TEMPORARY CHANGE REQUEST

TCR NO. TCR-P-094,R1-002

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: TCR-P-094 **Revision No.:** R1

Document Title: Cyber Security Policy

Reason for change:
Update responsibilities to reflect the updated ITD organization

Update referenced documents

Change description:
Added Chief Information Security Officer responsibility

Modified Referenced Documents:
4. NIST SP 800-53 Rev. 4 - Recommended Security Controls for Federal Information Systems,
9. NIST SP 800-60 Rev.1- Guide for Mapping Types of Information & Information Systems to Security Categories Vol. 1 & Vol. 2,
Added Reference Document
11. DOE Office of Science Program Cyber Security Plan

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:
Cyber Security Policy	**1/4/13**	Head, Information Technology Department & CIO
	Supersedes: P-094, R1 Dated: February 12, 2010	**Approved:** Director

TCR-P-094, R1-002

Applicability

This policy is applicable to all PPPL Departments, Projects and operations.

Introduction

Title III of the E-Government Act (Public Law 107-347), "Federal Information Security Management Act (FISMA)" requires that all federal agencies and their contractors develop and implement an agency-wide information security program to safeguard the Information Technology (IT) assets and data of the respective agency. As a contractor to the Department of Energy, PPPL is obliged to implement such a program.

Policy

It is PPPL policy to follow NIST which is referenced below and provides the necessary framework for cyber security policies. The Information Technology Department Head & Chief Information Officer (CIO) together with the Chief Information Security Officer have lead responsibility for the PPPL cyber security program and development of PPPL's Cyber Security Program Plan. **TCR-P-094, R1-002**

Referenced Documents:

1. DOE Order 205.1B Department of Energy Cyber Security Program,
2. Federal Information Security Management Act (FISMA),
3. NIST SP 800-137 – Information Security Continuous Monitoring for Federal Information Systems and Organizations,
4. NIST SP 800-53 Rev. 3 - Recommended Security Controls for Federal Information Systems,
5. FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems,
6. FIPS PUB 200 – Minimum Security Requirements for Federal Information and Information Systems,
7. NIST SP 800-30 Rev 1 - Guide for Conducting Risk Assessments,
8. NIST SP 800-37 Rev. 1 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach,
9. NIST SP 800-60 Rev.1- Guide for Mapping Types of Information & Information Systems to Security Categories Vol. 1 & Vol. 2, **TCR-P-094, R1-002**
10. DOE Policy 205.1 – Department of Energy Cyber Security Management Policy
11. DOE Office of Science Program Cyber Security Plan **TCR-P-094, R1-002**