5 Star Data Systems, LLC

“Cyber Hygiene” Check List

September 1, 2025

Introduction

“Cyber hygiene” refers to a collection of practices and simple security measures that individuals or companies can adopt to safeguard their valuable information, including digital assets, systems, and data, from cyber threats.

Small and medium organizations often become easier targets for malicious actors due to inadequate budgets or technical expertise in establishing basic cyber hygiene. Below are a set of 15 practices, derived from the Center of Internet Security v8.1 Implementation Group 1 controls. The controls are cross referenced to analogous controls found in the NIST cybersecurity framework (CSF) v2.0 and the NIST SP800-171R3 controls (which are those used for CMMC compliance). The list of 15 controls below will fulfill most of the requirements for level 1 CMMC compliance.

Many of the controls in the list below will already be set up and maintained by a small business’ IT department.

1. Inventory and Control of Enterprise Assets

- **Description:** Identify and manage all connected hardware assets.
- **NIST CSF v2.0:** ID.AM-1, ID.AM-2
- **SP 800-171R3:** 3.4.1, 3.4.2

2. Inventory and Control of Software Assets

- **Description:** Catalogue and control all software, only allowing authorized programs.
- **NIST CSF v2.0:** ID.AM-3, PR.IP-1
- **SP 800-171R3:** 3.4.3

3. Data Protection

- **Description:** Safeguard sensitive information at rest and in transit.
- **NIST CSF v2.0:** PR.DS-1, PR.DS-2
- **SP 800-171R3:** 3.1.13, 3.8.9

4. Secure Configuration of Enterprise Assets and Software

- **Description:** Apply and maintain secure asset configurations.
- **NIST CSF v2.0:** PR.IP-1, PR.IP-2
- **SP 800-171R3:** 3.4.6, 3.4.7

5. Account Management

- **Description:** Manage personnel and service accounts; remove unused accounts.
- **NIST CSF v2.0:** PR.AC-1
- **SP 800-171R3:** 3.5.1, 3.5.2

6. Access Control Management

- **Description:** Limit user access based on least privilege and need-to-know.
- **NIST CSF v2.0:** PR.AC-4
- **SP 800-171R3:** 3.1.5

7. Continuous Vulnerability Management

- **Description:** Regularly scan for and remediate vulnerabilities.
- **NIST CSF v2.0:** DE.CM-8, PR.IP-12
- **SP 800-171R3:** 3.11.2

8. Audit Log Management

- **Description:** Collect and analyze logs for suspicious activities.
- **NIST CSF v2.0:** DE.CM-7, PR.PT-1
- **SP 800-171R3:** 3.3.1, 3.3.2

9. Email and Web Browser Protections

- **Description:** Ensure security controls on email and web platforms.
- **NIST CSF v2.0:** PR.DS-3, PR.DS-4
- **SP 800-171R3:** 3.1.1, 3.1.14

10. Malware Defenses

- **Description:** Deploy anti-malware measures on all endpoints.
- **NIST CSF v2.0:** PR.IP-9
- **SP 800-171R3:** 3.14.2

11. Data Recovery

- **Description:** Maintain backup processes for data restoration.
- **NIST CSF v2.0:** PR.IP-4, PR.IP-5
- **SP 800-171R3:** 3.8.8

12. Network Infrastructure Management

- **Description:** Secure and manage network devices.
- **NIST CSF v2.0:** PR.PT-4
- **SP 800-171R3:** 3.13.1, 3.13.2

13. Security Awareness and Skills Training

- **Description:** Conduct regular workforce security training.
- **NIST CSF v2.0:** PR.AT-1, PR.AT-2
- **SP 800-171R3:** 3.2.1

14. Service Provider Management

- **Description:** Assess IT service providers for security compliance.
- **NIST CSF v2.0:** ID.SC-1

- **SP 800-171R3:** 3.12.4

15. Incident Response Management

- **Description:** Create and maintain an incident response plan.
- **NIST CSF v2.0:** RS.CO-1, RS.CO-2
- **SP 800-171R3:** 3.6.1, 3.6.2

Checklist

Notes	#	Control Title
	1	Inventory and Control of Enterprise Assets
	2	Inventory and Control of Software Assets
	3	Data Protection
	4	Secure Configuration of Enterprise Assets and Software
	5	Account Management
	6	Access Control Management
	7	Continuous Vulnerability Management
	8	Audit Log Management
	9	Email and Web Browser Protections
	10	Malware Defenses
	11	Data Recovery
	12	Network Infrastructure Management
	13	Security Awareness and Skills Training
	14	Service Provider Management
	15	Incident Response Management

Enhanced Cyber Hygiene Checklist (with Practical Steps)

1. Inventory and Control of Enterprise Assets

- Practical Steps: Maintain a regularly updated inventory of computers, servers, mobile devices, network equipment, and printers. Review asset lists quarterly and deactivate, remove, or secure unused hardware immediately.

2. Inventory and Control of Software Assets

- Practical Steps: Keep a software inventory of all approved/installed applications and operating systems. Remove unauthorized or outdated software upon discovery. Enable automatic software updates where possible.

3. Data Protection

- Practical Steps: Identify critical or sensitive data, restrict access, and encrypt files both at rest and in transit. Use secure transfer methods (e.g., VPN, SFTP) and regularly audit shared data locations for permission changes.

4. Secure Configuration of Enterprise Assets and Software

- Practical Steps: Apply secure settings to all systems; disable unnecessary services, default accounts, or features. Use configuration templates where possible, review configurations after system deployment, and document exceptions.

5. Account Management

- Practical Steps: Create accounts with only necessary privileges, promptly revoke or disable unused accounts (especially after employee departures), and periodically review active account lists for inaccuracies or unnecessary access.

6. Access Control Management

- Practical Steps: Assign access rights based on least privilege; regularly review permissions for sensitive systems and data. Use role-based access controls (RBAC) and require manager approval for elevated privileges.

7. Continuous Vulnerability Management

- Practical Steps: Run vulnerability scans monthly (or more often) and prioritize fixes for critical issues. Subscribe to relevant security alerts and patch immediately when serious vulnerabilities are disclosed.

8. Audit Log Management

- **Practical Steps:** Enable logging on all key systems (servers, applications, firewalls). Retain logs for at least 90 days, monitor regularly for suspicious behavior, and review logs following any security incident.

9. Email and Web Browser Protections

- **Practical Steps:** Use spam filtering, block known malicious sites, and enable attachment/link scanning in email clients. Disable unnecessary browser extensions and auto-downloads.

10. Malware Defenses

- **Practical Steps:** Install and routinely update anti-malware/antivirus software on all endpoints. Schedule regular full scans and review quarantine logs to confirm infections are addressed.

11. Data Recovery

- **Practical Steps:** Schedule automated daily backups for business-critical information, verify backup integrity weekly, and test the restoration process at least quarterly.

12. Network Infrastructure Management

- **Practical Steps:** Change default credentials on all network devices, apply firmware updates regularly, use network segmentation where possible, and audit device access settings every six months.

13. Security Awareness and Skills Training

- **Practical Steps:** Conduct annual cyber awareness training for all employees, provide phishing simulation exercises, and distribute tip sheets for common threats.

14. Service Provider Management

- **Practical Steps:** Vet vendors for their security practices before onboarding. Request security certifications or policies and conduct annual reviews of provider compliance.

15. Incident Response Management

- **Practical Steps:** Draft and share an incident response plan, define notification procedures for key contacts, run simulated breach exercises at least once a year, and keep contact lists updated.