FREE — INCLUDED WITH ASSESSMENT

The 12-Point Remote Work Security Checklist

Every IT team should verify these 12 points before enabling remote access. Any item you cannot tick with confidence is worth discussing in your free Readiness Assessment session.

48 hours. One request. Fully secured remote employee.

---

01 Device Enrollment

MDM enrollment required

All remote devices must be enrolled in your Mobile Device Management (MDM) system before they are permitted to connect to corporate resources. Unenrolled devices are an unmanaged and unmonitored endpoint, a direct entry point for attackers.

02 MFA Enforcement

Multi-factor authentication enforced on all portals

MFA must be enforced on VPN access, remote desktop portals, cloud application SSO, and all administrative interfaces. A stolen password without MFA gives an attacker full access. MFA is the single highest-impact control for remote access security.

03 EndpointProtection

EDR installed on every remote device

Endpoint Detection and Response (EDR) must be installed and active on every device used for remote work, including personal devices where allowed. EDR provides real-time threat detection, behavioral monitoring, and incident response

04 Zero TrustAccess

ZTA implemented — no open VPN exposure

Traditional VPN grants broad network access once connected. Zero Trust Access (ZTA) grants access only to specific applications and resources, scoped to the user's role. This eliminates lateral movement risk and dramatically reduces the blast

05 Least-Privilege IAM

Identity and access policies scoped to role

Every remote user should have access only to the systems and data required for their role, nothing more. Over-provisioned access is one of the most common and most exploited gaps in remote work security. Audit IAM policies quarterly and upon any

06 Offboarding Controls

Former employee credentials revoked within 24 hours

When an employee leaves the organization, all remote access credentials, VPN accounts, SSO profiles, cloud access tokens, and device certificates, must be revoked within 24 hours. Dormant credentials are a persistent and frequently exploited attack

07

Session Audit Trail

All remote sessions logged with full audit trail

Every remote access session should generate a log entry covering: who connected, from which device, at what time, to which systems, and for how long. This is essential for incident response, compliance reporting, and detecting anomalous access

08

Security Awareness Training

All remote employees trained on security protocols

Remote employees are disproportionately targeted by phishing, social engineering, and credential theft attacks. Security awareness training, covering phishing recognition, password hygiene, device security, and incident reporting, must be done

09

Standardized Request Process

Remote work request process documented and enforced

Ad-hoc remote work setup, approved via WhatsApp, email, or verbal request, produces inconsistent security outcomes. A standardized ITSM-based request process ensures every remote employee goes through the same security checklist before

10

Device Encryption

Full-disk encryption enabled on all remote endpoints

Full-disk encryption (BitLocker, FileVault, or equivalent) must be enabled on every device used for remote work. A lost or stolen unencrypted device exposes all locally stored data, including cached credentials, emails, and documents.

11

Incident Response Testing

IR plan tested specifically for remote access breach scenarios

Your incident response plan should include a specific playbook for remote access compromise, covering credential revocation, session termination, device quarantine, and forensic evidence collection. This plan should be tested at least annually.

12

Compliance Verification

Remote access aligned with PDPL, ISO 27001, and NCA requirements

Remote access controls must be documented and verifiable for compliance purposes. Key requirements include data residency controls (PDPL), access control documentation (ISO 27001 Annex A.9), and remote access security standards (NCA ECC).