Published on *University of Colorado* (https://www.cu.edu)

High Impact Security Standards [1]

The following summarizes the recommneded security standards and requirements for protecting highly confidential information when it is processed, stored, or transmitted. The checklist is meant as a guide to help users overview each of the categories necessary for keeping highly confidential information protected. If all boxes can be checked, all highly confidential information is consided to meet the minimum security requirements of protection.

Control Family	Summary	?
Access Control	Limit system access of systems to authorized users by separating individual duties and monitoring remote access. Control, monitor, and encrypt highly confidential information on all platforms, including remote devices, and systems to control the flow of highly confidential information.	
Awareness and Training	To ensure that users, managers, and system administrators are properly trained and aware of their security impact associated with their activity within organizational systems.	
Audit and Accountability	Keep track of system activity by establishing and maintaining accurate and up to date audit logs and records in case of unlawful system activity.	
Configuration Management	Establish base configurations that control and monitor access and use of software, hardware, firmware, and documentation in organizational systems.	
Identification and Authentication	Have multifactor authentication mechanisms to access networks by enforcing proper passwords and verifications of users between privileged and non-privileged accounts.	
Incident Response	Establish and test incident handling responses for organizational systems and keep documentation of incidents of the systems.	
Maintenance	Perform maintenance on organizational systems by providing controls, sanitizing equipment, checking media for malicious code, requiring authentication for nonlocal maintenance, and supervising maintenance activity and personnel.	
Media Protection	Protect highly confidential information on both digital and paper media during transport, in storage, and before disposal.	

Control Family	Summary	?
Personnel Security	Ensure that organizational systems containing highly confidential information are protected prior to, during, and after individuals have access.	
Physical Protection	Protect and monitor physical access to the organizational system and its operating environments.	
Risk Assessment	Assess the risk to organizational systems from associated processing storage, or transmission of highly confidential information. This includes periodically scanning for vulnerabilities and applications and remediating them once found.	
Security Assessment	Ensure that the security controls in organizational systems are working properly and have plans in place to properly describe how systems are operated, implemented, and connected to other systems, as well as eliminate and correct deficiencies.	
System and Communications Protection	Protect highly confidential information by monitoring, controlling, and protecting communication within the organizational system. This is excecuted by using cryptographic mechanisms, monitoring remote access, monitoring user activity and communication, and controlling network connections associated with communication.	
System and Information Integrity	Protect organizational systems from malicious code and potential attacks by regularly scanning files, especially when external sources are executed, as well as monitoring communication and unauthorized use of the organizational systems.	

For more information, a more detailed view of the controls can be viewed here [2]. [3] The information found on this page is a summary of the National Institute of Standards and Technology 800-171 Revision 2 documentation for protecting highly confidential information in nonfederal systems and organizations. The full text of the NIST 900-171 document can be found here [4].

Groups audience:
Office of Information Security

Source URL: https://www.cu.edu/security/high-impact-security-standards

Links
[1] https://www.cu.edu/security/high-impact-security-standards
[2] https://www.cu.edu/system/files/pages/242885-high-impact-security-standards/docs/high-impact-standards.xlsx
[3] https://www.cu.edu/High%20Impact%20Standards.xlsx
[4] https://www.cu.edu/updated-hi-standards-nistsp800-171r2.pdf