DATA SHEET

FISMA-NIST SP 800-171 Framework Guide

Commercial organizations that do business with the U.S. government or handle U.S. government data are required to comply with NIST SP 800-171 regulations. These requirements are directly linked to NIST SP 800-53 and deal with the protection of Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations.

RackFoundry Total Security Management is an enterprise-grade cyber security solution that delivers unparalleled threat detection and protection. Along with Fortress Labs and RackFoundry's internal Security Operations Centers (SOC), RackFoundry helps organizations of all sizes achieve and maintain NIST SP 800-171 compliance. This document explains, in detail, how RackFoundry Total Security Management relates to each relevant security control.

Control Number	Control Description	Related NIST SP 800-53 controls	RackFoundry TSM Ability
Access Control			
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	AC-2 Account Management AC-3 Access Enforcement AC-17 Remote Access	Logging, Reporting, and Alerting features monitor access activities.
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2 Account Management AC-3 Access Enforcement AC-17 Remote Access	Logging, Reporting, and Alerting features monitor access activities.
3.1.3	Control the flow of CUI in accordance with approved authorizations.	AC-4 Information Flow Enforcement	Agent-based and agent-less File Integrity Monitoring (FIM) monitors for unauthorized file access; Behavioral monitoring detects unusual activity; SIEM generates alerts for security threats involving CUI.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5 Separation of Duties	Behavioral Monitoring detects attempts to cross role boundaries.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6 Least Privilege AC-6(1) Authorize Access to Security Functions AC-6(5) Privilege Accounts	Monitor logon activities with customized policies.
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	AC-6(2) Non-Privilege access for Non-Security Functions	Monitor logon activities with customized policies.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	AC-6(9) Auditing use of privilege functions AC-6(10) Prohibit non-privileged users from executing privilege functions	Monitor event logs when privileged functions are executed.
3.1.8	Limit unsuccessful logon attempts.	AC-7 Unsuccessful Logon Attempts	Rackfoundry TSM sends alert notifications for logon failures.
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	AC-9 Previous Logon (Access) Notification	Banner with appropriate notices can be displayed upon logging in to the console.

Control Number	Control Description	Related NIST SP 800-53 controls	RackFoundry TSM Ability
3.1.10	Use session lock with pattern - hiding displays to prevent access/viewing of data after period of inactivity.	AC-11 Session Lock AC-11(1) Pattern hiding Displays	RackFoundry TSM times out after inactivity and prevents access to dashboard.
3.1.11	Terminate (automatically) a user session after a defined condition.	AC-12 Session Termination	RackFoundry TSM times out after inactivity and prevents access to dashboard.
3.1.12	Monitor and control remote access sessions	AC-17(1) Automated Monitoring Controls	RackFoundry TSM monitors remote desktops and VPN logs; Behavioral monitoring picks up unusual user activity.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC-17(2) Protection of Confidentiality / integrity using encryption	RackFoundry TSM includes VPN functionality and monitors cryptographic remote access sessions; RackFoundry's SOC ensures secure connection to dashboard.
3.1.14	Route remote access via managed access control points.	AC-17(3) Managed Access Control Points	RackFoundry TSM monitors remote access control points and generates events/alerts.
3.1.15	Authorize remote execution of privileged commands and remote access to security - relevant information.	AC-17(4) Managed Access Control Points	RackFoundry TSM monitors remote access control points and generates events/alerts; Alerts include information about location, user, date, time, result of the event, etc.
3.1.16	Authorize wireless access prior to allowing such connections	AC-18 Wireless Access	RackFoundry TSM monitors wireless devices through the wireless access controller.
3.1.20	Verify and control/limit connections to and use of external information systems.	AC-20 Use of external Information systems AC-20 (1) Limit on Authorized Use	Automatically detect when new devices are added to the environment and monitor logs and network traffic.
3.1.21	Limit use of organizational portable storage devices on external information systems.	AC-20(2) Portable Storage Devices	RackFoundry TSM monitors logs involving portable storage devices including files copied, users/devices involved; Alert notifications are generated when unusual activity is detected.

Control Number	Control Description	Related NIST SP 800-53 controls	RackFoundry TSM Ability
3.1.22	Control information posted or processed on publicly accessible information systems.	AC-22 Publicly Accessible Content	RackFoundry TSM can be used to monitor access to publicly accessible information systems.
Audit and Accountability			
3.3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	AU-2 Audit Events AU-3 Content of audit records AU-3(1) Additional Audit Information AU-12 Audit Generation	RackFoundry TSM monitors audit logs and picks up important information such as user activity, username, timestamp, etc.; Utilize up to 30 TB of storage to retain logs for years and maintain an accurate audit trail.
3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	AU-2 Audit Events AU-3 Content of audit records AU-3(1) Additional Audit Information AU-12 Audit Generation	RackFoundry TSM monitors audit logs and picks up important information such as user activity, username, timestamp, etc.; Utilize up to 30 TB of storage to retain logs for years and maintain an accurate audit trail.
3.3.3	Review and update audited events.	AU-2(3) Reviews and Updates	RackFoundry TSM monitors audited events; RackFoundry's SOC automatically reviews all events and alerts.
3.3.4	Alert in the event of an audit process failure.	AU-5 Response to audit processing failures	RackFoundry TSM sends notifications for audit process failures.
3.3.5	Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	AU-6(1) Process Integration AU-6(3) Correlate audit repositories	RackFoundry TSM utilizes four threat intelligence feeds to correlate event data, analyze indicators of compromise, and automatically detect security threats.
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	AU-7 Audit Reduction and report generation	RackFoundry TSM includes pre-configured compliance reports, including NIST SP 800-171.

Control Number	Control Description	Related NIST SP 800-53 controls	RackFoundry TSM Ability
3.3.7	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	AU-8 Time Stamps AU-8(1) Synchronization with authorized time source	RackFoundry TSM integrates with Active Directory and pulls in timestamp information.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	AU-9 Protection of Audit Information	Data-at-rest is protected with AES-256 encrypted to FIPS 140-2 DoD standards and data in transit is encrypted using TLS v1.2 AES-GCM with SHA-2 signature.
3.3.9	Limit management of audit functionality to a subset of privileged users.	AU-9(4) Access by subset of privileged users	RackFoundry TSM supports role-based access within the console.
Configuration Management			
3.4.1	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	CM-2 Baseline Configuration CM-6 Configuration Settings CM-8 Information System component inventory CM-8(1) Updates during installations/Removals	RackFoundry TSM's File Integrity Monitoring (FIM) detects any changes to the configuration on Windows, Linux, MacOS, and Solaris Systems, among others.
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	CM-2 Baseline Configuration CM-6 Configuration Settings CM-8 Information Systems component inventory CM-8(1) Updates during installations/Removals	RackFoundry TSM monitors changes to security settings; RackFoundry's SOC reviews security configuration settings.
3.4.3	Track, review, approve/disapprove, and audit changes to information systems.	CM-3 Configuration change control	RackFoundry TSM can be configured to monitor logs of changes to information systems.
3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	CM-7(1) Periodic Review CM-7(2) Prevent program execution	RackFoundry TSM can monitor access to programs, functions, ports, protocols and services and it has built-in Firewall and Port Management functionality.
3.4.9	Control and monitor user-installed software.	CM-11 User installed Software	RackFoundry TSM sends alert notifications for user-installed software.

Control Number	Control Description	Related NIST SP 800-53 controls	RackFoundry TSM Ability
Identification and Authentication			
3.5.1	Identify information system users, processes acting on behalf of users, or devices.	IA-2 Identification and Authorization (organizational users) IA-5 Authenticator Management	User and device activity can be monitored within the solution utilizing the search tool; User activity reports can be generated.
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	IA-2 Identification and Authorization (organizational users) IA-5 Authenticator Management	User and device activity can be monitored within the solution utilizing the search tool; User activity reports can be generated.
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA-2(1) Network access to privilege users IA-2(2) Network access to non-privilege users IA-2(3) Local access to privilege accounts	RackFoundry TSM monitors information relating to privilege or non-privilege access for local and remote accounts.
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.	IA-2(8) Network access to privilege accounts -Replay protection IA-2(9) Network access to non-privilege accounts - Replay protection	RackFoundry TSM integrates with Active Directory to employ replay-resistant authentication.
Incident Response			
3.6.1	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	IR-2 Incident Response Training IR-4 Incident Handling IR-5 Incident Monitoring IR-6 Incident Reporting IR-7 Incident Response Assistance	RackFoundry TSM policies can be defined in accordance with organizational incident handling policies; RackFoundry's SOC utilizes a proven triage processes to review/analyze incidents, determine appropriate responses, and notify users accordingly.
3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization	IR-2 Incident Response Training IR-4 Incident Handling IR-5 Incident Monitoring IR-6 Incident Reporting IR-7 Incident Response Assistance	RackFoundry TSM policies can be defined in accordance with organizational incident handling policies; RackFoundry's SOC utilizes a proven triage processes to review/analyze incidents, determine appropriate responses, and notify users accordingly.

Control Number	Control Description	Related NIST SP 800-53 controls	RackFoundry TSM Ability
3.6.3	Test the organizational incident response capability.	IR-3 Incident Response Testing IR-3(2) Coordinated with related plans	RackFoundry TSM policies can be defined in accordance with organizational incident handling policies; RackFoundry's SOC utilizes a proven triage processes to review/analyze incidents, determine appropriate responses, and notify users accordingly.
Risk Assessment			
3.11.2	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	RA-5 Vulnerability Scanning RA-5(5) Privileged Access	RackFoundry TSM includes an internal Vulnerability Scanner to detect device vulnerabilities.
3.11.3	Remediate vulnerabilities in accordance with assessments of risk.	RA-5 Vulnerability Scanning	RackFoundry TSM's Vulnerability Scanner assesses the severity of each vulnerability and provides steps for remediation.
System and Communications Protection			
3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	SC-7 Boundary Protection SA-8 Security Engineering Principles	RackFoundry TSM includes a VPN, stateful Firewall, Intrusion Prevention/Detection System (IPS/IDS) and Web Application Firewall (WAF) to protect, monitor, and control transmitted information.
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	SC-7(5) Deny By Default / Allow By Exception	RackFoundry TSM's Firewall can be configured with "deny all" policies.
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	SC-8 Transmission Confidentiality and Integrity SC-8(1) Cryptographic or Alternate Physical Protection	RackFoundry TSM includes a site-to-site VPN with multiple encryption algorithms options such as AES-256.

Control Number	Control Description	Related NIST SP 800-53 controls	RackFoundry TSM Ability
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	SC-13 Cryptographic Protection	Data-at-rest is protected using FIPS 140-2 DoD Standards.
3.13.13	Control and monitor the use of mobile code.	SC-18 Mobile Code	RackFoundry TSM monitors mobile code and generates alerts if malicious mobile code is detected.
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	SC-19 Voice over Internet Protocol	RackFoundry TSM monitors VoIP data packets.
3.13.15	Protect the authenticity of communications sessions.	SC-23 Session Authenticity	RackFoundry TSM's VPN utilizes common encryption algorithms such as AES-192 and AES-256 to protect the authenticity of communication sessions.
3.13.16	Protect the confidentiality of CUI at rest.	SC-28 Protection of Information at Rest	Data-at-rest is protected with AES-256 encrypted to FIPS 140-2 DoD standards.
System and Information Integrity			
3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	SI-2 Flaw Remediation SI-3 Malicious Code Protection SI-5 Security Alerts, Advisories, and Directives	RackFoundry TSM provides continuous monitoring and rapid alert notifications to help users address security concerns in a timely manner.
3.14.2	Provide protection from malicious code at appropriate locations within organizational information systems.	SI-2 Flaw Remediation SI-3 Malicious Code Protection SI-5 Security Alerts, Advisories, and Directives	RackFoudry TSM includes an Intrusion Prevention/Detection System (IPS/IDS), Web Application Firewall (WAF) and stateful Firewall to protect against malicious code.
3.14.3	Monitor information system security alerts and advisories and take appropriate actions in response.	SI-2 Flaw Remediation SI-3 Malicious Code Protection SI-5 Security Alerts, Advisories, and Directives	RackFoundry TSM provides actionable alerts when a security threat is detected; RackFoundry has staffed Security Analysts to help determine appropriate response plans.
3.14.4	Update malicious code protection mechanisms when new releases are available.	SI-3 Malicious Code Protection	Threat intelligences feeds utilized within RackFoundry TSM are automatically updated every few minutes.

Control Number	Control Description	Related NIST SP 800-53 controls	RackFoundry TSM Ability
3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	SI-3 Malicious Code Protection	RackFoundry TSM includes an internal Vulnerability Scanner to detect device vulnerabilities.
3.14.6	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI-4 Information System Monitoring SI-4(4) Inbound and Outbound Communications Traffic	RackFoundry TSM deploys in-line with traffic or connects to a mirror port to monitor inbound and outbound communications traffic and detect security threats; RackFoundry TSM also monitors logs and utilizes HIDS agents.
3.14.7	Identify unauthorized use of the information system.	SI-4 Inbound and Outbound Communication traffic	RackFoundry TSM utilizes behavioral monitoring and correlation rules to alert on unauthorized usage. RackFoundry TSM performs reputational analysis of external connections to alert on threats.

RackFoundry TSM effectively addresses the need to protect CUI with real-time, continuous monitoring and advanced threat detection. Additionally, RackFoundry's Security Operations Centers (SOC) are staffed 24/7/365 to provide rapid assistance. We understand that maintaining NIST SP 800-171 is a full-time job and it is our goal to provide customers with the needed security tools and services to effectively and efficiently meet compliance.

About RackFoundry

RackFoundry, the maker of Total Security Management (TSM), is a leader in complete coverage security appliances, secure cloud services and professional services such as SecurityXpert that provides security expertise to organizations of all sizes and industries. The RackFoundry security team, FortressLabs™, help find new vulnerabilities in the wild, mitigate any found vulnerabilities, and head up the RackFoundry Security Operations Center.

For more information visit us at www.rackfoundry.com.