REVEALRISK
SECURE YOUR BUSINESS

For more information: contact us at: info@revealrisk.com

Remote Work Information Security Health-Check Assessment

Purpose: This assessment is designed to help companies that have made (or are making) rapid leaps to get their workforce online and working remotely in a secure manner. It is intended to help those responsible for accelerating these needs to understand control areas that need to be considered (even if after-the-fact due to urgency/pressures). Regardless of the urgency, pace, and decisions previously made, this guide will help you address ensure information security controls are in place.

People /Culture Questions

1. **Culture:** Do you have an existing culture of remote working that includes technology (e.g. Laptops), process (e.g. training), and people (e.g. regular telecommuters)?

☐ Yes ☐ No

Notes:

2. **Workforce Policy / Guidance**: Do you have workforce policy, training, and communications/awareness activities that employees are aware of which provides guidance on using approved tools such as chat and filesharing while avoiding risky behaviors like social media and personal email accounts?

☐ Yes ☐ No

Notes:

3. **Secure File Storage and Backup:** Do employees know where to securely store files when working remotely (e.g. laptop, home computer, cloud storage) and are those files securely backed-up? Are any special handling precautions around customer or privacy data in remote settings addressed?

☐ Yes ☐ No

Notes:

4. **Phishing - Simulated Exercises:** Does the organization provide any phishing / social engineering education or simulated testing to be aware and vigilant of the increased volume of malicious attempts linked to Covid-19?

☐ Yes ☐ No

Notes:

5. **BYOD / Personal Devices:** Do you have a BYOD program, and is it formal (e.g. clear policies on how personal assets are used for business) or informal (e.g. users are able to log in from their device of choice when convenient)?

☐ Yes ☐ No

Notes:

6. **Social Media Use:** Does the organization have clear guidance on use of social media type tools for work purposes (e.g. interacting or sharing files via tools like Facebook Messenger, WhatsApp, WeChat, etc.) For official accounts or regulated employees, are there controls in place to protect account integrity and ensure compliance?

☐ Yes ☐ No

Notes:

7. **Reporting a Concern:** Do employees know where to report an information security related concern? Is your call center scalable for higher volumes?

☐ Yes ☐ No

Notes:

Process and Technical Questions

8. **IT Enabled Controls / Default Settings:** Do you have prior IT/Security projects that have been completed to enable secure remote work (Multifactor Authentication, VPN, secure file share, secure video conference settings, etc.)?

☐ Yes ☐ No

Notes:

9. **IT Infrastructure Scale:** Can your IT infrastructure scale to support the increased volume of more remote users (e.g. collaboration software and controls, higher VPN sessions, etc.)

☐ Yes ☐ No

Notes:

10. **Device Management:** Are mobile and remote devices (including laptops) actively managed to ensure devices are encrypted, software and operating systems are patched and maintained at acceptable baselines, and devices can be remotely wiped if lost or stolen?

☐ Yes ☐ No

Notes:

11. **Tele/Video Conference:** Does the organization have a preferred / procured secure video/teleconference service with minimum security settings enforced?

☐ Yes ☐ No

Notes:

Our highly experienced team at Reveal Risk is available for free 30-minute discussions around specific recommendations against any gaps you may have, prioritization of action against these elements for your specific organization, or general Q&A on any concerns you may have.