



Kansas Health Policy Authority Operational Policy

Title: Contingency Plan Policy

Number: POL-IT:2007-06

Effective date: 5-10-2007

Date Revised: None

Date of Annual Review: 5-19-08

Authority: POL-IT:2007-01

CATEGORY

Information Technology

SUBJECT

Security Planning

BACKGROUND

Kansas Health Policy Authority is responsible for properly protecting State government assets. This policy addresses KHPA's requirements as written by the HIPAA Security Rule in 45 CFR 164.308(a)(7)(i) [2003] and the State of Kansas Information Technology Executive Council's Default Information Technology Security Requirements, March 2006 version, section 8.2.

POLICY STATEMENT

KHPA's Chief Financial Officer is responsible for keeping the Business Contingency Plan updated to assure the continuation of vital State operations in the event of a disaster. The Business Contingency Plan contains the internal policies, procedures, and recovery strategies that are to be employed should a disaster occur. Examples of disasters include fire, vandalism, system failure, and natural disaster. In the event of a disaster all time-sensitive services, systems, and applications must be restored and available on a priority basis to maintain vital KHPA operations.

Time-sensitive applications include those systems whose loss or unavailability is unacceptable to the citizen's of Kansas. The loss or unavailability of support services provided to these applications may adversely affect the continuation of vital programs and services or the fiscal or legal integrity of KHPA operations.

SPONSOR/CONTACT

Chief Operations Officer