

# Must Have IT Checklists for Small Businesses

## IT Risks Checklist

---

- ☐ What are the cyber threats most relevant to your industry?
- ☐ Where is your sensitive data stored? (e.g. On-premises server, cloud, etc.)
- ☐ What compliance regulations are required for your business? Does your IT meet these standards?
- ☐ What are the physical risks to your systems? (e.g. Power outages, severe weather, etc.)
- ☐ When was your last risk assessment?
- ☐ Who is responsible for recovery in the event of downtime?

## AI Use & Governance Checklist

---

- ☐ Have you defined what AI tools are approved for business use?
- ☐ Have you defined what information can and cannot be entered into an AI prompt?
- ☐ Who owns your AI policy and oversees implementation and oversight?
- ☐ What AI tools or integrations have access to your systems, files, emails, data, etc.?
- ☐ How do you ensure oversight? (e.g. How do you ensure a lapse in policy is monitored and flagged)
- ☐ Have employees been trained on proper AI use, and do they have access to the policy for future use?
- ☐ Do employees know who to go to with AI-related questions?

## User Permissions Checklist

---

- ☐ Is multifactor authentication (MFA) turned on for email, remote access, and other business applications?
- ☐ Does your business utilize a password manager to ensure long and unique passwords for every account and system?
- ☐ Who is responsible for admin rights?
- ☐ How often are user permissions reviewed?
- ☐ Is there a documented process for changes in users? (e.g. Onboarding, offboarding, job responsibility changes)
- ☐ Do employees use personal devices? Are there policies and permissions in place for those devices? Do you have documentation of these devices and the data and systems they have access to?
- ☐ Are there permissions for physical access to server rooms, network equipment, or paper records?

## Backup & Recovery Checklist

---

- ☐ What data and systems are included in backups?
- ☐ How often are backups meant to occur?
- ☐ Is at least 1 copy of the backup kept in a secure, offsite location?
- ☐ Who is responsible for monitoring backups and ensuring they are completed?
- ☐ Are backups regularly tested? How long would it take for systems to come back online from backup? Is that information documented?
- ☐ Do you have a priority list of systems or data that must be brought back up first?

## Incident Response Checklist

---

- ☐ Who is responsible in case of a suspected data breach? Is there contact information easy to access?
- ☐ Are there documented immediate steps to contain the breach? Are they easy to access and well known?
- ☐ Who has authority to make decisions if an incident occurs?

- ☐ Do you understand your regulatory requirements for notification? (e.g. Notifying patients if their sensitive data was accessed or stolen)
- ☐ Do you have cyber insurance? What are your policy requirements?
- ☐ Has your plan been tested in the past year?
- ☐ After an incident, do you have a review process to determine mistakes made and initiate a plan to address gaps?

## **Vendor & Third-Party Access Checklist**

---

- ☐ Do you have a documented list of vendors with access to your systems and data?
- ☐ Are there user permissions in place for these vendors?
- ☐ Is there a documented process for approving or removing access?
- ☐ Do your vendors have their own security procedures in place for accessing your systems and data?
- ☐ Do your contracts outline who is responsible if your data was compromised through a vendor-based breach?