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, IT Department and PPPL CIO
		Supersedes: NEW Lab-wide policy. Cancels IT Department Policy ITD-003	**Approved:** Director

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, ITD Systems and Network Engineering; ITD System and Network Engineer

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 retained.

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) 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 helpdesk.pppl.gov/home under the DOE and PPPL Computer Policies link.