

Security controls from the NIST publication 800-53...

NIST sets the security standards for agencies and contractors – and given the evolving threat landscape, NIST is influencing data security in the private sector as well.

It's structured as a set of security guidelines, designed to prevent major security issues that are making the headlines nearly every day.

NIST SP 800-53 Defined

- NIST SP 800-53 defines the standards and guidelines for federal agencies to architect and manage their information security systems.
- It was established to provide guidance for the protection of agency's and citizen's private data.
- Federal agencies must follow these standards, and the private sector should follow the same guidelines.



NIST SP 800-53 breaks the guidelines up into 3 Minimum Security Controls spread across 18 different control families.

Minimum Security Controls:

- High-Impact Baseline
- Medium-Impact Baseline
- Low-Impact Baseline

Control Families:

- AC – Access Control
- AU – Audit and Accountability
- AT – Awareness and Training
- CM – Configuration Management
- CP – Contingency Planning
- IA – Identification and Authentication
- IR – Incident Response
- MA – Maintenance
- MP – Media Protection

- PS – Personnel Security
 - PE – Physical and Environmental Protection
 - PL – Planning
 - PM – Program Management
 - RA – Risk Assessment
 - CA – Security Assessment and Authorization
 - SC – System and Communications Protection
 - SI – System and Information Integrity
 - SA – System and Services Acquisition
-

What's The Purpose and Benefit of NIST SP 800-53

- Standardization
 - Risk Control
 - Reduce IT Risk Problem
-

NIST 800-53 Compliance Best Practices



Discover and Classify Sensitive Data:

- Locate and secure all sensitive data
- Classify data based on business policy

Map Data and Permissions

- Identify users, groups, folder and file permissions
- Determine who has access to what data

Manage Access Control

- Identify and deactivate stale users
- Manage user and group memberships
- Remove Global Access Groups
- Implement a least privilege model

Monitor Data, File Activity, and User Behavior

- Audit and report on file and event activity
- Monitor for insider threats, malware, misconfigurations and security breaches
- Detect security vulnerabilities and remediate