FRANKFORD'S SOLUTIONS

As of July 2026

Cyber Security Checklist for SMEs

IT security step by step, no dedicated security team required

This checklist is for managing directors and staff responsible for IT in small and medium-sized companies. It covers the essential basics, from passwords and backups to a simple incident plan. Work through the items at your own pace and tick off what is already in place.

Passwords and access

- [ ] Introduce a password manager and use a unique, long password for every service.
  Without a password manager, unique passwords per service are not realistic in daily work.
- [ ] Enable multi-factor authentication (MFA) at least for email, cloud services and remote access.
- [ ] Change default passwords on routers, printers, NAS devices and other hardware.
- [ ] Grant administrator rights only to people who genuinely need them.
  A standard user account is enough for everyday work.
- [ ] Avoid shared accounts. Every person works with their own login.
- [ ] Disable all accounts of departing employees on their last working day.
  A fixed offboarding checklist makes sure no account is forgotten.

Devices and updates

- [ ] Keep a simple inventory of all devices, software and important accounts.
  You cannot protect what you do not know about.
- [ ] Turn on automatic updates for operating systems, browsers and applications.
- [ ] Replace software and devices that no longer receive security updates.
- [ ] Make sure active malware protection is running on every computer.
  On Windows, the built-in Microsoft Defender is sufficient.
- [ ] Enable full-disk encryption on all laptops.
  On Windows this is BitLocker or device encryption, on Apple it is FileVault. Modern smartphones are usually encrypted by default.
- [ ] Set an automatic screen lock on all devices.

Backups

- [ ] Back up your data following the 3-2-1 rule.
  Three copies, two different types of storage, one copy off-site.

- [ ] Automate your backups.
  Manual backups tend to be forgotten in daily business.
- [ ] Keep at least one backup copy disconnected from the network.
  That way it survives a ransomware attack.
- [ ] Test your restore process at least twice a year.
  A backup only counts once you have proven you can restore from it.

Network and Wi-Fi

- [ ] Set up a separate guest Wi-Fi for visitors and private devices.
- [ ] Protect your company Wi-Fi with WPA2 or WPA3 and a long password.
- [ ] Allow external access to your company network only through a VPN.
- [ ] Keep the firmware of your router and firewall up to date.

Phishing and email

- [ ] Train your team to spot phishing emails at least twice a year.
  Short sessions with real examples work better than one long training session per year.
- [ ] Always confirm payment instructions and changed bank details by phone using a known number.
- [ ] Define who suspicious emails should be reported to.
  Nobody who reports should fear consequences. Not even after clicking a link.

Incidents and suppliers

- [ ] Create an emergency contact list: who is informed internally and who is your external IT contact.
  Keep a printed copy too. In a real incident your systems may be down.
- [ ] During an incident, document times, affected systems and actions taken from the very start.
- [ ] Clarify in advance when a data breach must be reported to the data protection authority.
  Under the GDPR the general deadline is 72 hours.
- [ ] Check whether your company falls under Austria's NISG 2026 (NIS2) from October 2026.
  The law takes effect on 1 October 2026 for medium-sized and larger companies in 18 sectors, affected companies must register by 31 December 2026.
- [ ] For new cloud services, check where the data is stored and whether a data processing agreement is in place.
- [ ] Ask your IT providers how they handle MFA, updates and backups themselves.

If you need support with any of these points, Frankford's IT-Solutions in Innsbruck is happy to help. Just get in touch, no strings attached.

Frankford's IT-Solutions GmbH · Fallmerayerstraße 14, 6020 Innsbruck, Austria · frankford-it.at · eduard.frankford@frankford-it.at · As of July 2026