CRYPTOITDATA

Cybersecurity for SMEs: the 25-point checklist

Tick what is true today, not what is planned. Every unticked point becomes a task with an owner and a deadline.

Governance and NIS2

- [ ] 1 We have checked in writing whether the company falls under OUG 155/2024: size, sector in the annexes, exceptions.
- [ ] 2 If we are in scope, we have notified DNSC and we know the notification date.
- [ ] 3 Management has approved the security measures in writing and appointed an internal owner.
- [ ] 4 We know the reporting deadlines: 24 hours, 72 hours, one month.

Identities and access

- [ ] 5 MFA active on all email accounts.
- [ ] 6 MFA active on VPN, remote access and administrator accounts.
- [ ] 7 Administrator accounts are separate and used only for administration.
- [ ] 8 Leavers' accounts are closed within 24 hours at most.
- [ ] 9 We review every quarter who has access to what.

Data and backup

- [ ] 10 Critical data has three copies, on two types of media, one outside the network.
- [ ] 11 The offline or immutable copy cannot be deleted with a domain account.
- [ ] 12 We have tested a full restore in the last three months and timed it.
- [ ] 13 We know how old restored data can be (RPO) and how fast we recover (RTO).

Systems

- [ ] 14 We have a complete inventory of equipment, software and internet-exposed services.
- [ ] 15 Critical fixes on internet-exposed systems are installed within 14 days at most.
- [ ] 16 We have no systems without vendor security support, or they are isolated and documented.
- [ ] 17 All laptops, workstations and servers have active, monitored endpoint protection.
- [ ] 18 All laptop disks are encrypted.

Email and people

- [ ] 19 SPF, DKIM and DMARC are configured, with DMARC at least at p=quarantine.
- [ ] 20 Automatic forwarding to external addresses is blocked or raises an alert.
- [ ] 21 Payments and bank account changes requested by email are confirmed by phone.
- [ ] 22 Every new employee completes anti-phishing training in their first week.

Incidents and suppliers

- [ ] 23 We have a 1–2 page incident response plan, printed and tested yearly.
- [ ] 24 Emergency contacts (IT provider, bank, insurer, DNSC) are also kept offline.
- [ ] 25 We have a list of suppliers with access to our systems, with named accounts and incident notification clauses.

> The thresholds (for example 14 days for critical fixes or a test restore every three months) are CRYPTOITDATA recommendations for an SME, not legal requirements. The NIS2 deadlines (24 hours, 72 hours, one month; DNSC notification within 30 days at most) are those of Romanian OUG 155/2024, consolidated text as of 8 November 2026. Full guide with sources: cryptoitdata.eu/en/blog/securitate-cibernetica-imm-ghid