IT CHECKLIST · BUSINESS OWNERS, MANAGERS & HR

New Employee IT Onboarding & Security Checklist

Give every new hire the access they need on day one—and nothing they don't. Covers accounts, devices, security basics and a clean offboarding when someone leaves.

Employee name	Start date	Manager
Role / department	Device / asset tag	Completed by

1 Before day one

- [ ] User account created with the correct name, title and department.
- [ ] Microsoft 365 (or Google Workspace) licence assigned; mailbox and shared mailboxes set up.
- [ ] Added to the right groups, Teams channels and shared folders — **only what the role needs**.
- [ ] Laptop or desktop prepared: updates installed, disk encryption on, endpoint protection active.
- [ ] Required business applications installed and licensed.
- [ ] Phone extension / VoIP account and voicemail set up.
- [ ] Email signature applied.
- [ ] Building access card or fob issued and recorded.

2 Day one

- [ ] **Multi-factor authentication** (MFA) enrolled on the employee's phone.
- [ ] Temporary password changed; password manager set up.
- [ ] Signed in to email, Teams and business apps; printers and Wi-Fi connected.
- [ ] Acceptable use and security policy reviewed and acknowledged.
- [ ] Shown how to **report suspicious emails** and who to call for IT help.
- [ ] Shown how to start a remote support session (trilliumsystemsolutions.ca/resources.html).

3 First week

- [ ] Security awareness basics covered: phishing, fake invoices, urgent payment requests.
- [ ] Files saved to company storage (OneDrive / SharePoint), not only the local device.
- [ ] Backups confirmed for the employee's device and data.
- [ ] Mobile device policy applied if company email is on a personal phone.
- [ ] Manager confirms access is correct — nothing missing, nothing extra.

4 Ongoing

- [ ] Automatic updates enabled and checked monthly.
- [ ] Access reviewed whenever the employee changes roles.
- [ ] Short security refresher at least once a year.

5 Offboarding (when the employee leaves)

- [ ] **Account disabled on the last day**; sessions signed out and MFA methods removed.
- [ ] Password reset; mail forwarded or converted to a shared mailbox as approved.
- [ ] Files and ownership of shared documents transferred to the manager.
- [ ] Laptop, phone and accessories returned and wiped or reassigned.
- [ ] Building fob / access card deactivated; alarm and door codes changed if shared.
- [ ] Licences removed or reassigned; vendor and app accounts closed.
- [ ] Shared passwords the employee knew are changed.

Tip: keep a completed copy of this checklist in the employee's file. It makes offboarding faster and gives you a record if access is ever questioned.

Let us handle onboarding

Trillium can set up accounts, devices and security for every new hire, and close everything down when they leave.

+1 (647) 229-9247
info@trilliumsystemsolutions.ca
trilliumsystemsolutions.ca