Backup

Purpose: The intent of the following policy is to protect data and to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

Policy: Database, file backups, and configuration files for critical systems (i.e. hardware firewalls) will be kept current, systematically performed, and precisely labeled and organized. All Virtual Machine server images, which create or update mission critical data on a daily basis, will be iteratively backed up on a daily basis to minimize the exposure to loss of mission critical data. Other critical devices, such as computers and laptops, will be backed up on an assigned schedule. In addition, Uninterruptable Power Supplies (UPS) will be issued for servers and high-value IT systems to prevent unintentional data loss during a brownout or power loss.

This policy applies to all equipment and data owned and operated by the organization.

Procedure and/or Process:

Data can be destroyed by system malfunction or accidental or intentional means. Adequate backups will allow data to be readily recovered as necessary. The ongoing availability of data is critical to the operation of the agency. In order to minimize any potential loss or corruption of this data, the Data Systems Department is responsible for providing and operating administrative applications needed to ensure that data is adequately backed up by following the appropriate system backup procedures:

Accounting System:

Accounting data files are backed up to a USB drive daily. The USB drive is then taken off the premises for the evening or weekend. The USB drive is returned to the office the next workday and then the whole process is repeated.

Domain Systems:

All local network-shared drives and local servers are backed up nightly to a rapid-removal capable hard drive. The server performing the backups is physically segregated from the other servers and is to be automatically powered off during daily operations, only turning on at night to perform iterative backups. The hard drive can be quickly and safely removed from an externally-accessible hot-swap bay in the event of an impending disaster, such as a hurricane or ransomware attack.

Non Domain Systems:

Files stored on systems that are not joined to the domain are backed up quarterly to an external portable USB hard drive.

Uninterruptable Power Supply (UPS) Equipment:

The Information Systems Specialist is responsible for the purchase, maintenance, and replacement of all UPS's in the agency. At the time of a power failure, critical IT Equipment will start operating on UPS power. Users must immediately save any work in progress, exit out of all programs, and shutdown their system.