MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

IT AUDIT REPORT

Example Law Firm (demo report)

Audit date: 25 November 2026 · kancelaria-demo.example · Auditor: Sebastiano Blanco, MeshPC · 3 computers

OVERALL RATING

Needs urgent action

There are threats that could stop the business or lead to a data leak.

Results by area

Domain and email	Microsoft 365	Accounts, passwords and MFA	Computers
To improve checked 10 of 10	Not checked	To improve checked 1 of 1	Urgent checked 12 of 12

Backups	Network and Wi-Fi	NIS2 readiness
Not checked	Urgent checked 6 of 6	Not checked

Good · To improve · Urgent · Not checked

Areas marked “Not checked” were not covered by this report. The full audit covers all 8 areas and takes 60–90 minutes.

Top priorities

1. **Operating system still supported**
   An unsupported system gets no security fixes – known holes stay open for good.
   What we found: 3 of 3: RECEPCJA-PC – Windows 10 Pro 22H2 – support ended 14 Oct 2025; LAPTOP-SZEF – Windows 11 …
   Recommendation: Upgrade to a supported version (Windows 11 25H2; macOS 15, 26 or 27); hardware that does not meet the requirements should be replaced, or covered by Windows 10 ESU in the meantime.

2. **Updates installed**
   Missing updates are the most common way ransomware gets into small businesses.
   What we found: 2 of 3: RECEPCJA-PC – last update 2026-08-02 (115 days ago); MacBook-Kasia – last update …
   Recommendation: Automatic installation of system and application updates with an enforced restart within a few days (e.g. Windows Update for Business / Intune) and a regular compliance check.

3. **Antivirus / EDR active and up to date**
   Without active protection, malware runs unnoticed.
   What we found: 3 of 3: RECEPCJA-PC – several active antiviruses at once: Windows Defender, Avast Free …
   Recommendation: One active protection product per computer; an EDR-class solution (e.g. Microsoft Defender for Business) with tamper protection and central alert visibility.

SAMPLE

MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

Action plan

Priority reflects the severity of the threat: points that could stop the business or lead to a data leak are marked urgent.

URGENT – WITHIN 7 DAYS

D1 **Operating system still supported** — Urgent

What we found: 3 of 3: RECEPCJA-PC – Windows 10 Pro 22H2 – support ended 14 Oct 2025; LAPTOP-SZEF – Windows 11 Pro 24H2 – support ended 2026-10-13; MacBook-Kasia – macOS 14.7 – no longer gets security fixes

Recommendation: Upgrade to a supported version (Windows 11 25H2; macOS 15, 26 or 27); hardware that does not meet the requirements should be replaced, or covered by Windows 10 ESU in the meantime.

D2 **Updates installed** — Urgent

What we found: 2 of 3: RECEPCJA-PC – last update 2026-08-02 (115 days ago); MacBook-Kasia – last update 2026-10-20 (36 days ago)

Recommendation: Automatic installation of system and application updates with an enforced restart within a few days (e.g. Windows Update for Business / Intune) and a regular compliance check.

D3 **Antivirus / EDR active and up to date** — Urgent

What we found: 3 of 3: RECEPCJA-PC – several active antiviruses at once: Windows Defender, Avast Free Antivirus; LAPTOP-SZEF – Windows Defender (no EDR); MacBook-Kasia – built-in XProtect only

Recommendation: One active protection product per computer; an EDR-class solution (e.g. Microsoft Defender for Business) with tamper protection and central alert visibility.

D4 **Disk encryption (BitLocker / FileVault)** — Urgent

What we found: 3 of 3: RECEPCJA-PC – disk not encrypted; LAPTOP-SZEF – BitLocker on, key backup not confirmed; MacBook-Kasia – FileVault off (laptop)

Recommendation: BitLocker with TPM (Windows) or FileVault (macOS) on all computers, laptops first; recovery keys stored in Entra ID or the MDM.

G1 **Office services exposed to the internet** — Urgent

What we found: office address 203.0.113.25: open ports 443, 3389

Recommendation: Remove port forwards for admin services on the router (RDP, SMB, NAS panel, SSH); remote access only through a VPN with MFA.

HIGH – WITHIN 30 DAYS

A9 **Look-alike domains** — Urgent

What we found: Look-alike domains with working email: kancelaria-dem0.example; registered: kancelaria-demo.example.com, kancelariademo.example

Recommendation: Check who owns the domains (WHOIS/RDAP), report abuse to the registrar, consider registering the key variants and warn staff and the accounts team.

D7 **Remote access tools** — Urgent

What we found: 2 of 3: RECEPCJA-PC – AnyDesk, TeamViewer; MacBook-Kasia – AnyDesk (unmanaged)

Recommendation: One remote support tool with a company account, MFA and a session log; uninstall the others and block their installation.

SAMPLE

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

D8 **Outdated or vulnerable software** — Urgent

What we found: 2 of 3: RECEPCJA-PC – WinRAR 6.11.0 (CVE-2025-8088), Microsoft Office Professional Plus 2016 – unsupported, Java 8 Update 251; LAPTOP-SZEF – 7-Zip 23.01

Recommendation: Uninstall software the vendor no longer supports, update the rest to current versions and put it under automatic updates.

F5 **Risky services on the network (SMBv1, Telnet, RDP)** — Urgent

What we found: 192.168.1.1 Telnet; 192.168.1.10 nas.local SMBv1

Recommendation: Turn off SMBv1 and Telnet on all devices (updating NAS and printer firmware where needed) and restrict RDP to specific addresses or to VPN connections.

F6 **DNS filtering (blocking malicious sites)** — Urgent

What we found: 3 of 3 without filtering (DNS: 192.168.1.1)

Recommendation: DNS filtering that blocks malicious and phishing domains (e.g. Quad9, Cloudflare Gateway, DNSFilter), set on the router and on laptops used outside the office.

A7 **Website software up to date** — Urgent

What we found: The website runs on PHP 8.1, which no longer gets security fixes.

Recommendation: Update the CMS, plugins and PHP to versions that still receive security fixes; hide the Server/X-Powered-By headers and the generator tag.

D6 **Automatic screen lock** — Urgent

What we found: 3 of 3: RECEPCJA-PC – no automatic lock; LAPTOP-SZEF – locks after 15 min; MacBook-Kasia – locks after 15 min

Recommendation: Screen lock after at most 10 minutes of inactivity, enforced by policy (GPO, Intune or an MDM profile) and requiring a password or PIN.

D10 **Hardware age** — Urgent

What we found: 2 of 3: RECEPCJA-PC – OptiPlex 3050, BIOS from 2017; MacBook-Kasia – MacBook Air M1 (~2020)

Recommendation: A replacement plan for computers older than 6 years, starting with those that do not meet the Windows 11 requirements.

D12 **USB storage control** — Urgent

What we found: 3 of 3: RECEPCJA-PC – USB storage unrestricted; LAPTOP-SZEF – USB storage unrestricted; MacBook-Kasia – USB storage unrestricted

Recommendation: A policy that blocks or logs USB storage use (GPO or Intune Device Control), with exceptions for approved encrypted devices.

PLANNED – WITHIN 90 DAYS

A6 **Website SSL certificate and HTTPS** — To improve

What we found: kancelaria-demo.example: no HSTS header; www.kancelaria-demo.example: no HSTS header

Recommendation: An auto-renewing certificate, a 301 redirect from http to https for both the domain and www, and a Strict-Transport-Security header with max-age of at least 6 months (RFC 6797).

SAMPLE

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

A10 **Company email addresses in known data breaches** — To improve

What we found: Company addresses only in older breaches.

Recommendation: Reset the passwords of accounts found in breaches, enforce MFA and check that the same passwords are not used for other services.

C6 **Local admin rights on computers** — To improve

What we found: 2 of 3: RECEPCJA-PC – user anna is an admin; MacBook-Kasia – user kasia is an admin

Recommendation: Everyday work on a standard account; installs through a separate admin account managed e.g. with Windows LAPS or Intune Endpoint Privilege Management.

D5 **Computer firewall** — To improve

What we found: 2 of 3: RECEPCJA-PC – firewall off: Private; MacBook-Kasia – macOS firewall off

Recommendation: Firewall on for the domain, private and public profiles, managed centrally; inbound rules only for required services.

D9 **Disk health and free space** — To improve

What we found: 2 of 3: RECEPCJA-PC – 9% free (21 GB); MacBook-Kasia – 12% free (30 GB)

Recommendation: Back up the data and replace any disk with SMART warnings; free up space to at least 20% on the system disk.

D11 **Central device management (Intune / RMM)** — To improve

What we found: 2 of 3: RECEPCJA-PC – not managed; MacBook-Kasia – not managed

Recommendation: Enrol the computers in Microsoft Intune (or another MDM/RMM) to enforce security policies, updates and inventory.

G2 **Known vulnerabilities on the public IP** — To improve

What we found: 203.0.113.25: potential vulnerabilities to verify (2): CVE-2023-44487, CVE-2024-3400

Recommendation: Verify the listed CVEs on the edge device (router, firewall, NAS) and install firmware updates or turn off the exposed service.

A4 **Email provider (MX records)** — To improve

What we found: Email on a hosting server: mx.hosting-provider.example

Recommendation: Consider business-grade email with anti-spam and anti-phishing protection (e.g. Exchange Online with Defender for Office 365); until then, enable the filtering available at the current provider.

A5 **Email encryption between servers (TLS, MTA-STS)** — To improve

What we found: STARTTLS could not be tested (port 25 blocked on the way); no MTA-STS.

Recommendation: Require TLS for SMTP connections, publish an MTA-STS policy in enforce mode (RFC 8461) and TLS-RPT reporting (RFC 8460).

A8 **Domain protection (DNSSEC, transfer lock)** — To improve

What we found: DNSSEC: no, transfer lock: yes; domain paid until 2027-10-01

Recommendation: Enable DNSSEC at the DNS operator and publish the DS record at the registrar (RFC 4033); keep the transfer lock and automatic domain renewal on.

SAMPLE

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

F4 **Devices on the office network** — To improve

What we found: devices on 192.168.1.25/24: 3 – list in the appendix to confirm with the client; unnamed, with open admin ports: 192.168.1.1 (80,443,23)

Recommendation: An inventory of network devices with an assigned owner, default passwords changed and unknown devices disconnected.

Next step
We are happy to go through the results, answer questions about any point and help agree the order of the work. Contact: +48 789 599 983, info@meshpc.pl.

SAMPLE

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

Appendix: all points checked

NO.	CHECK	STATUS	WHAT WE FOUND
A. Domain and email			
A1	SPF record (who may send email for the domain)	Good	`v=spf1 a mx include:_spf.hosting-provider.example ~all (DNS lookups: 4)`
A2	DKIM signature on outgoing email	Good	`DKIM: x (2048-bit+)`
A3	DMARC policy (protection against impersonation)	Good	`v=DMARC1; p=quarantine; sp=quarantine; adkim=r; aspf=r; fo=1; rua=mailto:dmarc@kancelaria-demo.example`
A4	Email provider (MX records)	To improve	`Email on a hosting server: mx.hosting-provider.example`
A5	Email encryption between servers (TLS, MTA-STS)	To improve	`STARTTLS could not be tested (port 25 blocked on the way); no MTA-STS.`
A6	Website SSL certificate and HTTPS	To improve	`kancelaria-demo.example: no HSTS header; www.kancelaria-demo.example: no HSTS header`
A7	Website software up to date	Urgent	`The website runs on PHP 8.1, which no longer gets security fixes.`
A8	Domain protection (DNSSEC, transfer lock)	To improve	`DNSSEC: no, transfer lock: yes; domain paid until 2027-10-01`
A9	Look-alike domains	Urgent	`Look-alike domains with working email: kancelaria-dem0.example; registered: kancelaria-demo.example.com, kancelariademo.example`
A10	Company email addresses in known data breaches	To improve	`Company addresses only in older breaches.`
C. Accounts, passwords and MFA			
C6	Local admin rights on computers	To improve	`2 of 3: RECEPCJA-PC – user anna is an admin; MacBook-Kasia – user kasia is an admin`
D. Computers			
D1	Operating system still supported	Urgent	`3 of 3: RECEPCJA-PC – Windows 10 Pro 22H2 – support ended 14 Oct 2025; LAPTOP-SZEF – Windows 11 Pro 24H2 – support ended 2026-10-13; MacBook-Kasia – macOS 14.7 – no longer gets security fixes`
D2	Updates installed	Urgent	`2 of 3: RECEPCJA-PC – last update 2026-08-02 (115 days ago); MacBook-Kasia – last update 2026-10-20 (36 days ago)`

SAMPLE

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

NO.	CHECK	STATUS	WHAT WE FOUND
D3	Antivirus / EDR active and up to date	Urgent	3 of 3: RECEPCJA-PC – several active antiviruses at once: Windows Defender, Avast Free Antivirus; LAPTOP-SZEF – Windows Defender (no EDR); MacBook-Kasia – built-in XProtect only
D4	Disk encryption (BitLocker / FileVault)	Urgent	3 of 3: RECEPCJA-PC – disk not encrypted; LAPTOP-SZEF – BitLocker on, key backup not confirmed; MacBook-Kasia – FileVault off (laptop)
D5	Computer firewall	To improve	2 of 3: RECEPCJA-PC – firewall off: Private; MacBook-Kasia – macOS firewall off
D6	Automatic screen lock	Urgent	3 of 3: RECEPCJA-PC – no automatic lock; LAPTOP-SZEF – locks after 15 min; MacBook-Kasia – locks after 15 min
D7	Remote access tools	Urgent	2 of 3: RECEPCJA-PC – AnyDesk, TeamViewer; MacBook-Kasia – AnyDesk (unmanaged)
D8	Outdated or vulnerable software	Urgent	2 of 3: RECEPCJA-PC – WinRAR 6.11.0 (CVE-2025-8088), Microsoft Office Professional Plus 2016 – unsupported, Java 8 Update 251; LAPTOP-SZEF – 7-Zip 23.01
D9	Disk health and free space	To improve	2 of 3: RECEPCJA-PC – 9% free (21 GB); MacBook-Kasia – 12% free (30 GB)
D10	Hardware age	Urgent	2 of 3: RECEPCJA-PC – OptiPlex 3050, BIOS from 2017; MacBook-Kasia – MacBook Air M1 (~2020)
D11	Central device management (Intune / RMM)	To improve	2 of 3: RECEPCJA-PC – not managed; MacBook-Kasia – not managed
D12	USB storage control	Urgent	3 of 3: RECEPCJA-PC – USB storage unrestricted; LAPTOP-SZEF – USB storage unrestricted; MacBook-Kasia – USB storage unrestricted
F. Network and Wi-Fi			
F2	Wi-Fi security	Good	Firma: WPA2-Personal CCMP (key strength checked with the client)
F4	Devices on the office network	To improve	devices on 192.168.1.25/24: 3 – list in the appendix to confirm with the client; unnamed, with open admin ports: 192.168.1.1 (80,443,23)
F5	Risky services on the network (SMBv1, Telnet, RDP)	Urgent	192.168.1.1 Telnet; 192.168.1.10 nas.local SMBv1
F6	DNS filtering (blocking malicious sites)	Urgent	3 of 3 without filtering (DNS: 192.168.1.1)

SAMPLE

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

NO.	CHECK	STATUS	WHAT WE FOUND
G. Servers and internet exposure			
G1	Office services exposed to the internet	Urgent	`office address 203.0.113.25: open ports 443, 3389`
G2	Known vulnerabilities on the public IP	To improve	`203.0.113.25: potential vulnerabilities to verify (2): CVE-2023-44487, CVE-2024-3400`

Computers covered by the audit

COMPUTER	SYSTEM	MODEL	USER	LAST UPDATE
RECEPCJA-PC	Windows 10 Pro 22H2	Dell Inc. OptiPlex 3050	anna	2026-08-02
LAPTOP-SZEF	Windows 11 Pro 24H2	Lenovo ThinkPad T14 Gen 4 (laptop)	jan	2026-11-12
MacBook-Kasia	macOS 14.7	Apple MacBook Air (laptop)	kasia	2026-10-20

Devices found on the office network

IP ADDRESS	NAME	MAC	OPEN PORTS
192.168.1.1	– (router)	AA-BB	80, 443, 23
192.168.1.10	nas.local	CC	445, 5000 SMBv1
192.168.1.25	RECEPCJA-PC (RECEPCJA-PC)		445
192.168.1.40	–		9100, 80

The audit was read-only – we changed nothing in your systems. Audit data is kept under our confidentiality agreement and deleted after 90 days.

SAMPLE