Integris.

Remote Workplace Security Assessment

Did you know that the FBI is receiving 3 to 4 thousand cybersecurity complaints a day since businesses have shifted to remote work? The risk has never been higher, and you need to be ready.

Take this assessment to evaluate how to secure your remote workforce in these 6 critical categories:

Password / Security	YES	NO
1. Have you and your team discussed your admin user strategy?	☐	☐
2. Do any of your users also have administrative rights on their main account?	☐	☐
3. Do all users with Microsoft tenant admin rights have enforced MFA?	☐	☐
4. Do all users have MFA enforced?	☐	☐
5. Have you enabled and enrolled self-service password reset?	☐	☐
6. Do you have conditional access policies restricting Microsoft use to the appropriate location and conditions for your Information security policy?	☐	☐

Email Protection	YES	NO
1. Do you block common attack vector attachment types? EX – .doc, .exe	☐	☐
2. Do you block attachments with office macros enabled?	☐	☐
3. Do you have email auto forwarding blocked in your tenant?	☐	☐
4. Do you have sender protection framework (SPF) configured? (A way to tell the world where my mail should be coming from)	☐	☐
5. Have you enabled Domain Keys Identified Mail (DKIM)? (Mail integrity protection) (If you don't know what this is, answer no)	☐	☐
6. Do you have DMARC to validate email and enforce SPF and DKIM?	☐	☐

Integris.

Information Governance - Protecting Data	YES	NO
1. Do you have data loss prevention policies enabled?	☐	☐
2. Can you send an encrypted message? (Unauthorized users cannot intercept/read)	☐	☐
3. Do you have retention policies on deleted mail? (Example: keeping mail on file 90 days after deletion for later reference)	☐	☐
4. Do you have sensitivity labels assigned to data so that it can be protected better as the value rises to your organization? (Example – classifying public vs non-public data to	☐	☐

Teams Security	YES	NO
1. Are your users allowed to create their own teams?	☐	☐
2. Do you allow all outside entities to participate as guests in your team channels?	☐	☐
3. Do you let your external guests to chat with your users without restriction?	☐	☐
4. Do you allow 3rd party cloud storage interaction in teams? (Ex. DropBox)	☐	☐
5. Do you have meeting policies that allow anonymous requests?	☐	☐
6. When sharing files with OneDrive for business, can you share without the recipient signing in? (Default state – anyone with link can open)	☐	☐
7. Have you moved your known folders (Desktop, Documents), and shared server files to OneDrive and Teams for daily use?	☐	☐

Secure Remote Access	YES	NO
1. Do you use a VPN (virtual private network) to access legacy information systems where necessary?	☐	☐
2. Do you use single sign on to seamlessly shift from web application to web application?	☐	☐

Integris.

Managed Devices		YES	NO
1.	Are your existing legacy computers bound to Intune for mobile device management?	☑	☐
2.	Can you use autopilot to automatically refresh machines for new users?	☑	☐
3.	Have you configured application protection policies to protect data on company owned devices?	☑	☐
4.	Do you allow employees to use their cell phones to access company data?	☐	☑
5.	Do you allow employees to use their own laptops/home computers to access company data?	☐	☑
6.	Do your company owned devices have to be at a certain health level to access company data?	☑	☐
7.	Do your company machines automatically return to a known baseline when refreshed and placed in use?	☑	☐

How Did You Do?

Count all your checkmarks in the boxes with the orange

30-32 correct answers:

Congratulations! You are in good shape. Consider a free Modern Workplace Consultation to see if there are any more steps you can take to really "up" your security game.

25-30 correct answers:

Your protections are "so-so." You have many of the bases covered, but you have vulnerabilities that need to be addressed. A free Iconic IT Modern Workplace Consultation will help you bridge the gaps in your cybersecurity.

> 25 correct answers:

Your network is at high risk for a breach or other catastrophic failure. We recommend scheduling a completely free, no obligation Modern Workplace Consultation to have a professional advise you on the next steps you should be taking to secure your network right now before it's