



New Employee IT Onboarding Checklist

A clean checklist for creating accounts, assigning equipment, and securing access from day one.

Your IT Department. Your Cybersecurity Team. Your Technology Partner.

Network Solutionist, LLC

Serving Wilmington, Newark, Middletown, Dover, Rehoboth Beach, and businesses across Delaware.



Before the Start Date

Done	Security Item	Why It Matters
[]	Confirm employee name, role, department, manager, start date, and location.	Accurate details prevent account and access errors.
[]	Identify required applications, mailboxes, groups, shared drives, and Teams.	Access should match job duties, not copy a previous employee blindly.
[]	Prepare workstation, laptop, phone, printer access, and peripherals.	Equipment should be ready before the employee begins work.
[]	Create accounts using a standard naming convention.	Consistency simplifies support and auditing.
[]	Assign Microsoft 365 license and security group membership.	Group-based access reduces one-off permissions.
[]	Set temporary password and require password change or secure enrollment.	Initial access should not remain reusable.
[]	Enroll MFA and backup verification methods.	MFA must be ready before sensitive access is granted.
[]	Apply endpoint protection, updates, encryption, and management agent.	A device should be secured before production use.
[]	Document asset tag, serial number, and assigned user.	Inventory accuracy matters for lifecycle and insurance.
[]	Schedule security awareness and acceptable use review.	Expectations should be clear from day one.

First Day Handoff

- Provide login instructions securely.
- Confirm email, Teams, printer, shared folder, and key application access.
- Review phishing reporting and support contact process.
- Confirm backup or OneDrive known-folder protection where applicable.
- Record any missing access requests for manager approval.

Helpful Reference Points



-
- FTC guidance recommends protecting data, limiting access, using strong passwords, and training employees on security practices.

Disclaimer

This guide is for general educational purposes and does not replace a formal cybersecurity assessment, compliance review, or incident response engagement.

Need help turning this into an action plan?

Network Solutionist, LLC can help assess, secure, monitor, and support your business technology environment. (302) 485-9850 | info@nsolutionist.com | nsolutionist.com

