BR-SYSTEMS · ENGLISH EDITION

IT security checklist for SMEs

A concise baseline across organisation, identity, devices, network and recovery.

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	Name an accountable owner for IT security.
02	Maintain an inventory and remove unknown assets.
03	Use MFA and separate privileged accounts.
04	Patch operating systems, applications and network equipment.
05	Apply endpoint protection with monitored alerts.
06	Use network segmentation and reviewed firewall rules.
07	Back up according to 3-2-1 and test restoration.
08	Prepare incident contacts and reporting paths.
09	Review suppliers, remote access and shared accounts.
10	Repeat the assessment and track outstanding actions.

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