

**Polk County Government**  
**PHYSICAL SAFEGUARDS**  
**Contingency Planning**  
**Data Criticality and Access Control Policy and Procedures**

**Policy 603.G**

**Effective: April 19, 2005**

**Revision Date:**

## **I. Policy**

- A. Polk County Government will assess the relative criticality of specific applications and data in support of other contingency plan components, as part of the disaster recovery plan.
- B. Polk County Government will establish and implement, as necessary, procedures that allow Polk County Government facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

## **II. Procedures**

- A. The Information Technology Department will develop a matrix using an inventory of all software applications and the importance of the application to Polk County Government to determine a prioritization for disaster recovery. See *Applications and Data Criticality Analysis Form*.
  - 1. Inventory all software applications.
  - 2. Determine on the basis of most, average and least important, the necessity of the software application to Polk County Government.
- B. The matrix will be used to determine which software applications are most important to Polk County Government and thereby determine how efforts will be focused in a disaster event. The matrix may direct:
  - 1. What application gets restored first?
  - 2. Which applications receive the first line of assistance?
- C. The Information Technology Department will be responsible for documenting all activities relating to the applications and data criticality analysis. The documentation will be maintained and retained by the Privacy Officer for six years from the date of creation.
- D. The Information Technology Department will be the primary contact for determining how access will be achieved in the event that data access is disrupted.

- E. The Information Technology Department will list all workforce members and tasks that will be related to data recovery at the time of the disruption.
- F. The Information Technology Department will develop a list of contact individuals that will operate as primary contacts in the data recovery effort. The list will be developed based on knowledge of the system and understanding of data recovery processes.
  - 1. The contact individuals may include a data recovery company or a technology expert who can assist in the recovery process.
- G. The Parks and Buildings Department, in coordination with the Emergency Management Office and Law Enforcement will designate who has access to the facility and the information systems after a disaster.
- H. The Parks and Buildings Department, coordination with the Emergency Management Office and Law Enforcement will also develop a secondary list authorizing facility access in the event that individuals authorized to access the facility in a disaster are not available.
- I. The Parks and Buildings Department, in coordination with the Emergency Management Office and Law Enforcement will be responsible for developing and implementing a plan that will secure the building in the event of a disaster.
- J. The Information Technology Department, Parks and Buildings Department, in coordination with the Emergency Management Office and Law Enforcement will document all activities related to contingency operations and data recovery. The documentation will be maintained and retained for at least six years from the date of creation.