MISSOURI DEPARTMENT OF TRANSPORTATION **PERSONNEL POLICY MANUAL**	**Chapter Title** Employee Conduct		
	Policy Title Data Breach		
	Policy Number 2515	**Page** 1 of 4	**Effective Date** December 31, 2017
Approved By Micki Knudsen, Human Resources Director Signature on File	**Supersedes Policy Number** n/a	**Page** n/a	**Prior Effective Date** n/a

POLICY STATEMENT

The purpose of this policy is to provide a process for the department to respond to a theft or unauthorized access of department data and to play a significant role in the department's business continuity plan. This policy covers all department data and the people, processes, and technologies that handle it. As the data owner, the department is responsible for ensuring it meets or exceeds all compliance requirements driven by applicable data protection laws and regulations. Non-compliance with this policy may be cause for disciplinary action, up to and including, termination.

DEFINITIONS

Data: Includes, but is not limited to, all documents, whether they are in paper, electronic, or some other format. The department should be aware of what data it has in its possession and its storage location(s).

Theft or Unauthorized Access of Data: Includes, but is not limited to, a stolen, lost or improperly accessed laptop, phone, or other electronic device that contains data, along with stolen, lost, or improperly accessed electronic or paper documents or files containing data.

Third Parties: Includes, but is not limited to, contractors, state agencies, other governmental entities, and private individuals.

Physical Criminal Conduct: As it relates to this policy, includes, but is not limited to, breaking and entering into department property where data is located or stealing information technology resources or equipment that contains data.

Information Technology Resources: Networks, workstations, servers, computers, all supporting software, cellular and standard telephones, printers, fax machines, and copiers.

Information Technology Equipment: Refers to hardware such as personal computers, notebook computers, hand-held electronic communication devices, cellular telephones and software, as well as operating systems and software required to perform activities such as word processing, statistical analysis, graphics, and computer aided drafting.

PROVISIONS/REQUIREMENTS

1. The department is responsible for identifying and classifying its data in order to prepare for any data related disaster, including a breach. The data's classification level plays a significant role in determining the magnitude of the breach and the department's corresponding response. For more information about data classification, please review the Office of Administration (OA) Information Technology and Services Division's (ITSD) Data Classification Policy.

2. It is the responsibility of each district/division/office to instruct employees on the reporting procedures and requirements of the Data Breach policy.

3. Any department employee or contractor who suspects theft or unauthorized access of department data shall immediately call the Audits and Investigations Division (AI) at 573-751-7446.

4. AI will investigate all reported theft or unauthorized access, in coordination with the appropriate law enforcement agency as needed, and work with the Chief Counsel's Office (CCO) and the Information Systems Division (IS) to determine the scope and nature of the breach.

5. In addition to a theft or unauthorized access of data, signs of tampering with locked file cabinets or storage lockers, or indication of the exposure to unauthorized individuals or entities of confidential electronic data, or any other indication that data is, or might have been, potentially compromised must be reported to AI.

6. Any third parties that are involved or impacted by any theft or exposure must be identified.

7. The district engineer or division leader/state engineer where the reported theft or unauthorized access occurred must be notified as soon as possible. In addition, AI will assist in determining the data's owner, and coordinate notification with the appropriate district/division/office if it has not already occurred.

A. Based on the severity of the breach as determined by CCO, AI, and IS, a call center may need to be established to field questions from potentially impacted individuals.

B. Based on the severity of the breach as determined by CCO, AI, and IS, a website with information about the breach may need to be established to inform the general public, impacted individuals, and the press.

8. Depending upon the situation, one or more methods may be employed to provide any required notifications. Therefore, the department's Communications Division (CR) may need to coordinate such efforts with legal guidance from CCO, which may include sharing information with the media. Notifications may include:

A. Print – Impacted individuals may need to be contacted about the details of the breach via post, email, or telephone.

B. Social Media – CR should have a social media plan in place to field questions and communicate directly with potentially impacted individuals.

C. Contractor Employees – In the event of a data breach that exposes contractor data, CR shall notify the affected contractors so that they may in turn notify their employees.

9. In the event of a breach, the department may elect to offer credit monitoring and reporting services to impacted individuals.

10. As a breach may disrupt critical human and information technology resources for a prolonged period of time, IS shall establish the necessary backup processes to ensure business continuity.

11. In the event of a breach, IS will be responsible for the following.

A. IS will act as the primary technical incident responder. IS, with the assistance of the Security Operations Center within OA's Office of Cyber Security (OCS), will lead the technical investigative efforts and work with legal guidance from CCO. IS will establish the root cause of the breach, quarantine impacted state managed hosts, remediate existing vulnerabilities, and provide a technical timeline of the incident. IS will manage multiple incident response procedures and will 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.

B. Throughout the breach lifecycle, IS will provide technical assistance and guidance to AI and CCO, and to any designees. IS will guide the department through the technical aspects of the incident and work closely with OCS until incident 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.

C. Based on guidance from AI and CCO, IS and 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. IS and OCS will preserve the evidence based on the requirements handed down from CCO. Where applicable, IS will ensure proper chain of custody throughout the evidence collection and preservation lifecycle.

D. Based on guidance from IS and OCS, the department may disable or otherwise modify the operation of roadside message boards in the event of a data breach that threatens the department's ability to exclusively control the operation of the boards.

E. If a data breach involves the theft or exposure of data concerning the design, operation, security, or structural vulnerabilities of the department's infrastructure including, but not limited to, roads, bridges, or multimodal structures, the department shall alert the relevant local law enforcement agencies where that infrastructure is found. The department shall take all prudent precautions to protect customers if the data breach might precipitate or enable an attack on physical infrastructure.

CROSS REFERENCES

Personnel Policy 2503, "Communications and Information Systems"