VARONIS

National Institute of Standards and Technology

Special Publication 800-171, Rev. 3:
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Overview of NIST SP 800-171

In 2010, the U.S. government launched a framework of cybersecurity standards to address data security for private contractors. Rather than using the existing National Institute of Standards and Technology (NIST) SP 800-53, which is a series of security controls for internal federal agencies, NIST developed a shorter list of standards for government contractors to abide by, titled "NIST Special Publication (SP) 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." Because federal contractors are likely to process data that the federal government considers controlled unclassified information (CUI), the federal government requires these contractors to protect that data.

While NIST SP 800-171 is based heavily on and is consistent with NIST SP 800-53, private companies are given some flexibility in the actual implementation of the security controls. If contractors are already compliant with the popular ISO 27001 or the Framework for Critical Infrastructure Cybersecurity, it's easy to comply with NIST SP 800-171 as the frameworks are similar in nature. Appendix D of the NIST SP 800-171 standard provides a convenient mapping of the controls in publication to these other data security standards.

How Varonis maps to the NIST SP 800-171 Rev. 3 framework

Here's how Varonis can help organizations achieve data security as expected by NIST SP 800-171:

800-171 Control family	Description	How Varonis helps
3.1 Access Control	**Summary of relevant controls:**	**How Varonis helps:**
3.1.1 Account Management	Organizations must: • **Specify authorized users** of the information system, group and role membership, access authorizations (i.e., privileges), and other attributes (as required) for each account • **Monitor the use of system accounts** and disable accounts when the accounts have expired, been inactive for a defined period of time, the accounts are no longer associated with the user, the accounts are in violation of policy, or significant risks associated with individuals are discovered.	By combining user and group information from Active Directory, Okta, AWS IAM, or other directory services, lightweight directory access protocol, networking information systems, or other directory services, Varonis provides organizations with a comprehensive view of their permissions structures. Both logical and physical permissions are displayed and organized, highlighting and optionally aggregating file system and share permissions. Users can flag, tag, and annotate files, objects, and folders to track, analyze, and report on users, groups, and data. Varonis monitors account activity and can distinguish between privileged and normal users. It also allows for automatic disabling of accounts that have been inactive for a set period of time.
3.1.2 Access Enforcement	Organizations **must enforce approved authorizations** for logical access to information and system resources in accordance with applicable access control policies.	Varonis can restrict access to certain information types, can assert and enforce application access, provides attribute-based access control, defines mechanisms for individual user access to personally identifiable information (PII), and can enable organizations to enforce mandatory and discretionary access control to data. Varonis does this by drawing on user and group information from directory services and automatically (or manually if needed) blocking or allowing access based on organizational access policies.
3.1.5 Least Privilege	The organization must: • Employ the **principle of least privilege**, allowing only authorized system access for users (or	Varonis enables organizations to make intelligent decisions about who needs access to data and who doesn't based on activity and directory services information. Varonis maps granular permissions to

	processes acting on behalf of users) which are **necessary to accomplish assigned organizational tasks**. • **Review the privileges assigned to roles or classes of users** to validate the need for such privileges • **Reassign or remove privileges** as necessary	sensitive data for each user and group and enables you to easily perform regular access reviews to validate the need for such privileges. It provides automated policy enforcement capabilities to automatically enforce least privilege access based on data sensitivity, staleness, location, link type, user, group, and more.
3.1.6 Least Privilege – Privileged accounts	The organization must: • **Require that users (or roles) with privileged accounts use non-privileged accounts** when accessing non-security functions or non-security information	Varonis monitors privileged account activity to identify when privileged accounts are used to access non-security functions and non-security information.
3.1.7 Least Privilege – Privileged Functions	The organization must: • **Prevent non-privileged users from executing privileged functions**. • Log the execution of privileged functions	Varonis can pull in user and group information from directory services to identify users that have admin-like permissions and can perform privileged functions. Varonis monitors all activity in the environment and can log the execution of privileged functions and alert to abnormal privileged activity that could indicate a threat.
3.1.22 Publicly Accessible Content	The organization must: • Train authorized individuals to **ensure that publicly accessible information does not contain CUI**. • **Review the content on publicly accessible systems for CUI** and remove such information, if discovered.	Varonis automatically identifies when CUI is publicly accessible and provides automated remediation policies to continuously remove public exposure of CUI data as it is discovered.
3.2 Awareness and Training	**Summary of relevant controls:**	**How Varonis helps:**
3.2.1 Literacy Training and Awareness	The organization must: • Provide **security and privacy literacy training** to system users on recognizing and reporting indicators of insider threat, social engineering, and social mining.	Our Cyber Resiliency Assessment can help you stress-test your environment by simulating attacks on your regulated data and CUI. In doing so, we can help your security team learn by: • Assessing your threat detection capabilities against modern adversaries • Classifying sensitive data and measuring

		overexposure and non-compliant access • Documenting detection gaps, Zero-Trust posture, and remediation priorities • Preparing and educating your team to handle advanced incidents
3.3 Audit and Accountability	**Summary of relevant controls:**	**How Varonis helps:**
3.3.1 Event Logging	Organizations must: • Specify organization-defined event types for logging within the system	Varonis monitors and maintains a complete and normalized log of data activity, including every authentication, login, open, read, write, share, download, upload, and move. With a unified audit record of all files, objects, SaaS, IaaS, database, email, network, and Directory Services activity, Varonis provides visibility into users' actions across different data repositories. The log can be viewed interactively via email reports or exported via Excel, CSV, or PDF. The audit log is enriched with additional information such as a timestamp, the target of the action, event description, account affiliation Client IP, and country of origin. Varonis maintains the audit trail for 90 days by default, but options to extend are available.
3.3.3 Audit Record Content	Organizations must ensure that audit records contain information that establishes the following: • **What** type of event occurred • **When** the event occurred • **Where** the event occurred • **Source** of the event • **Outcome** of the event • **Identity** of any individuals, subjects, or objects/entities associated with the event • **Provide** additional information for audit records as needed	
3.3.3 Audit Record Generation	Organizations must: • Generate audit records for the selected event types and audit record content specified in 3.3.1 and 3.3.21 • Retain audit records for a time period consistent with the records retention policy	
3.3.5 Review, Analysis, and Reporting	Organizations must: • **Review and analyze** information system audit records • **Report findings** to appropriate personnel. • Analyze and correlate audit records across different repositories to **gain organization-wide situational awareness.**	

3.3.6 Audit Record Reduction and Report Generation	Organizations must: • **Implement an audit record reduction and report generation capability** that supports audit record review, analysis, reporting requirements, and after-the fact investigations of incidents • **Preserve the original content and time ordering of audit records.**	
3.3.7 Time Stamps	Organizations must: • Use internal system clocks to **generate time stamps for audit records**	
3.3.8 Protection of Audit Information	Organizations must: • **Protect audit information and audit logging tools** from unauthorized access, modification, and deletion • **Authorize access to management of audit logging functionality** to only a subset of privileged users or roles	Varonis provides role-based access controls within its platform to restrict the access, modification, and deletion of audit logs to only a subset of users and roles.

3.4 Configuration Management	**Summary of relevant controls:**	**How Varonis helps:**
3.4.2 Configuration Settings	Organizations must **identify, document, and approve any deviations** from established configuration settings.	Varonis continuously monitors security configurations and alerts to deviations from the established configuration settings. It baselines the security posture against common frameworks and regulations including NIST, ISO, and HIPAA to detect configuration drift and potential compliance violations.
3.4.3 Configuration Change Control	Organizations must **monitor and review activities** associated with configuration-controlled changes to the system.	
3.4.4 Impact analyses	Organizations must **verify that the security requirements for the system continue to be satisfied** after the system changes have been implemented.	
3.4.5 Access Restrictions for Change	Organizations must **define, document, approve, and enforce physical and logical access restrictions** associated with system changes.	Varonis maps permissions to storage systems and identifies users that have privileged permissions to make changes to system configurations. This provides

		organizations with the ability to review permissions and enforce logical access restrictions associated with system changes.
3.4.5 Information Location	Organizations must: • **Identify and document the location of CUI** and the system components on which the information is processed and stored • **Document changes to the system or system component** location where CUI is processed and stored	Varonis automatically identifies and classifies CUI data across the organization's data estate, presenting it in an intuitive tree format to clearly indicate its location within the system. Varonis continuously monitors system changes, providing alerts and documentation when modifications in system configuration pose risks to CUI and other sensitive data.

3.6 Incident Response	**Summary of relevant controls:**	**How Varonis helps:**
3.6.1 Incident Handling	Organizations must **implement an incident-handling capability that is consistent with the incident response plan** and includes preparation, detection and analysis, containment, eradication, and recovery.	Varonis' Managed Data Detection and Response (MDDR) service provides a team of in-house cybersecurity analysts that monitor your environment 24x7x365 that can assist in investigating and responding to incidents reported by Varonis alerts. The team can assist with forensic analysis of data breaches, containment, eradication, and recovery, and most importantly, can provides monthly security posture assessments to help train your security team by making recommendations to improve future detection and response. Varonis also provides comprehensive incident reporting capabilities that enable you to identify, track and document security incidents. Alerts can be configured to be automatically sent to organization-defined authorities and other relevant personnel. Our Cyber Resiliency Assessment can help
3.6.2 incident Monitoring, Reporting, and Responsive Assistance	Organizations must: • **Track and document** system security incidents • **Report suspected incidents** to the organizational incident response capability within an organization-defined time period • Report incident information to **organization-defined authorities** • Provide an incident response support resource that **offers advice and assistance to system users on handling and reporting incidents**.	
3.6.3 Incident Response Testing	Organizations must test the effectiveness of the incident response capability.	

3.6.4 Incident Response Training	Organizations must provide incident response training to system users consistent with assigned roles and responsibilities	you stress-test your environment by simulating attacks on your regulated data and CUI. In doing so, we can help your security team learn by: • Assessing your threat detection capabilities against modern adversaries • Classifying sensitive data and measuring overexposure and non-compliant access • Documenting detection gaps, Zero-Trust posture, and remediation priorities • Preparing and educating your team to handle advanced incidents • Provide your team with best practices and tips to enhance your security posture and incident response capabilities.

3.6.5 Incident Response Plan	Organizations must:
	• Develop an incident response plan that
	  ○ Provides the organization with a roadmap for implementing its incident response capability
	  ○ Describes the structure and organization of the incident response capability
	  ○ Provides a high-level approach for how the incident response capability fits into the overall organization
	  ○ Defines reportable incidents
	  ○ Addresses the sharing of incident information, and
	  ○ Designates responsibilities to organizational entities, personnel, or roles.
	• Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing	

3.9 Personnel Security	Summary of relevant controls:	How Varonis helps:
3.9.2 Personnel Termination and Transfer	When **individual employment is terminated**, organizations must: • **Disable system access** within an organization-defined time period • **Terminate or revoke authenticators and credentials** associated with the individual	Varonis offers the capability to automatically disable, suspend, and revoke the permissions of terminated employees. Additionally, it can help adjust the permissions for reassigned or transferred users to ensure their privileges and data access align with their new role.

	When individuals are **reassigned or transferred to other positions** in the organization, organizations must: • **Modify access authorization** to correspond with any changes in operational need	

3.11 Risk Assessment	Summary of relevant controls:	How Varonis helps:
3.11.1 Risk Assessment	The organization must: • Assess the **risk (including supply chain risk) of unauthorized disclosure** resulting from the processing, storage, or transmission of CUI. • **Update risk assessments** at an organization-defined frequency	Varonis continuously monitors your environment, providing live risk assessments to help determine the exposure and risk of your CUI and other sensitive data. Varonis tracks activity to detect unauthorized or risky use of CUI data and alerts to behavior that could indicate a threat. Varonis also continuously assesses the risk of third-party apps connected to your data stores by mapping their permissions and monitoring their activity to identify potential supply chain risks.
3.11.2 Vulnerability Monitoring and Scanning	The organization: • **Monitor and scan the system for vulnerabilities** at an organization-defined frequency and when new vulnerabilities affecting the system are identified • **Remediate system vulnerabilities** within an organization-defined response time	Varonis continuously monitors data repositories and identity management systems to detect misconfigurations and vulnerabilities that could put CUI and sensitive information at risk. Varonis offers automated remediation policies to address the identified issues, aiding in maintaining compliance with NIST SP 800-171 standards.
3.11.4 Risk Response	Organizations must **respond to findings** from security assessments, monitoring, and audits.	Varonis offers automated remediation capabilities designed to address and resolve identified risks. These include revoking excessive privileges, correcting organization-wide and public exposure, disabling inactive privileged accounts, rectifying critical misconfigurations, enforcing data lifecycle requirements, and more.
3.12 Security Assessment and Monitoring	**Summary of relevant controls:**	**How Varonis helps:**
3.12.1 Security Assessment	Organizations must **assess the security requirements for the system and its operating environment** at a frequency defined by the organization to determine whether the requirements have been	Varonis continuously monitors your environment, providing a real-time view of your security posture. This allows you to identify where CUI and other sensitive data are at risk due to excessive access or

	satisfied.	misconfigurations. Varonis monitors activity in near-real time to detect unauthorized or risky use of CUI data and alerts you to behavior that may indicate a potential threat. Varonis collaborates with its clients to develop an action plan, set milestones, and establish security objectives. We conduct quarterly business reviews and office hours with our clients to assess progress toward security milestones and offer recommendations for improving their security posture and achieving their security goals.
3.12.02 Plan of Action and Milestones	Organizations must **develop a plan of action and milestones** for the system: • To **document the planned remediation actions** to correct weaknesses or deficiencies noted during security assessments and • To **reduce or eliminate** known system vulnerabilities	
3.12.3 Continuous Monitoring	Organizations must **develop and implement a system-level continuous monitoring strategy** that includes ongoing monitoring and security assessments.	
3.13 System and Communications Protection	• **Summary of relevant controls:**	**How Varonis helps:**
3.13.4 Information in Shared System Resources	Organizations must **prevent unauthorized and unintended information transfer** via shared system resources.	Varonis offers advanced threat detection capabilities by leveraging behavioral-based alerting to identify both internal and external threats automatically. Varonis provides proactive alerts regarding potential risks to your data, such as unusual access to sensitive information, attempts at privilege escalation, or atypical file upload/download activities. Varonis effectively prevents malicious actors from exfiltrating, deleting, or altering your data in real time by implementing automated responses.
3.14 System Information Integrity	**Summary of relevant controls:**	**How Varonis helps:**
3.14.03 Security Alerts, Advisories, and Directives	Organizations must: • **Receive system security alerts, advisories, and directives** from external organizations on an ongoing basis. • **Generate and disseminate** internal system security alerts, advisories, and directives, as necessary.	Varonis continuously updates its expert-built threat detection policies as new threats emerge to ensure that your critical data remains secure.
3.14.6 System Monitoring	Organizations must: • Monitor the system to **Detect attacks and indicators of compromise** • Identify **unauthorized use** of the	Varonis monitors VPN, DNS, firewall, and web activity in context with data, email, and identity behaviors to provide an expanded field of vision to help catch, investigate, and stop threats before they can access or steal data. By leveraging

	system • Monitor inbound and outbound communications traffic **to detect unusual or unauthorized activities** or conditions	advanced user and entity behavior analytics, Varonis detects anomalous activities at the network perimeter, such as traffic to malicious sites, unusual VPN access, or DNS tunneling. Varonis is instrumental in preventing data exfiltration, malware infiltration, and other security threats. Varonis' Managed Data Detection and Response (MDDR) team will monitor your environment 24x7x365 to detect unusual or unauthorized activities. Our world-class team of elite threat hunters, forensic analysts, and incident responders will help triage, investigate, and respond to the threats.
3.14.8 Information Management and Retention	The organization must **manage and retain CUI within the system, and CUI output from the system** in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	Varonis enables you to create custom policies that enforce the lifecycle, retention, and residency requirements of CUI data in accordance with applicable laws and guidelines. It identifies data that falls within these policies — such as stale CUI data — and automatically moves it to secure a location for archival or deletion.
3.17 Supply Chain Risk Management	**Summary of relevant controls:**	**How Varonis helps:**
3.1.17 Supply Chain Requirements and Processes	The Organization must: • Establish a process for **identifying and addressing weaknesses or deficiencies in the supply chain** elements and processes. • Enforce the following security requirements to **protect against supply chain risks** to the system, system components, or system services and to limit the harm or consequences from supply chain-related events.	Varonis continuously identifies and assesses the risk of third-party apps connected to your data stores by mapping their permissions and monitoring their activity to help identify potential supply chain risks. Varonis can then enable organizations to terminate connections to risky third-party apps, either by user or the entire environment.

Ready to experience the Varonis difference

Reduce your risk without taking any. Contact our team to learn what will be covered in your free data risk assessment.

Contact us

About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data: sensitive files and emails; confidential customer, patient, and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects cyber threats from both internal and external actors by analyzing data, account activity, and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation.

Varonis products address additional important use cases including data protection, data governance, Zero Trust, compliance, data privacy, classification, and threat detection and response. Varonis started operations in 2005 and has customers spanning leading firms in the financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education sectors.