DropSecure
Encrypt. Protect. Prevent

Meet and exceed CMMC requirements for secure file transfer

DropSecure CMMC practice support checklist

CMMC Practice	Description	How DropSecure helps with compliance
Access Control (AC)		
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Only authorized recipients get access to documents. Even DropSecure cannot access your documents, allowing you to achieve the highest compliance possible.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	We have extensive roles based access control (RBAC) so only authorized users can execute.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.	Yes, only privileged accounts have access to security functions.
AC.2.005	Provide privacy and security notices consistent with applicable CUI rules.	Yes. All end users are notified of changes
AC.2.007	Employ the principle of least privilege, including for specific security functions andprivileged accounts.	Everything is private by default and only accessible by authorized recipients.
AC.2.009	Limit unsuccessful login attempts.	This policy is configurable. Account administrator can determine how many unsuccessful attempts are allowed before locking the account.
AC.2010	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	After the session timeout, users will need to re-authenticate
AC.3.012	Protect wireless access using authentication and encryption.	Regardless of the transport mode everything is protected via authentication and encryption
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Yes, all data and documents, even filenames are encrypted with AES-256 based symmetric encryption and the keys are then protected by Asymmetric encryption.
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Yes, administrators can define different roles and access levels for CUI, reducing the risk of collusion.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Yes, any functions not accessible are protected and reported in logs
AC.3.019	Terminate (automatically) user sessions after a defined condition.	Yes, sessions are automatically terminated after a default 30 mins of inactivity.

DropSecure CMMC practice support checklist

CMMC Practice	Description	How DropSecure helps with compliance
Audit and Accountability (AU)		
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	Each user gets a unique ID and all actions are tracked
AU.2.042	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.	All audit activity is available online. Administrators have full visibility of all account activity.
AU.2.043	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	All times are recorded in UTC and can be converted to the user's local time zone when needed.
AU.2.044	Review audit logs	The DropSecure platform enables system administrators and CUI managers to review logged events. The logs cannot be deleted or modified.
AU.3.045	Review and update logged events	The logs can be reviewed but not updated or deleted.
AU.3.046	Alert in the event of an audit logging process failure.	To be implemented
AU.3.048	Collect audit information (e.g., logs) into one or more central repositories.	DropSecure can push the logs to your SIEM systems
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Logs are only viewable by Administrators and CUI managers.
AU.3.050	Limit management of audit logging functionality to a subset of privileged users.	Logs in DropSecure platform are protected from editing and deletion
AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Logs can be exported to a SIEM system for further analysis and correlation with other events.
AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting.	Logs can be exported to a SIEM system for further analysis and correlation with other events.

DropSecure CMMC practice support checklist

CMMC Practice	Description	How DropSecure helps with compliance
Security Assessment (CA)		
CA.2.157	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	DropSecure's government solution runs on AWS government infrastructure which is SOC compliant.
CA.2.158	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	DropSecure continuously monitors its services and they are running on AWS government cloud which is SOC compliant.
CA.2.159	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	DropSecure continuously monitors its services and they are running on AWS government cloud which is SOC compliant.
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	DropSecure continuously monitors its services and they are running on AWS government cloud which is SOC compliant.
CA.3.162	Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.	DropSecure continuously monitors its services and they are running on AWS government cloud which is SOC compliant.
CA.4.163	Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement.	DropSecure continuously monitors its services and they are running on AWS government cloud which is SOC compliant.

DropSecure CMMC practice support checklist

CMMC Practice	Description	How DropSecure helps with compliance
Configuration Management (CM)		
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	DropSecure can provide the configuration information for its government cloud.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	DropSecure employs extensive RBAC (role based access controls) to provide only the required access to necessary individuals
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	DropSecure employs extensive RBAC (role based access controls) to provide only the required access to necessary individuals
CM.2.066	Analyze the security impact of changes prior to implementation.	Any changes go through extensive testing and security assessment.
Systems and Communications Protection (SC)		
SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Yes, we use AES-256 encryption which is FIPS 140-2 validated.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards	All data and documents, even filenames, are encrypted with AES-256 based symmetric encryption and the keys are then protected by asymmetric encryption.
SC.3.190	Protect the authenticity of communications sessions.	All exchanges happen via SSL
SC.3.191	Protect the confidentiality of CUI at rest.	Due to our end-to-end encryption, data is protected at rest by default.