IMPLEMENTATION REFERENCE

Microsoft 365 Tenant Initial Setup Checklist

LIFECYCLE — ☐ Pending ■ Complete

01 PRE-DEPLOYMENT PLANNING 9

- ☐ Define goals (email migration, collaboration, security, intranet...)
- ☐ Inventory current systems (email, file servers, identity providers)
- ☐ Choose Microsoft 365 plan and licensing model
- ☐ Identify compliance requirements (GDPR, retention policies...)
- ☐ Define user groups, roles and access needs
- ☐ Decide identity model (Cloud-only / Hybrid / Federation)
- ☐ Decide primary domain name(s) and email address format
- ☐ Prepare DNS access

02 TENANT CREATION & INITIAL SETUP 8

- ☐ Create Microsoft 365 tenant
- ☐ Set global admin accounts (minimum 2)
- ☐ Configure tenant region and data residency
- ☐ Add and verify custom domain(s)
- ☐ Configure MX record (mail flow)
- ☐ Configure SPF, DKIM, DMARC (email authentication)
- ☐ Configure Autodiscover record
- ☐ Configure Teams / Skype DNS records (if used)

03 IDENTITY & USER MANAGEMENT 9

- ☐ Create users (manual or bulk import)
- ☐ Assign licenses
- ☐ Configure user attributes (UPN, email aliases)
- ☐ Configure password policies
- ☐ Enable Multi-Factor Authentication (MFA)
- ☐ Set up Conditional Access policies
- ☐ Install and configure Azure AD Connect (hybrid only)
- ☐ Sync users and groups; test sync and login

04 EMAIL — EXCHANGE ONLINE 11

- ☐ Set up Exchange Online and configure accepted domains
- ☐ Configure mail flow rules
- ☐ Enable anti-spam and anti-phishing policies
- ☐ Configure Defender for Office 365 (if licensed)
- ☐ Set up Safe Links and Safe Attachments
- ☐ Choose migration method (Cutover / Staged / Hybrid / IMAP)
- ☐ Migrate mailboxes and validate data integrity
- ☐ Update MX record to Microsoft 365
- ☐ Decommission legacy email system

05 FILE STORAGE & COLLABORATION 8

- ☐ Enable OneDrive; configure sharing policies and storage limits
- ☐ Create SharePoint site collections (team & communication sites)
- ☐ Define structure by department / project; set permissions
- ☐ Define Teams structure (org-wide, departments, projects)
- ☐ Configure Teams policies (messaging, meetings, apps)
- ☐ Integrate Teams with SharePoint and OneDrive

06 INTRANET SETUP 7

- ☐ Design intranet architecture
- ☐ Create communication site (home page) with navigation and news
- ☐ Configure permissions and audience targeting
- ☐ Migrate internal documents
- ☐ Create pages for departments, HR, IT...
- ☐ Add search configuration and metadata structure

07 SECURITY & COMPLIANCE 12

- ☐ Enable Secure Score recommendations
- ☐ Configure Conditional Access policies
- ☐ Enforce MFA for all users
- ☐ Set up Microsoft Intune; configure device compliance policies
- ☐ Enable MDM / Mobile Application Management (MAM)
- ☐ Configure Data Loss Prevention (DLP)
- ☐ Set retention policies and labels
- ☐ Enable auditing and alerting
- ☐ Configure eDiscovery
- ☐ Set up legal hold (if required)
- ☐ Ensure GDPR compliance settings

08 ENDPOINT & APPLICATION DEPLOYMENT 4

- ☐ Deploy Microsoft 365 Apps (Office applications)
- ☐ Configure update channels
- ☐ Set up device enrollment (Intune or other MDM)
- ☐ Configure Outlook profiles and Teams clients

09 TESTING & VALIDATION 5

- ☐ Test login and MFA scenarios
- ☐ Validate mail flow (internal and external)
- ☐ Test Teams meetings and collaboration features
- ☐ Verify SharePoint / OneDrive access and permissions
- ☐ Conduct pilot rollout with selected users

10 USER MIGRATION & ROLLOUT 4

- ☐ Communicate rollout plan to all users
- ☐ Provide training materials
- ☐ Migrate remaining users in phases
- ☐ Support users during transition period

11 POST-DEPLOYMENT TASKS 8

- ☐ Review Secure Score and improve security posture
- ☐ Optimize licensing usage
- ☐ Clean up inactive users and groups
- ☐ Set up monitoring and alerts; review audit logs regularly
- ☐ Monitor service health dashboard
- ☐ Implement backup solution (third-party if needed)
- ☐ Test restore procedures

12 GOVERNANCE & ONGOING MANAGEMENT 4

- ☐ Define governance policies (naming, lifecycle, sharing)
- ☐ Establish provisioning processes for Teams and Sites
- ☐ Regularly review access, permissions and security posture
- ☐ Conduct periodic security reviews

13 DOCUMENTATION & TRAINING 4

- ☐ Document architecture and configurations
- ☐ Create admin runbooks
- ☐ Train IT staff and helpdesk
- ☐ Provide end-user training sessions

14 DECOMMISSION LEGACY SYSTEMS 3

- ☐ Shut down old email and file systems
- ☐ Archive legacy data if required
- ☐ Update integrations and external dependencies

+ OPTIONAL — HIGHLY RECOMMENDED 4

- ☐ Implement Zero Trust security model
- ☐ Enable passwordless authentication
- ☐ Integrate with SIEM (e.g. Microsoft Sentinel)
- ☐ Automate processes (Power Automate, scripts)