A GUIDE FROM EXPRESS

NYC Small Business IT Support Readiness Checklist

Security Baseline: Multi-Factor Authentication and Access Controls

Every NYC small business should verify that multi-factor authentication (MFA) is enforced across all cloud applications, remote access tools, and administrative accounts. MFA remains the single most effective control against credential-based attacks. Review your current environment to confirm that password policies require minimum length and complexity, that privileged accounts are separated from standard user accounts, and that former employee access is revoked within 24 hours of termination. For businesses in regulated sectors, document who has access to sensitive data and whether that access follows the principle of least privilege.

- Enable MFA on all email, file-sharing, and remote desktop services
- Audit administrative accounts quarterly and remove unnecessary privileges
- Maintain an offboarding checklist with IT access revocation as a mandatory step
- Require unique credentials for each user; prohibit shared logins for any business application

Backup Health: The 3-2-1 Rule and Recovery Testing

A backup strategy is only as reliable as your last successful restore. Apply the 3-2-1 rule: three copies of data, on two different media types, with one copy stored offsite or offline. For NYC businesses, consider geographic separation given local risks such as flooding or extended power outages. Verify that backup jobs complete without error, that retention periods match your operational needs, and that ransomware cannot reach offline or immutable copies. Schedule quarterly recovery drills for critical systems, not just file-level restores.

- Confirm automated daily backups for servers, workstations, and cloud data
- Test full system recovery at least once per quarter and document the time required
- Maintain one offline or air-gapped backup copy that is unreachable by network-based threats
- Review backup logs weekly for failure alerts or incomplete jobs

Incident Response: Defined Roles and Communication Plans

When a security incident occurs, hesitation amplifies damage. Your readiness checklist should include a written incident response plan with defined roles: who declares an incident, who contacts your managed IT services provider, who communicates with staff, and who handles external notifications. For NYC businesses, consider whether you must report breaches to the New York State Attorney General under the SHIELD Act, which requires notification of affected residents and the AG's office. Keep printed and offline copies of the response plan, since digital copies may be inaccessible during an active incident.

- Designate an internal incident lead and at least one backup contact
- Include your managed IT services provider's escalation path in the plan
- Define thresholds for when to engage legal counsel or cyber insurance carriers
- Prepare template communications for customers, vendors, and regulators

Compliance Basics: SHIELD Act and Industry-Specific Obligations

New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act applies to any business that collects private information from New York residents, regardless of where the business is headquartered. The law requires reasonable safeguards for data security and mandates breach notification within specific timeframes. Beyond SHIELD, NYC small businesses in healthcare must assess HIPAA obligations, those handling payment cards need PCI DSS alignment, and financial services firms may face NYDFS cybersecurity regulations. Your IT support readiness review should map which frameworks apply to your data and whether your current controls satisfy their requirements.

- Inventory all categories of private information your business collects and stores
- Verify that your managed IT services include security measures aligned with SHIELD Act standards
- Document which compliance frameworks apply and the date of your last gap assessment
- Retain records of security policies and employee training for regulatory examination

Vendor and Supply Chain IT Risk

Third-party vendors with access to your systems or data introduce risk that your own security controls cannot fully contain. Your readiness checklist should include a current inventory of all vendors with network access, cloud application integrations, or data processing roles. For each, confirm whether they maintain acceptable security practices, whether your agreements include security requirements, and whether you have a process to assess new vendors before onboarding. This is especially relevant for NYC businesses that rely on specialized local service providers or shared workspace technology.

- Maintain a current list of all vendors with system or data access
- Review vendor security practices annually and after any reported breach
- Require contractual security commitments from any vendor handling sensitive data
- Disable dormant vendor accounts and integrations that are no longer needed

Evaluating Managed IT Services: What to Ask a Prospective Provider

When assessing managed IT services for your NYC business, move beyond marketing materials to verify operational specifics. Ask how they handle after-hours emergencies, what their process is for onboarding new clients, and how they document your environment. Request clarity on whether they provide strategic planning or only reactive support. For businesses in the New York NY service area, consider whether the provider understands local compliance requirements and can support hybrid or remote work arrangements common in the city. A readiness checklist helps you compare providers against your actual needs rather than generic feature lists.

- Request a detailed onboarding timeline and discovery process
- Ask how they prioritize and communicate during simultaneous client incidents
- Confirm whether security monitoring and patch management are included or additional
- Verify their experience with your industry and applicable compliance frameworks