Ntirety

Checklist

6 Critical Questions for Better Remote Workforce Cybersecurity

There's more to working remote than employees checking email out of the office. Enabling a remote workforce effectively requires extensive planning and thorough communication in several critical areas of your business IT.

Ensure your IT infrastructure, cybersecurity, and internal teams are all working effectively together by answering these key questions about your remote workforce.

☐ Do you currently have a documented remote work IT plan or policy in place?

This should include an up-to-date inventory of IT services and tools, cybersecurity and compliance requirements, and other business-specific details to enable effective remote work

☐ Are you using or prepared to use:

VIRTUAL DESKTOPS INFRASTRUCTURE (VDI)
Technology designed to provide local and remote workers with secure, managed virtual computers. For easy resource management and better security, the business determines what applications and services are available on the virtual desktops.

VIRTUAL PRIVATE NETWORKS (VPN)
Individual users are able to connect to an organization's network from a remote location using a computer or device connected to the Internet.

☐ Do you have a documented cybersecurity plan in place?

This should include all policies and practices that should be followed, either on-location and remotely, to protect data and infrastructure—especially if your company must meet specific compliance requirements.

☐ Do you have to meet compliance requirements (HIPAA, PCI, CCPA, etc.)?

Specific industries and states require businesses to meet specific regulatory IT requirements, or be penalized for non-compliance. Required businesses are audited based on specific compliance standards.

□ Have you confirmed that you can still meet your compliance requirements even when working remote?

While a business may be fully compliant with staff on-location, compliance standards must still be met when working remote—plus your business may fall under different compliance requirements when remote (for example PCI for online sellers).

□ Do you have a documented Business Continuity/Disaster Recovery (BCDR) plan for how to respond in a cybersecurity emergency?

A BCDR plan ensures that business will continue even during a disaster with clear steps and actions that will help protect and restore mission-critical IT systems. These plans include up-to-date inventories of IT assets, diligent backups, scheduled testing, and defined responsibilities amongst teams. Comprehensive BCDR plans must support the five critical aspects of your cloud environment: Availability, Performance, Resilience, Security, and Capacity.

▶ Need guidance to ensure your remote workforce is secure? Ntirety offers a full suite of Remote Workforce Enablement services—from tactical tools like VDI and VPN to fully managed BCDR solutions. **Learn more by scheduling a consultation at Ntirety.com/Get-Started today.**

About Ntirety
In 2018, Hostway and HOSTING merged to create Ntirety—an industry leader in providing secure digital transformation solutions, featuring full-stack services across the entire lifecycle to help IT leaders harness data. Ntirety delivers experienced and secure migration services, complex managed cloud infrastructure, and application solutions for mission-critical software. Our team of engineers deliver reliable and scalable managed cloud and hybrid cloud solutions to thousands of customers across fourteen geographically diverse data centers around the world—all while ensuring strict compliance to PCI, HITRUST, HIPAA, FERPA, and GDPR guidelines. The Ntirety mission is simple—to provide the best customer experience from the industry's best team. Visit Ntirety.com for more information.

Ntirety®