TEMPORARY CHANGE REQUEST

TCR NO.TCR-P-095,R0-003
(e.g., TCR-ENG-021,R0-001)

The Temporary Change Request (TCR) Form is to be used to process urgent or minor changes for PPPL Policies, Organization/Mission Statements and Procedures. The TCR should be used when changes are:
1) urgent, and can not wait the 2-4 week period for Department Head review/comment, or
2) minor, and do not warrant Department Head review.

Person Requesting Change: Marc Cohen **Phone Ext:** 3404

Department Name: Information Technology Department

Document Number: P-095 **Revision No.:** R0

Document Title: Protection of Personally Identifiable Information

Reason for change:

Update titles

Change description: (Summarize and attach changed pages, with changes clearly indicated)

Cyber Security Officer (CSO) updated title to Chief Information Security Officer (CISO)

1. Does this TCR significantly alter the intent or scope of the document? **YES:** **NO:** **X**

2. Does this TCR significantly impact **ES&H**? **YES:** **NO:** **X**

If 1 or 2 is **YES**, Explain why the changes should not be routed for Department Head review:

Department/Division Head Approval **Date**

Chief Planning Officer/designee **Date**

Release/Effective date of this TCR: **1/9/18**

Incorporate this TCR into next revision of this document? **YES:X** **NO:**

Subject:	Effective Date:	Initiated by:
Protection of Personally Identifiable Information (PII) on PPPL Information Systems	November 1, 2007	Chief Information Officer
	Supersedes: New	**Approved:** Director

TCR P-095, R0-003

Definition: Personally Identifiable Information (PII):
Any information about an individual, including but not limited to: education, financial transactions, medical history, criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security numbers, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Classes of PII
PPPL has designated two classes of PII:

Public PII
PII that is available in public sources such as telephone books, public websites, business cards, university listings, etc. For example, *first and last name, address, work telephone number, email address, home telephone number, and general educational credentials*. Public PII must be protected with at least NIST SP 800-53 R 4 "low level controls".

Protected PII
PII that, if compromised, can cause serious or severe harm to an individual (such as identity theft). For example: *An individual's first name or first initial and last name in combination with any of the following types of information including, but not limited to, social security number; passport number; credit card numbers; security clearances; bank account numbers; biometrics; date and place of birth; mother's maiden name; criminal, medical and financial record; educational transcripts; etc*. Protected PII requires enhanced protection per NIST SP 800-53 R 4 "moderate level controls" or better.

INTRODUCTION

Millions of personal privacy records maintained by companies, government agencies, and educational entities have been lost or stolen in recent years. Department of Energy Laboratories have experienced such information losses. Due to the importance of protecting Personally Identifiable Information (PII), and the potential negative impact if PII is lost or stolen, PPPL has established policy intended to protect and safeguard PII.

The United States Office of Management and Budget (OMB) has required federal agencies to implement protective measures developed by the National Institute of Standards and Technology (NIST), including those related to encryption, remote access, and risk assessments. The DOE has issued DOE Order 206.1 "*Department of Energy Privacy Program*" that is consistent with OMB guidance.

PPPL maintains several information systems that contain PII. The PPPL Information Technology Department (IT) has implemented controls to protect against the loss of PII within the PPPL networks and those controls are tested and audited for effectiveness. However, with the advent of laptop computers and the numerous other types of portable electronic devices that can be used to store information, additional controls and safeguards are needed to ensure the protection of PII.

POLICY

It is PPPL policy that all individuals who maintain or access PII information must be authorized, in accordance with the PPPL Confidentiality Policy, to access that information.

Requirements for Protected PII Stored on Computers or other Electronic Media:

- All electronic copies of Protected PII must reside within the PPPL network, which has been designated as the PPPL "accreditation boundary", in accordance with DOE guidance.
- The IT Department must be notified of all computers, computer systems, handheld and electronic devices that contain PII.
- Protected PII is not to be downloaded to mobile devices (such as laptops, Personal Digital Assistants (PDAs), or removable media, or to systems outside the protection of the accreditation boundary).
- Protected PII cannot be downloaded to home PC's that access the lab from off-site.
- Personally Identifiable Information may not be printed to a remote printer (outside of the physical PPPL perimeter or outside PPPL network accreditation boundary).

Waiver

If there is an operational or business need to store Protected PII outside the PPPL Network (i.e., the accreditation boundary), in particular on laptops and mobile devices, a waiver may be granted. Waivers must be approved by the PPPL Chief Information Officer (CIO) and documented in the System Security Plan (SSP). In instances where a waiver has been granted, the controls as specified by the PPPL CIO will be applied. In particular, specific encryption will be required to protect PII.

Remote Access

If there is an operational or business need to access Protected PII data from outside the accreditation boundary, an automatic disconnect after 30 minutes, or less, of inactivity will be enforced. In addition, two-factor authentication (e.g., password and confirmation of computer identification) will be required to access Protected PII.

Incident Reporting

Within 45 minutes after discovery of a real or suspected loss of Protected PII data, the PPPL Chief Information Security Officer (CISO) will report incidents involving PII in accordance with PPPL procedure ENG-034. The CISO is an employee of the IT Department reporting directly to PPPL's Chief Information Officer (CIO). TCR-P-095,R0-003

References

PPPL Confidentiality Policy and Statement (PPPL Personnel Practices Manual)
ENG-034, Cyber Security Incident Response
DOE O 205.1B, Department of Energy Cyber Security Program
DOE O 206.1 Department of Energy Privacy Program