

INFORMATION TECHNOLOGY

Information Technology Infrastructure

Data Backups, Data Processing Recovery, and Contingency Planning

This regulation supersedes Regulation 6221.1

I. PURPOSE

To establish an IT Business Continuity program for the Fairfax County Public Schools (FCPS) computer systems and facilities.

II. SCOPE

A. Definitions

1. The term "computer system(s)" as used herein includes all of the following used in the administrative network: hardware; software; data; communication devices; terminals; printers; and micro, mini, mainframe, and personal computers.
2. The term "backup" as used herein refers to the process of copying all files and programs resident on the computer disk(s) onto either magnetic tapes or additional disk(s).
3. The term "disaster" as used herein refers to the natural, accidental, or willful destruction of electronic data processing facilities, which can cause a significant disruption of information processing capabilities for a period of time, adversely affecting the normal operations of an organization.
4. The term "business impact analysis" or "BIA" as used herein refers to an analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
5. The term "business continuity plan" or "BCP" as used herein refers to the documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption. IT policy and procedures designed to maintain or restore computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

6. The term “contingency plan” as used herein refers to policy and procedures designed to maintain or restore IT operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.
7. The term “disaster recovery plan” or “DRP” as used herein refers to a documented plan for restoring critical applications in the event of a major hardware or software failure or destruction of facilities.

B. Applicability

This regulation applies to all computer systems of the FCPS administrative computer network.

III. RESPONSIBILITY

The Office of Information Technology Operations shall establish an individual as program administrator, responsible for the coordination and ongoing maintenance of a formal IT Business Continuity program.

IV. DISASTER RECOVERY PLANNING

- A. The Office of Information Technology Operations shall plan for the possibility of a disaster occurring to the computer systems and shall incorporate necessary actions into the normal activities of the FCPS Network Operations Center to ensure data recovery capabilities.
- B. Guidelines shall be established and enforced for maintaining the environmental standards of the Network Operations Center.
- C. Preventive measures shall be taken to ensure the physical safety of the Network Operations Center to include, but not be limited to, smoke sensors, water sensors, alarms, fireproof safes, and a fire suppression system.
- D. All computer and computer-related equipment shall be inventoried and insured for current replacement costs in accordance with the current version of Policy 5710.
- E. The Department of Information Technology shall coordinate with the various system sponsors a plan for supporting all critical applications should a disaster occur.

V. COMPUTER SYSTEM BACKUP RESPONSIBILITIES

- A. The Office of Information Technology Operations, Department of Information Technology, shall be responsible for the backup of all computer systems located within the Network Operations Center. A complete set of backup tapes shall be produced and should be stored off site to provide for the recovery of data and software should a disaster occur.
- B. Program managers shall ensure that source documents or transaction listings are available to replace data should a disaster occur. This information must be available for reentry on a daily and monthly basis.
- C. Program managers shall be responsible for the backup of all microcomputers and personal computer applications and software as necessary. When possible, backup data shall be stored off site in a safe and secure manner.

See also the current version of: Policy 5710, Property and Casualty Coverage and Bonds