Comprehensive Remote Employee and Security Checklist

IT Security Checklist

- □ **Endpoint Security**
  - □ Use AI & ML to stop zero day threats
  - □ Turn on USB Scanning/Control, Firewall, Web filtering, Anti-Ransomware
  - □ Upgrade to EDR for deeper analysis, if budget allows
- □ **Email Security**
  - □ Scan emails both in/out
  - □ Enable DLP for sensitive data
  - □ Enable URL rewrites
  - □ Utilize phishing campaigns for awareness
- □ **Virtual Private Networks (VPN)**
  - □ Assume all non-corporate owned networks are compromised
  - □ Use Split Tunnel VPN for non-sensitive websites to reduce overhead on HQ firewall
  - □ Enable Multi-Factor Authentication to validate access
  - □ Use VPN to validate device hygiene before granting access
- □ **Single Sign-On (SSO) & 2FA**
  - □ Eliminate Password Reuse & Complexity
  - □ Prevent Credential Compromise with 2FA
- □ **Mobile Device Management (MDM)**
  - □ Ability to Locate, Lock, Patch, and Wipe devices
- □ **DNS Level Content Filtering**
  - □ Prevent malicious content from reaching the endpoint
- □ **Vulnerability & Patch Management**
  - □ Create a patch management policy with a set schedule & endpoint vulnerability assessment plan
  - □ Scan and assess network internally & externally
- □ **Enable Device and/or File Encryption**
- □ **Provide Secure Ways to Backup and Share Files**
  - □ Ex. OneDrive with time expiring links
- □ **Create Policies & FAQ Docs for Remote users**
- □ **Review Incident Response Procedure**

Remote Employee Checklist

- □ **Secure the Workspace**
  - □ Ensure devices will be used for business purposes only
  - □ If using outside of house, check surrounding and ensure no one can see over your shoulder
  - □ Only Use Secure Wi-Fi if possible
  - □ Turn on VPN and lock device when finished
- □ **Home Network Security**
  - □ Change router/all devices default password
  - □ Ensure wireless encryption is enabled on home Wi-Fi networks (WPA2 Recommended)
  - □ Check for firmware updates for any device on the network
- □ **Never Share Work Devices with Family or Friends**
- □ **Avoid use of corporate files or resources on personal devices unless using a virtual desktop or VPN connection**
- □ **Be Extra Vigilant About Phishing Emails**
  - □ Verify links by hovering and checking the URL
  - □ Don’t open attachments from unknown sources
- □ **Report Lost or Stolen Devices Immediately**
- □ **Update Emergency Contacts With Your Employer**
- □ **Review Corporate Policy and FAQs**

For more information on how Ingram Micro can help

CyberSecurity@Ingrammicro.com

SecurityLineCard.com

INGRAM MICRO® SECURITY