PKWARE®

SOLUTION SHEET

CONTROLLED UNCLASSIFIED INFORMATION

MEET NIST 800-171 AND CMMC REQUIREMENTS WITH PKWARE

Organizations that do business with the federal government often store, process, and transmit sensitive information. In many cases, this information is not considered classified, but still requires protection against loss, theft, or inappropriate access.

NIST Special Publication 800-171 provides standards for ensuring the security and confidentiality of "controlled unclassified information" (CUI) when shared with nonfederal organizations. The Cybersecurity Maturity Model Certification (CMMC) measures the ability of vendors and their supply chains to protect CUI and Federal Contract Information (FCI).

Organizations that handle CUI and FCI can use PKWARE's automated data security technology to meet a wide range of requirements for data protection, access control, and reporting.

AUTOMATED, DATA-CENTRIC SECURITY

PKWARE simplifies compliance with NIST 800-171 requirements, as well as other government and industry mandates.

PKWARE's data-centric technology makes it possible to maintain control over sensitive data even in the most complex use cases. Our platform provides an array of integrated capabilities, designed for maximum flexibility and ease of use.

- Administrators use the PKWARE Enterprise Manager console to define data discovery, data classification, and data protection policies.
- PKWARE endpoint agents monitor file activity on laptops, desktops, and servers. New and modified files are scanned for data that meet's the organization's definition of sensitive information.
- Files containing sensitive data can be classified, encrypted, redacted, moved, or deleted based on company policy.
- Additional PKWARE components extend the organization's policy enforcement to mainframe and midrange systems, mobile devices, and proprietary applications.

PKWARE'S APPROACH TO COMPLIANCE

Data security mandates like NIST 800-171 are complex and multi-faceted, requiring the efforts of multiple departments within an organization, along with multiple vendors, partners, and advisors.

PKWARE strives to simplify compliance by providing a wide range of capabilities within a single data security platform.

Our automated, data-centric technology allows organizations to protect sensitive data on every enterprise operating system, and to create tailored workflows that meet their unique security and compliance needs.

Companies can use PKWARE to meet a variety of NIST 800-171 standards and achieve the desired CMMC maturity level. PKWARE solutions can be used to address requirements for data classification, data protection, encryption key management, and activity logging.

PKWARE's technology is also designed to fit easily into your organization's IT and security ecosystem, simplifying implementation and aiding in compliance with requirements in other functional areas such as user authentication, network security, and employee training.

MEETING NIST 800-171 STANDARDS WITH PKWARE

NIST 800-171 REQUIREMENTS	PKWARE CAPABILITIES

3.1 ACCESS CONTROL

- **3.1.1** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)
- **3.1.2** Limit system access to the types of transactions and functions that authorized users are permitted to execute
- **3.1.3** Control the flow of CUI in accordance with approved authorizations
- **3.1.4** Separate the duties of individuals to reduce the risk of malevolent activity without collusion
- **3.1.5** Employ the principle of least privilege, including for specific security functions and privileged accounts
- **3.1.19** Encrypt CUI on mobile devices and mobile computing platforms

ENCRYPTION & KEY MANAGEMENT

PKWARE automatically detects and encrypts files containing sensitive data (as defined by organizational policy).

- Files can be encrypted using different keys (with access granted to different users or groups) based on file contents, file type, file location, or other criteria.
- Through integration with Outlook, PKWARE can detect and encrypt sensitive data in outgoing email messages and attachments.
- Access to encryption keys is managed at the organizational level, ensuring that the company maintains visibility and control over CUI and FCI at all times.
- PKWARE can encrypt and decrypt data on every enterprise operating system, including servers, endpoints, and mobile devices.

POLICY MANAGEMENT & ADMINISTRATION

The PKWARE Enterprise Manager provides a role-based administration console to manage data security activity across the organization.

Administrative functions can be configured to preserve separation of duties. For example, security administrators can create encryption keys based on AD groups, which are managed separately by AD administrators.

3.1 AUDIT AND ACCOUNTABILITY

- **3.3.1** Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity
- **3.3.2** Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions
- **3.3.5** Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity
- **3.3.6** Provide audit record reduction and report generation to support on-demand analysis and reporting
- **3.3.8** Protect audit information and audit logging tools from unauthorized access, modification, and deletion

REPORTING

PKWARE's Data Security Intelligence reporting capabilities allow security teams and audit personnel to monitor data discovery, classification, and encryption activity across the organization.

- Activity logs indicate which files are protected, where the files are stored, and which users have accessed them
- Administrators can filter reporting data by time and event type, and search for specific terms within event logs
- Output can be viewed directly, picked up via SIEM agent, or retrieved via API
- Activity logs cannot be altered

NIST 800-171 REQUIREMENTS	PKWARE CAPABILITIES
3.4 CONFIGURATION MANAGEMENT • **3.4.2** Establish and enforce security configuration settings for information technology products employed in organizational systems • **3.4.3** Track, review, approve or disapprove, and log changes to organizational systems	**ADMINISTRATION** The PKWARE Enterprise Manager provides granular capabilities for configuring security policies and administrative settings. Policy changes can be configured to require review and approval by a second administrator prior to implementation.
3.8 MEDIA PROTECTION • **3.8.1** Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital • **3.8.2** Limit access to CUI on system media to authorized users • **3.8.4** Mark media with necessary CUI markings and distribution limitations • **3.8.6** Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards • **3.8.9** Protect the confidentiality of backup CUI at storage locations	**ENCRYPTION & KEY MANAGEMENT** PKWARE applies persistent AES-256 encryption to files containing CUI, FCI, and other sensitive data. Once encrypted, files remain inaccessible to unauthorized users at rest and in transit. Encryption can be used to protect data on endpoints, servers, removable storage devices, and backup media, as well as in the cloud. **DATA CLASSIFICATION** PKWARE Data Classification applies visual labels and metadata tags to files containing sensitive data. Visual markers alert users to a file's proper handling, and metadata tags can be used to facilitate action by DLP or other security technology.
3.9 PERSONNEL MANAGEMENT • **3.9.2** Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers	**POLICY MANAGEMENT** Access to encryption keys (and encrypted CUI or FCI) can be automatically revoked when a user's Active Directory credentials are suspended or removed. Administrators can also revoke access manually as needed.
3.13 SYSTEM AND COMMUNICATIONS PROTECTION • **3.13.2** Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems • **3.13.8** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards • **3.13.10** Establish and manage cryptographic keys for cryptography employed in organizational systems • **3.13.16** Protect the confidentiality of CUI at rest	**APPLICATION PROGRAMMING INTERFACES** PKWARE's Software Development Kit and command line interfaces provide the means for data protection capabilities to be built into applications and repeatable processes. **ENCRYPTION & KEY MANAGEMENT** PKWARE uses strong, FIPS-validated encryption to protect CUI and FCI at rest and in transit. PKWARE leverages existing encryption key stores and also provides its own key management system. Additionally, the PKWARE appliance can create and store crypto keys in a FIPS 140-2 level 3 HSM.

PKWARE®

A global leader in enterprise data protection, PKWARE provides solutions for more than 35,000 customers around the world. Having introduced the ZIP file (the world's most widely used data compression standard) thirty years ago, PKWARE continues to innovate, helping organizations meet ever-evolving challenges in data protection and file management.

PKWARE solutions help organizations eliminate security gaps, manage sensitive data, and meet their data compliance goals. Our automated, data-centric security technology allows companies to ensure that their sensitive data is always protected according to organizational policy.

POLICY MANAGEMENT

The PKWARE Enterprise Manager allows administrators to define and apply data security policies across the entire organization.

DATA DISCOVERY

PKWARE detects sensitive data as soon as it appears on laptops, desktops, and servers, and enables automated rule-based action.

DATA CLASSIFICATION

PKWARE can apply metadata tags and visual labels to increase user compliance and facilitate policy-based remediation.

DATA PROTECTION

PKWARE secures sensitive data against unauthorized use through encryption, redaction, quarantine, or deletion.

REPORTING

Administrators can monitor activity in real time and demonstrate compliance with internal policies and external mandates.