# Onboarding Checklist

Use this checklist to share essentials so we can secure, stabilize, and go live without disruption—without surprises.

### Client Information

| | | | |
|---|---|---|---|
| Company Name: | | Date: | |
| Primary Contact: | | NLS Contact: | |

## Section A: Company & Contacts

*Key stakeholders and communication preferences for onboarding and ongoing support.*

- ☐ Primary decision maker *(name, role, email, mobile)*
- ☐ Billing/agreements contact *(if different from primary)*
- ☐ Day-to-day IT contact *(who handles IT requests internally)*
- ☐ Preferred communication channel *(email, Teams, Slack, phone)*
- ☐ Decision cadence and escalation path *(who approves changes)*
- ☐ Office manager / facilities contact *(for on-site coordination)*
- ☐ Emergency contact *(after-hours critical issues)*

## Section B: Vendors & Licensing

*Current service providers and software licensing details we need to coordinate or take over.*

### Internet & Connectivity

- ☐ Internet/ISP provider and account info *(provider name, account #, public IP)*
- ☐ Circuit type and bandwidth *(fiber, cable, fixed wireless, Mbps)*
- ☐ Secondary/failover connection *(if applicable)*
- ☐ ISP support contact *(phone, portal login)*

### Phone & Communications

- ☐ Phone / UCaaS provider *(current vendor, contract status)*
- ☐ Phone numbers to port *(list all DIDs, toll-free, fax)*
- ☐ Auto-attendant / call flow documentation *(if available)*
- ☐ Current monthly cost *(for comparison purposes)*

### Cloud & Productivity

- ☐ Microsoft 365 subscription *(plan type, user count, admin access)*
- ☐ Google Workspace subscription *(plan type, user count, admin access)*
- ☐ Other cloud services *(Dropbox, Box, Salesforce, etc.)*
- ☐ Current licensing costs *(monthly/annual)*

### Security Tools

- ☐ Antivirus / EDR / XDR platform *(current vendor, coverage)*

- ☐ Email security / spam filtering *(vendor, configuration)*
- ☐ DNS filtering / web security *(vendor, policy)*
- ☐ SIEM / log management *(if applicable)*

## Domain & Certificates

- ☐ Domain registrar & DNS host *(GoDaddy, Cloudflare, etc.)*
- ☐ DNS records visibility *(do you have access?)*
- ☐ TLS/SSL certificates *(issuer, expiration dates)*
- ☐ Website hosting provider *(if NLS will manage)*

## Line-of-Business Applications

- ☐ Critical LOB apps *(EHR, ERP, accounting, legal, etc.)*
- ☐ Vendor support contacts *(for each critical app)*
- ☐ Hosting model *(on-prem, cloud, hybrid)*

## Section C: Access & Security

*Current security posture and access credentials we need to manage your environment.*

### Administrative Access

- ☐ Global admin credentials *(M365, Google, or on-prem domain)*
- ☐ Firewall / router admin access *(IP, credentials, VPN)*
- ☐ Switch / AP management access *(controller, cloud portal)*
- ☐ Server admin credentials *(local admin, domain admin)*
- ☐ Hypervisor access *(VMware, Hyper-V, Proxmox)*

### Identity & Authentication

- ☐ SSO/IdP in use *(Microsoft Entra ID, Okta, Google, other)*
- ☐ MFA enforcement policy *(which accounts, exceptions)*
- ☐ Conditional access policies *(if configured)*
- ☐ Password policy *(complexity, rotation, manager)*
- ☐ Shared/service accounts *(list any shared credentials)*

### Remote Access

- ☐ VPN solution *(vendor, configuration, user count)*
- ☐ Remote desktop / RMM *(existing tools if any)*
- ☐ Third-party remote access *(vendor tools, TeamViewer, etc.)*

## Section D: Network & Infrastructure

*Physical and logical network architecture for documentation and optimization.*

### Network Documentation

- ☐ High-level network diagram *(if available)*
- ☐ IP addressing scheme *(subnets, DHCP ranges, static IPs)*
- ☐ VLAN configuration *(segmentation, naming)*

### Network Hardware

- ☐ Firewall model & firmware *(make, model, version)*
- ☐ Switch models & topology *(managed/unmanaged, PoE)*
- ☐ Wireless APs & controller *(make, model, management)*
- ☐ UPS / power protection *(locations, capacity)*

### Servers & Compute

- ☐ On-premises servers *(physical, make, model, specs)*
- ☐ Virtual machines *(host, guest OS, purpose)*
- ☐ Cloud resources *(Azure, AWS, GCP VMs/services)*
- ☐ Server room / rack location *(for on-site visits)*

### Printers & Periphertic

- ☐ Network printers / MFPs *(make, model, IP addresses)*
- ☐ Specialty devices *(scanners, label printers, badge readers)*

## Section E: Data & Backups

*Backup infrastructure and data protection requirements.*

### Backup Infrastructure

- ☐ Backup platform *(Veeam, Datto, Acronis, native M365, etc.)*
- ☐ Backup targets *(local NAS, cloud, offsite)*
- ☐ Backup schedule *(frequency, retention)*
- ☐ Last successful restore test *(date & scope)*

### Critical Data

- ☐ Critical file shares *(paths, size, access groups)*
- ☐ Critical mailboxes *(executives, shared, compliance)*
- ☐ Databases to protect *(SQL, application DBs)*
- ☐ Retention requirements *(legal, compliance, business)*

### Recovery Objectives

- ☐ Target RPO *(recovery point objective)*
- ☐ Target RTO *(recovery time objective)*
- ☐ DR plan exists? *(documented disaster recovery)*

## Section F: Devices & Endpoints

*Endpoint inventory and management policies.*

### Device Inventory

- ☐ Windows workstations *(count by OS version)*
- ☐ macOS devices *(count by version)*
- ☐ Linux workstations *(if applicable)*
- ☐ Mobile devices *(iOS, Android count)*
- ☐ Tablets *(iPad, Surface, etc.)*

### Device Management

- ☐ Domain join status *(Entra ID, on-prem AD, workgroup)*
- ☐ MDM / endpoint management *(Intune, Jamf, other)*
- ☐ EDR/XDR agent coverage *(gaps if any)*
- ☐ Encryption status *(BitLocker, FileVault)*

### Policies

- ☐ Patch/compliance policy *(current tooling)*
- ☐ Local admin rights policy *(who has admin, approval process)*
- ☐ BYOD policy *(if applicable)*
- ☐ Hardware refresh cycle *(typical replacement age)*

## Section G: Constraints & Timing

*Scheduling constraints and compliance considerations.*

### Change Windows

- ☐ Change freeze / blackout windows *(month-end, year-end, etc.)*
- ☐ Preferred maintenance windows *(after-hours, weekends)*
- ☐ Critical business hours *(when downtime is unacceptable)*

### Compliance & Deadlines

- ☐ Compliance obligations *(HIPAA, PCI-DSS, SOC 2, CMMC, etc.)*
- ☐ Upcoming audits *(dates, scope)*
- ☐ Critical deadlines *(renewals, go-lives, seasonal peaks)*
- ☐ Cyber insurance requirements *(specific controls required)*

### Onboarding Preferences

- ☐ Target go-live date *(when to complete transition)*
- ☐ User training needs *(security awareness, new tools)*
- ☐ Communication preferences *(how to announce changes to staff)*

### Reference: Day-One Security Baselines

NLS implements these protections within the first week of onboarding:

- ☐ MFA/SSO enforced with least-privilege admin model
- ☐ EDR/XDR + email/DNS security active on all endpoints
- ☐ Patch hygiene & monitoring in place
- ☐ Backup validation & restore tests scheduled
- ☐ Documented support paths & SLAs communicated

## Reference: Four-Step Onboarding Timeline

Typical managed IT onboarding completes in 2-4 weeks:

**1. Discovery & Options (Day 0-1):** 15-min discovery; options within one business day; risk scorecard.

**2. Kickoff & Access (Week 1):** Team intro; comms & SLAs; secure access with MFA/least-privilege.

**3. Secure & Stabilize (Week 1-2):** Baseline protections; patch; backup verification; monitoring.

**4. Migrate & Go-Live (Week 2-4):** Migrations; standards; documentation; executive readout.

## Notes

## Questions or ready to start?

Email: info@nolimitsystems.com • Phone: (608) 285-2252 • Web: nolimitsystems.com