



Small Business Security Basics Checklist

A baseline security foundation for businesses of any size
27 items • nexsitnm.com

USER ACCOUNTS AND ACCESS

- Create individual accounts for each employee -- never share credentials.
- Grant employees the minimum level of access they need to do their job.
- Disable or delete accounts immediately when an employee leaves.
- Use strong, unique passwords for all accounts and enforce this policy for staff.
- Enable multi-factor authentication on all business accounts.
- Conduct periodic access reviews to ensure former employees have no lingering access.

ENDPOINT SECURITY

- Deploy endpoint security software on all company devices.
- Enable automatic operating system updates across all workstations.
- Encrypt hard drives on laptops and any device that leaves your facility.
- Establish a policy for personally owned devices accessing company data.
- Require screen lock after a short period of inactivity on all devices.

NETWORK SECURITY

- Use a business-grade firewall, not a consumer router.
- Separate guest or customer Wi-Fi from your internal business network.
- Change default passwords on all network equipment.
- Restrict access to sensitive systems by IP address or network segment where possible.
- Review firewall rules periodically and remove rules that are no longer needed.

EMAIL AND PHISHING

- Enable spam filtering and anti-phishing controls on your email platform.
- Configure SPF, DKIM, and DMARC records to prevent email spoofing.
- Train employees to recognize phishing attempts and report them.
- Establish a verification procedure for wire transfers and sensitive financial requests.

BACKUPS AND RECOVERY

- Back up all critical business data automatically on a daily basis.
- Store backups in at least one location that is not connected to your main network.
- Test your backup recovery at least quarterly.
- Document your recovery process so any team member can execute it in an emergency.

POLICIES AND AWARENESS

- Have a written acceptable use policy for company technology.

- Conduct security awareness training for all employees at least annually.
 - Have a documented incident response plan so your team knows what to do if something goes wrong.
-

This checklist is provided for informational purposes by Nexus IT Services, LLC. It is not a substitute for a professional security assessment. Contact us at (575) 263-6855 or nexusitnm.com if you need help implementing any of these items.