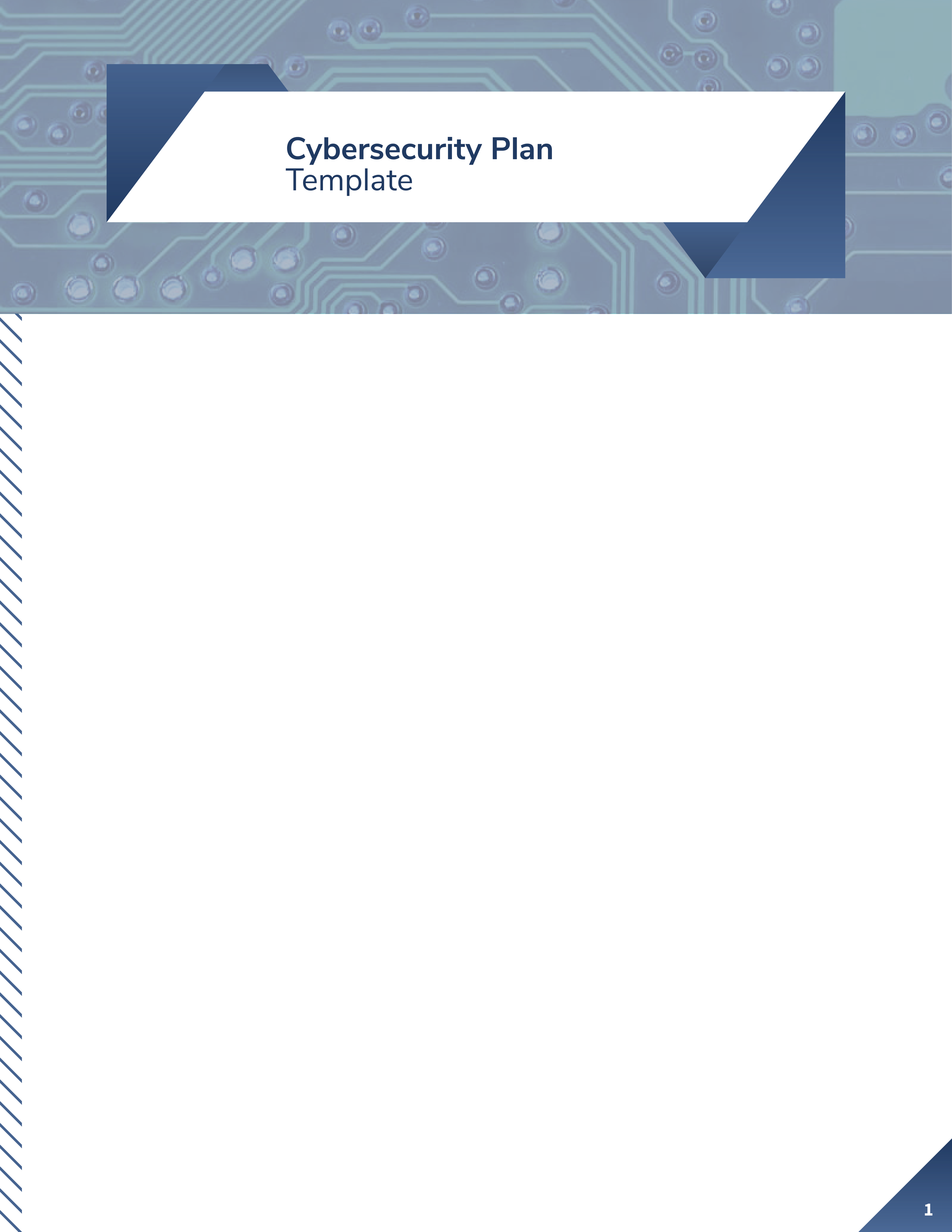
**How to use this document**

The template beginning on page 2 is incomplete and cannot be used without modifications based on the specifics of your organization. Each section is broken into two or three subsections.

1. Principles (in BLUE)
2. Policy examples (in GREEN)
3. References (where available, in PURPLE)

The [ORG] references should be replaced with the name or synonym of your organization.

All BLUE text should be removed from your final policy. These guidelines are provided to help you think through each section.

All GREEN text should be tailored to your organization if you intend to use the example, or removed if you do not.

PURPLE text should be removed from your final policy. The references are for your use and are not required in each section. However, it may be useful to acknowledge somewhere in your document where you obtained the ideas or text for your policy.

This template has eight sections: Purpose, Scope, Plan Framework, and five sections — Identify, Protect, Detect, Respond, and Recover — that align to the Core Functions outlined in the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF). You will need to adapt this document to a framework that works for your environment.

This document covers only the minimum needed in a cybersecurity policy. It is a starting point for you to frame your thinking and organize your priorities.

This document also is not a set of procedures. A policy defines what is important while procedures define how to carry out the policy. All procedures are left for you to develop.

We hope this document is helpful as your organization starts down the cybersecurity journey.

Best of luck,

Matt Sievers, Matthew Schroeder, Alexander Romero, and Liv Erickson

Fellows, Winter 2020

**[ORG] Cybersecurity Plan**

# Purpose

Principle: Publicly state why cybersecurity is important to your organization.

Policy Example:

Our cybersecurity plan is one of the primary mechanisms we have to show our customers and partners that we take protecting their data and our shared business seriously. This plan reviews our operating environment, identifies key roles, and documents our policies for protecting and responding to potential cybersecurity risks.

# Scope

Principle: Define how the policy applies to the organization. This includes:

* Who: which personnel?
* What: which equipment, networks, or processes?
* When: are there any time or status restrictions?
* Where: which locations?
* Exceptions: what are the situations where the policies do not apply?

Policy Example:

This policy applies to all employees and contractors accessing any [ORG] system, network, and data, at any time, from any location, whether from [ORG’s] or personal devices. There are no exceptions to this policy. Deviations must be approved by [ORG’s] Chief Information Security Officer (CISO).

(signatures and titles)

**Approved by / Date Last Modified by / Date**

# /Users/ryanolson/Downloads/Practical Cybersecurity for Small Businesses (8)/Letter - 2.pngPlan Framework

Principle: A strong cybersecurity plan should be based on a well-established framework from the expert community. Identify the framework your plan uses and how it is adapted for your business.

Policy Example:

We are using the NIST Cybersecurity Framework (CSF) as the foundation for this cybersecurity plan. As described in NIST’s document, “Framework for Improving Critical Infrastructure Cybersecurity,” the CSF is an internationally recognized standard that “enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.”

The CSF categorizes practices into five Core Functions that are divided into categories and subcategories. We have adapted it to our business by focusing on 12 subcategories —spread across five Core Functions — that we believe will have the most impact on our cybersecurity posture. The outline below shows the core functions and associated subcategories. For more information on the NIST CSF, see <https://www.nist.gov/cyberframework>.

* Identify (NIST CSF)
  + Legal and Regulatory Requirements (ID.AM-6)
  + Roles and Responsibilities (ID.GV-3)
* Protect (NIST CSF)
  + Account Management (PR.AC-4)
  + Account Authentication and Password Management (PR.AC-7)
  + User Training (PR.AT-1)
  + Data Backups (PR.IP-4)
  + Incident Response Plan (PR.IP-9)
  + Incident Recovery Plan (PR.IP-9)
  + Vulnerability Management Plan (PR.IP-12)
* Detect (NIST CSF)
  + Execution of the Vulnerability Management Plan (DE.CM-4 and DE.CM-8)
* Respond (NIST CSF)
  + Execution of the Incident Response Plan (RS.RP-1)
* Recover (NIST CSF)
  + Execution of the Incident Recovery Plan (RC.RP-1)

References:

* Our Policy Mappings document
  + <https://www.aspentechpolicyhub.org/project/big-security-for-small-business>
* Cybersecurity Framework
  + <https://www.nist.gov/cyberframework>
* Center for Internet Security (CIS) Controls
  + <https://www.cisecurity.org/controls/>
* ISO/IEC 27001
  + <https://www.iso.org/isoiec-27001-information-security.html>

# Identify

## ***Legal and Regulatory Requirements/Users/ryanolson/Downloads/Practical Cybersecurity for Small Businesses (8)/Letter - 3.png***

Principle: Identify the applicable requirements and explain how your organization demonstrates compliance.

Policy Example:

* California Consumer Privacy Act (CCPA)
  + Applicability: The CCPA is not applicable to our business. We are based in Colorado, and while we do business with California residents via online sales, we do not meet one of the three additional criteria:
    - Have $25 million or more in annual revenue; or
    - Possess the personal data of more than 50,000 consumers, households, or devices; or
    - Earn more than half of annual revenue selling consumers’ personal data.
  + Compliance: While the CCPA does not apply, we are following some of the principles set forth in the law:
    - We have implemented CCPA-compliant consumer privacy notifications and request options on our website to provide a consistent user experience.
    - We have implemented internal processes to respond to customers’ requests about their data, including the rights stipulated in the CCPA.

References:

* Speak with an attorney specializing in your industry.
* Local resources for organizational assistance, such as Small Business Development Centers, can also get you started. <https://www.sba.gov/business-guide/manage-your-business/stay-legally-compliant>
* The National Conference of State Legislatures (NCSL) is an excellent resource for reviewing passed and pending legislation across all states.
  + <https://www.ncsl.org/>
  + Topic page example, Data Security Laws: <https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx>

## ***Roles and Responsibilities***

Principle: Identify who is responsible for each aspect of the cybersecurity plan.

Policy Example:

* Business Owner/CEO
  + Vision and accountability for cybersecurity response
* Chief Information Security Officer (CISO) or Head of IT
  + Defines cybersecurity policies
  + Directs all preventive and response activities
  + Directs user training content and requirements
  + Directs regular exercises of cybersecurity posture
* Employee
  + ****Completes user training as defined by the CISO
  + Follows established cybersecurity policies and procedures

References:

* Your business plans may already document roles and responsibilities for non-cybersecurity areas, which can be adapted for this section.
* NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, is an excellent resource for cybersecurity roles. Appendices A and B provide titles, duties, and descriptions for 50+ roles. This resource does not outline responsibilities for business owners/CEOs and employees, but it is an excellent place to start.
  + <https://csrc.nist.gov/publications/detail/sp/800-181/final>

# Practical%20Cybersecurity%20for%20Small%20Businesses%20(8)/Letter%20-%205.pngProtect

## ***Account Management***

Principle: Define how administrator and user accounts are managed, including creation, deletion, logging of use, and auditing.

Accounts should follow the principles of *least privilege* and *separation of duties*. Least privilege means that users only have the access rights they need to carry out their jobs. This is especially important for administrator accounts, which should not be used except for system administration purposes. Separation of duties means that critical tasks, especially relating to money, cannot be completed without the involvement of more than one person, a measure intended to prevent fraud or abuse.

Policy Example:

* All employees and contractors shall have their own accounts
* Normal, day-to-day accounts shall not be given administrator access
* Accounts should be deleted and credentials revoked when an employee leaves [ORG], for any reason
* Logging of usage shall be enabled for all accounts. At a minimum, user and administrator logins shall be logged
  + Logging helps detect the misuse of accounts by users or by those compromised by malware
* Account audits shall be conducted on a regular, at least monthly, interval to identify “rogue” accounts

References:

* The Center for Internet Security (CIS) Controls 4 and 16 provide an overview of best practices for account management.
  + <https://www.cisecurity.org/controls/>

## ***Authentication and Password Management***

Principle: Define how user accounts are authenticated and how passwords are managed. At a minimum, multi-factor authentication and password managers should be considered, even if they are not an appropriate solution for your organization.

Policy Example:

* Employees and contractors shall:
  + Enable authentication on all devices (passphrase, PIN, biometrics, etc.)
  + Enable multi-factor authentication (MFA) on email, inventory management, and payment or banking accounts or services
  + Use a password manager for all [ORG] accounts or services
  + Never use or reuse the same passphrase on two or more systems
  + Never share [ORG] accounts

References:

* The Center for Internet Security (CIS) Control 4 discusses best practices for passwords.
  + <https://www.cisecurity.org/controls/>
* NIST Interagency Report 7621 Revision 1, *Small Business Information Security: The Fundamentals*, Chapter 4 Working Safely and Securely, discusses using passwords and password managers.
  + <https://doi.org/10.6028/NIST.IR.7621r1>
* The Global Cyber Alliance’s Cybersecurity Toolkit has walkthroughs for creating strong passwords, enabling multi-factor authentication, and using a password manager.
  + <https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/>

## ***Data Backups and Practical%20Cybersecurity%20for%20Small%20Businesses%20(8)/Letter%20-%206.pngDisposal***

Principle: Define how data backups are performed on your organization’s devices and network. At a minimum, automatic backup settings on common devices (i.e., Windows, Apple, Android) should be considered, even if they are not an appropriate solution for your organization.

Define when and how retained data should be disposed, especially according to applicable national and state laws.

Policy Example:

* Employees and contractors shall:
  + Enable automatic data backup on all devices. If unavailable, a solution must be made in coordination with the CISO of [ORG]
* Critical data shall:
  + Be backed up according to a “3-2-1” principle, with at least three copies made, located in at least two different locations, including at least one off-site location, such as in the “cloud”
  + Be automatically backed up:
    - One copy stored on the local machine
    - One copy stored in [SERVICE’S] cloud and distributed across multiple geographic regions
* Data, especially customer data, shall be retained and disposed of according to the Federal Trade Commission’s (FTC) Disposal Rule and other applicable national or state laws

References:

* The Center for Internet Security (CIS) Control 10 discusses best practices for data backup and recovery.
  + <https://www.cisecurity.org/controls/>
* NIST Interagency Report 7621 Revision 1, *Small Business Information Security: The Fundamentals*, Section 3.5 Recover, discusses how to perform data backup and recovery.
  + <https://doi.org/10.6028/NIST.IR.7621r1>
* The Global Cyber Alliance’s Cybersecurity Toolkit has walkthroughs for enabling data backups on Apple’s Mac and Microsoft’s Windows 10.
  + <https://gcatoolkit.org/smallbusiness/defend-against-ransomware/>
* The Federal Trade Commission has information for complying with the Disposal Rule.
  + <https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how>
  + Text of the Disposal Rule: <https://www.ecfr.gov/cgi-bin/text-idx?SID=a54ce7f8704c5096b83c75cde70a7d9d&mc=true&node=pt16.1.682&rgn=div5>
* The National Conference of State Legislatures (NCSL) maintains a list of data disposal laws across all states.
  + <https://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx>

## ***Vulnerability Management***

Principle: Define how vulnerabilities are managed on your network. At a minimum, address how to approach automatic update settings on common devices (i.e., Windows, Apple, Android) and anti-virus and anti-malware scanning. Indicate whether or not you have adopted  a vulnerability disclosure policy (VDP).

VDPs provide mechanisms and protections for ethical hackers to inform organizations about potential vulnerabilities in their software or networks. Such policies generally follow the following principles, adapted from *The CERT Guide to Coordinated Vulnerability Disclosure* (references below):

* **Reduce Harm**: Decrease the potential for damage by publishing vulnerability information, using exploit mitigation technologies, reducing days of risk, releasing high-quality patches, and automating vulnerable host identification and patch deployment.
* **Presume Benevolence**: Assume that any individual who has taken the time and effort to reach out to a vendor or a coordinator to report an issue is likely benevolent and sincerely wishes to reduce the harm of the vulnerability.
* **Avoid Surprise**: Surprise tends to increase the risk of a negative outcome from the disclosure of a vulnerability and should be avoided.
* **Incentivize Desired Behavior**: It is usually better to reward good behavior than to punish bad behavior. Incentives for responsible disclosure are important as they increase the likelihood of future cooperation between security researchers and organizations.
* **Ethical Considerations**: Ethical guidelines from professional societies are applicable in the coordinated vulnerability disclosure (CVD) process.
* **Process Improvement**: Participants in the CVD process should learn from their experience and improve their process accordingly. CVD can also provide important feedback to an organization's software development lifecycle (SDL).
* **CVD as a Wicked Problem**: Vulnerability disclosure is a multifaceted problem. There are likely no "right" answers, only "better" or "worse" solutions in a given context.

Policy Example:

* Employees and contractors shall:
  + Enable automatic updates on all devices that connect to [ORG’s] network
  + Install updates within 24 hours unless otherwise directed by the CISO of [ORG]
  + Not disable or interrupt automated vulnerability scanning
* Anti-virus and anti-malware software shall be installed on all devices that connect to the [ORG] network
  + Automated vulnerability scanning shall be enabled and run regularly (e.g., at least daily)
  + Deviations from this policy —for example, if a device cannot run anti-virus software — must be approved by [ORG’s] CISO
* Coordinated Vulnerability Disclosure Policy
  + All [ORG’s] websites will have a security.txt file explaining the VDP and how to responsibly submit a vulnerability
  + [ORG] will maintain a security@[ORG EMAIL] address to receive disclosures and inquiries
  + Those following the responsible disclosure guidelines will be granted safe harbor from [ORG]

References:

* The Center for Internet Security (CIS) Controls 3 and 8 discuss best practices for vulnerability management.
  + <https://www.cisecurity.org/controls/>
* NIST Interagency Report 7621 Revision 1, *Small Business Information Security: The Fundamentals*, Section 3.2 Protect, discusses system patching, while Section 3.3 Detect discusses anti-malware scanning.
  + <https://doi.org/10.6028/NIST.IR.7621r1>
* The Global Cyber Alliance’s Cybersecurity Toolkit has walkthroughs for setting up automatic updates.
  + <https://gcatoolkit.org/smallbusiness/update-your-defenses/>
* Other excellent resources for VDPs — including templates and services to help set up and run your program — are listed here, with no preference or endorsement.
  + The US Government’s Cybersecurity and Infrastructure Security Agency (CISA) issued Binding Operational Directive 20-01 requiring all federal organizations to implement a VDP. The document provides a wealth of information about why the programs are important and how the government is implementing them.
    - Develop and Publish a Vulnerability Disclosure Policy: <https://cyber.dhs.gov/bod/20-01/>
    - Template VDP: <https://cyber.dhs.gov/bod/20-01/vdp-template/>
  + The Software Engineering Institute’s (SEI) Computer Emergency Response Team (CERT) published a guide for VDPs with extensive resources. The document links to many other sources, including templates from other organizations.
    - CERT Guide: <https://vuls.cert.org/confluence/display/CVD/The+CERT+Guide+to+Coordinated+Vulnerability+Disclosure>
    - Other Templates: <https://vuls.cert.org/confluence/pages/viewpage.action?pageId=47677527>
    - GitHub Page for CERT-developed templates: <https://github.com/CERTCC/vulnerability_disclosure_policy_templates>
  + disclose.io is a “cross-industry, vendor-agnostic standardization project for safe-harbor best practices to enable good-faith security research.”
    - Main page: <https://disclose.io/>
    - US-specific Template: <https://github.com/disclose/disclose/blob/master/terms/core-terms-USA/core-terms-USA.md>
  + I Am The Cavalry provides an overview of disclosure, maintains a list of businesses with VDPs, and provides links to other resources, including companies that will run a VDP for your business:
    - <https://www.iamthecavalry.org/about/disclosure/>
    - <https://www.iamthecavalry.org/resources/disclosure-programs/>

***Incident Response and Recovery***

Principle: Define how your organization responds to and recovers from incidents on your network. At a minimum, address how affected customers and partners will be notified.

Policy Example:

* The CISO of [ORG] will direct all incident response and recovery actions, which may include:
  + Containment of the incident, which may require isolation of accounts and equipment
  + Notification of various roles and teams (senior executives, emergency personnel, cybersecurity professionals, legal professionals, service providers, insurance providers, etc.)
  + Remediation of the incident, which may require complete rebuilding of equipment
  + Investigation of how the incident occured
  + Changes to prevent future incidents
* [ORG] shall notify customers and partners within 72 hours upon discovering an incident that has affected their data or services

References:

* The Center for Internet Security (CIS) Control 19 discusses best practices for incident response.
  + <https://www.cisecurity.org/controls/>
* NIST Interagency Report 7621 Revision 1, *Small Business Information Security: The Fundamentals*, Section 3.4 Respond, discusses incident response planning.
  + <https://doi.org/10.6028/NIST.IR.7621r1>
* NIST SP 800-161, Revision 2, *Computer Security Incident Handling Guide*, provides information on creating an incident response plan.
  + <https://www.nist.gov/publications/computer-security-incident-handling-guide>
* NIST SP 800-184, *Guide for Cybersecurity Event Recovery*, provides more information on creating an incident recovery plan.
  + <https://www.nist.gov/publications/guide-cybersecurity-event-recovery>

# Practical%20Cybersecurity%20for%20Small%20Businesses%20(8)/Letter%20-%2010.pngDetect

## ***Execution of the Vulnerability Management Plan***

Principle: Demonstrate the ability to detect vulnerabilities, intrusions, and other issues on your network by executing a vulnerability management plan.

Policy Example:

* The execution of the vulnerability management plan will be audited on a regular basis, at least monthly
  + Any portions without active use will be tested through at least a tabletop exercise
  + All portions must be tested through a functional exercise every six months

References:

* The NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, provides more information on conducting incident exercises.
  + <https://www.nist.gov/privacy-framework/nist-sp-800-84>

# Practical%20Cybersecurity%20for%20Small%20Businesses%20(8)/Letter%20-%2011.pngRespond

## ***Execution of the Incident Response Plan***

Principle: Demonstrate you can respond to incidents on your network by executing your incident response plan.

Policy Example:

* The execution of the incident response plan will be audited on a regular basis, at least monthly
  + Any portions without active use will be tested through at least a tabletop exercise
  + All portions must be tested through a functional exercise every six months

References:

* NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, provides more information on conducting incident exercises.
  + <https://www.nist.gov/privacy-framework/nist-sp-800-84>
* NIST SP 800-161, Revision 2, *Computer Security Incident Handling Guide*, provides more information on executing an Incident Response Plan.
  + <https://www.nist.gov/publications/computer-security-incident-handling-guide>

# RecoverPractical%20Cybersecurity%20for%20Small%20Businesses%20(8)/Letter%20-%2012.png

## ***Execution of the Incident Recovery Plan***

Principle: Demonstrate you can recover from incidents on your network by executing your incident recovery plan.

Policy Example:

* The execution of the incident recovery plan will be audited on a regular basis, at least monthly
  + Any portions without active use will be tested through at least a tabletop exercise
  + All portions must be tested through a functional exercise every six months

References:

* The 2006 NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, provides more information on conducting incident exercises.
  + <https://www.nist.gov/publications/guide-test-training-and-exercise-programs-it-plans-and-capabilities>
* NIST SP 800-184, *Guide for Cybersecurity Event Recovery*, provides more information on executing an incident recovery plan.
  + <https://www.nist.gov/publications/guide-cybersecurity-event-recovery>

[Extra Page]