

## **HR Investigation Standard**

### **Introduction**

Office of Management and Enterprise Services requires all employees (including contractors, volunteers or any individual representing OMES) to conduct themselves professionally in accordance with established OMES policies, procedures and/or directives. Every employee shall fulfill the duties of the office or position conferred upon the employee and shall conduct themselves at all times in a manner befitting the office or position held by the employee.

### **Purpose**

This document establishes guidelines for a systematic and confidential process for HR investigations of employees suspected of involvement in cybersecurity incidents, including but not limited to data breaches, unauthorized access, data theft or other security violations. This standard helps protect sensitive information, prevent future incidents and ensure investigations are conducted ethically and legally in case of suspected employee misconduct necessitating further investigation. This standard supports the state's efforts to minimize institutional risk and provide a safe environment.

All investigations are treated confidentially to the extent possible. Information is disclosed strictly on a need-to-know basis. All individuals involved in an investigation process are expected to maintain confidentiality of the proceedings. Confidentiality does not mean the details of the investigation will be withheld from the accused party or parties, or that OMES is constrained from divulging details of the investigation in appropriate circumstances.

All employees are required to cooperate during any official investigation. Failure to cooperate may be grounds for disciplinary action up to and including termination.

### **Definitions**

Employee – Includes contractors, volunteers or any individual representing OMES.

Investigator – Human Resources and Cyber Command.

### **Standard**

During the investigation, the state agency may place a state employee on administrative leave and require the employee to remain available during specified work hours to meet with investigators or other state agency officials, as necessary.

Depending on the results of the internal investigation, the employee may be subject to progressive disciplinary action, immediate termination, or involvement of local law enforcement, as circumstances dictate.

Investigation process.

- The investigation will be conducted discretely and professionally, minimizing disruption to normal business operations.
- Investigators will follow the established procedures for collecting evidence, interviewing witnesses and analyzing digital records.
- The chain of custody for digital evidence must be maintained, and the Cyber Command analyst will follow the Forensics Process SOP.

Analysis and Findings.

- Evaluate all evidence and information gathered during the investigation.

- Determine whether the complaint or allegation is substantiated.
- Prepare a clear and comprehensive report of findings.

**Timeliness.**

- Investigations should be conducted promptly and efficiently to minimize disruption to the workplace and ensure a fair and timely resolution.

**Training and Continuous Improvement.**

- OMES personnel, including HR/Cyber Command responsible for conducting investigations, should receive regular training on investigative techniques, software/hardware to aid the investigation, legal requirements and best practices.

**Compliance**

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

**Rationale**

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

**References**

- [OMES Code of Conduct.](#)
- [OMES Code of Ethics.](#)
- [OMES Computer and Mobile Computing Device Usage.](#)
- [Anti-Violence/Bullying – Violence in the Workplace.](#)
- [OMES Complaint and Investigation Process.](#)
- [Civil Service and Human Capital Modernization Rules, 260: 130-19-8.](#)
- [IS 03.01.07 Digital Forensic SOP.](#)
- [IS 03.01.06 HR Investigation SOP.](#)

**Revision history**

This standard is subject to periodic review to ensure relevancy.

<b>Effective date:</b> 01/12/2024	<b>Review cycle:</b> Annual
<b>Last revised:</b> 01/12/2024	<b>Last reviewed date:</b> 01/12/2024
<b>Approved by:</b> Joe McIntosh, Chief Information Officer	