

Subject: Procedure for Identification, Handling and Storing “Official Use Only” Information	Effective Date: June 2, 2016	Initiated by: Deputy Director for Operations
	Supersedes NEW	Approved: Director

Management System (Primary): 10.00 Safeguards and Security
Management System Owner: Head, Best Practices and Outreach
Management Process: 10.03 Security
Process Owner: Head, Best Practices and Outreach
Sub-Process: 10.03.06 Information Security
Sub-Process Owner: Head, Site Protection
Subject Matter Expert (SME): Head, Best Practices and Outreach; Head, Site Protection;
 Head, Human Resources (PII Officer); Head, Information
 Technology; Head, Business Operations

APPLICABILITY

This policy applies to all Princeton Plasma Physics Laboratory (PPPL) staff and activities that generate or use Official Use Only information.

INTRODUCTION

It is PPPL policy that Official Use Only (OUO) information must be controlled and protected according to DOE directives and contract requirements.

PPPL staff, visitors and contractors may not release OUO documents informally or without following proper protocol (e.g., may not be posted on a website or sent to a person without a “need to know” the information, etc.) as defined in this document.

PPPL OUO Information/Documents:

1. May not be shared with persons who do not have a “need to know.”
2. Must be appropriately reviewed prior to public release under a Freedom of Information Act (FOIA) request.
3. Must be consistently marked, handled, protected, and controlled throughout the Laboratory.

REFERENCES

DOE Order 471.3, Administrative Change 1, *Identifying and Protecting Official Use Only Information*

DOE M 471.3.1, Manual for *Identifying and Protecting Official Use Only Information*, Dated 1-13-11

PPPL Policy P-095, *Protection of Personally Identifiable Information (PII) on PPPL Information Systems*

Office of Classification OUO Web page

<http://www.hss.energy.gov/Classification/QualityMgt/ouo.html>

DEFINITIONS

Business Sensitive Information	Documents or information that are not considered OUO but are a sensitive nature and requiring additional internal controls and protection from public release or release to persons without a specific “need to know”.
DOE	Department of Energy
FOIA	Freedom of Information Act
PII	Personally Identifiable Information
PPPL Procedure	A document that specifies a series of specific steps to be followed to accomplish work or to carry out a policy or requirement. Procedures establish controls meant to mitigate risk, improve efficiency, or assure compliance.
Originator	Person who creates and/or originates the information requiring OUO review
OUO	Official Use Only – An unclassified document that is originated within a DOE/NNSA office, produced by PPPL that may contain OUO information. Any employee from an office or contractor with cognizance over such information may determine whether such a document contains OUO information. OUO enables the implementation of certain controls to protect and manage the information.
OUO Coordinators	Individuals assigned by the Subject Matter Experts [Head, Best Practices and Outreach; Head, Site Protection; Head, Human Resources (PII Officer); Head, Information Technology; Head, Business Operations] to: track the OUO documents and users in the assigned areas (e.g., business operations, cyber security, security, personal records, etc.); to ensure that OUO is managed and controlled in accordance with procedures and contract requirements; and to assign personnel to complete OUO training as required.
OUO SME	OUO Subject Matter Expert – PPPL staff person responsible for being the point of contact within the organization and with other entities (including the DOE) to make determinations regarding OUO applicability and processing
Sensitive Information	Information whose release can potentially cause damage to government, commercial, or private interests: and release potentially falls under a FOIA exemption 2-9.

PROCEDURES

A. DETERMINING AND PROCESSING OUO INFORMATION

RESPONSIBILITY

ACTION

- | | |
|-----------------------------------|---|
| Cognizant Employee/
Originator | <ol style="list-style-type: none"> 1. Determines if information is OUO (see Attachment 1): <ol style="list-style-type: none"> a. Checks to see if <u>specific</u> DOE guidance exists that information is OUO and then identifies it as OUO (for example, information issued by HS-60, a program office, or a DOE/NNSA contractor). b. If there is <i>no</i> specific DOE guidance, then identifies |
|-----------------------------------|---|

information as OOU if release of the information meets two criteria:

1. Cause Damage: In the opinion of the person making the determination, release has the potential to damage governmental, commercial, or private interests if the information is released to persons who have no business purpose for their jobs or other DOE-authorized activity, and,
2. Release potentially falls under a FOIA exemptions 2-9 (see Attachment 1).

NOTE: Consult guidance issued under paragraphs 5a(3), 5a(4), or 5b(2) of DOE O 471.3. and review I-2 DOE M 471.3-1 for specific guidance regarding OOU applicability.

- c. If the information is considered to have the potential for such damage, then the employee should consult with the appropriate OOU SME or OOU Coordinator to determine whether or not document, or portions of the document, are OOU.

NOTE: If the employee finds no basis for identifying the information as OOU after consultation with SME, then the employee must not mark the document as containing OOU information.

2. Determines information to be OOU information and marks the document according to Attachment 2. The document will include the following marking on at least the pages that contain OOU.

OFFICIAL USE ONLY

Maybe exempt from public release under the Freedom of Information Act (5 U.S.C.552), exemption number and category:

Department of Energy review required before public release

Name/Org: _____ Date: _____ Guidance (if applicable):

3. Removes OOU markings after document or information is no longer considered OOU. OOU Markings Applied Based on Employee's Evaluation may be removed by (1) the employee who initially applied the marking, (2) the supervisor of the employee who initially applied the marking, or (3) a FOIA authorizing official who approves the release of the document in response to a request made under FOIA. However, these persons must be trained in OOU procedures. (See Attachment 2 OOU Marking Requirements.)
4. **Note** --- documents that DO NOT reach the level of OOU designation but require additional internal protections may be designated as "Business Sensitive" (as opposed to "Confidential" which is utilized by the federal government to denote classified documentation or information). Such documents --- which may include personnel, operations, budget, and other proprietary emails, letters, assessments, reports, etc. --- shall be subject to document controls as established by the author or owner of the information or document.

B. ACCESSING OOU INFORMATION**RESPONSIBILITY****ACTION**Cognizant Employee/
Originator

1. Determines if requests for access to the OOU document are for PPPL “business purposes” or other DOE-authorized activity. Determines if document requested has additional restrictions prior to granting access (e.g. Export Controlled Information, Source Selection Information, etc.). (The requestor does not need a security clearance, to be a DOE employee, or have US citizenship for access.)

Note: The *Originator*, not requestor, reviews and approves the business need for access.

2. Once approved, access to the OOU document may be granted utilizing hand-to-hand delivery or other acceptable transmission method (see Attachment 3).

C. PROTECTING OOU INFORMATION**RESPONSIBILITY****ACTION**OOU Document
Possessor

1. Uses the document for business-purposes only, and takes precautions to ***prevent access*** to OOU documents by other persons who do not have a business need for access to the information to do their jobs (for example, doesn’t read an OOU document in a public place such as a cafeteria, or bus).
2. Does not share the OOU documents(s) or information with persons who do not have a business-related purpose to see the information.
3. Takes precautions when ***transmitting*** OOU documents to others via telephone, email, mail, etc. (***See Attachment 3 – OOU Transmission Requirements for detailed and explicit guidance on OOU document transmission controls.***)
4. Takes precautions when ***storing*** OOU Documents:
 - a. Hardcopies must be stored in a locked room, locked file cabinet, desk, briefcase, etc., when not in use (Note: PII/Privacy Act information must be locked up). The method chosen shall be that which effectively restricts access to OOU documents/information to authorized persons only.
 - b. Electronic documents must be password protected and will be stored on a secure PPPL server established for storing these kinds of documents. Access to this server will be limited to those who have a business-purpose for access to the OOU information being stored in the location.

- 5. While copies of the document may be made without permission of the originator, takes precautions *minimizing the numbers of copies* of OOU documents and *ensuring the copies are marked and protected*.
 - 6. When no longer needed, destroys paper *OOU documents* by using a strip-cut shredder with strips no more than 1/4" wide or any method approved for classified documents or by the PPPL security office.
- OOU Coordinators
- 7. Track OOU documents and users in the assigned area to ensure that OOU documents are controlled properly, and that originators and users complete training as required.

TRAINING REQUIREMENTS

- SPD
- 1. Yearly familiarization training for originators of OOU information including OOU designation requirements, document marking, handling, storage, and disposal.
 - 2. Target Audience: All originators of OOU information and PPPL DOE clearance holders.
Instructor: Site Protection Division

Training Methods: X Briefing X Classroom X Online

Frequency: X Annual
- Head, SPD
- 3. Notify the Human Resources Training Office of the training so that they will be aware of the training requirements and be able to provide assistance and guidance in the course development, implementation, tracking, and maintenance.

RECORDS REQUIREMENTS SPECIFIC TO THIS PROCEDURE

Records Custodians must assure records are maintained as follows:

Record	Record Custodian	Location	Retention Time
List of OOU documents and originators names	OOU Coordinators	Assigned Department/ Division	TBD

The OOU documents will be kept by the originators or owners of the primary copy of the document per records requirements for that document type.

ATTACHMENTS

- 1. FOIA Exemptions
- 2. OOU Marking Requirements
- 3. OOU Transmission Requirements
- 4. OOU Flowchart

PPPL	PRINCETON PLASMA PHYSICS LABORATORY	PROCEDURE	No. GEN-039 Rev 0 Page 1 of 2
	FREEDOM OF INFORMATION ACT (FOIA) EXEMPTIONS		Attachment 1

ATTACHMENT 1

Freedom of Information Act (FOIA) Exemptions

Exemption 2 – Circumvention of Statute

- Not Applicable at PPPL

Exemption 3 – Statutory Exemption

- Disclosure of information is prohibited by statute
- Not OOU if information is otherwise classified or controlled (e.g., RD, FRD, TFNI, UCNI)

Examples

- Federal Technology Transfer Act – Protected CRADA information
- Procurement Integrity Act – Source selection information
- Internal Revenue Code – Taxpayer identification numbers
- Patent Act – Applications for patents
- Arms Export Control Act – Certain information concerning export license applications
- Export Administration Act – information pertaining to license applications under the Act
- National Security Act of 1947 – Intelligence sources and methods
- Espionage Act – Information pertaining to communication intelligence and cryptographic devices

Exemption 4 – Commercial/Proprietary

- Trade secrets
- Commercial or financial information whose release would
- Impair the Government’s ability to obtain information in the future,
- Cause competitive harm, or
- Affect program effectiveness

Examples

- Trade secret information (e.g., Coca Cola formula)
- Financial information, such as income, profits, losses, costs
- Contract proposal, solicited or unsolicited
- Customer/supplier lists
- Government credit card numbers
- Security measures for commercial entities performing work for the Government

Exemption 5 – Privileged Information

- Three primary privileges
- Deliberative process (a.k.a. “pre-decisional”)
- Attorney-Work Product
- Attorney-Client

Examples

- Documents concerning potential budget cuts
- Documents concerning potential cancellation of a program
- Documents concerning potential DOE property purchases
- Communications between attorneys and their clients in which attorney is conveying legal advice

FREEDOM OF INFORMATION ACT (FOIA) EXEMPTIONS**Attachment 1**

- Documents prepared by or for attorneys reflecting research and analysis of legal issues for consideration in rendering legal advice or for litigation

Exemption 6 – Personal Privacy

- Constitutes a “clearly unwarranted invasion of personal privacy”
- Personally Identifiable Information (PII) is OOU

Examples (when associated with an individual)

- Social Security Number (even when not associated with an individual)
- Place of birth, date of birth
- Mother’s maiden name
- Medical history
- Financial data

(Note - Information usually not OOU under Exemption 6 includes federal employee’s name, title, grade, position description, and duty station)*Exemption 7 – Law Enforcement*

- Includes (but is not limited to)
- Release could reasonably be expected to endanger the life or physical safety of any individual or
- Information would disclose techniques and procedures for law enforcement investigations or prosecutions

Examples

- Investigative information
- Civil, criminal investigations
- Personnel investigations
- National security/terrorism investigations
- Security measures to protect Federal officials
- Security measures for Federal buildings
- Security manuals
- Classification guides

Exemption 8 – Financial Institutions

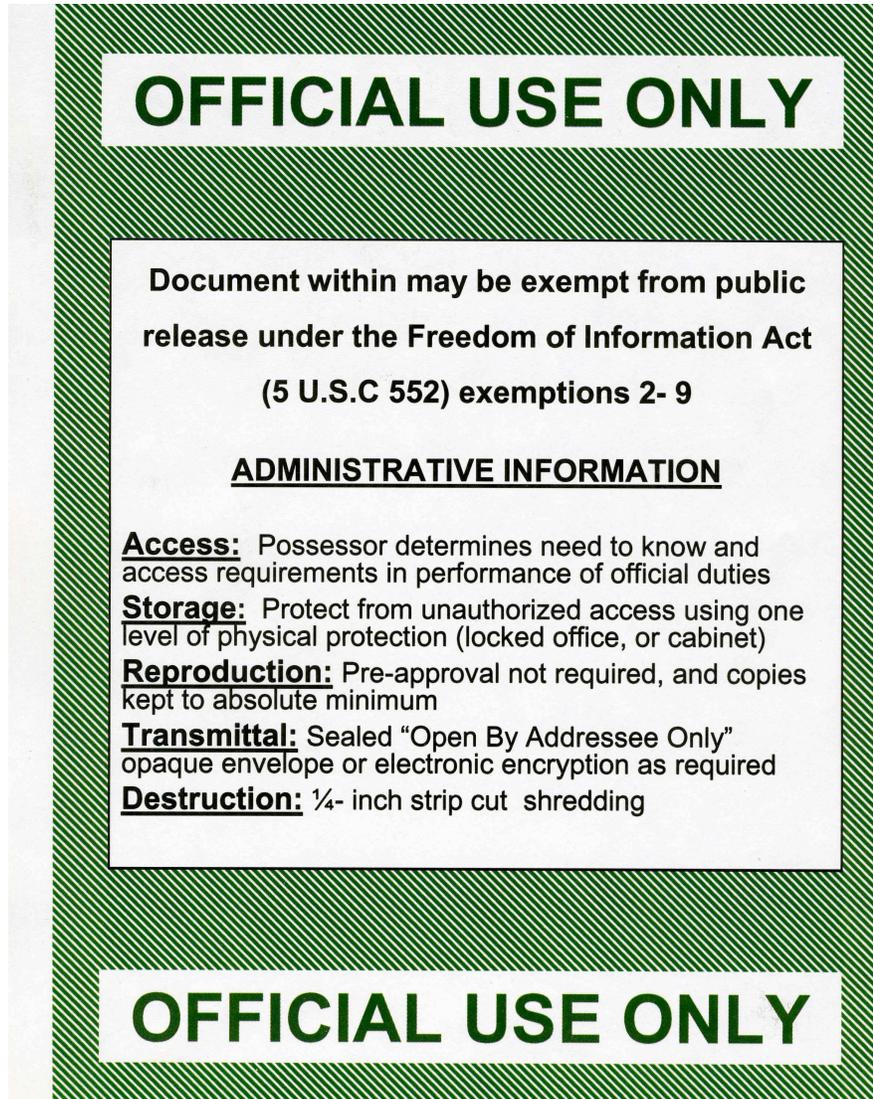
- Evaluations of a financial institution’s stability prepared by, on behalf of, or for use of an agency responsible for regulation of financial institutions (FDIC, etc.)

Exemption 9 – Wells

- Technical and scientific information about any type of well

Examples

- Geothermal well BTU production
- Ground water inventories and well yields in gallons per minute
- Natural gas reserves



OFFICIAL USE ONLY

MARKING A DOCUMENT CONTAINING OUO

- A. Front Marking: The front marking includes the applicable FOIA exemption number and related category name (i.e., Exemption 2 - Circumvention of Statute; Exemption 3 - Statutory Exemption; Exemption 4 - Commercial/Proprietary; Exemption 5 - Privileged Information; Exemption 6 - Personal Privacy; Exemption 7 - Law Enforcement; Exemption 8 - Financial Institutions; Exemption 9 - Wells) and the name and organization of the employee making the determination and identifies the guidance used if the determination was based on guidance. The employee making the determination ensures that the following marking is placed on the front of each document containing OUO information.

OUO MARKING REQUIREMENTS**Attachment 2****OFFICIAL USE ONLY**

Maybe exempt from public release under the Freedom of Information Act (5 U.S.C.552), exemption number and category: _____ Department of Energy review required before public release Name/Org: _____ Date: _____ Guidance (if applicable): _____

- B. Page Marking: The employee making the determination must ensure that the words “Official Use Only” (or “OUO” if space is limited) are placed on the bottom of each page or, if more convenient, on only those pages containing the OUO information.
- C. Marking E-mail Messages: The first line of an e-mail message must contain the abbreviation “OUO” before the beginning of the text. If the message itself is not OUO but an attachment contains OUO information, the message must indicate that the attachment is OUO. The attachment must have all required OUO markings.
- D. Marking Special Format Documents: Special format documents (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audiotapes, videotapes, DVDs, or CD-ROMs, etc.) must be marked in a manner consistent with paragraphs “A” and “B” above so persons possessing the documents and persons with access to the information in or on the documents are aware they contain OUO information. When space is limited (e.g., the frame of a 35-mm slide), the page marking (“B”) is sufficient.
- E. Marking Documents Maintained in Restricted Access Files: Documents that may contain OUO information that are maintained in restricted access files (e.g., personnel office files) do not need to be reviewed and marked while in these files or when retrieved from the files for reference, inventory, or similar purposes as long as the documents will be returned to the files and are not accessible by individuals who are not authorized to access to the OUO information. However, a document removed from these files and not to be returned (or a copy of such document) must be reviewed to determine whether it contains OUO information and, if appropriate, marked. (NOTE: Documents that are moved from one restricted access file location to another for storage purposes do not need to be reviewed.) Documents that are removed for criminal, civil, or administrative law enforcement or prosecution purposes need not be reviewed or marked where parallel controls to this order are in place.
- F. Transmittal Document: A document that (1) transmits an attachment or enclosure marked as containing OUO information and (2) does not itself contain classified or controlled information must be marked on its front as follows to call attention to the presence of OUO information in the attachments or enclosures: **Document Transmitted Contains OUO Information**
- G. Removal of OUO Markings - The below mark will be placed on the bottom front page of all documents no longer deemed OUO:

**DOES NOT CONTAIN
OFFICIAL USE ONLY INFORMATION
Name/Org: Date:**

TRANSMISSION OF OUO DOCUMENTS

Transmission of OUO documents and information must be controlled to assure protection of the information. The following transmission controls are required:

1. By Mail – inside facility: Place in sealed, opaque envelope or wrapping with recipient’s address and “TO BE OPENED BY ADDRESSEE ONLY” on outside
2. By Mail - outside facility: Place in sealed, opaque envelope or wrapping with recipient’s address, **return address**, and “TO BE OPENED BY ADDRESSEE ONLY” on outside (same requirements as inside facility, but must include return address); utilize U.S. mail – First Class, Express, Certified, Registered, or any commercial carrier
3. By Hand between facilities or within a facility: May be hand-carried and must control access to document
4. Over telecommunications circuits: use encryption whenever possible.
Note: If encryption capabilities are not available and transmission by mail is not a feasible alternative, then regular e-mail or facsimile machines may be used to transmit the document.
 - a. By Unencrypted Facsimile: An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that he or she can control the document when it is received.
 - b. By E-mail without Encryption: If encryption is not available and some form of protection is desired, the OUO information may be included in a word processing file that is protected by a password and attached to the email message. The sender will call or send a second email to the recipient with the password needed to access the file.
5. Transmission over Voice Circuits: OUO information transmitted over voice circuits should be protected by encryption whenever possible. However, if such encryption capabilities are not available and transmission by other encrypted means is not a feasible alternative, then regular voice circuits may be used.
6. Electronic Information:
 - a. All shared OUO documents must be kept in limited-access-electronic files or directories accessible only to those with a business-related purpose for access to the documents. Access controls reviewed at least annually by the IS.
 - b. Backup CDs, memory sticks, etc., with OUO shall be treated the same as hard copies – that is, stored in a locked room, cabinet, desk, etc., when not in use. The method chosen shall be that which effectively restricts access to OUO to authorized persons only.
 - c. No CD, memory stick, laptop, etc., may have PII without the documented permission of the CIO.
 - d. Computers, laptops, etc., will be periodically surveyed by the IS to be sure they are meeting requirements.
 - e. CDs, memory sticks, computers, etc., with OUO information must be properly destroyed. Contact or provide the physical items to Cyber Security for destruction.
7. Processing OUO information on Automated Information Systems: An automated information system (AIS) or AIS network must provide methods (e.g., authentication, file access controls, encryption, firewalls, passwords, etc.) to prevent access to OUO information stored on the system by persons who do not require the information to perform their jobs or other DOE-authorized activities.

OUO FLOW CHART

Attachment 4

