# MSP cybersecurity checklist

A self-audit for managed service providers to evaluate and strengthen their own cybersecurity posture.

You manage client networks, patch fleets, and fight ransomware for a living — but how's your own security posture? This checklist helps MSPs assess internal and client-facing cybersecurity practices before attackers find the cracks.

## 1. Internal security foundations

- [ ] MFA is enforced on every internal and customer-facing system
- [ ] Privileged access management (PAM) tools are in place for all admin accounts
- [ ] Password manager is deployed (no "shared Excel" credential sheets)
- [ ] Centralized logging is enabled for internal systems and staff endpoints
- [ ] Staff background checks and offboarding processes are standardized

**Tip:** If your techs can access all clients with one credential set, you're one phishing click away from a disaster headline.

## 2. Endpoint and patch management

- [ ] Automated patch deployment is configured for internal systems and client environments
- [ ] Endpoint detection and response (EDR) are running and monitored
- [ ] Unused or legacy tools are removed from RMM and PSA stacks
- [ ] Application allowlisting or controlled app policies are enforced
- [ ] Local admin rights are removed from internal users

**Tip:** Your RMM is a goldmine target — treat it like production infrastructure, not just tooling.

## 3. Network and infrastructure hardening

- [ ] Firewalls and VPNs are regularly updated and audited
- [ ] Network segmentation is implemented between management, production, and guest networks
- [ ] Secure remote access is configured (no direct RDP exposure)
- [ ] Configuration backups are encrypted and stored offsite
- [ ] DNS filtering or threat intelligence-enabled gateway is in place

**Tip:** If your RMM or PSA can be reached over the open internet, you're hosting a buffet.

## 4. Cloud and SaaS security

- [ ] MFA is enforced for M365, Google Workspace, PSA, RMM, and ticketing systems
- [ ] Conditional access or geofencing is configured
- [ ] Audit logs are enabled and reviewed monthly
- [ ] Shared mailbox and API credentials are secured
- [ ] Cloud backups are protected by separate credentials

**Tip:** Cloud apps are only as secure as their settings. Tighten access controls and monitor integrations like they're part of your network.

## 5. Monitoring and incident response

- [ ] SIEM or SOC are in place (in-house or via partner)
- [ ] 24/7 alerting and escalation workflows are documented
- [ ] Incident response plan is tested at least once per year
- [ ] Designated security contact for vendors and clients is in place
- [ ] Playbooks for RMM/PSA compromise and ransomware incidents are in place

**Tip:** Practice your breach response when it's calm — not when Reddit's already talking about it.

## 6. Staff training and culture

- [ ] Quarterly phishing simulations are conducted for internal staff
- [ ] Security awareness is baked into onboarding
- [ ] Acceptable use and data handling policies are documented
- [ ] Regular tabletop exercises or response simulations are conducted
- [ ] Internal red team or peer review on privilege escalation paths is performed

**Tip:** The weakest link isn't your firewall — it's your favorite tech with 19 browser tabs open.

## 7. Vendor and supply chain security

- [ ] Vendors are vetted for SOC 2, ISO 27001, or similar certifications
- [ ] Contracts are reviewed for data-handling and breach-notification clauses
- [ ] Least-privilege access is granted to third parties
- [ ] Integrations are audited for unused or legacy API tokens
- [ ] Security contact list for all key vendors is updated quarterly

**Tip:** If one of your integrations goes rogue, so do you.

## 8. Backup and recovery

- [ ] 3-2-1 rule is enforced for both internal and managed client backups
- [ ] Immutable or air-gapped backups are tested for restorability
- [ ] Backup encryption is verified
- [ ] Separate credentials are maintained for backup systems
- [ ] Recovery time and point objectives (RTO/RPO) are documented

**Tip:** If your backup server lives in the same AD domain as production, that's not redundancy — that's irony.

## How'd you do?

- 30+ checks: You're a fortress — share your story at the next MSP meetup.
- 20–29 checks: Solid foundation but tighten the seams.
- Fewer than 20 checks: Every MSP starts somewhere. Shore up the basics, then tackle the tougher fixes — one layer at a time.

Strong security starts with strong patching, clear visibility, and smart vulnerability management. **Demo PDQ Connect** and simplify your stack.