CIS Center for Internet Security®

# Implementation Groups

The CIS Critical Security Controls® (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 developed Implementation Groups (IGs). IGs are the recommended guidance to prioritize implementation of the CIS Controls. In an effort to assist enterprises of every size, IGs are divided into three groups. They are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls. Each IG identifies a set of Safeguards (previously referred to as CIS Sub-Controls), that they need to implement. There are 153 Safeguards in CIS Controls v8.

Every enterprise should start with IG1. IG1 provides 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 IG1, we then identified an additional set of Safeguards for organizations with more resources and expertise, but also greater risk exposure. This is IG2. Finally, the rest of the Safeguards make up IG3.

These IGs 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.

ESSENTIAL CYBER HYGIENE
IG1
IG2
IG3

**IG1** is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

**56**
**Cyber defense Safeguards**

ESSENTIAL CYBER HYGIENE
IG1
IG2
IG3

**IG2** assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

**74**
**Additional cyber defense Safeguards**

ESSENTIAL CYBER HYGIENE
IG1
IG2
IG3

**IG3** assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

**23**
**Additional cyber defense Safeguards**

**Total Safeguards** **153**

## Essential Cyber Hygiene

CIS Controls v8 defines Implementation Group 1 (IG1) as essential cyber hygiene and represents an emerging minimum standard of information security for all enterprises. IG1 is the on-ramp to the CIS Controls and consists of a foundational set of 56 cyber defense Safeguards. The Safeguards included in IG1 are what every enterprise should apply to defend against the most common attacks.

**For more information, visit www.cisecurity.org/controls.**

| Number | Control/Safeguard | IG1 | IG2 | IG3 |
|---|---|---|---|---|
| **01** | **Inventory and Control of Enterprise Assets** | | | |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ● | ● | ● |
| 1.2 | Address Unauthorized Assets | ● | ● | ● |
| 1.3 | Utilize an Active Discovery Tool | | ● | ● |
| 1.4 | Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory | | ● | ● |
| 1.5 | Use a Passive Asset Discovery Tool | | | ● |
| **02** | **Inventory and Control of Software Assets** | | | |
| 2.1 | Establish and Maintain a Software Inventory | ● | ● | ● |
| 2.2 | Ensure Authorized Software is Currently Supported | ● | ● | ● |
| 2.3 | Address Unauthorized Software | ● | ● | ● |
| 2.4 | Utilize Automated Software Inventory Tools | | ● | ● |
| 2.5 | Allowlist Authorized Software | | ● | ● |
| 2.6 | Allowlist Authorized Libraries | | ● | ● |
| 2.7 | Allowlist Authorized Scripts | | | ● |
| **03** | **Data Protection** | | | |
| 3.1 | Establish and Maintain a Data Management Process | ● | ● | ● |
| 3.2 | Establish and Maintain a Data Inventory | ● | ● | ● |
| 3.3 | Configure Data Access Control Lists | ● | ● | ● |
| 3.4 | Enforce Data Retention | ● | ● | ● |
| 3.5 | Securely Dispose of Data | ● | ● | ● |
| 3.6 | Encrypt Data on End-User Devices | ● | ● | ● |
| 3.7 | Establish and Maintain a Data Classification Scheme | | ● | ● |
| 3.8 | Document Data Flows | | ● | ● |
| 3.9 | Encrypt Data on Removable Media | | ● | ● |
| 3.10 | Encrypt Sensitive Data in Transit | | ● | ● |
| 3.11 | Encrypt Sensitive Data at Rest | | ● | ● |
| 3.12 | Segment Data Processing and Storage Based on Sensitivity | | ● | ● |
| 3.13 | Deploy a Data Loss Prevention Solution | | | ● |
| 3.14 | Log Sensitive Data Access | | | ● |

| Number | Control/Safeguard | IG1 | IG2 | IG3 |
|---|---|---|---|---|
| **04** | **Secure Configuration of Enterprise Assets and Software** | | | |
| 4.1 | Establish and Maintain a Secure Configuration Process | ● | ● | ● |
| 4.2 | Establish and Maintain a Secure Configuration Process for Network Infrastructure | ● | ● | ● |
| 4.3 | Configure Automatic Session Locking on Enterprise Assets | ● | ● | ● |
| 4.4 | Implement and Manage a Firewall on Servers | ● | ● | ● |
| 4.5 | Implement and Manage a Firewall on End-User Devices | ● | ● | ● |
| 4.6 | Securely Manage Enterprise Assets and Software | ● | ● | ● |
| 4.7 | Manage Default Accounts on Enterprise Assets and Software | ● | ● | ● |
| 4.8 | Uninstall or Disable Unnecessary Services on Enterprise Assets and Software | | ● | ● |
| 4.9 | Configure Trusted DNS Servers on Enterprise Assets | | ● | ● |
| 4.10 | Enforce Automatic Device Lockout on Portable End-User Devices | | ● | ● |
| 4.11 | Enforce Remote Wipe Capability on Portable End-User Devices | | ● | ● |
| 4.12 | Separate Enterprise Workspaces on Mobile End-User Devices | | | ● |
| **05** | **Account Management** | | | |
| 5.1 | Establish and Maintain an Inventory of Accounts | ● | ● | ● |
| 5.2 | Use Unique Passwords | ● | ● | ● |
| 5.3 | Disable Dormant Accounts | ● | ● | ● |
| 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts | ● | ● | ● |
| 5.5 | Establish and Maintain an Inventory of Service Accounts | | ● | ● |
| 5.6 | Centralize Account Management | | ● | ● |
| **06** | **Access Control Management** | | | |
| 6.1 | Establish an Access Granting Process | ● | ● | ● |
| 6.2 | Establish an Access Revoking Process | ● | ● | ● |
| 6.3 | Require MFA for Externally-Exposed Applications | ● | ● | ● |
| 6.4 | Require MFA for Remote Network Access | ● | ● | ● |
| 6.5 | Require MFA for Administrative Access | ● | ● | ● |
| 6.6 | Establish and Maintain an Inventory of Authentication and Authorization Systems | | ● | ● |
| 6.7 | Centralize Access Control | | ● | ● |
| 6.8 | Define and Maintain Role-Based Access Control | | | ● |

| Number | Control/Safeguard | IG1 | IG2 | IG3 |
|---|---|---|---|---|
| **07** | **Continuous Vulnerability Management** | | | |
| 7.1 | Establish and Maintain a Vulnerability Management Process | ● | ● | ● |
| 7.2 | Establish and Maintain a Remediation Process | ● | ● | ● |
| 7.3 | Perform Automated Operating System Patch Management | ● | ● | ● |
| 7.4 | Perform Automated Application Patch Management | ● | ● | ● |
| 7.5 | Perform Automated Vulnerability Scans of Internal Enterprise Assets | | ● | ● |
| 7.6 | Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets | | ● | ● |
| 7.7 | Remediate Detected Vulnerabilities | | ● | ● |
| **08** | **Audit Log Management** | | | |
| 8.1 | Establish and Maintain an Audit Log Management Process | ● | ● | ● |
| 8.2 | Collect Audit Logs | ● | ● | ● |
| 8.3 | Ensure Adequate Audit Log Storage | ● | ● | ● |
| 8.4 | Standardize Time Synchronization | | ● | ● |
| 8.5 | Collect Detailed Audit Logs | | ● | ● |
| 8.6 | Collect DNS Query Audit Logs | | ● | ● |
| 8.7 | Collect URL Request Audit Logs | | ● | ● |
| 8.8 | Collect Command-Line Audit Logs | | ● | ● |
| 8.9 | Centralize Audit Logs | | ● | ● |
| 8.10 | Retain Audit Logs | | ● | ● |
| 8.11 | Conduct Audit Log Reviews | | ● | ● |
| 8.12 | Collect Service Provider Logs | | | ● |
| **09** | **Email and Web Browser Protections** | | | |
| 9.1 | Ensure Use of Only Fully Supported Browsers and Email Clients | ● | ● | ● |
| 9.2 | Use DNS Filtering Services | ● | ● | ● |
| 9.3 | Maintain and Enforce Network-Based URL Filters | | ● | ● |
| 9.4 | Restrict Unnecessary or Unauthorized Browser and Email Client Extensions | | ● | ● |
| 9.5 | Implement DMARC | | ● | ● |
| 9.6 | Block Unnecessary File Types | | ● | ● |
| 9.7 | Deploy and Maintain Email Server Anti-Malware Protections | | | ● |

| Number | Control/Safeguard | IG1 | IG2 | IG3 |
|---|---|---|---|---|
| **10** | **Malware Defenses** | | | |
| 10.1 | Deploy and Maintain Anti-Malware Software | ● | ● | ● |
| 10.2 | Configure Automatic Anti-Malware Signature Updates | ● | ● | ● |
| 10.3 | Disable Autorun and Autoplay for Removable Media | ● | ● | ● |
| 10.4 | Configure Automatic Anti-Malware Scanning of Removable Media | | ● | ● |
| 10.5 | Enable Anti-Exploitation Features | | ● | ● |
| 10.6 | Centrally Manage Anti-Malware Software | | ● | ● |
| 10.7 | Use Behavior-Based Anti-Malware Software | | ● | ● |
| **11** | **Data Recovery** | | | |
| 11.1 | Establish and Maintain a Data Recovery Process | ● | ● | ● |
| 11.2 | Perform Automated Backups | ● | ● | ● |
| 11.3 | Protect Recovery Data | ● | ● | ● |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | ● | ● | ● |
| 11.5 | Test Data Recovery | | ● | ● |
| **12** | **Network Infrastructure Management** | | | |
| 12.1 | Ensure Network Infrastructure is Up-to-Date | ● | ● | ● |
| 12.2 | Establish and Maintain a Secure Network Architecture | | ● | ● |
| 12.3 | Securely Manage Network Infrastructure | | ● | ● |
| 12.4 | Establish and Maintain Architecture Diagram(s) | | ● | ● |
| 12.5 | Centralize Network Authentication, Authorization, and Auditing (AAA) | | ● | ● |
| 12.6 | Use of Secure Network Management and Communication Protocols | | ● | ● |
| 12.7 | Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure | | ● | ● |
| 12.8 | Establish and Maintain Dedicated Computing Resources for All Administrative Work | | | ● |

## 13 Network Monitoring and Defense

| Number | Control/Safeguard | IG1 | IG2 | IG3 |
|---|---|---|---|---|
| 13.1 | Centralize Security Event Alerting | | ● | ● |
| 13.2 | Deploy a Host-Based Intrusion Detection Solution | | ● | ● |
| 13.3 | Deploy a Network Intrusion Detection Solution | | ● | ● |
| 13.4 | Perform Traffic Filtering Between Network Segments | | ● | ● |
| 13.5 | Manage Access Control for Remote Assets | | ● | ● |
| 13.6 | Collect Network Traffic Flow Logs | | ● | ● |
| 13.7 | Deploy a Host-Based Intrusion Prevention Solution | | | ● |
| 13.8 | Deploy a Network Intrusion Prevention Solution | | | ● |
| 13.9 | Deploy Port-Level Access Control | | | ● |
| 13.10 | Perform Application Layer Filtering | | | ● |
| 13.11 | Tune Security Event Alerting Thresholds | | | ● |

## 14 Security Awareness and Skills Training

| | | | | |
|---|---|---|---|---|
| 14.1 | Establish and Maintain a Security Awareness Program | ● | ● | ● |
| 14.2 | Train Workforce Members to Recognize Social Engineering Attacks | ● | ● | ● |
| 14.3 | Train Workforce Members on Authentication Best Practices | ● | ● | ● |
| 14.4 | Train Workforce on Data Handling Best Practices | ● | ● | ● |
| 14.5 | Train Workforce Members on Causes of Unintentional Data Exposure | ● | ● | ● |
| 14.6 | Train Workforce Members on Recognizing and Reporting Security Incidents | ● | ● | ● |
| 14.7 | Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates | ● | ● | ● |
| 14.8 | Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks | ● | ● | ● |
| 14.9 | Conduct Role-Specific Security Awareness and Skills Training | | ● | ● |

## 15 Service Provider Management

| | | | | |
|---|---|---|---|---|
| 15.1 | Establish and Maintain an Inventory of Service Providers | ● | ● | ● |
| 15.2 | Establish and Maintain a Service Provider Management Policy | | ● | ● |
| 15.3 | Classify Service Providers | | ● | ● |
| 15.4 | Ensure Service Provider Contracts Include Security Requirements | | ● | ● |
| 15.5 | Assess Service Providers | | | ● |
| 15.6 | Monitor Service Providers | | | ● |
| 15.7 | Securely Decommission Service Providers | | | ● |

## 16 Application Software Security

| Number | Control/Safeguard | IG1 | IG2 | IG3 |
|---|---|---|---|---|
| 16.1 | Establish and Maintain a Secure Application Development Process | | ● | ● |
| 16.2 | Establish and Maintain a Process to Accept and Address Software Vulnerabilities | | ● | ● |
| 16.3 | Perform Root Cause Analysis on Security Vulnerabilities | | ● | ● |
| 16.4 | Establish and Manage an Inventory of Third-Party Software Components | | ● | ● |
| 16.5 | Use Up-to-Date and Trusted Third-Party Software Components | | ● | ● |
| 16.6 | Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities | | ● | ● |
| 16.7 | Use Standard Hardening Configuration Templates for Application Infrastructure | | ● | ● |
| 16.8 | Separate Production and Non-Production Systems | | ● | ● |
| 16.9 | Train Developers in Application Security Concepts and Secure Coding | | ● | ● |
| 16.10 | Apply Secure Design Principles in Application Architectures | | ● | ● |
| 16.11 | Leverage Vetted Modules or Services for Application Security Components | | ● | ● |
| 16.12 | Implement Code-Level Security Checks | | | ● |
| 16.13 | Conduct Application Penetration Testing | | | ● |
| 16.14 | Conduct Threat Modeling | | | ● |

## 17 Incident Response Management

| | | | | |
|---|---|---|---|---|
| 17.1 | Designate Personnel to Manage Incident Handling | ● | ● | ● |
| 17.2 | Establish and Maintain Contact Information for Reporting Security Incidents | ● | ● | ● |
| 17.3 | Establish and Maintain an Enterprise Process for Reporting Incidents | ● | ● | ● |
| 17.4 | Establish and Maintain an Incident Response Process | | ● | ● |
| 17.5 | Assign Key Roles and Responsibilities | | ● | ● |
| 17.6 | Define Mechanisms for Communicating During Incident Response | | ● | ● |
| 17.7 | Conduct Routine Incident Response Exercises | | ● | ● |
| 17.8 | Conduct Post-Incident Reviews | | ● | ● |
| 17.9 | Establish and Maintain Security Incident Thresholds | | | ● |

## 18 Penetration Testing

| | | | | |
|---|---|---|---|---|
| 18.1 | Establish and Maintain a Penetration Testing Program | | ● | ● |
| 18.2 | Perform Periodic External Penetration Tests | | ● | ● |
| 18.3 | Remediate Penetration Test Findings | | ● | ● |
| 18.4 | Validate Security Measures | | | ● |
| 18.5 | Perform Periodic Internal Penetration Tests | | | ● |