



Information Classification Standard

DOC-IT-IS-8-2
Revision 1.1
November 1, 2025

REVISION HISTORY

This revision history lists all changes to this document, the date of each revision, and the reason for each revision.

<u>Rev.</u>	<u>Rev. Date</u>	<u>Revision Description</u>
1.0	November 1, 2022	<i>Initial Version</i>
1.1	November 1, 2025	<i>Updated data classifications, added PHI and government data classifications such as FCI and CUI</i>

Table of Contents

1.0 Security Standard – Information Classification	4
1.0.1 Executive Summary	4
1.0.2 Purpose.....	4
1.0.3 Scope	4
1.1 Information Classification Standards	5
1.2 Commercial Information Classification Definitions.....	6
1.3 Government Information Classification Definitions.....	7
1.4 Commercial Information Labeling Standards.....	8
1.5 Government Information Labeling Standards.....	10
1.6 Commercial Information Handling Standards.....	11
1.7 Government Information Handling Standards.....	14
1.8 Encryption Standards.....	15
1.9 Definitions and Terms	16

1.0 Security Standard – Information Classification

1.0.1 Executive Summary

Information classification is the process in which the organization assesses the data that they hold and the level of protection it should be given. Information classification also includes labeling and handling requirements. RXO classifies commercial data as Public, Internal, Proprietary, and Confidential.

Certain commercial information (non-Government information) may also have legal labeling and handling requirements that must be followed, such as for Personally Identifiable Information (PII) or Protected Health Information (PHI) and must always be classified as Confidential. Labeling, handling, and other restrictions for PHI are regulated by the Health Insurance Portability and Accountability Act (HIPAA).

RXO also follows Government classification standards for Government or National Defense information, to include Public, Federal Contract Information (FCI), and Controlled Unclassified Information (CUI). CUI may be CUI Basic or CUI Specified. RXO must follow the labeling, handling, and other restrictions of the International Traffic in Arms Regulations (ITAR) for any items on the United States Munitions List (USML).

Risk	No Risk	Low Risk	Medium Risk	High Risk
Commercial Data	Public	Internal (Sensitive)	Proprietary (Private)	Confidential
Government Data	Public	Non-Public Unclassified	Controlled Unclassified Information (CUI)	Classified Information
	Public Information	Federal Contract Information (FCI)	CUI Basic	CUI Specified
Export Information				Export Controlled
				EAR, ITAR (CUI SP EXPT), NOFORN

1.0.2 Purpose

The purpose of this policy is to establish an enterprise-wide approach for the consistent handling of all Company Information with respect to security, access, confidentiality, and conformity with contracts, local, state, federal, and international law, and the Company's Code of Business Ethics.

1.0.3 Scope

This policy applies to all RXO entities, employees, contractors, consultants, temporary workers, and third-party partners. This policy covers all Company Information which includes, but is not limited to, Company and customer information regardless of the form it may take (e.g., text, graphics, video, voice, etc.) or the media on which it resides (e.g., paper, electronic, portable media).

Systems or processes that cannot comply with these standards require an exception from the Global Security Office.

1.1 Information Classification Standards

- All Company Information must be classified, protected, and destroyed in accordance with this Information Classification Standard.
- Information owners are responsible for classifying the information in their data information repositories.
- Information that has not yet been classified must be treated as Confidential. See Information Classification Definitions below.
- Information must be protected and handled in accordance with its classification. See Information Handling Standards below.
- The classification and handling of duplicated, printed, copied, or reproduced information must remain consistent with the original information.
- Information containing differing Classification Levels must be classified at the most restrictive applicable Classification Level.
- Deployment and use of encryption technologies (encryption algorithms, encryption keys, digital signatures, and digital certificates) in accordance with this standard must be approved by the Global Security Office (gso@RXO.com) and must follow the Company Cryptography Policy. The export of encryption technologies is regulated by U.S. and international laws. Contact the Legal Department with questions regarding legal restrictions.

1.2 Commercial Information Classification Definitions

RXO uses four levels of Information Classification for Commercial Information: Public, Internal, Proprietary, and Confidential. The table below defines these levels and provides examples.

	PUBLIC	INTERNAL	PROPRIETARY	CONFIDENTIAL
Definition	Information that has been publicly released and can be disclosed	Information that is intended to be generally available within the Company but not publicly released	- Information that is protected by legal or contractual obligations - Information that if exposed to any security risk or otherwise disclosed, would violate International, federal, state or local law - Information to which internal access is restricted to a limited group of authorized individuals (need to know) - Company information of a non-confidential or non-sensitive nature that is shared externally if there is an authorized business requirement	- Information for which disclosure could result in significant financial loss, legal liability, or impair the Company's ability to conduct business - Optional Data Sub-classes are Financial, Legal, PHI, and PII
Examples	- Press releases - Marketing materials - Public filings (e.g., annual reports) - External websites	- Communications of a non-restricted or non-sensitive nature - Internal budget information - Income and expense statements - Accounts Receivable and Accounts Payable reports - Company Policies - Operational process documentation - Organizational Charts - Company Phone Directory	- Non-personally identifiable payroll information - Confidential customer information - Company intellectual property - Contracts - Employee dispute information	- All personally identifiable information about employees and customers (e.g., Social Security Numbers / National ID's, credit card numbers, bank account numbers, drivers' license numbers, etc.) - Protected health information - Information regarding Company strategic initiatives (e.g., potential merger/acquisition information) - Government investigation information - Attorney/client privileged information - Pre-release financial information
Risk	No Risk	Low Risk	Medium Risk	High Risk

1.3 Government Information Classification Definitions

RXO follows the appropriate categories of Government Information Classification: Public, FCI, CUI BASIC, and CUI SPECIFIED. The table below defines these levels and provides examples.

	PUBLIC	FCI	CUI BASIC	CUI SPECIFIED
Definition	Information that has been publicly released and can be disclosed	Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.	Government created or owned UNCLASSIFIED information, or information that an entity creates for or on behalf of the Government, that a law, regulation or policy requires or permits an agency to handle using safeguarding or dissemination controls. Protection may be required for national defense, privacy, law enforcement, contractual protections, or other reasons.	CUI where laws, Federal regulations, and Government-wide policies that authorize that category require safeguards different from the safeguards established for CUI Basic in 32 CFR 2002.14(c).
Examples	- Press releases - Marketing materials - Public filings (e.g., annual reports) - External websites	- Emails transmitted from the DoD to the defense contractor (and vice versa) - Subcontracts and policies needed by the defense contractor - Information garnered as a result of instant messaging, video conferencing, etc. with the DoD - Workflows and processes needed to fulfill the terms of the DoD contract	- PII, or Personally Identifiable Information - PII of military vendors, customers, bases, etc. - DoD Controlled Technical Information - Critical Infrastructure and DoD Critical Infrastructure - Nuclear Information - Intelligence information - Patent, Legal or Law Enforcement Information - Complete List can be found at https://www.dodcui.mil/	- Export Administration Regulations (EAR) - Export controlled information covered under the US Commerce Control List. - International Traffic in Arms Regulations (ITAR) - Export controlled information covered under the US Munitions List - Not Releasable to Foreign Nationals (NOFORN) - Export controlled information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-US citizens
Risk	No Risk	Low Risk	Medium Risk	High Risk

1.4 Commercial Information Labeling Standards

Information classified as Proprietary or Confidential must be labeled as described in the table below.

	PUBLIC	INTERNAL	PROPRIETARY	CONFIDENTIAL
Mailing / Shipping	None	None	Mark envelope/container "RXO Proprietary"	Mark envelope/container "RXO Confidential" Optional sub-class may also be added. Eg. "RXO Confidential - PII"
Facsimile (FAX)	None	None	Mark cover sheet "RXO Proprietary"	Mark cover sheet "RXO Confidential" Optional sub-class may also be added. Eg. "RXO Confidential - PHI"
Printed	None	None	Ensure that printed material is marked "RXO Proprietary" on the title page, document footers, watermark, or file name.	Confidential documents should not be printed if possible. If documents must be printed ensure that printed material is marked "RXO Confidential" on the title page, document footers, watermark, or file name. Optional sub-class may also be added. Eg. "RXO Confidential - PII"
Electronic Storage (Unstructured)	None	None	Ensure that electronic documents are marked "RXO Proprietary" on the title page, document footers, watermark, or file name.	Ensure that electronic documents are marked "RXO Confidential" on the title page, document footers, watermark, or file name.
Electronic Storage (Structured)	None	None	Proprietary Information in structured data sources such as databases must be documented and kept up to date.	Confidential Information in structured data sources such as databases must be documented and kept up to date.
Electronic Mail	None	None	Ensure that email with Proprietary content, including attachments, are marked "RXO Proprietary" in the Subject Line.	Confidential Information should not be emailed if possible. If Confidential Information must be emailed, ensure that email with Confidential content, including attachments, are marked "RXO

				Confidential” in the Subject Line. Optional sub-class may also be added. Eg. “RXO Confidential – PHI”
Electronic Display	None	None	If feasible mark displayed data as “RXO Proprietary”	If feasible mark displayed data as “RXO Confidential”
Removable Media	None	None	See Electronic Storage (Unstructured) and (Structured)	See Electronic Storage (Unstructured) and (Structured)

1.5 Government Information Labeling Standards

Information classified as FCI or CUI must be labeled according to the latest Federal regulations as described in the table below.

PUBLIC	FCI	CUI BASIC	CUI SPECIFIED
None	FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems	- CUI Registry, https://www.dodcui.mil/Home/Policy/ 32 CFR 2002.20, Marking CUI - DoDI 5200.48 - DoDI 5200.01	- CUI Registry https://www.dodcui.mil/Home/Policy/ 32 CFR 2002.20, Marking CUI - DoDI 5200.48 - DoDI 5200.01

1.6 Commercial Information Handling Standards

Documents				
	PUBLIC	INTERNAL	PROPRIETARY	CONFIDENTIAL
Mailing / Shipping	None	Seal envelope or container	- Seal envelope/container - Use dual containers and mark internal envelope or container "RXO Proprietary"	- Seal routing envelope/container - Use dual containers and mark internal envelope/container "RXO Confidential" - Encrypt electronic information according to electronic storage handling guidelines in this document - For shipments outside the company, use Registered Mail or follow shipping company guidelines for shipping sensitive information
Facsimile (FAX)	None	None	Mark cover sheet "RXO Proprietary"	Confidential documents should not be faxed if at all possible. If FAX must be used: - Mark cover sheet "RXO Confidential" - Sender and receiver must be at their respective FAX machine until transmission is complete unless the receiving FAX machine is in a secured area - For Faxes sent on a regular basis to the same number, program the receiving number into the FAX machine - If feasible configure the FAX machine so that received Faxes are printed face down
Printed	None	If feasible, print documents face down and retrieve documents from printer without delay	- Ensure that printed material is marked "RXO Proprietary" - Use pull or PIN controlled printing if available - If pull or PIN controlled printing is not available, print documents face down (if feasible) and retrieve from printer without delay	Confidential documents should not be printed if at all possible. If documents must be printed: - Ensure that printed material is marked "RXO Confidential" (with optional subclass) - Use pull or PIN controlled printing if available; If pull or PIN controlled printing is not available, print documents face down (if feasible) and retrieve documents from printer without delay - After printing, use black permanent marker to redact confidential information not required for the business purpose
Document Destruction	None	Dispose of in an RXO controlled facility	Cross-cut shred or deposit in locked shred bin	Cross-cut shred or deposit in locked shred bin

Document Storage	None	- Internal Use: May leave unattended in a secured RXO facility - External Use: Documents must remain in the control of the entrusted individual or party.	- Information must remain in the control of the individual or party to whom it was entrusted - Documents must be locked up when unattended - Limit access to those with a "need-to-know"	- Information must remain in the control of the individual or party to whom it was entrusted - Documents must be locked up when unattended - Limit access to those with a "need-to-know"
-------------------------	------	---	--	--

Electronic Information				
	PUBLIC	INTERNAL	PROPRIETARY	CONFIDENTIAL
Electronic Storage	None	- External Use: - Information must remain in the control of the individual or party to whom it was entrusted - Information on portable devices must be encrypted and portable devices must be locked and out of sight when unattended	- Limit access to those with a “need-to-know” - Information must remain in the control of the individual or party to whom it was entrusted - Information on portable devices must be password protected, encrypted at rest, and portable devices must be locked and out of sight when unattended	- Limit access to those with a “need-to-know” - Information must remain in the control of the individual or party to whom it was entrusted - Information on portable devices must be password protected, encrypted and portable devices must be locked and out of sight when unattended - Encrypt information while at rest, implement access control auditing and disallow administrator access.
Electronic Transfer	None	Verify recipient's “need-to-know” prior to transfer	- Verify recipient's “need-to-know” prior to transfer - For external communications, encrypt or use a secure transmission method if practical; communicate encryption credentials on a different channel (e.g. by phone or text).	- Verify recipient's “need-to-know” prior to transfer - For external communications, the use of encryption and/or a secure transmission method is required; communicate encryption credentials on a different channel (e.g., by phone or text).
Electronic Destruction	None	Ensure proper deletion and destruction of electronic information	Ensure proper deletion and destruction of electronic information. Refer to IT Asset Disposal Standard for more information.	Ensure proper deletion and destruction of electronic information. Refer to IT Asset Disposal Standard for more information.
Electronic Display	None	Information should be displayed only with RXO employees or third parties who have executed an NDA	- Information should be displayed only with those with a “need-to-know” or with third parties who have executed an NDA - If feasible, mark displayed data as “RXO Proprietary”	- Information should be displayed only with those with a “need-to-know” or with third parties who have executed an NDA - If feasible, redact PII and other confidential information to avoid inadvertent disclosure - If feasible, mark displayed data as “RXO Confidential” (with optional subclass)

1.7 Government Information Handling Standards

Government Information must be protected and handled in accordance with its classification and all applicable and regulations. Most handling requirements can be found in various Executive Directives, the code of Federal Regulations (CFR), the Department of Defense Issuances (DoDI), the Federal Acquisition Regulation (FAR), and the Defense Federal Acquisition Regulation Supplement (DFARS). See table below for the most common Government Information handling requirements.

	PUBLIC	FCI	CUI BASIC	CUI SPECIFIED
Handling Regulations	None	FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.	- DoDI 5200.48, Controlled Unclassified Information (CUI) 32 CFR 2002, Controlled Unclassified Information CUI - FAR 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities - DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting - DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements - DFARS 252.204-7020, NIST SP 800-171 DoD Assessments - DFARS 252.204-7021, Cybersecurity Maturity Model Certification (CMMC) Requirements - The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations	- CUI Registry, https://www.dodcui.mil/Home/Policy/ - DoDI 5200.48, Controlled Unclassified Information (CUI) 32 CFR 2002, Controlled Unclassified Information CUI - ITAR: 22 CFR 120-130 - EAR: 15 CFR 730-774

1.8 Encryption Standards

The following algorithms and key lengths are approved for encryption.

Symmetric Key Encryption and Decryption

- AES
- TDEA (Triple-DES, TDES, 3DES)
- SKIPJACK is approved for decryption only.

Digital Signatures

- DSA
- RSA
- Elliptic Curve DSA (ECDSA)

Hash Standards

- SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256

Message Authentication

- AES
- HMAC

Key Length

- Symmetric key lengths of at least 128 bits.
- Elliptic curve key lengths of at least 160-224 bits.
- RSA key lengths of at least 1248-2048 bits. In particular, the CA/Browser Forum Extended Validation (EV) Guidelines require a minimum key length of 2048 bits. Also, current research shows that factoring a 1024-bit RSA modulus is within practical reach.
- DSA key lengths of at least 2048 bits.

1.9 Definitions and Terms

FCI	Federal Contract Information
CUI	Controlled Unclassified Information
PII	Personally Identifiable Information
PHI	Protected Health Information
HIPAA	Health Insurance Portability and Accountability
DoD	Department of Defense
CFR	Code of Federal Regulations
EAR	Export Administration Regulations
ITAR	International Traffic in Arms Regulations
NOFORN	Not Releasable to Foreign Nationals
NDA	Non-Disclosure Agreement
FAR	Federal Acquisition Regulation
DFARS	Defense Federal Acquisition Regulation Supplement
NIST	National Institute of Standards and Technology
SP	Special Publication
DoDI	Department of Defense Issuances (or Instruction)
CMMC	Cybersecurity Maturity Model Certification
AES	Advanced Encryption Standard
TDEA	Triple Data Encryption Algorithm
DSA	Digital Signature Algorithm
RSA	Rivest-Shamir-Adleman cryptography algorithm
SHA	Secure Hash Algorithms
HMAC	Hash-based Message Authentication Code
CA	Certification Authority

Certificate of Review

Information Classification Standard

December 18th 2025 11:00:40 am

Name	Job title	Stakeholder type	Action	Timestamp
Mark Gutman		Policy Owner	Submitted	Friday, November 21, 2025 10:11 AM EST
Faisal Khan		Policy Approver	Approved	Tuesday, December 2, 2025 11:26 AM EST
Mark Gutman		Policy Admin	Published	Thursday, December 18, 2025 11:00 AM EST