QUICK GUIDE INTELLIGENT iT CYBERSECURITY

Remote Work Security Best Practices

Essential security controls to protect your workforce — anywhere they connect.

Remote and hybrid work expands your attack surface. This guide outlines the key controls every organization should implement to secure distributed teams.

SECURE CONNECTIVITY

- Deploy always-on VPN or Zero Trust Network Access (ZTNA) for all remote connections to company resources.
- Require WPA3 or WPA2-Enterprise for Wi-Fi connections; prohibit use of public/open Wi-Fi for work without VPN.
- Use split tunneling only when security policies allow; route sensitive traffic through corporate network.

IDENTITY & AUTHENTICATION

- Enforce MFA on all accounts — prioritize phishing-resistant methods (FIDO2 keys, authenticator apps).
- Implement conditional access policies: block sign-ins from unknown devices, locations, or risky sessions.
- Require strong, unique passwords (16+ characters) managed through an enterprise password manager.

DEVICE MANAGEMENT

- Enroll all devices (company and BYOD) in Mobile Device Management (MDM) with compliance policies.
- Require full-disk encryption (BitLocker, FileVault) on all laptops and workstations.
- Enable automatic OS and application updates; enforce a maximum patch window of 14 days.
- Deploy EDR (Endpoint Detection & Response) on all endpoints with centralized alerting.

PHISHING & SOCIAL ENGINEERING

- Conduct monthly or quarterly phishing simulations and track improvement over time.
- Implement advanced email filtering with link rewriting, attachment sandboxing, and impersonation protection.
- Train employees to verify unusual requests (wire transfers, credential resets) through a second communication channel.

DATA PROTECTION

- Restrict download and sync of sensitive data to managed, compliant devices only.
- Enable Data Loss Prevention (DLP) policies in email, cloud storage, and collaboration tools.
- Require cloud-based file storage (OneDrive, SharePoint, Google Drive) instead of local-only storage.
- Disable USB storage devices via group policy unless explicitly approved.

ENDPOINT PROTECTION & MONITORING

- Centralize logging and monitoring for all remote endpoints through SIEM or managed SOC.
- Enable automatic screen lock after 5 minutes of inactivity on all devices.
- Implement remote wipe capability for lost or stolen devices.