CONTOSO Inc.

Contoso, Inc Information Classification and Handling Standard

31-Dec-2020

Version 5.6

Proprietary statement

Published by Contoso, Inc.

Document information

Document title	Contoso, Inc Information Classification and Handling Standard
Document owner	Chief Information Security Officer
Review cycle	Annual

Document revision history

Date	Description	Version	Author
8-Mar-2012	New document. This is the system content that was formerly in the Sensitive Information Policy	4.0	Stakeholder name
9-Jul-2013	Annual review.	4.1	Stakeholder name
28-Jan-2016	Annual review.	4.2	Stakeholder name
18-Mar-2016	Annual review.	4.3	Stakeholder name
30-May-2017	Updating to new template.	4.4	Stakeholder name
15-Mar-2018	Revised document to be in line with SAP information classification document. In particular, the document was refocused to address GDPR needs for handling PII. Added new company logo.	5.0	Stakeholder name
04-Jun-2018	Updated company name to Contoso, Inc. Incorporated reviewer information.	5.1	Stakeholder name
10-Aug-2018	Minor change to approval table format	5.2	Stakeholder name
06-Dec-2018	Changed doc ID; minor edits.	5.3	Stakeholder name
17-Apr-2020	Added line to section 1.4, Responsibilities	5.4	Stakeholder name
17-Jul-2020	Added PCI info.	5.5	CISO name
2-Nov-2020	Merged PS and CTE	5.6	CDT

Table of contents

Proprietary statement 2

Document revision history 3

1 Information classification and handling standard 5

1.1 Introduction 5

1.2 Summary 5

1.3 Scope 5

1.4 Responsibilities 5

2 Information identification 6

2.1.1 Asset identification and authentication standard 6

2.2 Asset identification 7

2.2.1 Asset classification 7

2.2.2 Information Asset Classification Categories 7

3 Information handling 12

4 Notification 15

5 Public Sector information 15

5.1 Access to CUI information 15

5.2 Marking CUI information 15

5.3 Transmission of CUI documents 16

5.4 Email transmission of CUI information 16

5.5 Distribution of CUI documents 17

5.6 Handling and storing of CUI information 17

5.7 Reporting CUI incidents 17

5.8 CUI references 17

NIST SP 800-171 Appendix D: 17

1 Information classification and handling standard

1.1 Introduction

At Contoso, Inc, information is collected and processed to deliver services to clients, hire employees, and develop intellectual capital, products, and services. These information resources, both physical and electronic, can be critical assets and have varying degrees of sensitivity. Thus, they require appropriate protection mechanisms and procedures.

1.2 Summary

An information asset includes both documents and data, whether physical or electronic (such as paper documents stored in file cabinets, electronic documents stored on a computer, or data in a database), that are used for a business purpose. This standard provides the criteria and requirements for classifying and handling information assets based on their sensitivity and the level of risk that may result if the information asset were to be inappropriately used, lost, disclosed, modified, or accessed by an authorized or unauthorized party. The standard enables Contoso, Inc employees to:

- Recognize the sensitivity of information assets and associate the information to one of three categories in use for all environments--**Confidentia**l, **Internal Use,** or **Public—**or the additional category of **Controlled Unclassified Information (CUI)** in use in our Public Sector environments.
- Apply appropriate handling and security controls to protect information proportionate to its sensitivity level.

1.3 Scope

This standard is globally applicable, and the requirements extend to all Contoso, Inc business units, employees, contract workers, consultants, and temporary employees.

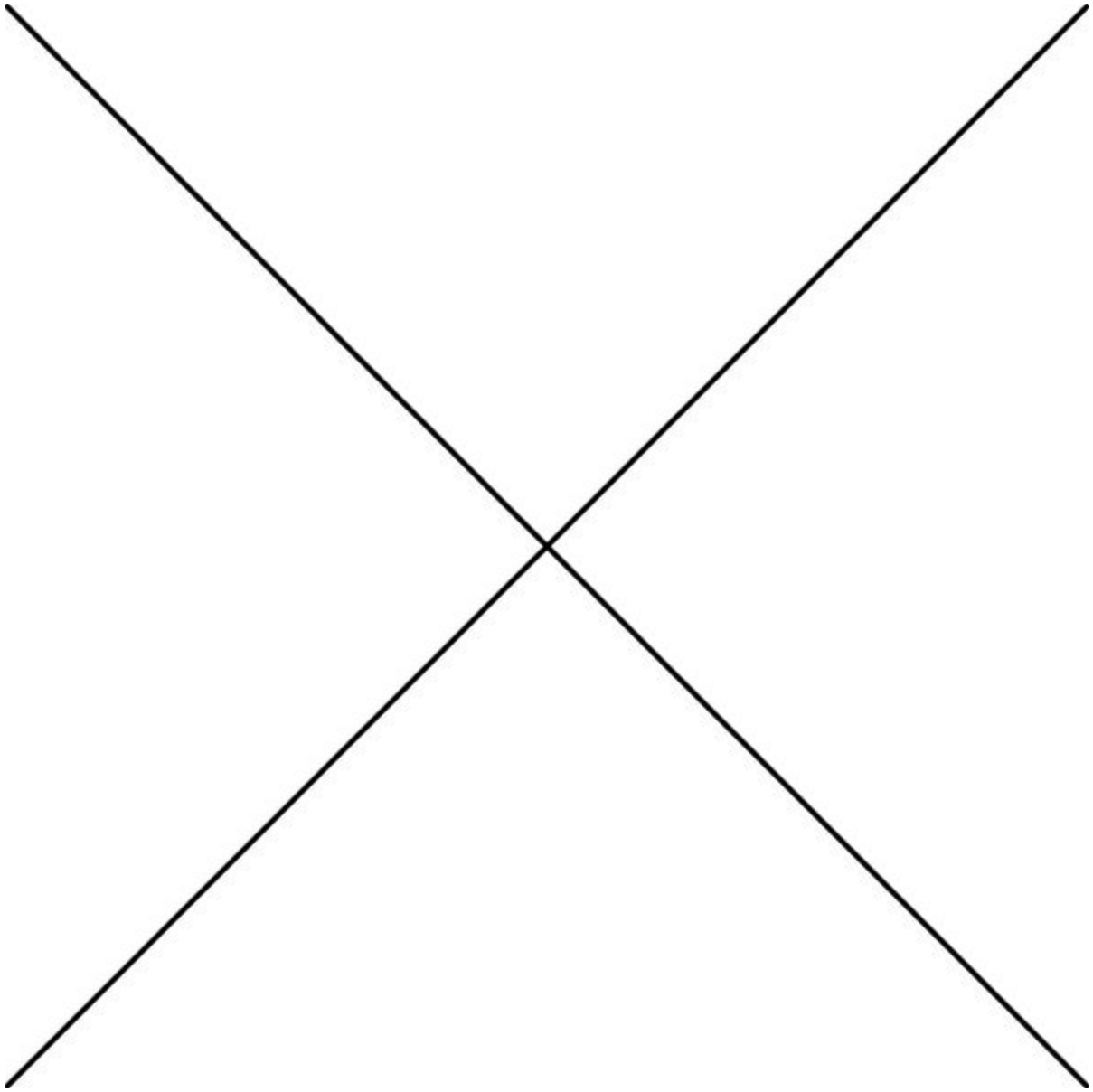
The requirements in this standard extend to all forms of information used throughout Contoso, Inc, including physical hardcopy documentation and electronic data stored on various information systems and media.

1.4 Responsibilities

All individuals are responsible for recognizing the sensitivity of information used during day-to-day operations and determining the appropriate classification levels in accordance with the requirements outlined below. Individuals must handle information appropriately to achieve Contoso, Inc's desired level of security.

2 Information identification

The following flowchart shows the general steps for determining a document's classification. See the **Contoso, Inc's CISO and Director** of this standard for specific information for how to apply these classifications.



Additional resources for owners for all customer information classification, security, and incident response can be found in the following documents:

1.1.1 Asset identification and authentication standard

TBD

2.1 Asset identification

Asset identification is a requirement to ensure that the status of each system can be quickly determined during a security incident or disaster. Inventories can be used as checklists to determine the scope of any incident.

Each asset is inventoried to include:

- Information owner
- Asset location
- Primary application (role type)
- Sensitivity
- Criticality
- Hardware
- Brand
- Operating system
- Applications
- Process owners

1.1.2 Asset classification

The purpose of classifying information assets is to determine the security measures are needed to protect the information assets from the risk of unauthorized use, disclosure, modification, and deletion. The following information asset types are used in this standard for purpose of grouping assets: Contoso, Inc information; Contoso, Inc project information; client information; employee/contractor/intern information; Contoso, Inc human resource information; user authentication information; and technology information.

The Information Asset Classification model at Contoso, Inc comprises three (3) distinct categories - **Confidential**, **Internal Use** and **Public** - designed to classify information based on the level of risk that may result from information being used, accessed, or disclosed in an unauthorized or inappropriate manner. There is also a classification related only to public sector documents: CUI. This classification is discussed in *[internal website link]*. Each information asset classification category has corresponding handling requirements to assist individuals in applying appropriate safeguards and handling procedures. The categories used to classify information are defined below and in the corresponding tables.

1.1.3 Information Asset Classification Categories

High Risk Information Asset Table – Confidential

Category description	Confidential information, the highest level of classification, is the information that Contoso, Inc and end users have a legal, regulatory and/or contractual obligation to protect. It is intended solely for restricted use within the corporation and is limited to those with an explicit, predetermined “need to know.”
Access criteria	Access to information is limited to a minimum number of individuals with a prearranged or confirmed need to know.

	Information owner may grant other Contoso, Inc employees' access for specific business reasons. Contoso, Inc will not disclose to a third party without signing a non-disclosure agreement (NDA) requiring the third party to protect such information.
Potential risk impact	Unauthorized use, access or disclosure of confidential information outside of Contoso, Inc could have a major adverse impact on the company, including: Significant and material financial, client, reputational, or regulatory impact. Compromise of Contoso, Inc's competitive position, exposure of confidential strategic initiatives, or affect the financial success of a product or service. Disclosure of information that could provide an attacker with information that can be used to compromise the Contoso, Inc's network or systems.

Medium Risk Information Asset Table – Internal Use

Category description	Internal Use information is information that, due to technical or business sensitivity, is limited to employees, interns, and contractors that have a business requirement to access the data and have signed a non-disclosure agreement. It is intended for use only within the corporation.
Access criteria	Access to information is generally restricted to employees, contractors or interns employed by Contoso, Inc for use within the company. Contoso, Inc does not disclose to a third party without signing a non-disclosure agreement (NDA) requiring the third party to protect such information.
Potential risk impact	Unauthorized use, access or disclosure of information outside of the company could have a moderate adverse impact on the company, including Moderate but unfavorable financial, client, reputational, or regulatory impact.

Low Risk Information Asset Table – Public

Category description	Public information is information that can be disclosed to anyone without violating an individual's right to privacy or impacting Contoso, Inc in any way. This information has been made available for public distribution through authorized company channels. Public information does not require special protection.
Access criteria	Access to information is unrestricted for Individuals when used for business related purposes.
Potential risk impact	Unauthorized use, access, or disclosure of information outside of Contoso, Inc would have no unfavorable financial, client, reputational, or regulatory impact.

The following tables contain examples of the information in each classification category. The examples are grouped into information asset types according to the kind of information that may be used throughout Contoso, Inc. These tables are provided as guides to assist in determining the classification of information assets and are not intended to be all- encompassing. It is important that

each individual exercise sound judgment when classifying information assets and recognize that the following exceptions may apply:

- Information assets used in combination with one another should be reviewed to determine if a higher-level classification is necessary (such as first and last name, home address or telephone number used in combination with social security number is considered confidential and must be handled accordingly)
- The confidential category should be considered if there is uncertainty as to the appropriate classification of an information asset that is not intended for internal use or public disclosure;
- Information subject to specific contractual or government regulatory controls must be handled in accordance with the applicable set of controls.

Requirements for the handling of these information assets follow each set of examples. For questions regarding classification of an information asset, contact the Security Team.

High Risk Information Asset Type and Example Table – Confidential

Contoso, Inc information	• General ledgers • Integration process documents • Product design/functional requirements • MKS change request list • Data files containing Information protected by legislation/regulations • Financial information • Contoso, Inc marketing strategies • Contoso, Inc strategic plans • Customer terms and conditions • Service-level agreements • SOC 1 & 2 reports, security audit reports and risk assessments • Results from security assessments (including internal and third-party) • Critical risks and security threats • Business continuity and disaster recovery audits, plans, and reports • Nonpublic Contoso, Inc strategic information (pending merger, acquisition or divestiture plans) • Nonpublic Contoso, Inc financial information such as current or projected earnings, and actual or contingent liabilities • Executive meeting notes and/or minutes • Planned management and organizational changes • Non-public information pertaining to corporate litigation **Note**: For Contoso, Inc HR information, see the following types: "Customer/Employee/Contractor/Intern sensitive personal information" and "Contoso, Inc Human Resources information" types below.

Contoso, Inc project information	Information regarding a customer's business and operations disclosed about the Contoso, Inc Application configuration and/or implementation Information prepared as part of pending or ongoing litigation.
Payment Card Industry (PCI) data	PCI data includes cardholder data and sensitive authentication data (SAD). Cardholder data includes: ● Primary account number ● Cardholder name ● Expiration date ● Service code ● Sensitive authentication data includes: ● Full track data (magnetic-stripe data or equivalent) ● CAV2/CVC2/CVV2/CID ● PINs/PIN blocks
Customer/employee/ contractor/ intern sensitive personal information	Personal information means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples are, users of the Contoso, Inc Application, such as: ● Social Security Number ● Individual Taxpayer Identification Number ● Date of birth ● Driver's license number ● Race, national or ethnic origin, religious beliefs or associations ● Age, sex, sexual orientation, marital status or family status ● Identifying number, symbol or other particular assigned to them ● Health care history, including a physical or mental disability ● Political opinions ● Trade union membership ● Offenses (including alleged offenses) ● Criminal records ● Genetic data ● Biometric data for the purpose of uniquely identifying a natural person ● Customer/supplier lists ● Any information received under the terms of a confidentiality agreement ● Geo-location information

Contoso, Inc Human Resource information	The following obtained as part of job function or supervisory responsibility: ● Salaries, bonuses, disciplinary actions, investigations or background checks ● Information pertaining to incentive programs ● Executive succession plans ● Employee performance reviews ● Promotional information/metrics
Customer information	● Customer/supplier lists ● Any information received under the terms of a confidentiality agreement ● Data defined as confidential by a customer
Employee/contractor /intern information	Personal data, or Personally Identifiable Information (PII), that can be used in combination with a person's name, address or telephone number, to determine the identity of any individual. Examples include, but are not limited to, users of the following: ● Social Security Number ● Individual Taxpayer Identification Number ● Date of birth ● Driver's license number ● Race, national or ethnic origin, religious beliefs or associations ● Age, sex, sexual orientation, marital status or family status ● Identifying number, symbol or other particular assigned to them ● Health care history, including a physical or mental disability
Contoso, Inc Human Resource information	The following obtained as part of job function or supervisory responsibility: ● Salaries, bonuses, disciplinary actions, investigations or background checks ● Information pertaining to incentive programs ● Executive succession plans ● Employee performance reviews
User authentication information	User name or user ID in combination with: ● Corresponding password ● Information used to reset a password or validate a user's identity (such as strong authentication challenge questions and responses) ● Biometric data (such as fingerprint or retinal encoding)
Technology information	Contoso, Inc application information: ● Application source code ● Information pertaining to unmitigated security vulnerabilities ● Encryption keys or passphrases ● Security system configuration settings or parameters

Medium Risk Information Asset Type and Example Table –Internal Use

Internal use	• Statements of work • Contoso, Inc PS Internal Knowledge Sharing Log • Status reports • PS assignment tracker spreadsheet • Telephone directory • Organization charts • Policies and standards • Disaster recovery and business continuity plans • Security reviews and scan outcomes
Customer/employee/ contractor/intern personal information	• Personal data means and any information relating to an identified or identifiable natural person (data subject): • Personal information such as name, email, location, telephone number • Marketing contact status • Metrics and reporting status for employees/teams in operational processes
Contoso, Inc Human Resource information	The data retained by Human Resources is related to employee training, operational processes and benefits.
Contoso, Inc operational information	Any information which is used during operational processes such as what is in wikis; knowledge bases (KBs, excluding how-to information for customers); document storage such as OneDrive or 3rd- party tools (only if approved).

Low Risk Information Asset Type and Example Table –Public

Public	• Contoso, Inc application brochures • Benefits of using Contoso, Inc application document • Contoso, Inc application standard suite of reports release notes • Marketing brochures • Customer disclosure statements • Interviews with news media • Press releases

3 Information handling

Once information is identified as confidential, the following precautions must be taken with respect to such information:

- **Information labeling**
  Employees are required to label all confidential information as Confidential, on every page of the paper and/or electronic document. This is particularly important when sharing Contoso, Inc confidential information with third parties, as non-disclosure agreements that Contoso, Inc has with third parties often require that information be marked as confidential for it to be treated as confidential. However, the absence of a confidentiality marking does not necessarily mean that information is not confidential, and employees are advised to consider the nature of the information and to treat it as confidential if uncertain as to the exact classification of the information.
- **Information retention/destruction**
  Information that is created, received, or stored in any type of media, whether paper or electronic, must be retained for a period that meets business, legislative, regulatory, and customer requirements. Once the retention period has passed, the data must be disposed of in a manner appropriate for the information classification. (The **Contoso, Inc Data Retention Standard** gives specific guidelines for the necessary times for data retention.)
- **Access**
  Only those individuals designated with approved access and signed non-disclosure agreements are granted access to confidential information.

Logical access limitations include:

- Compliance with current Contoso, Inc security policies and procedures.

Physical access precautions include:

- Lock premises and restrict access via key, identity card or password/passcode.
- Limit company information on key cards.
- Put fax machines and copiers in appropriate areas.
- Restrict access to filing cabinets.
- Clean whiteboards after each use.
- Restrict access to computers via passwords or other ID verification.
- Set unattended computers to automatically lock and to blacken their screens.

High Risk Information Asset Type Handling Requirements Table – Confidential

Email	Use only SAP email when sending to an authorized party outside of Contoso, Inc. Pay special attention so that no inadvertent email addresses are accidentally selected or included in distribution lists. Review all content and attachments closely to ensure appropriateness of the information being sent.
Mail/shipping	External distribution – Confidential information must be delivered directly in signature-required, tamper-evident envelopes. Internal distribution – Confidential information must be delivered directly to the authorized personnel.
Paper documents	Confidential information must not be left unattended when it is printed, faxed, and/or copied.

	Confidential information must be locked in file cabinets, desks, safes, or other furniture when not being used. Iron Mountain containers are provided for secure disposal of hard-copy information.
Electronic storage/workstations	Confidential information must not be stored, copied, written, or otherwise held on any system not owned or otherwise controlled by Contoso, Inc without written authorization. This applies to home computers, other email systems, and other instant messaging systems. Information stored on a system owned by Contoso, Inc is subject to the then-current Contoso, Inc security policies and procedures. Customer information *is prohibited* from being stored on any non-Contoso, Inc network or system. It should also not be kept on an employee's workstation or network *past the immediate time of usage.* All customer data should be stored in *encrypted format on files or in databases* **and** shared only with the password for encryption provided in separate email or transfer of information. Workstations must be locked (using Windows + L on a Windows computer or Command + Control + Q or Control + Shift + Power button on a Macintosh) when left unattended. Passwords must not be shared or written down. Confidential information must not be stored on internal team shared drives *unless access is restricted* to individuals with a need to know.
Fax	Use a corporate fax cover page when faxing to identify the recipient. Remove the document immediately after copying/scanning/faxing
Scanning	Scanned documents automatically saved to company shared network drives must be immediately deleted by the individual responsible for scanning. Original documents must not be left unattended after scanning is complete.
Paper	Dedicated containers are provided in many offices for secure disposal of hard copy information. Otherwise, use the available shredders.

Medium Risk Information Asset Type Handling Requirements Table – Internal Use

Media protection	All media that contains confidential information must be stored in a secure environment. Media that is physically transported must be properly labelled and locked in containers for shipment. Electronic storage media containing confidential information must be sanitized appropriately by overwriting or degaussing before disposal. Customer information is prohibited from being stored on removable media devices. Electronic storage media containing information marked as internal use must be sanitized appropriately by overwriting or degaussing prior to disposal.
PAN/PCI/Cardholder Data	Beyond being handled as sensitive and confidential, the following other rules apply to all cardholder information: PAN will not be fully exposed in any UI element in any Contoso, Inc controlled system. Access to full PAN digits will not be allowed to any Contoso, Inc personnel.

	PAN display will obscure all but the first 6 digits of a credit card to the user OR the last 4 digits of the PAN to all users. For further information, please see the ARCH 129 standard.
Internal document storage and online documentation	All internal document storage and online documentation storage should be reviewed on an annual basis for removal of old and no-longer-used documentation. (BOX/OneDrive and wiki/KB/team websites)

4 Notification

The Contoso, Inc Security and Legal teams must be notified in a timely manner if confidential information of any kind is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of Contoso, Inc's systems has taken place or is suspected of taking place.

5 Public Sector information

If you are in a public sector venue, the following information must be considered.

Controlled unclassified information (CUI) is *unclassified information* that requires safeguarding and dissemination controls pursuant to law, regulation, or government-wide policy, as listed in the CUI Registry (https://www.archives.gov/cui) by the National Archives and Records Administration (NARA).

This standard provides federal agencies with recommended requirements for protecting the confidentiality of CUI when the CUI is resident in non-federal information systems and organizations. The requirements apply only to components of non-federal information systems that process, store, or transmit CUI, or that provide security protection for such components.

5.1 Access to CUI information

Contoso, Inc associates who are U.S. citizens are permitted access to CUI information must provide that they have a need to know. Non-U.S. citizens may not have access to CUI unless the project leader has determined there is a need-to-know and has received written verification from the government sponsor that the non-U.S. citizen may be given access. The project leader must contact the Facility Security Officer (FSO) once permission is granted.

5.2 Marking CUI information

Information that has been determined to qualify for CUI status is indicated by markings (paragraph or page). Markings are applied at the time documents are created to properly protect the information. It is the responsibility of the document's originator to determine whether the information may qualify for CUI status and to ensure that markings are applied as required either at origination or on a later date.

Unclassified documents and material, including information in electronic form containing CUI information, is marked according to: https://fas.org/sgp/CUImarking-2016.pdf

- See https://fas.org/sgp/cui/marking-2016.pdf for proper marking of CUI documents.

  "The use of CUI coversheets is optional except when required by Agency policy."

- The following caveat must be included on the cover of the document as well:

  "This document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act."

- Each document determined to contain CUI/FOUO information must identify the originating agency or office.

CUI documents must be:

- Marked as "CUI" in accordance with marking guidance found on the CUI Registry (https://www.archives.gov/CUIregistry/category-detail/privacy-info).
- Protected in accordance with 32 CFR Part 2002, "Controlled Unclassified Information."
- Disseminated in accordance with any limited dissemination control markings applied to the information. The CUI Registry lists all limited dissemination control markings that can be applied to CUI.

CUI documents must follow these rules:

- Transmittal documents that have attachments, but no classified material attached, must be marked with the following statement or a similar one: "UNCLASSIFIED// ATTACHMENT."

5.3 Transmission of CUI documents

- CUI hard-copy documents and material can be transmitted via first-class mail, parcel post, or (for bulk shipments) fourth-class mail. Do not place CUI markings on the outside of the package or envelope, including interoffice mail. CUI information can be placed in a sealed envelope with the phrase "To be opened by _____ only" or "Eyes only."
- Whenever practical, electronic transmission of CUI information (for example, data, website, or email) must be by approved secure communications systems or systems using other protective measures such as Public Key Infrastructure (PKI) or transport layer security (for example, https).
- CUI faxes may be sent. Before faxing, notify the receiving party that a CUI document is being sent to ensure that appropriate protections are in place at the receiving fax.
- Use of wireless telephones must be avoided when other options are available.
- If you are planning to discuss CUI on the phone, make a need-to-know determination. Discussions must be limited to project members, appropriate clients, or government colleagues who have a need-to-know.

5.4 Email transmission of CUI information

Always include either the proper CUI banner marking and the "[CONTOSO, INC Sensitive]" caveat when sending information within the domain.

For emails that contain CUI, follow these requirements:

- Ensure that all recipients on an CONTOSO, INC distribution list are authorized to view CUI information before sending CUI to a distribution list.
- Include a banner marking above the email text.
- Include a banner marking above the email text when forwarding or responding to CUI received by email.

- Include Subject-Line indicators of CUI in the email text.
- Send the email via encrypted email or password-protect the document unless the sponsor has otherwise approved emailing without these measures.
- Always include the "[CONTOSO, INC Sensitive]" caveat when sending information within the internal domain.

5.5 Distribution of CUI documents

Because CUI is a dissemination control marking that is used to identify unclassified information or material that may not be appropriate for public release, only a duly trained and authorized Officer (a government official) can determine that information can be released to members of the public. This distribution requires the advanced coordination and approval of the program director.

5.6 Handling and storing of CUI information

Information must be handled in a manner that provides assurance that unauthorized persons do not gain access.

Always do the following:

- Attach a copy of the Contoso, Inc CUI cover sheet to each document after printing (contact your FSO if you need additional copies of this cover sheet).
- Store CUI documents in a locked container, desk drawer, cabinet, or a locked office whenever the documents are not actively being used.
- Use a sealed envelope to protect CUI information when it is hand-carried on official trips outside of Contoso, Inc.
- When storing CUI on the Contoso, Inc network, password-protect the information.
- Store on removable media that is encrypted.

Never do the following:

- Store CUI information on a non-Contoso, Inc computer (DoDM 5200.01-V4)
- Post on the Internet
- Leave CUI in print bins, on or near printers, or in an individual's mail slot

5.7 Reporting CUI incidents

All CUI incidents must be reported. See the **Contoso, Inc Public Sector Incident Response Standard** for information.

5.8 CUI references

NIST SP 800-171 Appendix D:

This appendix provides a complete listing of the security controls in the NIST Special Publication 800-53 moderate baseline, one of the sources (along with FIPS Publication 200) for the final CUI security requirements described earlier in this section. Tables E-1 through E-17 contain the tailoring actions (by family) that have been carried out on the security controls in the moderate baseline in accordance with the tailoring criteria established by NIST and NARA.31. The tailoring actions facilitated the development of the CUI-derived security requirements that supplement the basic

security requirements obtained from the security requirements in FIPS Publication 200.32. There are three primary criteria for eliminating a security control or control enhancement from the moderate baseline, including any of the following:

- The control or control enhancement is uniquely federal (that is, primarily the responsibility of the federal government).
- The control or control enhancement is not directly related to protecting the confidentiality of CUI.
- The control or control enhancement is expected to be routinely satisfied by non-federal organizations without specification.

Other references are:

- DoDM 5200.01-V4: DoD Information Security Program: Controlled Unclassified Information (CUI) https://www.dodig.mil/Portals/48/Documents/Policy/520001_vol4.pdf
- https://fas.org/sgp/CUImarking-2016.pdf (Markings)
- https://www.archives.gov/CUIregistry/category-detail/privacy-info (CUI Registry)