of a hack or ransomware.

Good to know: Microsoft guarantees the availability of the service, but protecting your data against accidental deletion, departing employees or ransomware remains your responsibility.

6. Users and monitoring

- ☐ Employees are trained to spot phishing, with regular simulations.
- ☐ Everyone knows how to report a suspicious message, and does so without fear.
- ☐ The audit log is enabled and security alerts are followed up.
- ☐ Microsoft Secure Score is reviewed every month to measure progress.

Where to start?

Timeframe	Priorities
This week	MFA for everyone, dedicated admin accounts, legacy authentication disabled.
This month	SPF, DKIM and DMARC, independent backup, restricted anonymous sharing.
This quarter	Device management with Intune, conditional access, awareness programme.

Let's talk about your project

Need help? 7IT Cybersecurity carries out a security review of your Microsoft 365 environment and gives you a clear, prioritized action plan.

contact@7itgroup.com [WhatsApp +237 671 59 84 67](https://www.whatsapp.com/channel/0029va333333333333333333) www.7itgroup.com