Your Essential Holiday IT Checklist: Keep Your Business Secure, Productive & Ready for the New Year

The holidays are a busy time for every organization—reduced staffing, travel, last-minute projects, and year-end deadlines. It's also when cybercriminals take advantage of lower oversight and slower response times.

To help you head into the season with confidence, On-Site PC Services (OSPC) created a Holiday IT Preparedness Checklist designed for business owners and non-technical leaders. These are practical, high-impact steps that reduce risk, protect your data, and keep your operations running smoothly even when your team is out.

This guide includes essential Managed IT, cybersecurity, and data protection best practices—aligned with the services OSPC provides every day.

Why a Holiday IT Checklist Matters

• Higher cyberattack risk due to reduced monitoring.

• Slower response times when key personnel are out.

• Greater operational impact if systems go down while decision-makers are unavailable.

• Increased data-loss exposure from postponed backups or unattended systems.

A proactive checklist helps avoid downtime, minimize security exposure, and ensure continuity.

Holiday IT Checklist for Business Leaders

1. Confirm Critical Backups Are Running

☐ Verify your server and Microsoft 365 backups are completing successfully.

☐ Confirm restore testing has been performed recently.

☐ Ensure backup retention meets compliance needs.

Outcome: Protects your business from accidental deletion, hardware failure, or holiday-timed ransomware attacks.

2. Review User Access and Permissions

☐ Disable or update access for terminated employees.

☐ Validate permissions for shared folders, systems, and cloud apps.

☐ Review admin-level accounts for accuracy and security.

Outcome: Reduces insider threats, accidental access, and compliance risk.

3. Update Patch & Security Policies

☐ Confirm all devices have recent Windows and application patches.

☐ Validate security agents like MDR/EDR, Zero Trust, and privileged access controls are active.

☐ Schedule any pending updates before the break.

Outcome: Eliminates vulnerabilities and reduces exposure during off-hours.

4. Communicate Your Holiday Support Plan

☐ How to contact OSPC support.

☐ What issues are considered urgent.

☐ The internal decision-maker to call if a system requires approval or authorization.

Outcome: Faster response, less confusion, fewer delays.

5. Secure Employee Travel & Remote Access

☐ Require MFA for all logins.

☐ Ensure remote desktop and VPN access are properly secured.

☐ Remind employees not to use public Wi-Fi without a secure connection.

Outcome: Prevents unauthorized access and travel-related breaches.

6. Confirm Hardware Stability Before the Break

☐ Review device health reports for aging or unstable hardware.

☐ Schedule proactively needed maintenance before the holiday slowdown.

☐ Validate server and network monitoring alerts are functioning.

Outcome: Avoids downtime and emergency repairs during the holidays.

7. Prepare for Year-End Projects & Renewals

☐ Check upcoming license renewals for Microsoft 365 and other SaaS tools.

☐ Schedule any equipment projects for early Q1.

☐ Review your technology roadmap with your IT provider or vCIO.

Outcome: Prevents subscription lapses and aligns IT planning with next year's goals.

How OSPC Helps Keep You Protected During the Holidays

- Continuous monitoring of servers, networks, and backups
- Managed MDR/EDR and Zero Trust application protection
- Rapid remote and onsite support
- Clear communication and documentation to reduce risk

Ready to Strengthen Your IT Before the Holidays?

If you'd like help preparing your environment—or want a more detailed assessment of your cybersecurity and IT readiness—OSPC is here to support you.

Contact us today to schedule a year-end IT review or discuss Managed IT & Cybersecurity services.