AXIS INSURANCE SERVICES, LLC

Axis Management Home User Network Security Checklist

While working from home has some benefits, it does raise a concern that employees at home networks might not be as secure as in their regular offices. The following checklist was to designed to help you figure out how to safely work from home.

Employee name:	
Employee Phone # / Cell #:	
Date Completed:	

1. Document your Internet Service Provider (ISP):	
2. Document Manufacturer and Model of your home router / firewall: Recommendation: Routers should be no more than 4 years old.	
3. Document any additional wireless or networking devices in use: (This would include things like Wireless Access Points, Range Extenders, etc.)	
4. Do you know the administrative login to your home router / firewall? Please do NOT document the password on this form Recommendation: All users should have this information and keep it safe.)	
5. Has the administrative password been changed from the default and is it “complex”? Recommendation: Administrative passwords should be a minimum of 8 characters and contain upper case, lower case, numbers and symbols.	
6. Are administrative logins disabled from the WAN interface? Not all routers have this setting. But if available, administrative logins should not be permitted from the internet	
7. Are administrative logins forced to HTTPS? Not all routers have this setting. But if available, administrative logins should be forced to SSL or HTTPS	
8. Firmware version of your router / firewall: Recommendation: Router firmware should be routinely checked and kept on the most current release of firmware available from the manufacturer.	

9. Does your home router / firewall have Guest WiFi capability? Not all routers have this capability.	
10. If Guest WiFi is available, is Guest WiFi enabled and in use? Recommendation: Using your routers Guest functionality is an easy way to isolate your work computer from the rest of your home network.	
11. Is your WiFi (or Guest WiFi) currently configured for WPA2(or higher) encryption? Recommendation: ALL WiFi networks should have WPA2 encryption enabled. Even networks your work computer is not connected to.	
12. Is your WiFi passphrase “complex”? Please do NOT enter the passphrase on this form Recommendation: Your WiFi passphrase should contain a combination of upper case, lower case, number and symbols. And should be changed periodically.	
13. Is your router configured to use your ISP default DNS servers? Recommendation: DNS servers should be changed from the ISP default to a secure alternate like OpenDNS servers.	
14. Is WPS enabled on your router? WPS is the technology that allows connecting devices to your WiFi through the use of a special button on the device and the router, without the use of the passphrase. This is considered insecure and should be disabled.	
15. Was your router installed by you (or someone in your home) or by your ISP?	
16. Does your home router have a firewall setting and is it enabled? Not all routers have firewall capability. But if it does it should be enabled.	
17. Is your work computer connected via wire or wireless?	
18. Run a speed test at www.speedtest.net and record results.	

19. How many users are typically connected to your home network (include all the users in your home)?	
20. How many people in your home are currently using your network to work from home?	

Disclaimer: This checklist is only a recommendation and you should check with your firms IT company before doing any assessment.