

Cyber Hygiene Ladder Resources

The following resources may help guide and inform you about actions you can take to improve your cybersecurity hygiene. Some of these resources may reference or promote specific services or products; however, we do not recommend or endorse any particular service or product. You are encouraged to conduct your own research before selecting any service or product that may be of interest to you.

1. Cybersecurity Policies

Where to get free templates:

<https://www.sans.org/information-security-policy>

<https://www.cisecurity.org/->

[/media/project/cisecurity/cisecurity/data/media/files/uploads/2024/08/cis-ms-isac-nist-cybersecurity-framework-policy-template-guide-2024.pdf](https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2024/08/cis-ms-isac-nist-cybersecurity-framework-policy-template-guide-2024.pdf)

2. Passwords

Guidance on strong passwords:

<https://www.cisa.gov/secure-our-world/use-strong-passwords>

<https://www.nist.gov/cybersecurity/how-do-i-create-good-password>

3. Multi-Factor Authentication

Guidance on multi-factor authentication:

<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication>

<https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication>

4. Password Manager

Guidance on password managers:

<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers>

<https://www.staysafeonline.org/articles/password-managers>

5. Data Classification

Guidance on data classification:

<https://www.nccoe.nist.gov/data-classification>

<https://dir.texas.gov/resource-library-item/data-classification-guide-v11>

6. System Backup

Guidance on system backups:

<https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf>

7. Encryption

Cyber Hygiene Ladder Resources

Guidance on encryption:

<https://www.hhs.gov/hipaa/for-professionals/faq/2021/what-is-encryption/index.html>

<https://cloud.google.com/learn/what-is-encryption>

Windows:

<https://support.microsoft.com/en-us/windows/device-encryption-in-windows-cf7e2b6f-3e70-4882-9532-18633605b7df>

Mac OS:

<https://support.apple.com/guide/mac-help/protect-data-on-your-mac-with-filevault-mh11785/mac>

Linux:

<https://linuxsecurity.com/features/authoritative-guide-on-linux-disk-encryption>

8. Data Retention and Disposal

Guidance on data retention and disposal:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf>

https://ori.hhs.gov/education/products/rcradmin/topics/data/tutorial_11.shtml

9. Access Control

Guidance on access control:

<https://www.nist.gov/identity-access-management>

<https://www.microsoft.com/en-us/security/business/security-101/what-is-access-control>

10. Review of Permissions

Guidance on assigning permissions:

Windows: <https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/configure/user-access-control>

Mac: <https://support.apple.com/guide/mac-help/change-permissions-for-files-folders-or-disks-mchlp1203/mac>

Linux: <https://www.geeksforgeeks.org/linux-unix/set-file-permissions-linux/>

11. Firewall

Guidance on firewalls:

<https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use>

Cyber Hygiene Ladder Resources

Windows Firewall: <https://support.microsoft.com/en-us/windows/firewall-and-network-protection-in-the-windows-security-app-ec0844f7-aebd-0583-67fe-601ecf5d774f>
MacOS: <https://support.apple.com/guide/mac-help/change-firewall-settings-on-mac-mh11783/mac>

12. Network Diagram

Guidance on network diagrams:

<https://www.lucidchart.com/pages/network-diagram>
<https://www.security.uci.edu/program/risk-assessment/network-diagram/>
<https://www.glimfy.com/blog/network-diagram-examples>

13. Network Monitoring

Guidance on network monitoring:

<https://www.vmware.com/topics/network-monitoring>
<https://www.ibm.com/think/topics/network-monitoring>
<https://www.cisco.com/site/us/en/learn/topics/networking/what-is-network-monitoring.html>

14. Personal Device Usage:

Guidance on personal device usage:

<https://www.nccoe.nist.gov/mobile-device-security/bring-your-own-device>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-22.pdf>

15. VPN for Remote Employees:

Guidance on VPN usage:

<https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks>
<https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn>
<https://www.fortinet.com/resources/cyberglossary/what-is-a-vpn>

16. Cybersecurity Training

Free resources:

[HHS Security Awareness and Training](#)
[ESET Cybersecurity Awareness Training](#)
[Texas DIR Cybersecurity Awareness Training](#)
[CDSE Cybersecurity Training](#)
[Wiser Security Awareness Training](#)

Cyber Hygiene Ladder Resources

[Online NIST Learning Content](#)

[CISA Cybersecurity Awareness & Training](#)

Paid for resources:

[ESET Cybersecurity Awareness Training](#)

[KnowBe4](#)

17. Cybersecurity Training Frequency

Guidance on training:

<https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-training-exercises>

<https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices>

<https://www.cisa.gov/topics/cybersecurity-best-practices>

18. Cybersecurity Reporting

Guidance on reporting:

<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/responding-cyber-incident>

<https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting>

19. Simulated Training

Guidance on simulated training: (We do not endorse or recommend any of the products mentioned. Please do additional research when choosing a provider.)

<https://www.adaptivesecurity.com/blog/the-complete-guide-to-cyber-security-simulation-training>

<https://learn.microsoft.com/en-us/defender-office-365/attack-simulation-training-get-started>

20. Specialized Training

Free training and Guidance on specialized training

HIPAA: <https://www.hhs.gov/hipaa/for-professionals/training/index.html>

PCI-DSS: <https://www.sans.org/for-organizations/workforce/compliance-training/pci-dss>

CUI: <https://securityawareness.dcsa.mil/cui/index.html>

21. Incident Response Plan

Templates to guide you on developing your IRP:

<https://cloud.google.com/discover/incident-response-plan-template>

Cyber Hygiene Ladder Resources

https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

https://essentialguide.docs.cisecurity.org/en/latest/bp/incident_response.html

22. Incident Response Team

Guidance on IRT:

<https://www.paloaltonetworks.com/cyberpedia/what-is-an-incident-response-team>

https://www.w3schools.com/cybersecurity/cybersecurity_incident_response.php

23. Incident Response Plan Testing

Guidance on IRP Testing:

<https://www.cisa.gov/resources-tools/services/incident-response-planning-testing-strategies-consultation-documentation>

<https://www.techtarget.com/searchsecurity/tip/CISOs-guide-How-to-test-an-incident-response-plan>

24. Breach Notification

Guidance on breach notifications:

HIPAA: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

<https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule>

25. Cyber Insurance

Guidance on cyber insurance (We do not endorse any of the insurance listed below):

<https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance>

<https://www.fortinet.com/resources/cyberglossary/cyber-insurance>

26. Inventory

Guidance on inventory:

<https://www.paloaltonetworks.com/cyberpedia/what-is-it-asset-inventory>

<https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators>

<https://www.cm-alliance.com/cybersecurity-blog/how-inventory-management-and-cybersecurity-ensure-business-continuity>

27. Test System Changes

Guidance on handling system changes:

<https://www.ibm.com/think/topics/system-testing>

<https://www.indeed.com/career-advice/career-development/system-testing>

28. System Settings

Cyber Hygiene Ladder Resources

Guidance on system settings:

<https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines>

<https://www.sciencedirect.com/topics/computer-science/security-baseline>

29. Software Updates

<https://www.cisa.gov/resources-tools/training/keep-your-devices-operating-system-and-applications-date>

<https://www.staysafeonline.org/articles/software-updates>

30. Logging

Guidance on Logging:

Free logging tool from CISA: <https://www.cisa.gov/resources-tools/services/logging-made-easy>

Guidance on logging:

<https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/logging-and-protective-monitoring>

31. Log Reviewal

Guidance on log analyst:

<https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/log-analysis/>

<https://www.ibm.com/think/topics/log-analysis>

32. Log Retention:

Guidance on log management:

<https://csrc.nist.gov/pubs/sp/800/92/r1/ipd>

<https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/log-management/>

Log management policy free template:

<https://www.sans.org/information-security-policy/log-management-policy>

33. Network Separation:

Guidance on network separation:

<https://www.cisa.gov/news-events/news/securing-enterprise-wireless-networks>

<https://www.spectrum.com/business/small-business/insights/business-insights/secure-your-business-wifi-network-in-6-steps>

34. Wi-Fi Password

Guidance on creating passwords:

<https://www.nist.gov/cybersecurity/how-do-i-create-good-password>

<https://www.cisa.gov/secure-our-world/use-strong-passwords>

Cyber Hygiene Ladder Resources

35. Firmware Update

Guidance on updating firmware:

<https://www.ninjaone.com/blog/what-is-a-firmware-update/>

Router: <https://www.lenovo.com/us/en/glossary/how-to-update-router-firmware/?orgRef=https%253A%252F%252Fwww.google.com%252F&srsId=AfmBOotR94EKAFnDecYkKSHmSqI4VPghhgeaZn980ywp0TVVulszFm>

Note: Check the website of your router's manufacturer to find additional guidance.

Windows: <https://learn.microsoft.com/en-us/windows-hardware/drivers/install/updating-device-firmware-using-windows-update>

36. Encryption Protocols

Guidance on encryption protocols:

<https://www.geeksforgeeks.org/computer-networks/what-is-wpa3-vs-wpa2/>

<https://www.portnox.com/cybersecurity-101/network-security/wpa3/>

37. Network Monitoring

Guidance on network monitoring:

<https://www.cisco.com/site/us/en/learn/topics/networking/what-is-network-monitoring.html>

<https://www.ibm.com/think/topics/network-monitoring>

<https://www.fortinet.com/resources/cyberglossary/network-monitoring>

38. SSID Broadcasting

Guidance on SSID broadcasting:

<https://www.fortinet.com/resources/cyberglossary/service-set-identifier-ssid>

<https://www.geeksforgeeks.org/computer-networks/service-set-identifier-ssid-in-computer-network/>

39. Media Sanitization

Guidance on media sanitization:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf>

<https://www.irs.gov/privacy-disclosure/media-sanitization-guidelines>

40. Portable Media Encryption/

41. Portable Media Tracking

Guidance on portable media encryption and tracking:

<https://www.cisa.gov/news-events/news/protecting-portable-devices-data-security>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1334.pdf>

Cyber Hygiene Ladder Resources

<https://www.cisa.gov/resources-tools/training/follow-cybersecurity-best-practices-protect-yourself-tracking-technologies-and-spyware>

42. Shred Policy

Guidance on shred policies:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf>

43. Physical Access Restriction

Guidance on physical access restrictions:

<https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter15.html>

https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Physical%2520Security%2520Convergence_508_01.05.2021.pdf

44. Key Inventory:

Guidance on Key Inventory:

<https://csf.tools/reference/nist-sp-800-53/r5/pe/pe-3/>

45. Visitor Logs:

Guidance on visitor logs:

<https://csf.tools/reference/nist-sp-800-171/r2/3-10/3-10-3/>

46. Background Check:

Guidance on background checks:

<https://www.eeoc.gov/background-checks>

<https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter10.html>

47. Employee Termination:

Guidance on employee termination:

<https://csf.tools/reference/nist-sp-800-53/r5/ps/ps-4/>

<https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter10.html>

48. Employee Agreement:

Guidance on employee agreements:

<https://csf.tools/reference/nist-sp-800-53/r4/ps/ps-6/>

49. Risk Assessment:

Guidance on risk assessments:

<https://www.cisa.gov/risk-assessments>

<https://csf.tools/reference/nist-sp-800-53/r5/ra/ra-3/>

Cyber Hygiene Ladder Resources

50. Cybersecurity Control Assessment

Guidance on cybersecurity control assessments:

<https://www.cisecurity.org/controls/cis-controls-assessment-specification>

<https://csf.tools/reference/nist-sp-800-53/r5/ca/ca-2/>