BR-SYSTEMS · ENGLISH EDITION

Microsoft 365 security for SMEs

Treat identity, administration, devices, data and recovery as separate control areas.

Personally accountable · clearly documented · vendor-transparent

From concern to an owned action plan

This guide is designed for small and medium-sized organisations that need practical decisions rather than generic fear or a product-first answer.

How to use it

Work through the actions with the people who own the affected business processes. Mark what is already evidenced, assign an owner to every gap and agree a realistic review date.

Decision principles

01	Start from business impact and responsibility.
02	Prefer written evidence over assumed status.
03	Keep alternatives and exit paths visible.
04	Test recovery and operating processes, not only settings.

Important

This publication provides technical orientation. It is not legal advice, a certification or a guarantee of security. Current law, contracts, manufacturer documentation and the organisation's specific risk context remain authoritative.

Practical action checklist

Use the right-hand side of a printed copy for owner, evidence and due date.

01	Require MFA and protect emergency administrator accounts.
02	Separate privileged roles from daily user accounts.
03	Apply Conditional Access from a documented baseline.
04	Review external sharing, guests and application consent.
05	Set email authentication and anti-phishing controls.
06	Connect device compliance to access where appropriate.
07	Define retention, backup and recovery independently.
08	Monitor risky sign-ins, admin activity and alert ownership.
09	Test onboarding, role changes and offboarding.
10	Review licences and security settings together at least annually.

A sensible next step

BR-Systems can help establish the baseline, prioritise the gaps and implement or operate the agreed measures. A short initial consultation is enough to determine whether that would be useful.

br-systems.eu · info@br-systems.eu · +49 179 160 1700