squadra technologies

secRMM

A NIST 800-171 Compliance Solution

What is NIST 800-171?

NIST 800-171 is a document of guidelines published by the National Institute of Standards and Technology (NIST). Compliance is required as of December 31, 2017 in order to "Protect Controlled Unclassified information in Nonfederal Information Systems and Organizations." Compliance is enforced and handled by the Department of Defense emphasizing the importance of the requirements set forth by NIST 800-171.

Squadra Technologies' secRMM

Squadra Technologies' security Removable Media Manager (secRMM) software provides security capabilities on three critical sections of NIST 800-171: Access Control (3.1), Audit and Accountability (3.3), and Media Protection (3.8), as well as a breadth of other security capabilities applicable to other guidelines and requirements.

Access Control (3.1)

3.1.18 Controlling the Connection of Mobile Devices

- NIST 800-171 Requirement: Prohibit unapproved devices to mount their filesystems.
- secRMM Solution: secRMM can unmount non-whitelisted devices from the operating system and logs the event.

3.1.21 Limiting the Use of Removable Storage Devices on External Information Systems

- NIST 800-171 Requirement: Contractors must limit or remove the use of removable storage devices. If removable storage devices are utilized, the appropriate tracking measures must be implemented.
- secRMM Solution: secRMM limits the usage of removable storage by using whitelisting policy rules.

NIST 800-171 Guidelines and Requirements

- Access Control (3.1)
- Awareness & Training (3.2)
- Audit and Accountability (3.3)
- Configuration Management (3.4)
- Identification and Authentication (3.5)
- Incident Response (3.6)
- Maintenance (3.7)
- Media Protection (3.8)
- Personnel Security (3.9)
- Physical Protection (3.10)
- Risk Assessment (3.11)
- Security Assessment (3.12)
- System and Communication Protection (3.13)
- System and Information Integrity (3.14)

Who needs to be Compliant?

Every federal government contractor that has Controlled Unclassified Information (CUI) must be compliant.

Squadra Technologies | 7575 West Washington Ave. Suite 127-252 Las Vegas, NV 89128 | +1 (562) 221-3079

squadra technologies

Audit and Accountability (3.3)

3.3.1 Retain System Audit Records In Order to Thoroughly Monitor Activity

- NIST 800-171 Requirement: Records must display a comprehensive list of when, where, source, and outcome of events and the identity of the user.
- secRMM Solution: secRMM contains information event data such as the source file path of the file copied, size, date last modified, userID, etc. secRMM also utilizes its own log, in addition to the Security event log, ensuring data is never lost.

Media Protection (3.8)

3.8.7 and 3.8.8 Controlling the Use of Removable Media

- NIST 800-171 Requirement: Implementing safeguards that prohibit unauthorized devices and devices without an identified user.
- secRMM Solution: secRMM can whitelist a variety of removable media devices such as USB drives, mobile devices, and external hard drives. secRMM also utilizes Active Directory to map devices to users.

3.8.9 Protecting the Confidentiality of Backup CUI at Storage Locations

- NIST 800-171 Requirement: Security and audit information pertaining to mobile devices and removable storage devices must be backed up and stored securely.
- secRMM Solution: All secRMM event data is stored in standalone Windows Event Log Backup files, ensuring all information is secure and protected.

secRMM also provides additional security capabilities in the following NIST 800-171 requirement areas:

- 3.4 Configuration Management
- 3.5 Identification & Authentication
- 3.7 Maintenance
- 3.9 Personnel Security
- 3.10 Physical Potection
- 3.11 Risk
- 3.12 Security Assessment
- 3.13 System & Comms
- 3.14 Stem & Info Integrity

For More Information Contact:
info@squadratechnologies.com

Free Trial Download Visit:
www.squadratechnologies.com