



Background Check Standard

Introduction

OMES utilizes a confidential pre-employment background check to reduce risk to the State of Oklahoma and has a standardized process for employing qualified individuals. OMES requires background checks for all final candidates, as well as state employees who are currently in positions where a background check is required by law or state policy. OMES also requires staff augmentation and professional services contractors to adhere to the same level of background checks.

In an effort to simplify background check requirements for federal regulations, OMES adheres to the requirements specified in the [Criminal Justice Information Service \(CJIS\) Security Policy, Version 5.9](#), as it is the most stringent and meets and/or exceeds the criteria for all others.

Purpose

OMES is committed to promoting a safe and secure working environment. To this end, this standard sets forth requirements for background checks for potential employees, current employees, staff augmentation and professional services contractors.

Standard

The State of Oklahoma requires background checks on all final candidates for state positions and contract engagements. OMES utilizes two different background checks: standard criminal and criminal justice information services.

- Standard criminal background checks are facilitated by OMES HCM and conducted by a third-party vendor. This type of check may include social security trace, county criminal records for seven years, federal criminal records for seven years and national sex offender and federal watch lists.
- Enhanced background checks are based on the most current version of the CJIS security policy and facilitated by the Department of Public Safety. This type of check provides identifying information and a set of fingerprints to the FBI to match against criminal background information maintained in its database. The FBI database includes information on both federal crimes and crimes reported by states.
 - It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.
 - Basic security awareness training is required within six months of initial assignment and every two years thereafter. This type of check is required for individuals requiring elevated credentials and meet the following criteria.
 - Requires computer access or access to any equipment that stores, processes or transmits criminal justice information, federal tax information and other types of sensitive data.
 - Requires physical access to sensitive areas of state facilities.

OMES requires a standard criminal background check on all final candidates for state positions and enhanced background checks for roles meeting the enhanced criteria outlined above. For new hires, a conditional offer of employment is based on the candidate's successful completion of the applicable background check. If a job offer is extended prior to the completion of the background check, the job offer is contingent upon the confirmation the background check was completed successfully.

OMES requires, at the vendor's expense, a standard criminal background check be completed on all candidates for staff augmentation and professional services engagements, with a pass/fail certificate provided to OMES. For roles meeting the enhanced criteria outlined above, enhanced background checks must be coordinated through OMES, also at the vendor's expense, and successful clearance is required for all individuals prior to the beginning of the engagement.

Employees who are under consideration for positions in which a background check is required by law or who are under consideration for positions that meet the criteria outlined above are required to undergo background checks.

All employees and contractors are subject to background rechecks based on position, role and/or regulatory requirements.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 51 O.S. §§ 151-172. OMES 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

- [Criminal Justice Information Service \(CJIS\) Security Policy, Version 5.9.](#)

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 05/11/2021	Review cycle: Annual
Last revised: 08/16/2024	Last reviewed: 08/16/2024
Approved by: Janet Morrow, Director of Risk, Assessment and Compliance	