Center for Internet Security®

CIS Controls®

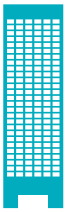
V7.1

Implementation Groups

The CIS Controls are internationally recognized for bringing together expert insight about threats, business technology, and defensive options into an effective, coherent, and simpler way to manage an organization's security improvement program. But in our experience organizations of every size and complexity still need more help to get started, and to focus their attention and resources.

To that end, we first took a "horizontal" look across all of the CIS Controls and identified a core set of Sub-Controls that organizations with limited resources and limited risk exposure should just do. We call this set Implementation Group (IG) 1. These provide effective security value with technology and processes that are generally already available, while providing a basis for more tailored and sophisticated action if that is warranted. Building upon Implementation Group 1, we then identified an additional set of Sub-Controls for organizations with more resources and expertise, but also greater risk exposure. This is Implementation Group 2. Finally, the rest of the Sub-Controls make up Implementation Group 3.

These Implementation Groups provide a simple and accessible way to help organizations of different classes focus their scarce security resources, and still leverage the value of the CIS Controls program, community, and complementary tools and working aids.



Implementation Group 3

A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Implementation Group 2

An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 1

An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

Definitions	1	2	3
Implementation Group 1 CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.	●		
Implementation Group 2 CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.	●	●	
Implementation Group 3 CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.	●	●	●

1-6 Basic

CIS Sub-Control / CIS Control Title		Implementation Groups 1	2	3
CIS Control 1: Inventory and Control of Hardware Assets				
1.1	Utilize an Active Discovery Tool		●	●
1.2	Use a Passive Asset Discovery Tool			●
1.3	Use DHCP Logging to Update Asset Inventory		●	●
1.4	Maintain Detailed Asset Inventory	●	●	●
1.5	Maintain Asset Inventory Information		●	●
1.6	Address Unauthorized Assets	●	●	●
1.7	Deploy Port Level Access Control		●	●
1.8	Utilize Client Certificates to Authenticate Hardware Assets			●
CIS Control 2: Inventory and Control of Software Assets				
2.1	Maintain Inventory of Authorized Software	●	●	●
2.2	Ensure Software Is Supported by Vendor	●	●	●
2.3	Utilize Software Inventory Tools		●	●
2.4	Track Software Inventory Information		●	●
2.5	Integrate Software and Hardware Asset Inventories			●
2.6	Address Unapproved Software	●	●	●
2.7	Utilize Application Whitelisting			●
2.8	Implement Application Whitelisting of Libraries			●
2.9	Implement Application Whitelisting of Scripts			●
2.10	Physically or Logically Segregate High Risk Applications			●
CIS Control 3: Continuous Vulnerability Management				
3.1	Run Automated Vulnerability Scanning Tools		●	●
3.2	Perform Authenticated Vulnerability Scanning		●	●
3.3	Protect Dedicated Assessment Accounts		●	●
3.4	Deploy Automated Operating System Patch Management Tools	●	●	●
3.5	Deploy Automated Software Patch Management Tools	●	●	●
3.6	Compare Back-to-Back Vulnerability Scans		●	●
3.7	Utilize a Risk-Rating Process		●	●
CIS Control 4: Controlled Use of Administrative Privileges				
4.1	Maintain Inventory of Administrative Accounts		●	●
4.2	Change Default Passwords	●	●	●
4.3	Ensure the Use of Dedicated Administrative Accounts	●	●	●
4.4	Use Unique Passwords		●	●
4.5	Use Multi-Factor Authentication for All Administrative Access		●	●
4.6	Use Dedicated Workstations For All Administrative Tasks			●
4.7	Limit Access to Scripting Tools		●	●
4.8	Log and Alert on Changes to Administrative Group Membership		●	●
4.9	Log and Alert on Unsuccessful Administrative Account Login		●	●

CIS Sub-Control / CIS Control Title		Implementation Groups 1	2	3
CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers				
5.1	Establish Secure Configurations	●	●	●
5.2	Maintain Secure Images		●	●
5.3	Securely Store Master Images		●	●
5.4	Deploy System Configuration Management Tools		●	●
5.5	Implement Automated Configuration Monitoring Systems		●	●
CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs				
6.1	Utilize Three Synchronized Time Sources		●	●
6.2	Activate Audit Logging	●	●	●
6.3	Enable Detailed Logging		●	●
6.4	Ensure Adequate Storage for Logs		●	●
6.5	Central Log Management		●	●
6.6	Deploy SIEM or Log Analytic Tools		●	●
6.7	Regularly Review Logs		●	●
6.8	Regularly Tune SIEM			●
CIS Control 7: Email and Web Browser Protections				
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	●	●	●
7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins		●	●
7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients		●	●
7.4	Maintain and Enforce Network-Based URL Filters		●	●
7.5	Subscribe to URL-Categorization Service		●	●
7.6	Log All URL Requests		●	●
7.7	Use of DNS Filtering Services	●	●	●
7.8	Implement DMARC and Enable Receiver-Side Verification		●	●
7.9	Block Unnecessary File Types		●	●
7.10	Sandbox All Email Attachments			●
CIS Control 8: Malware Defenses				
8.1	Utilize Centrally Managed Anti-Malware Software		●	●
8.2	Ensure Anti-Malware Software and Signatures Are Updated	●	●	●
8.3	Enable Operating System Anti-Exploitation Features / Deploy Anti-Exploit Technologies		●	●
8.4	Configure Anti-Malware Scanning of Removable Media	●	●	●
8.5	Configure Devices to Not Auto-Run Content	●	●	●
8.6	Centralize Anti-Malware Logging		●	●
8.7	Enable DNS Query Logging		●	●
8.8	Enable Command-Line Audit Logging		●	●

7-16 Foundational

CIS Sub-Control / CIS Control Title	Implementation Groups 1	2	3
CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services			
9.1 Associate Active Ports, Services, and Protocols to Asset Inventory		●	●
9.2 Ensure Only Approved Ports, Protocols, and Services Are Running		●	●
9.3 Perform Regular Automated Port Scans		●	●
9.4 Apply Host-Based Firewalls or Port-Filtering	●	●	●
9.5 Implement Application Firewalls			●
CIS Control 10: Data Recovery Capabilities			
10.1 Ensure Regular Automated Backups	●	●	●
10.2 Perform Complete System Backups	●	●	●
10.3 Test Data on Backup Media		●	●
10.4 Protect Backups	●	●	●
10.5 Ensure All Backups Have at Least One Offline Backup Destination	●	●	●
CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches			
11.1 Maintain Standard Security Configurations for Network Devices		●	●
11.2 Document Traffic Configuration Rules		●	●
11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes		●	●
11.4 Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	●	●	●
11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions		●	●
11.6 Use Dedicated Workstations for All Network Administrative Tasks		●	●
11.7 Manage Network Infrastructure Through a Dedicated Network		●	●
CIS Control 12: Boundary Defense			
12.1 Maintain an Inventory of Network Boundaries	●	●	●
12.2 Scan for Unauthorized Connections Across Trusted Network Boundaries		●	●
12.3 Deny Communications With Known Malicious IP Addresses		●	●
12.4 Deny Communication Over Unauthorized Ports	●	●	●
12.5 Configure Monitoring Systems to Record Network Packets		●	●
12.6 Deploy Network-Based IDS Sensors		●	●
12.7 Deploy Network-Based Intrusion Prevention Systems			●
12.8 Deploy NetFlow Collection on Networking Boundary Devices		●	●
12.9 Deploy Application Layer Filtering Proxy Server			●
12.10 Decrypt Network Traffic at Proxy			●
12.11 Require All Remote Logins to Use Multi-Factor Authentication		●	●
12.12 Manage All Devices Remotely Logging Into Internal Network			●

CIS Sub-Control / CIS Control Title	Implementation Groups 1	2	3
CIS Control 13: Data Protection			
13.1 Maintain an Inventory of Sensitive Information	●	●	●
13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization	●	●	●
13.3 Monitor and Block Unauthorized Network Traffic			●
13.4 Only Allow Access to Authorized Cloud Storage or Email Providers		●	●
13.5 Monitor and Detect Any Unauthorized Use of Encryption			●
13.6 Encrypt Mobile Device Data	●	●	●
13.7 Manage USB Devices		●	●
13.8 Manage System's External Removable Media's Read/Write Configurations			●
13.9 Encrypt Data on USB Storage Devices			●
CIS Control 14: Controlled Access Based on the Need to Know			
14.1 Segment the Network Based on Sensitivity		●	●
14.2 Enable Firewall Filtering Between VLANs		●	●
14.3 Disable Workstation-to-Workstation Communication		●	●
14.4 Encrypt All Sensitive Information in Transit		●	●
14.5 Utilize an Active Discovery Tool to Identify Sensitive Data			●
14.6 Protect Information Through Access Control Lists	●	●	●
14.7 Enforce Access Control to Data Through Automated Tools			●
14.8 Encrypt Sensitive Information at Rest			●
14.9 Enforce Detail Logging for Access or Changes to Sensitive Data			●
CIS Control 15: Wireless Access Control			
15.1 Maintain an Inventory of Authorized Wireless Access Points		●	●
15.2 Detect Wireless Access Points Connected to the Wired Network		●	●
15.3 Use a Wireless Intrusion Detection System		●	●
15.4 Disable Wireless Access on Devices if Not Required			●
15.5 Limit Wireless Access on Client Devices			●
15.6 Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients		●	●
15.7 Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	●	●	●
15.8 Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication			●
15.9 Disable Wireless Peripheral Access to Devices		●	●
15.10 Create Separate Wireless Network for Personal and Untrusted Devices	●	●	●

17-20 Organizational

CIS Sub-Control / CIS Control Title	Implementation Groups 1	2	3
CIS Control 16: Account Monitoring and Control			
16.1 Maintain an Inventory of Authentication Systems		●	●
16.2 Configure Centralized Point of Authentication		●	●
16.3 Require Multi-Factor Authentication		●	●
16.4 Encrypt or Hash All Authentication Credentials		●	●
16.5 Encrypt Transmittal of Username and Authentication Credentials		●	●
16.6 Maintain an Inventory of Accounts		●	●
16.7 Establish Process for Revoking Access		●	●
16.8 Disable Any Unassociated Accounts	●	●	●
16.9 Disable Dormant Accounts	●	●	●
16.10 Ensure All Accounts Have An Expiration Date		●	●
16.11 Lock Workstation Sessions After Inactivity	●	●	●
16.12 Monitor Attempts to Access Deactivated Accounts		●	●
16.13 Alert on Account Login Behavior Deviation			●
CIS Control 17: Implement a Security Awareness and Training Program			
17.1 Perform a Skills Gap Analysis		●	●
17.2 Deliver Training to Fill the Skills Gap		●	●
17.3 Implement a Security Awareness Program	●	●	●
17.4 Update Awareness Content Frequently		●	●
17.5 Train Workforce on Secure Authentication	●	●	●
17.6 Train Workforce on Identifying Social Engineering Attacks	●	●	●
17.7 Train Workforce on Sensitive Data Handling	●	●	●
17.8 Train Workforce on Causes of Unintentional Data Exposure	●	●	●
17.9 Train Workforce Members on Identifying and Reporting Incidents	●	●	●
CIS Control 18: Application Software Security			
18.1 Establish Secure Coding Practices		●	●
18.2 Ensure That Explicit Error Checking Is Performed for All In-House Developed Software		●	●
18.3 Verify That Acquired Software Is Still Supported		●	●
18.4 Only Use Up-to-Date and Trusted Third-Party Components			●
18.5 Use only Standardized and Extensively Reviewed Encryption Algorithms		●	●
18.6 Ensure Software Development Personnel Are Trained in Secure Coding		●	●
18.7 Apply Static and Dynamic Code Analysis Tools		●	●
18.8 Establish a Process to Accept and Address Reports of Software Vulnerabilities		●	●
18.9 Separate Production and Non-Production Systems		●	●
18.10 Deploy Web Application Firewalls		●	●
18.11 Use Standard Hardening Configuration Templates for Databases		●	●

CIS Sub-Control / CIS Control Title	Implementation Groups 1	2	3
CIS Control 19: Incident Response and Management			
19.1 Document Incident Response Procedures	●	●	●
19.2 Assign Job Titles and Duties for Incident Response		●	●
19.3 Designate Management Personnel to Support Incident Handling	●	●	●
19.4 Devise Organization-wide Standards For Reporting Incidents		●	●
19.5 Maintain Contact Information For Reporting Security Incidents	●	●	●
19.6 Publish Information Regarding Reporting Computer Anomalies and Incidents	●	●	●
19.7 Conduct Periodic Incident Scenario Sessions for Personnel		●	●
19.8 Create Incident Scoring and Prioritization Schema			●
CIS Control 20: Penetration Tests and Red Team Exercises			
20.1 Establish a Penetration Testing Program		●	●
20.2 Conduct Regular External and Internal Penetration Tests		●	●
20.3 Perform Periodic Red Team Exercises			●
20.4 Include Tests for Presence of Unprotected System Information and Artifacts		●	●
20.5 Create a Test Bed for Elements Not Typically Tested in Production		●	●
20.6 Use Vulnerability Scanning and Penetration Testing Tools in Concert		●	●
20.7 Ensure Results From Penetration Test Are Documented Using Open, Machine-Readable Standards			●
20.8 Control and Monitor Accounts Associated With Penetration Testing		●	●

CIS Center for Internet Security®

31 Tech Valley Drive
East Greenbush, NY 12061 USA
518.266.3460

Learn More:
www.cisecurity.org/controls