

A 15-item checklist

Tick an item only after you have checked it the way the text after the colon says.

- ☐ **Accounts.** Everyone has a second login factor (MFA, a code or a confirmation on the phone) for email, online banking, the CRM and hosting: the email admin centre shows no users without MFA.

- ☐ **Accounts.** There are two or three administrators, each with a separate admin account: review the list of roles in the admin centre.

- ☐ **Accounts.** Nobody who has left still has work access: compare the list of leavers from the past year with active accounts in email, the CRM and cloud drives.

- ☐ **Email.** SPF, DKIM and DMARC (domain records that protect your address from being faked) are set up: ask IT to show you these three records for your domain.

- ☐ **Email.** Automatic forwarding to external addresses is blocked: check the forwarding policy in the email admin centre.

- ☐ **Devices.** Laptops and phones install updates automatically: open the update settings on three random laptops.

- ☐ **Devices.** Laptop disks are encrypted and screens lock by themselves: check that BitLocker or FileVault is on.

- ☐ **Backups.** Important data is copied automatically and one copy is kept separately with different passwords: ask where exactly that copy is and who can access it.

- ☐ **Backups.** Restoring has been tested: restore one file and one database as of yesterday and time it.

- ☐ **Website.** The site's content management system, plugins and server are up to date: look at the versions and the last update date in the site's admin panel.

- ☐ **Website.** Access to the domain, hosting and site admin belongs to the company and is protected with MFA: try to log in without the contractor.

- ☐ **People.** Passwords are kept in a password manager, not in spreadsheets: search the shared drive for files with "passwords" in the name.

- ☐ **People.** Changes to bank details are confirmed by calling a known number: ask the accountant what they would do with an email about a supplier's new account.

- ☐ **Incidents.** There is a printed contact list (IT, bank, hosting, domain registrar, CERT-UA, cyber police); find that sheet and check two of the numbers.
- ☐ **Incidents.** Everyone knows who decides and what to do first if email is hacked: talk this scenario through in a 15-minute meeting.

Want to go through this checklist together? Write to us and we will review your scope.
veiltrack.io/en/contact