The Cybersecurity Handbook Security Plan Starter Kit

Use the following starter kit to take notes as you and your organization read through the Handbook and digest the material, and consider the accompanying questions with your colleagues to help generate productive discussion.

Be sure to reference the key "building blocks" in each section of the Handbook too to ensure that you are covering the important topics as you build your security plan. By the end of the Handbook, the building blocks, answers to these discussion questions, and your notes should form the foundation of a successful security plan!

Building a Culture of Security

A Strong Foundation: Securing Accounts and Devices

Communicating and Storing Data Securely

Staying Safe on the Internet

Protecting Physical Security

What To Do When Things Go Wrong

Building a Culture of Security

QUESTIONS TO CONSIDER:

- When can you schedule a conversation to review your security plan with the entire organization?
- What days or times work well for the organization to schedule regular conversations and training about security?
- What steps can leadership take to model good security behavior and a commitment to a security plan? How can others in the organization play a role in security?

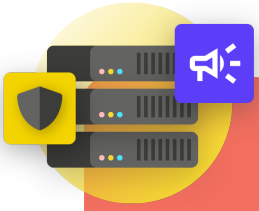
YOUR NOTES AND IDEAS:

A Strong Foundation: Securing Accounts and Devices

QUESTIONS TO CONSIDER:

- How will you implement account security measures - like a password manager and 2FA - across the organization? What obstacles might you encounter during implementation?
- How will your organization ensure that devices are kept secure and updated? As part of this, will the organization need a plan to address unlicensed software or computers?
- When is a good time to set up training for all staff on the dangers of phishing, malware, and device security best practices?

YOUR NOTES AND IDEAS:



Communicating and Storing Data Securely

QUESTIONS TO CONSIDER:

- How will your organization implement end-to-end encrypted messaging for secure communication? What obstacles might you encounter during implementation?
- How will your organization enforce a secure file sharing solution both internally and externally? What obstacles might you encounter during implementation?
- How will your organization implement a secure data storage and backup solution? What obstacles might you encounter during implementation?

YOUR NOTES AND IDEAS:

Staying Safe on the Internet

QUESTIONS TO CONSIDER:

- How will your organization implement secure browsing requirements such as HTTPS, a trusted browser, and, if appropriate, a VPN for staff?
- What will be the key elements of your organization's social media policy? How will it be enforced?
- How will your organization protect its websites and web properties?

YOUR NOTES AND IDEAS:

Protecting Physical Security

QUESTIONS TO CONSIDER:

- How will the organization distribute and enforce its office guest and access policy?
- Who is responsible for preparing staff for the physical and digital security challenges that they might face while on travel for work?
- What steps can staff take to keep their devices safe and secure both at the office and while on travel?

YOUR NOTES AND IDEAS:

What to Do When Things Go Wrong

QUESTIONS TO CONSIDER:

- How will the organization distribute and practice its incident response policy?
- Are there resources available for staff who might be in need of emotional and social support in the aftermath of an incident? If not, how might the organization be able to provide those resources in case of an incident?

YOUR NOTES AND IDEAS: