NIST

THE ULTIMATE NIST HANDBOOK

KEY STANDARDS AND LINKS

MINISTRY OF
MOS
SECURITY

📘 The Ultimate NIST Handbook: Key Standards and Links 📘

The Ultimate NIST Handbook

NIST Standard	Title	Brief Description	Standard URL
NIST 800-12	Handbook for Computer Security Managers	This publication serves as a starting point for those new to information security as well as those unfamiliar with NIST information security publications and guidelines. The intent of this special publication is to provide a high-level overview of information security principles by introducing related concepts and the security control families (as defined in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations) that organizations can leverage to effectively secure their systems1 and information.	https://csrc.nist.gov/pubs/sp/800/12/r1/final
NIST 800-13	Telecommunications Security Guidelines	Offers guidelines for securing telecommunications systems, including network security, encryption, and key management.	https://csrc.nist.gov/pubs/sp/800/13/final
NIST 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems	Outlines fundamental security principles and practices for IT systems, such as access control, system and network security, and incident response.	https://csrc.nist.gov/pubs/sp/800/14/final
NIST 800-18	Guide for Developing Security Plans for Federal Information Systems	Provides a step-by-step approach to developing security plans, including risk assessments, security controls, and incident response procedures.	https://csrc.nist.gov/pubs/sp/800/18/r1/final
NIST 800-30	Guide for Conducting Risk Assessments	Provides a comprehensive framework for managing risk, including risk assessment, risk mitigation, and risk monitoring.	https://csrc.nist.gov/pubs/sp/800/30/r1/final

📘 The Ultimate NIST Handbook: Key Standards and Links 📘

NIST 800-34	Contingency Planning Guide for Federal Information Systems	Offers guidance on developing contingency plans to address various disruptions, such as natural disasters, cyberattacks, and system failures.	https://www.nist.gov/privacy-framework/nist-sp-800-34
NIST 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy	Provides a systematic approach to managing risk across the entire lifecycle of an information system.	https://csrc.nist.gov/pubs/sp/800/37/r2/final
NIST 800-40	Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology	Provides detailed guidance on developing security plans, including specific controls and procedures.	https://csrc.nist.gov/pubs/sp/800/40/r4/final
NIST 800-41	Guidelines on Firewalls and Firewall Policy	Offers guidance on firewall technologies, deployment strategies, and policy development.	https://csrc.nist.gov/pubs/sp/800/41/r1/final
NIST 800-44	Guidelines on Securing Public Web Servers	Provides recommendations for securing web servers, including configuration guidelines, vulnerability management, and incident response.	https://csrc.nist.gov/pubs/sp/800/44/ver2/final
NIST 800-45	Guidelines on Electronic Mail Security	Offers guidance on securing email systems, including encryption, authentication, and spam filtering.	https://csrc.nist.gov/pubs/sp/800/45/ver2/final
NIST 800-47	Managing the Security of Information Exchanges	Provides guidance on securing interconnected systems, including network security, access control, and data protection.	https://csrc.nist.gov/pubs/sp/800/47/r1/final

📘 The Ultimate NIST Handbook: Key Standards and Links 📘

NIST 800-50	Building an Information Technology Security Awareness and Training Program	Provides guidance on developing and implementing security awareness and training programs.	https://csrc.nist.gov/pubs/sp/800/50/r1/final
NIST 800-53	Security and Privacy Controls for Federal Information Systems and Organizations	Provides a comprehensive set of security and privacy controls for federal systems and organizations.	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
NIST 800-54	Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation	Offers guidance on securing BGP, a protocol used to exchange routing information between networks.	https://csrc.nist.gov/pubs/sp/800/189/final
NIST 800-55	Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures	Provides guidance on measuring the effectiveness of security controls and processes.	https://csrc.nist.gov/pubs/sp/800/55/v1/ipd
NIST 800-57	Recommendation for Key Management Part 1: General	Provides guidance on key management practices, including key generation, distribution, and storage.	https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final
NIST 800-60	Guide for Mapping Types of Information and Systems to Security Categories	Provides guidance on classifying information and systems based on their sensitivity and criticality.	https://csrc.nist.gov/pubs/sp/800/60/r2/iwd
NIST 800-61	Computer Security Incident	Provides guidance on incident response planning, detection,	https://csrc.nist.gov/pubs/sp/800/61/r2/final

	Handling Guide	analysis, containment, eradication, recovery, and lessons learned.	
NIST 800-63	Electronic Authentication Guideline	Provides guidance on electronic authentication technologies and practices, including password management, biometrics, and smart cards.	https://pages.nist.gov/800-63-3/
NIST 800-82	Guide to Operational Technology (OT) Security	Provides guidance on securing industrial control systems, including SCADA systems and other critical infrastructure systems.	https://csrc.nist.gov/pubs/sp/800/82/r3/final
NIST 800-83	Guide to Malware Incident Prevention and Handling for Desktops and Laptops	Provides guidance on recovering from malware incidents, including malware removal, system restoration, and incident response.	https://csrc.nist.gov/pubs/sp/800/83/r1/final
NIST 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	This publication seeks to assist organizations in designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events in an effort to aid personnel in preparing for adverse situations involving information technology (IT).	https://csrc.nist.gov/pubs/sp/800/84/final
NIST 800-86	Guide to Integrating Forensic Techniques into Incident Response	Provides guidance on integrating forensic techniques into incident response processes.	https://csrc.nist.gov/pubs/sp/800/86/final
NIST 800-88	Guidelines for Media Sanitization	Provides guidance on sanitizing storage media to remove sensitive information.	https://csrc.nist.gov/pubs/sp/800/88/r1/final
NIST 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications	This Recommendation specifies methods for obtaining the assurances necessary for valid digital signatures: assurance of domain parameter validity, assurance of public key validity, assurance that the key pair owner actually possesses the	https://csrc.nist.gov/pubs/sp/800/89/final

		private key, and assurance of the identity of the key pair owner.	
NIST 800-92	Guide to Computer Security Log Management	This publication seeks to assist organizations in understanding the need for sound computer security log management. It provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise.	https://csrc.nist.gov/pubs/sp/800/92/final
NIST 800-94	Guidelines on Intrusion Detection Systems	Provides guidance on deploying and managing intrusion detection systems.	https://csrc.nist.gov/pubs/sp/800/94/final
NIST 800-95	Guide to Secure Web Services	This document describes how to implement those security mechanisms in Web services. It also discusses how to make Web services and portal applications robust against the attacks to which they are subject.	https://csrc.nist.gov/pubs/sp/800/95/final
NIST 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	It describes secure methods used to authenticate users in a wireless environment, and presents several sample case studies of wireless deployment. It also includes guidance on best practices for establishing secure wireless networks using the emerging Wi-Fi technology.	https://csrc.nist.gov/pubs/sp/800/97/final
NIST 800-98	Guidelines for Securing Radio Frequency Identification (RFID) Systems	The document also provides background information on RFID applications, standards, and system components to assist in the understanding of RFID security risks and controls. This document presents information that is independent of particular hardware platforms, operating systems, and applications.	https://csrc.nist.gov/pubs/sp/800/98/final
NIST 800-100	Information Security Handbook: A Guide for Managers	This Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and	https://csrc.nist.gov/pubs/sp/800/100/upd1/final

		implement an information security program.	
NIST 800-101	Guidelines on Mobile Device Forensics	This guide attempts to bridge the gap by providing an in-depth look into mobile devices and explaining the technologies involved and their relationship to forensic procedures.	https://csrc.nist.gov/pubs/sp/800/101/r1/final
NIST 800-111	Guide to Storage Encryption Technologies for End User Devices	This publication explains the basics of storage encryption, which is the process of using encryption and authentication to restrict access to and use of stored information.	https://csrc.nist.gov/pubs/sp/800/111/final
NIST 800-114	User's Guide to Telework and Bring Your Own Device (BYOD) Security	This publication provides recommendations for securing BYOD devices used for telework and remote access, as well as those directly attached to the enterprise's own networks.	https://csrc.nist.gov/pubs/sp/800/114/r1/final
NIST 800-115	Technical Guide to Information Security Testing and Assessment	Provides guidance on conducting security testing and assessments, including penetration testing, vulnerability scanning, and risk assessments.	https://csrc.nist.gov/pubs/sp/800/115/final
NIST 800-119	Guidelines for Securing the IPv6 Transition	Provides guidance on securing IPv6 networks and transitioning from IPv4 to IPv6.	https://csrc.nist.gov/pubs/sp/800/119/final
NIST 800-122	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	Provides guidance on protecting sensitive but unclassified information in non-federal systems and organizations.	https://csrc.nist.gov/pubs/sp/800/122/final
NIST 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information	Provides guidance on continuous monitoring practices to identify and respond to security threats.	https://csrc.nist.gov/pubs/sp/800/137/final

	Systems and Organizations		
NIST 800-145	The NIST Cloud Computing Framework	Provides a framework for assessing and managing risks associated with cloud computing.	https://csrc.nist.gov/pubs/sp/800/145/final

DID YOU FIND THIS CHECKLIST USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

MINISTRY OF MOS SECURITY

WWW.MINISTRYOFSECURITY.CO