Small Business Cybersecurity Program

Implementing a streamlined cybersecurity program based on CMMC Level 1 (the entry level) or NIST SP 800-171 controls, focusing on essential protections without overwhelming your resources.

Here's a practical approach with 35 key controls:

1. Access Control

1. Implement unique user accounts and strong authentication
2. Limit access based on job responsibilities
3. Control remote access with MFA
4. Manage default credentials and change default passwords
5. Control physical access to facilities and systems

2. Awareness & Training

6. Provide basic security awareness training
7. Train users on identifying social engineering attacks

3. Data Protection

8. Control information flow
9. Implement data backup solutions
10. Sanitize media before disposal
11. Protect confidential information
12. Encrypt sensitive data at rest and in transit

4. System Security

13. Identify and document system components
14. Control and monitor user-installed software
15. Implement boundary protection (firewalls)
16. Deploy antimalware solutions
17. Update systems and software regularly
18. Configure security settings on all devices
19. Control wireless access

5. Incident Response

20. Develop basic incident response procedures
21. Monitor and analyze audit logs
22. Report security incidents
23. Test incident response capability

6. Risk Management

24. Identify and document cybersecurity risks
25. Manage risk through policies and controls
26. Perform periodic security assessments

7. Configuration Management

27. Establish baseline configurations
28. Perform configuration change control
29. Restrict administrative privileges

8. Business Continuity

30. Develop and test contingency plans
31. Create backup and recovery procedures

9. Third-Party Security

32. Assess supply chain risks
33. Require security in contractual agreements

10. Maintenance

34. Perform timely maintenance
35. Control remote maintenance activities

Small Business Cybersecurity Controls: Definitions and Compliance Examples

1. Access Control

1.1. Implement unique user accounts and strong authentication

Definition: Establish individual accounts for each user and implement strong password requirements.

Compliance Example: Each employee has a unique username. Passwords must be at least 12 characters with a mix of uppercase, lowercase, numbers, and symbols. Password manager software is available to all employees.

1.2. Limit access based on job responsibilities

Definition: Restrict system access to only the information and resources necessary for job functions (principle of least privilege).

Compliance Example: Sales team members only have access to CRM and sales tools, not accounting systems. HR staff only access personnel files, not product development data.

1.3. Control remote access with MFA

Definition: Require multiple forms of authentication when accessing systems remotely.

Compliance Example: VPN access requires both a password and a code from an authenticator app. Cloud service logins require email verification codes in addition to passwords.

1.4. Manage default credentials and change default passwords

Definition: Identify and change all default usernames and passwords on systems and devices.

Compliance Example: Document that all network devices (routers, printers, etc.) have had default credentials changed. Implement procedure to verify this when new equipment is installed.

1.5. Control physical access to facilities and systems

Definition: Restrict physical access to sensitive areas and equipment.

Compliance Example: Server room requires key card access with logs of entry. Visitor management system records all non-employee access to facilities.

2. Awareness & Training

2.6. Provide basic security awareness training

Definition: Educate all users on cybersecurity best practices and company policies.

Compliance Example: Annual mandatory training for all employees with documentation of completion. Monthly security newsletters share updates and reminders.

2.7. Train users on identifying social engineering attacks

Definition: Specific training on recognizing and responding to phishing and other social engineering threats.

Compliance Example: Quarterly phishing simulations with results tracked. Training materials include real-world examples of phishing emails with explanations.

3. Data Protection

3.8. Control information flow

Definition: Monitor and control communications at external boundaries and key internal boundaries.

Compliance Example: Data loss prevention (DLP) tools scan outgoing emails for sensitive information. File sharing services are monitored for unauthorized transfers.

3.9. Implement data backup solutions

Definition: Perform regular backups of critical business data.

Compliance Example: Automated daily incremental backups and weekly full backups to both local and cloud storage. Monthly test restores to verify backup integrity.

3.10. Sanitize media before disposal

Definition: Securely erase or destroy media containing sensitive information before disposal.

Compliance Example: Documented process for wiping hard drives using DoD-compliant software. Contract with certified e-waste disposal company for physical destruction.

3.11. Protect confidential information

Definition: Identify and safeguard sensitive data using appropriate controls.

Compliance Example: Data classification policy defines levels of sensitivity. Sensitive documents are marked and have access restrictions. Quarterly data inventory audits.

3.12. Encrypt sensitive data at rest and in transit

Definition: Use encryption to protect sensitive information when stored and transmitted.

Compliance Example: All company laptops use full-disk encryption. Website uses TLS/SSL for all connections. Email encryption is available for sensitive communications.

4. System Security

4.13. Identify and document system components

Definition: Maintain inventory of hardware, software, and information systems.

Compliance Example: Asset management database contains all IT assets with ownership, location, and purpose. Updated monthly with automatic discovery tools.

4.14. Control and monitor user-installed software

Definition: Establish policies and technical controls for software installation.

Compliance Example: Standard users cannot install software without approval. Application whitelist permits only authorized software to execute.

4.15. Implement boundary protection (firewalls)

Definition: Monitor and control communications at network boundaries.

Compliance Example: Next-generation firewall deployed at internet connection. Firewall logs reviewed weekly. Firewall rules follow least-privilege principle.

4.16. Deploy antimalware solutions

Definition: Implement detection, prevention, and correction controls for malicious code.

Compliance Example: Endpoint protection software on all devices with centralized management. Weekly scans and real-time protection enabled.

4.17. Update systems and software regularly

Definition: Install security-relevant updates in a timely manner.

Compliance Example: Critical patches applied within 14 days. Monthly patch management report shows compliance status. Automated patch deployment for workstations.

4.18. Configure security settings on all devices

Definition: Establish and maintain secure configurations for systems and devices.

Compliance Example: Documented baseline configurations for different device types. Regular configuration compliance scans identify deviations.

4.19. Control wireless access

Definition: Protect wireless networks and control access.

Compliance Example: Wi-Fi uses WPA3 encryption. Separate networks for guests and internal users. MAC address filtering for critical systems.

5. Incident Response

5.20. Develop basic incident response procedures

Definition: Create and document plans for detecting and responding to security incidents.

Compliance Example: Documented incident response plan with roles and responsibilities. Annual review and update of procedures.

5.21. Monitor and analyze audit logs

Definition: Collect and review system activity records to detect unusual behavior.

Compliance Example: Centralized log collection from key systems. Weekly review of critical alerts. 90-day log retention policy.

5.22. Report security incidents

Definition: Establish procedures for reporting suspected security incidents.

Compliance Example: Internal reporting process with designated security contacts. Templates for documenting incidents. Clear escalation procedures.

5.23. Test incident response capability

Definition: Practice response activities to improve effectiveness.

Compliance Example: Annual tabletop exercise simulating a ransomware attack. Lessons learned documented and incorporated into updated procedures.

6. Risk Management

6.24. Identify and document cybersecurity risks

Definition: Identify, assess, and document cybersecurity risks.

Compliance Example: Risk register documents identified threats and vulnerabilities. Annual risk assessment with external consultant.

6.25. Manage risk through policies and controls

Definition: Develop and implement risk mitigation strategies.

Compliance Example: Written information security policies signed by all employees. Control selection based on identified risks and business impact.

6.26. Perform periodic security assessments

Definition: Regularly evaluate security controls for effectiveness.

Compliance Example: Annual vulnerability scanning of all systems. Remediation plans for identified vulnerabilities with tracking to completion.

7. Configuration Management

7.27. Establish baseline configurations

Definition: Document secure settings for each system type.

Compliance Example: Standard images for workstations with documented security settings. Configuration checklists for setting up new systems.

7.28. Perform configuration change control

Definition: Control changes to baseline configurations.

Compliance Example: Change management process requiring documentation and approval before system changes. Configuration changes logged and reviewed.

7.29. Restrict administrative privileges

Definition: Limit elevated system privileges to authorized personnel.

Compliance Example: Separate standard and administrative accounts for IT staff. Quarterly review of users with administrative access.

8. Business Continuity

8.30. Develop and test contingency plans

Definition: Create plans for maintaining essential business functions during disruptions.

Compliance Example: Business continuity plan identifies critical systems and recovery time objectives. Annual test of operations from alternate location.

8.31. Create backup and recovery procedures

Definition: Document processes for data restoration after an incident.

Compliance Example: Written backup procedures with responsibilities assigned. Quarterly restore tests with results documented.

9. Third-Party Security

9.32. Assess supply chain risks

Definition: Evaluate security risks from vendors and service providers.

Compliance Example: Vendor security assessment questionnaire completed before engaging new providers. Annual review of critical vendor security posture.

9.33. Require security in contractual agreements

Definition: Include security requirements in contracts with third parties.

Compliance Example: Standard security clauses in all vendor contracts. Right to audit provisions for critical service providers.

10. Maintenance

10.34. Perform timely maintenance

Definition: Conduct regular system maintenance according to manufacturer recommendations.

Compliance Example: Maintenance schedule for all hardware with completed actions tracked. Service contracts in place for critical systems.

10.35. Control remote maintenance activities

Definition: Monitor and approve remote maintenance sessions.

Compliance Example: Vendor remote access requires approval and uses temporary credentials. All remote maintenance sessions are logged and monitored.

Compliance Documentation

For effective compliance with frameworks like CMMC Level 1 or NIST SP 800-171, maintain the following documentation:

1. **System Security Plan (SSP):** Documents all implemented controls and security practices
2. **Policies and Procedures:** Written documents covering each control area
3. **Evidence Files:** Screenshots, logs, and records demonstrating control implementation
4. **Risk Assessment Reports:** Documentation of identified risks and mitigation plans
5. **Training Records:** Evidence of security awareness training completion
6. **Incident Reports:** Documentation of security incidents and responses
7. **Asset Inventory:** Current listing of all hardware, software, and information assets
8. **Plan of Action and Milestones (POA&M):** Tracking document for addressing identified gaps

Vendor Security Assessment Questionnaire

Introduction

This questionnaire is designed to assess the cybersecurity posture of vendors and service providers. Your thorough responses will help us evaluate potential security risks in our supply chain as part of our compliance with cybersecurity frameworks.

Company Name: ______________________________
Primary Contact: ____________________________
Contact Email: ______________________________
Contact Phone: _____________________________
Date Completed: ____________________________

1. General Security Information

1.1. Briefly describe your organization's information security program:

1.2. Do you have a designated security officer or team?
□ Yes □ No

1.3. If yes, please provide their contact information:

1.4. Which security frameworks or standards does your organization follow? (Check all that apply)
□ NIST CSF
□ NIST 800-171
□ ISO 27001
□ SOC 2
□ CMMC
□ PCI DSS
□ HIPAA
□ Other: ____________________

1.5. Has your organization completed any third-party security assessments or certifications?
□ Yes □ No

1.6. If yes, please list the most recent assessments/certifications and dates:

2. Security Policies and Procedures

2.1. Do you maintain written information security policies and procedures?
□ Yes □ No

2.2. How often are these policies reviewed and updated?
□ Annually
□ Bi-annually
□ When regulations change
□ Other: ______________________

2.3. Do you provide security awareness training to employees?
□ Yes □ No

2.4. How frequently is security training conducted?
□ Upon hire only
□ Annually
□ Quarterly
□ Monthly
□ Other: ______________________

2.5. Do you conduct background checks on employees?
□ Yes □ No

3. Access Control

3.1. Do you implement the principle of least privilege for system access?
□ Yes □ No

3.2. Do you require unique identification credentials for each user?
□ Yes □ No

3.3. Do you enforce password complexity requirements?
□ Yes □ No

3.4. Please describe your password policy (length, complexity, expiration):

3.5. Do you require multi-factor authentication for:
Remote access: □ Yes □ No
Admin accounts: □ Yes □ No
Cloud services: □ Yes □ No

3.6. How quickly are access rights removed when an employee leaves?
□ Same day
□ Within 24 hours
□ Within one week
□ Other: ______________________

4. Data Protection

4.1. Do you classify data based on sensitivity?
□ Yes □ No

4.2. Do you encrypt sensitive data:
At rest: □ Yes □ No
In transit: □ Yes □ No

4.3. What encryption standards do you use?

4.4. Do you have a data retention and destruction policy?
□ Yes □ No

4.5. How do you securely dispose of sensitive information?

---

5. System Security

5.1. Do you maintain an inventory of hardware and software assets?
□ Yes □ No

5.2. Do you have a patch management process?
□ Yes □ No

5.3. How quickly are critical security patches applied?
□ Within 24 hours
□ Within 1 week
□ Within 1 month
□ Other: ______________________

5.4. Do you use antivirus/endpoint protection software?
□ Yes □ No

5.5. Do you perform regular vulnerability scanning?
□ Yes □ No
Frequency: ______________________

5.6. Do you conduct penetration testing?
□ Yes □ No
Frequency: ______________________

6. Network Security

6.1. Do you use firewalls to protect your network?
□ Yes □ No

6.2. Do you segment your network?
□ Yes □ No

6.3. Do you monitor network traffic for suspicious activity?
□ Yes □ No

6.4. Do you have intrusion detection/prevention systems?
□ Yes □ No

6.5. How do you secure remote access to your network?

---

7. Incident Response

7.1. Do you have a documented incident response plan?
□ Yes □ No

7.2. Have you tested your incident response procedures?
□ Yes □ No

7.3. Do you have a process for notifying clients of security incidents?
□ Yes □ No

7.4. What is your timeframe for client notification in the event of a breach?

7.5. Have you experienced any security breaches in the last 24 months?
□ Yes □ No

7.6. If yes, please provide details (without sharing any confidential information):

---

8. Business Continuity

8.1. Do you have a business continuity plan?
□ Yes □ No

8.2. Do you regularly back up critical data?
□ Yes □ No
Frequency: ______________________

8.3. Do you test your recovery procedures?
□ Yes □ No
Frequency: ______________________

8.4. What is your recovery time objective (RTO) for critical systems?

---

9. Third-Party Risk Management

9.1. Do you assess the security of your own vendors and subcontractors?
□ Yes □ No

9.2. Do you require your subcontractors to comply with your security requirements?
□ Yes □ No

9.3. Do you include security requirements in your contracts with subcontractors?
□ Yes □ No

10. Cloud Services (if applicable)

10.1. Which cloud service providers do you use?

10.2. Do you encrypt data stored in the cloud?
□ Yes □ No

10.3. Do you maintain ownership and control of encryption keys?
□ Yes □ No

11. Mobile Device Security (if applicable)

11.1. Do you have a mobile device management (MDM) solution?
□ Yes □ No

11.2. Can you remotely wipe corporate data from mobile devices?
□ Yes □ No

11.3. Do you enforce security controls on mobile devices?
□ Yes □ No

12. Software Development (if applicable)

12.1. Do you follow secure coding practices?
□ Yes □ No

12.2. Do you conduct security testing during development?
□ Yes □ No

12.3. Do you scan code for vulnerabilities before release?
□ Yes □ No

13. Physical Security

13.1. Do you have physical access controls at your facilities?
□ Yes □ No

13.2. Do you maintain visitor logs?
□ Yes □ No

13.3. Do you have surveillance systems?
□ Yes □ No

14. Additional Information

14.1. Please provide any additional information about your security program that would be relevant to our assessment:

Certification

I certify that the information provided in this questionnaire is accurate and complete to the best of my knowledge.

Name: ___________________________
Title: ___________________________
Signature: _______________________
Date: ___________________________

For Internal Use Only

Reviewed by: __________________
Date: _________________________
Risk Assessment: □ Low □ Medium □ High
Notes: _______________________

Vendor Information Sheet

Company Information

Legal Business Name: ____

DBA (if different): ____

Tax ID Number / EIN: ____

Business Type:

- [ ] Corporation
- [ ] LLC
- [ ] Partnership
- [ ] Sole Proprietorship
- [ ] Non-Profit
- [ ] Other: ________________

Year Established: ____

Website: ____

Business Address:

Remittance Address (if different):

Primary Contact Information

Name: ____

Title: ____

Phone: ____

Email: ____

Secondary Contact Information

Name: ____

Title: ____

Phone: ____

Email: ____

Payment Information

Preferred Payment Method:

- [ ] ACH/Direct Deposit
- [ ] Check
- [ ] Credit Card
- [ ] Wire Transfer
- [ ] Other: __________________

ACH/Direct Deposit Details

Bank Name: ____

Account Name: ____

Account Type: ☐ Checking ☐ Savings

Routing Number: ____

Account Number: ____

Wire Transfer Details

Bank Name: ____

Bank Address: ____

SWIFT/BIC Code: ____

IBAN (if applicable): ____

Routing Number: ____

Account Number: ____

Account Name: ____

Special Instructions: ____

Check Payment Details

Make Check Payable To: ____

Mail Check To: ____

Payment Terms

Standard Payment Terms: ____

Early Payment Discount Available: ☐ Yes ☐ No

If yes, terms: ____

Currency: ____

Authorization for Changes

I authorize the following individuals to make changes to the vendor account information provided above, including payment instructions:

1. **Name:** ____

   Title: ____

   Phone: ____

   Email: ____

   Signature: ____

2. **Name:** ____

   Title: ____

   Phone: ____

   Email: ____

   Signature: ____

Change Verification Protocol

Changes to payment or banking information require:

- Written request on company letterhead
- Signature from authorized individual listed above
- Verification phone call to primary contact before processing
- Changes must be submitted at least 5 business days before next payment

Certification

I certify that the information provided is accurate and complete. I am authorized to provide this information on behalf of the company listed above.

Name: ____

Title: ____

Signature: ____

Date: ____

For Internal Use Only

Vendor ID: _________________

Received By: ____

Date Received: _________________

Verified By: ____

Date Verified: _________________

Entered Into System By: ____

Date Entered: _________________

Notes: ____