TELEWORK ESSENTIALS TOOLKIT

EXECUTIVE LEADERS

DRIVE CYBERSECURITY STRATEGY, INVESTMENT, CULTURE

After rapidly adopting wide-scale remote work practices in response to COVID-19, organizations have started planning for more permanent and strategic teleworking postures. An organization's executive leaders, IT professionals, and teleworkers all have roles to play in the shift from temporary to long-term or permanent telework strategies. The Cybersecurity and Infrastructure Security Agency (CISA) is providing these recommendations to support organizations in re-evaluating and strengthening their cybersecurity as they transition to long-term telework solutions.

ACTIONS

1 ORGANIZATIONAL POLICIES AND PROCEDURES

Review and update organizational policies and procedures to address the cybersecurity considerations raised by the shift to a remote workforce. Clearly communicate new remote work expectations and security requirements to the workforce. (STRATEGIC)

- National Cyber Security Alliance
- NIST Special Publication (SP) 800-46: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
- CISA Telework Guidance and Resources
- CISA Cyber Essentials Toolkit 1
- Cyber Readiness Institute Remote Work Resources: Securing a Remote Workforce and Making Your Remote Workforce Cyber Ready

2 CYBERSECURITY TRAINING REQUIREMENTS

Implement cybersecurity training requirements for your organization to improve working knowledge of cybersecurity concepts, current threats, and trends to empower workforce decision making when accessing organizational systems and data remotely. (STRATEGIC)

- CISA Cyber Essentials
- CISA Cyber Essentials Toolkit 2
- Cyber Readiness Institute Cyber Readiness Program

3 MOVING ORGANIZATIONAL ASSETS

Determine the cybersecurity risks associated with moving organizational assets beyond the traditional perimeter to activities not accessible by the organization's monitoring and response capabilities (e.g., printing at home, use of personal email accounts, use of personal devices, use of personal mobile devices). Develop, implement, and enforce enterprise-wide policies that address the threats and vulnerabilities presented by the new extended perimeter. These policies should include requirements for workers to securely configure and update corporate devices, personal devices, mobile devices, and home networks. (STRATEGIC)

- CISA and NSA Telework Best Practices
- NSA Telework and Mobile Security Guidance
- Cyber Readiness Institute Remote Work Resources: Top Three Dos & Don'ts for Remote Workers, Securing a Remote Workforce, and Making Your Remote Workforce Cyber Ready
- NIST National Cybersecurity Center of Excellence Mobile Device Security Guidance

4 CYBER SECURE, HYBRID CULTURE

Create a cyber secure, hybrid culture that includes remote employees, on-premise employees, and employees who may do both. Ensure policies focus on human behavior, address the basics in cyber hygiene—such as phishing, software updates, passwords/authentication, USB use, and removable media— and are clear, updated, and communicated to the workforce regularly. (STRATEGIC)

- Cyber Readiness Institute Cyber Readiness Program
- Cyber Readiness Institute Remote Work Resources: Creating a Cyber Ready Culture in Your Remote Workforce: Five Tips

As the Nation's risk advisor, CISA has compiled telework guidance to improve general cybersecurity posture. For the latest resources: CISA Telework Guidance

TELEWORK ESSENTIALS TOOLKIT

IT PROFESSIONALS

DEVELOP SECURITY AWARENESS AND VIGILANCE

After rapidly adopting wide-scale remote work practices in response to COVID-19, organizations have started planning for more permanent and strategic teleworking postures. An organization's executive leaders, IT professionals, and teleworkers all have roles to play in the shift from temporary to long-term or permanent telework strategies. The Cybersecurity and Infrastructure Security Agency (CISA) is providing these recommendations to support organizations in re-evaluating and strengthening their cybersecurity as they transition to long-term telework solutions.

ACTIONS

1 PATCHING AND VULNERABILITY MANAGEMENT

Ensure hardware and software inventories include new items added due to teleworking to ensure patching and vulnerability management are effective. Maintain patch and vulnerability management practices by keeping software up to date and scanning for vulnerabilities. Enable automatic software updates or use a managed solution wherever feasible. (TECHNICAL)

- CISA Tip on Understanding Patches and Updates
- GCA Cybersecurity Toolkit for Small Business: Know What You Have
- GCA Cybersecurity Toolkit for Small Business: Update your Defenses
- GCA Patch to Protect
- Cyber Readiness Institute Software Updates Guidance

2 ENTERPRISE CYBERSECURITY CONTROLS

Implement, maintain, and invest in enterprise cybersecurity controls to securely connect employees to the organization's network and assets. In modern IT environments, zero trust architecture may be preferable to virtual private network (VPN) solutions due to the lack of perimeter defense in cloud and distributed systems. Evaluate the current security architecture and ensure that it is properly protecting—and providing visibility into—remote sites and endpoints, including employees who may use public WiFi. (TECHNICAL)

- CISA Tip on Enterprise VPN Security
- NIST SP-800-207: Zero Trust Architecture
- GCA Public Wifi Wisdom

3 MULTI-FACTOR AUTHENTICATION

Enforce multi-factor authentication (MFA) for remote access to organizational systems and services. Develop contingency plans or solutions when MFA is not feasible or available. (TECHNICAL)

- CISA Tip on Supplementing Passwords with MFA
- CISA Guidance on MFA
- Work From Home Coalition Guidance on Enabling MFA on Microsoft Office and Google Suite
- GCA Cybersecurity Toolkit for Small Business: Beyond Simple Passwords
- Cyber Readiness Institute Authentication/ Passwords Guidance

4 ORGANIZATIONALLY APPROVED PRODUCTS

Maintain a list of organizationally approved products, including collaboration tools and teleconferencing applications. Provide users guidance on using these tools securely. (TACTICAL)

- CISA Tips for Video Conferencing
- CISA Guidance for Securing Video Conferencing
- CISA Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing
- GCA Cybersecurity Toolkit for Small Business: Know What You Have

5 FREQUENT BACKUPS

Perform frequent backups of the organization's systems and important files, verify backups regularly, and store backups offline and offsite. Prioritize protecting against ransomware attacks due to their potential for prolonged disruption in the telework environment. (TACTICAL/TECHNICAL)

- CISA Tip for Protecting Against Ransomware
- GCA Cybersecurity Toolkit for Small Business: Defend Against Ransomware (Backup)
- Cyber Readiness Institute Ransomware Playbook

6 DOMAIN-BASED MESSAGE AUTHENTICATION

Implement a Domain-Based Message Authentication, Reporting & Conformance (DMARC) validation system to address increased risk of phishing and business email compromise in remote working environments. (TECHNICAL)

- CISA Insights on Enhance Email & Web Security
- GCA Cybersecurity Toolkit for Small Business: Protect Your Email and Reputation

As the Nation's risk advisor, CISA has compiled telework guidance to improve general cybersecurity posture. For the latest resources: CISA Telework Guidance

TELEWORK ESSENTIALS TOOLKIT

TELEWORKERS – YOUR HOME NETWORK

DEVELOP SECURITY AWARENESS AND VIGILANCE

After rapidly adopting wide-scale remote work practices in response to COVID-19, organizations have started planning for more permanent and strategic teleworking postures. An organization's executive leaders, IT professionals, and teleworkers all have roles to play in the shift from temporary to long-term or permanent telework strategies. The Cybersecurity and Infrastructure Security Agency (CISA) is providing these recommendations to support organizations in re-evaluating and strengthening their cybersecurity as they transition to long-term telework solutions.

ACTIONS

1 CONFIGURED AND HARDENED

Ensure your home network is properly configured and hardened. Change all default passwords and use strong, complex passwords. Ensure your home wireless router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum and disable legacy protocols such as WEP and WPA. Ensure the wireless network name (service set identifier [SSID]) does not identify your physical location or router manufacturer/model. Use a protective Domain Name System (DNS) service. (TECHNICAL)

- CISA Tip on Securing Wireless Networks
- Center for Internet Security (CIS) Telework and Small Office Network Security Guide
- GCA Cybersecurity Toolkit for Small Business
- Work From Home Coalition Guidance

2 SECURE PRACTICES AND ORGANIZATIONAL POLICIES

Follow secure practices and organizational policies for handling sensitive data including: personally identifiable information (PII), protected health information (PHI), classified materials, intellectual property, and sensitive customer/client information. Avoid storing or transmitting sensitive organizational information on personal devices. If personal devices are approved for telework use, regularly apply the latest patch and security update on your devices. Follow your organization's guidance on securing your devices, including implementing basic security controls like password authentication and anti-virus software. (TACTICAL/TECHNICAL)

- Cyber Readiness Institute Data Protection Basics for Remote Workers
- Cyber Readiness Institute Authentication/Passwords Guidance
- GCA Cybersecurity Toolkit for Small Business

3 OPENING EMAIL ATTACHMENTS AN CLICKING LINKS

Use caution when opening email attachments and clicking links in emails. Increase your awareness of phishing tactics, current phishing campaigns, and social engineering to effectively report suspicious emails and communications. (TACTICAL)

- CISA Tip on Using Caution with Email Attachments
- Cyber Readiness Institute Phishing Guidance

4 COMMUNICATING SUSPICIOUS ACTIVITIES

Make sure you know the procedures for communicating suspicious activities to your organization's IT security team and promptly report all suspicious activity. (TACTICAL)

- Telework Security Basics

As the Nation's risk advisor, CISA has compiled telework guidance to improve general cybersecurity posture. For the latest resources: CISA Telework Guidance