CYBER READINESS
INSTITUTE

Cyber Readiness for the Hybrid Workplace — **Policies People Will Follow**

Every day more companies announce that they are shifting to a hybrid (remote-office) workplace for the foreseeable future or even permanently. The shift to the hybrid workplace has significant cybersecurity implications that span people, processes, and technology. Every organization needs to review and revise its policies and procedures for the hybrid workplace. People need to develop new habits based on the changes your organization is making, including the deployment of new technology. Your processes need to adapt to this new reality.

"Process" is a collection of linked activities that lead toward achieving a goal. In this case, the goal is having a cyber ready organization; the foundation for establishing processes in any organization is your policies. Policies are the rules that shape how people behave and the habits they develop.

For cyber readiness in small and medium-sized enterprises, we recommend you focus your policies on the core four issues (passwords, software updates, phishing and USBs/removable media) and incident response. Our Cyber Readiness Program includes policy templates you can use to get started and customize to create your own policies.

Here are some tips for creating effective policies or modifying existing ones for the hybrid workplace.

Get input from several people in your company from different functional areas and with diverse technology skill levels.

Determine whether the policies are appropriate for the hybrid workplace in which people will be changing locations and devices.

Make the policies easy to understand and implement, with minimum technical language.

- Ensure the policies are practical for people to follow and do their job. For example, if you have a "no USB" policy for transferring files between locations and devices, ensure you provide a practical alternative (e.g. cloud-based file sharing).

guide@cyberreadinessinstitute.com

Writing good policies is an important first step. Getting people to routinely follow them can be challenging. When implementing effective policies in a hybrid workplace, remember:

Hybrid workplaces will require people to change their behavior and develop new habits.

Changing behavior requires training, reinforced by frequent, short communications.

Tips for training:

- Use scenarios that illustrate the issue and are relevant to employees
- Only provide necessary information and always provide context
- Design your training to build awareness, gain commitment, and teach “how-to”

Tips for ongoing communication:

- Focus on changing one behavior at a time with a monthly cyber readiness theme
- Send a short weekly alert to highlight new cyber threats, a new cyber tip, and reinforce the importance of cyber readiness
- Start each video call or in-person meeting with a quick cyber tip or ask people how they are doing with their cyber ready habits

Stay tuned as we continue our hybrid workplace series to demystify cybersecurity by providing tips for managers and employees.

About CRI

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). Explore the building blocks of good cybersecurity with our Starter Kit or create a cyber readiness culture in your organization with the self-guided, online Cyber Readiness Program. Our Remote Work Resources and Hybrid Workplace Guides offer timely tips for addressing the evolving cyber challenges of today. To find out more, visit www.BeCyberReady.com.