Please Note: Cybersecurity is a rapidly evolving field. This document was last updated on February 2, 2019. Some of the technical guidance within this document may change, and some of the risks defined may increase or decrease in their potential likelihood or impact.

Appendix A: Building a Security Policy for Your Organization

Security policies can serve many purposes for organizations. Some prefer these documents to be legal policies that establish clear responsibilities and liability. This section focuses on elements of security policies that can be used to plan for effective cybersecurity practice. But, if your organization wishes to utilize more legally-oriented language, the SANS Institute maintains a consensus-based collection of organizational cybersecurity policy language that your organization can use, free of charge: https://www.sans.org/security-resources/policies

Each section will include a template for writing an organizational cybersecurity policy to implement the controls described in Section 2. These fillable templates, in combination with the best practices described in Section 3, can serve as a baseline cybersecurity policy for an organization.

Each template can be expanded as needed – while there may not be enough fields in the examples to capture all of the devices, accounts, etc. in an organization, each policy, best practice, and control can be modified to fit the context of a specific organization. More guidance on how to select a policy and implement a control can be found in Appendix C.

Strong Authentication

Read the description of this control here.

Additional implementation guidance can be found here.

Policy Selection:

- **Baseline:** Require multi-factor authentication for all organization-managed accounts. Turn on login alerts where offered.
- **Baseline +:** Require multi-factor authentication for all organization-managed accounts. Require the use of password managers. Turn on account monitoring where offered.
- **No Policy**

Policy Details: Person(s) responsible for implementing this policy:

(*Name*)

This individual is responsible for ensuring multifactor authentication is enabled on all critical accounts, and will serve as a resource for other staff who need assistance with MFA set up or recovery. This individual is also responsible for ensuring that back up MFA codes for organization-owned accounts are stored in a safe, secure place - such as an external USB drive in a locked cabinet.

What accounts are considered critical?

Account	MFA Forced?
(Account Name)	*(yes/no)*

Automatic Updates and Software Licenses

Read the description of this control here.

Additional implementation guidance can be found here.

Policy Selection:

- **Baseline:** Force automatic updates for all operating systems, productivity software, and web browsers, and require other software updates to be installed as quickly as possible. Ensure all software licenses are renewed in a timely fashion.
- **Baseline +:** Force automatic updates for all operating systems, productivity software, and web browsers, and require other software updates to be installed as quickly as possible. Auto-renew all critical software licenses.
- **No Policy**

Policy Details:

Person(s) responsible for implementing this policy:

(*Name*)

This individual is responsible for ensuring automatic updates are turned on for all required software, and that software and services licenses are current. They will also serve as a resource for any staff having trouble updating their software.

What software is considered critical?

Software or Operating System	Updates Forced?	Auto-Renew License?
(Software or OS Name)	*(yes/no)*	*(yes/no)*

The Cloud

Read the description of this control here.

Additional implementation guidance can be found here.

Policy Selection:

- **Baseline:** Migrate organizational email to a cloud-based provider
- **Baseline +:** Migrate organizational email, data storage, and productivity software to a cloud-based provider
- **No Policy**

Policy Details:

Person(s) responsible for implementing this policy:

(*Name*)

This individual is responsible for leading the migration to any new cloud-based services - either migrating data themselves, or managing a contract with a third party to conduct that migration. They should become knowledgeable users of that service, so that any staff struggling with the transition can use them as a resource.

What services are considered critical?

Software or Services	Cloud-based?
(Software or Service Name)	*(yes/no)*

What services or software will your organization migrate to the cloud?

Software or Services	Persons or third party responsible for migration	Timeline for migration
(Software or OS Name)	*(Staff/Contractor Name)*	*(Timeframe)*

It is *highly* recommended you enable strong authentication for any cloud-based services important to your organization.

HTTPS

Read the description of this control here.

Additional implementation guidance can be found here.

Policy Selection:

- **Baseline:** Ensure all organization-owned websites uses HTTPS
- **No Policy**

Policy Details:

Person(s) responsible for implementing this policy:

(*Name*)

This individual will be responsible for enabling HTTPS on any organization owned or supported sites - either themselves or by working with a third party contractor/servicer.

What sites does the organization own or support?

Site URL	Site Administrator	HTTPS enabled?	Timeline for enabling HTTPS?
(www.xyz.org)	*(Staff/Contractor Name)*	*(yes/no)*	*(Timeframe)*

Data Security

Read the description of this control here.

Additional implementation guidance can be found here.

Policy Selection:

- **Baseline:** Enable full-disk encryption on servers, cell phones, tablets, laptops, and desktops with access to critical or sensitive information.
- **Baseline +:** Enable full-disk encryption on all servers, cell phones, tablets, laptops, and desktops with access to organization resources. Regularly review permissions on cloud-based storage accounts to ensure access controls are appropriately granted and MFA is enabled. Consider adopting and implementing a device management system (learn more in the fleet management section).
- **No Policy**

Policy Details:

Person(s) responsible for implementing this policy:

(*Name*)

This individual will be responsible for ensuring critical devices are encrypted and access management reviews are conducted. They should become knowledgeable about how to enable device encryption, as well as how to review

the permissions of shared resources, so that any staff struggling with the transition can use them as a resource.

What devices do those staff members use to access critical or sensitive information? Those devices should have full disk encryption enabled.

Staff	Devices

All staff who store data deemed sensitive or critical to the organization should keep it in an encrypted state on their devices. Any data that can be stored and accessed from a shared or cloud service should remain there, under strong account security. Any information downloaded should not be held on individual devices unless necessary. If there are questions about the necessity of on-device access to certain sensitive data, employees should contact the owner of that data type.

Employees who do not have a direct mission or business need should never access sensitive information. In particular, HR or personnel files should only be accessed with the explicit permission of the organization's HR team.

Employees responsible for working with relevant account owners to manage, revoke, or edit access to sensitive data. The individual responsible for this policy shall implement an annual or semi-annual process to revise account permissions to ensure these permissions are up-to-date and commensurate with staff's current responsibilities. Employees who work with that data regularly are expected to contribute to that review.

What services do those staff members use to store or share critical or sensitive information? Those services should be subject to a regular review of permissions.

Service	Interval for reviewing permissions (quarterly, semi-annual, annual)