OFFICE OF ADMINISTRATION ADMINISTRATIVE POLICY

POLICY TITLE: **Breach Policy**	AUTHORIZED BY: **Sarah H. Steelman** Commissioner
POLICY : **C-19**	PAGE: **1 of 4**
ISSUED: **October 2018**	REVISED:

I. Purpose

The purpose of this policy is to provide a process for the Office of Administration to respond to a data breach and to play a significant role in the Office of Administration's business continuity plan.

II. Scope

This policy covers all Office of Administration data and the people, processes and technology that handle it.

III. Policy

A. Office of Administration Responsibilities

1) Data Classification

In order to prepare for any data-related disaster, including a breach, the Office of Administration is responsible for identifying and appropriately classifying the data it owns. The data's classification level plays a significant role in determining the magnitude of the breach and its corresponding response.

For purposes of this policy, "data" includes all information electronically stored or retained by the Office of Administration that is also owned by the Office of Administration. The Office of Administration should be aware of what data it has in its possession, and its storage location(s).

2) Reporting

Any Office of Administration employee or contractor who suspects that there has been a theft of or unauthorized access to Office of Administration data, and any ITSD employee or contractor who suspects that there has been a theft of or unauthorized access to any state agency's data, shall immediately call the Office of Cyber Security (OCS) at 573-751-3290 or 573-751-1550 (24 hours a day). OCS will investigate all suspected theft or unauthorized access reports and work with Office of Administration staff to determine what occurred.

A theft of or unauthorized access to data includes, but is not limited to, a stolen laptop, phone, or other electronic device.

If criminal conduct occurred such as breaking and entering or stealing equipment, the crime scene should be left undisturbed and a local law enforcement agency should be contacted based on the location and details of the incident. If a local law enforcement

agency is contacted, the name of the agency and the report number should be provided to OCS via the phone numbers specified above.
In reporting any incident, the Office of Administration will identify any third parties that are involved or impacted by any theft or exposure. Third parties could be contractors, state agencies, other governmental entities, and private individuals.

The Office of Administration should be notified of the reported theft or unauthorized access as soon as possible. In addition, OCS will assist in determining the data's owner and coordinate notification if it has not already occurred.

3) Public Relations

a. Call Center
Based on the severity of the breach as determined by the Office of Administration, a call center may need to be established to address questions from potentially impacted individuals.

b. Breach Website
Based on the severity of the breach as determined by Office of Administration, a website with information about the breach may need to be established to inform the general public, impacted individuals, and the media.

4) Notifications

Depending upon the situation, it may be necessary to notify the public, impacted individuals, or the media via one or more methods. The Office of Administration may need to coordinate such efforts.

a. Print
Based on Office of Administration and other third party requirements, impacted individuals may need to be contacted about the details of the breach via regular mail. Besides determining the content of the notifications, the Office of Administration may need to establish a mechanism to promptly print and mail any necessary notifications.

b. Email
Based on Office of Administration and other third party requirements, impacted individuals may need to be contacted about the details of the breach via email. Besides determining the content of the notifications, the Office of Administration may need to establish a mechanism to promptly email any necessary notifications.

c. Phone
Based on the Office of Administration and other third party requirements, impacted individuals may need to be contacted about the details of the breach via phone. Besides determining the content of the notifications, the Office of Administration may need to establish a mechanism to promptly call impacted individuals.

d. Social Media
The Office of Administration may have a social media plan to address questions and communicate with the public or potentially impacted individuals.

5) Credit Monitoring

In the event of a breach, the Office of Administration may elect to offer credit monitoring and reporting services.

6) Business Continuity

Because a breach may disrupt critical human and IT resources for a prolonged period of time, the Office of Administration may utilize backup processes to ensure business continuity.

B. ITSD Responsibilities

1) Incident Response

OCS will act as the primary technical incident responder. The Security Operations Center within OCS will lead the technical investigative efforts, with the advice of Office of Administration legal counsel. OCS will work to determine the root cause of the breach, quarantine impacted state managed hosts (i.e., any devices with an ITSD-configured IP address residing on a state wired or wireless network), remediate existing vulnerabilities, and provide a technical timeline of the incident. OCS manages multiple incident response procedures and can tailor them for the particular incident. If the breach reaches a magnitude of a statewide emergency, ITSD has a Memorandum of Understanding with the Missouri National Guard to assist in the incident response efforts.

OCS will share incident information with the Office of Administration for consideration of any appropriate disciplinary action, change in policy, and revision of data classification and retention procedures.

2) Technical Assistance and Guidance

   Throughout the breach response period OCS will provide technical assistance and guidance to the Office of Administration designees and their assigned legal staff. OCS will guide the Office of Administration through the technical aspects of the incident and work closely with them until closure. OCS will identify and interpret relevant information related to the breach including but not limited to logs, technical reports, vulnerabilities, exploits, and attack vectors.

3) Evidence Collection and Preservation

   With guidance from Office of Administration legal counsel, OCS will preserve any evidence associated with the breach including but not limited to logs, databases, files, server images, endpoint images, mobile devices, and screenshots. Where applicable, OCS will ensure proper chain of custody throughout the evidence collection and preservation period.

IV. <u>Policy Compliance</u>

The Office of Administration will review its breach policy and seek comments from OCS as circumstances indicate. As the data owner, the Office of Administration is responsible for meeting any compliance requirements driven by applicable data protection laws.