

TEMPORARY CHANGE REQUEST

TCR NO. **TCR-P-106,R0-001**

(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-106 Revision No.: 0

Document Title: Information technology (IT) Backup Policy

Reason for change:

Change Subject Matter Expert title to reflect new ITD organization

Point to new helpdesk ticketing system for additional information

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

Subject Matter Experts now include User Services Team Lead and Systems Administration Team Lead

The new link to the helpdesk system is help.pppl.gov.

1. Does this TCR significantly alter the intent or scope of the document? YES: NO:
2. Does this TCR significantly impact ES&H? YES: NO:

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: NO:

PPPL	PRINCETON PLASMA PHYSICS LABORATORY	POLICY		No. P-106 Rev. 0 page 1 of 1
		Subject: Information Technology (IT) Backup Policy	Effective Date: February 18, 2014	Initiated by: Head, Information Technology Department & CIO

TCR-P-106, R0-001

Management System (Primary): 06.00-Information Technology (IT) Management

Management System Owner: Deputy Director for Operations

Management Process: 06.16 Data/Information Capture and Storage

Process Owner: Head, IT Department

Subject Matter Experts (SMEs): Head, IT Department; Head, User Services Team
Lead; Systems Administrator Team Lead; ITD
System and Network Engineer **P-106,R0-001**

POLICY

File backups provide a means to restore the integrity of a computer system in the event of a hardware/software failure or physical disaster and provide a measure of protection against human error or the inadvertent deletion of important files. System backups are **not** intended to serve as an archival copy or to meet records retention requirements as required by procedure GEN-023.

Desktop, Laptop Backup and Retention policy

Desktop Backups are only intended for the restoration of user created data files due to accidental file deletion or catastrophic disk failure. ***Files are retained for 6 months after deletion, so if no request is made to restore the file within that period, it will no longer be available for restoration.*** Applications added by the end user, not ITD, are the user's responsibility, and thus media and activation keys should be retained. **P-106,R0-001**

Server Backup and Retention Policy

Server backups are intended for the restoration of files lost due to accidental file deletion or catastrophic disk failure. ***Unlike desktop backups, server backups are retained until tapes are recycled in the system, typically at 6 years of age. Therefore, a deleted file on a server can be restored up to 6 years or more after deletion.*** Server backup tapes are duplicated and sent offsite for storage and safe keeping. When backups start, experimental systems (e.g. NSTX-U) are scheduled first, before non-experimental systems, with the intent that these backups complete before operations are again started. Servers that contain sensitive data (ex. business systems) follow the Server Backup Policy with the addition of being encrypted before being transferred to tape.

More Information

More information about PPPL's backup process can be obtained at help.pppl.gov. **P-106,R0-001**