SECURITY TASKFORCE QUESTIONNAIRE

STAGE 1: STOP-GAP MEASURES, “CRAWLING IN SECURITY”

INTERNET CONNECTIVITY

WI-FI

1. Which Wi-Fi standard is in use? WEP, WPA2, or WPA3?
2. Is the SSID (or the name of the network) broadcasted or hidden?
3. Is the default password changed?
4. Is there control over what gets access to the intranet (devices inside your network) over Wi-Fi?
    - Is there an allowlist for certain devices or just a shared Wi-Fi password?
    - Is there a form of authentication for connecting to the network beyond the password?
    - Is the network monitored for how many devices are on it and whether the device is authorized?
5. Is there a guest Wi-Fi network that is separate from the rest of the intranet (on a separate VLAN)?

ETHERNET

6. How many Ethernet outlets are in the facility?
    - How many are in public areas?
    - How many are for company use?
7. Are the Ethernet ports that are not in use disabled, disconnected, or covered?
8. Is there control over what gets access to the intranet via Ethernet ports?
    - Is there an allowlist for certain devices?
    - Is there a form of authentication for connecting to the network?
    - Is the network monitored for how many devices are on it and whether the device is authorized?

DEVICE MANAGEMENT (STAGE ONE)

Regarding devices that are currently connected to the intranet:

9. How many are company-owned?
    - Are company-owned devices allowed to be taken home?
10. How many are privately owned/BYOD (bring your own device)?
11. How many have antivirus software installed?
12. Is there a written acceptable use policy that must be signed to connect to the intranet?
13. For each of the following that exists on your network, record the number of matching devices, the year they were installed/acquired, and the year of their latest update:

Category	Type	Number	Year installed	Latest update
Network	Router			
	Firewall			

Category	Type	Number	Year installed	Latest update
	Switch			
	Network-attached storage or file share			
	Printer			
	Camera/security system			
	Other			
Devices	Laptops			
	Tablets/mobile devices			
	Desktops and all-in-ones			
	Servers			
	Points of sale			
	VoIP phones			
	Smart devices (see IoT section below)			
Software	Operating systems			
	Antivirus software			
	Remote management software			
	Paid software			
	Free software			

PASSWORD POLICY

14. Is there a written password policy?
    - What criteria are set for strong passwords? (For example: must be a full phrase with a certain length and a complex combination of alphanumeric, numbers, and special characters)
15. How many passwords is each employee required to store or remember?
    - Is a password manager or password vault used?
    - Are passwords reused between multiple accounts or devices?
    - Are passwords shared on any account or device, whether online or offline?
    - Are passwords stored in a file on a device, written down, or neither?
16. Are passwords changed on a cycle?

MULTIFACTOR AUTHENTICATION (MFA)

Multifactor authentication is also known as 2FA (two-factor authentication). MFA requires a second form of identification beyond a username and password in order to confirm a user's identity. Common types of MFA:

Phone call	SMS	Biometrics	Authenticator app	Password token	Passkey

17. For each category below, record whether MFA is enabled or not and what kind of MFA is enabled:

Category	MFA enabled?	Type of MFA
Devices		
Software programs		
Online accounts		
Network accounts		

PATCH MANAGEMENT

18. Is there a patch management policy that determines when updates and upgrades will be performed?
19. Does somebody check all devices for operating system updates and install them as recommended on a weekly basis?
20. Does somebody subscribe to CISA advisories and notify the company to take appropriate steps as recommended?
21. Is software configured to automatically check for and install updates?
    - If so, what software is not configured this way?
    - Does somebody verify that updates are installed on all other software applications on a regular basis?
22. Is open-source software allowed?
    - Is open-source software reviewed for security updates?

PHYSICAL SECURITY

LOCKS

23. What types of locks are in use (key, electric, smart, biometric, commercial grade)?
24. A key inventory involves tracking all physical keys and codes so that a company knows who has them and can revoke access when needed. Is there a key inventory in place?
25. Are there tamper-proofing devices added to the exterior locks and areas with sensitive items?

ALARMS

26. Are alarms installed?
    - Who is responsible for monitoring the alarms (self or subscription-based)?
    - Who is responsible for responding to alarm notifications?
27. Which of the following alarm systems are installed that protect your business from theft or intrusion?
    - Entrance alarms or full facility alarms
    - Window or glass-break alarms
    - Motion detectors
    - Other
28. Are cameras in use? If so, where is the video data stored and who has access to it?
29. Are the alarm systems protected by passcodes?
    - Does each person have a unique passcode or one shared passcode for alarm systems?
    - Under what circumstances are the codes changed?
    - Are they changed on a regular basis?

LOCATION OF NETWORK EQUIPMENT

Network equipment includes devices that are connected to the network to make the network ready for employees and customers. Network equipment does not include workstations, registers, VoIP phones, printers, or devices that require daily use. Network equipment includes the following:

Router	Firewall	Phone/audio	Switch	Server	NAS/file share

30. Is all network equipment secured in private and locked areas?
    - Are there only floor-to-ceiling walls in the room—not a drop ceiling with access to adjacent rooms?
    - Are all devices on a secured rack or cabinet?
    - Are all unused ports locked or turned off?
31. Is there a UPS (uninterruptible power supply) or generator installed?
32. Is there a proper or safe cable management system deployed?
    - Are cables labeled?
33. Are locks to entrances and sensitive areas inspected at opening and closing times?
34. Is access control enforced?
    - If so, how?

IOT (INTERNET OF THINGS) DEVICES

IoT devices are smart devices that connect to a network, including (but not limited to) the following:

Smart camera	Smart speaker	Smart thermostat	Smart TV	Smart lock	Keypad	Smart vacuum	Smart refrigerator

35. Have all IoT devices had the default username and password changed, if applicable?
36. Are all devices secured in place when at rest?
37. Are devices checked for tampering? (Recorded serial numbers; cables and plugs checked for additional items)
38. Are IoT devices checked for updates?
39. Are there cameras or microphones built into any IoT devices?
    - If so, are any devices in locations where sensitive conversations or actions occur?
40. Are all IoT devices on a separate network (a guest network, air-gapped, separate VLAN, or private)?

COPYRIGHT NOTICE

ICON ATTRIBUTION

Icons provided by Icons8. For more information, visit https://icons8.com/.

DISCLAIMER

This questionnaire is intended to provide an initial understanding of your security needs and is not a substitute for professional advice or an exhaustive assessment of your situation. It is not designed to diagnose or solve any specific problems. The author or the organization distributing this questionnaire will not be liable for any outcomes or decisions made based on the responses to this questionnaire. Always consult with a professional in the relevant field for accurate information.