CIS CONTROLS V7.1

Center for Internet Security

OVERVIEW

The Center for Internet Security (CIS) developed the Critical Security Controls for Effective Cyber Defense. The 20 controls are based on the latest information about common attacks and reflect the combined knowledge of commercial forensics experts, individual penetration testers and contributors from U.S. government agencies.

IT security leaders use CIS Controls to quickly establish the protections providing the highest payoff in their organizations. They guide you through a series of 20 foundational and advanced cybersecurity actions, where the most common attacks can be eliminated.





1 Inventory and Control of Hardware Assets 2 Inventory and Control of Software Assets 3 Continuous Vulnerability Management 4 Controlled Use of Administrative Privileges 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers 6 Maintenance, Monitoring and Analysis of Audit Logs

7	Email and Web Browser Protections	12 Boundary Defense
8	Malware Defenses	13 Data Protection
9	Limitation and Control of Network Ports, Protocols, and Services	14 Controlled Access Based on the Need to Know
10	Data Recovery Capabilities	15 Wireless Access Control
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	16 Account Monitoring and Control

Organizational

17 Implement a Security
Awareness and Training
Program

18 Application Software
Security

19 Incident Response
and Management

20 Penetration Tests and
Red Team Exercises

Source: www.cisecurity.org/blog/cis-controls-version-7-whats-old-whats-new/

BASIC CONTROLS 1-6

Center for Internet Security

at only ed from
uthorized l prevented
erabilities,
nfiguration
ons, Servers ration of nange
cover from
nfigur ons, S ration nange

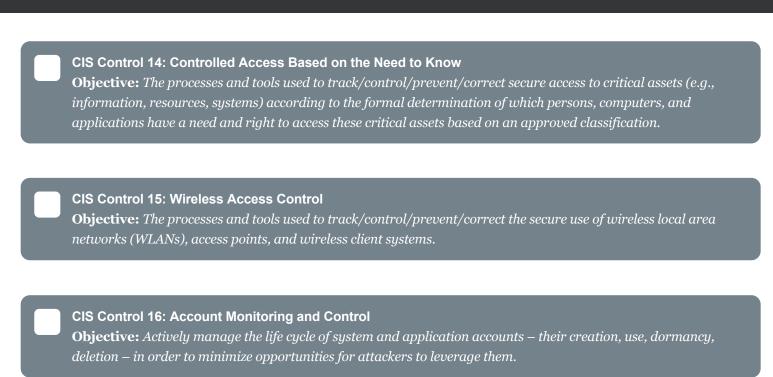
FOUNDATIONAL CONTROLS 7-16

Center for Internet Security

CIS Control 7: Email and Web Browser Protections Objective: Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.
CIS Control 8: Malware Defenses Objective: Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.
CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services Objective: Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.
CIS Control 10: Data Recovery Capabilities Objective: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches Objective: Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
CIS Control 12: Boundary Defense Objective: Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

FOUNDATIONAL CONTROLS 7-16

Center for Internet Security



ORGANIZATIONAL CONTROLS 17-20

Center for Internet Security

CIS Control 17: Implement a Security Awareness and Training Program

Objective: For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

CIS Control 18: Application Software Security

Objective: Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

CIS Control 19: Incident Response and Management
Objective: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

CIS Control 20: Penetration Tests and Red Team Exercises

Objective: Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.