Biometric Data Security Standard

Introduction
The State of Oklahoma uses biometric identification systems to increase security and control access to certain agency buildings. OMES Information Security recognizes the sensitivity of biometric data and is committed to ensuring the confidentiality and security of the data.

Purpose
This document defines the guidelines for collection, use, safeguarding, storage, retention and destruction of biometric data collected by the state.

Definitions
Biometric data – Information regarding a measurable physical or behavioral characteristic specific to an individual.

Biometric identifier – Biometric data used to digitally identify a person to grant access to systems, devices or data. Examples are retinal or iris scan, fingerprint, voiceprint or scan of the hand or face geometry. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used or stored for health care treatment.

Hash – A function that converts an input of data into an encrypted output of a fixed length. A hash is created using an algorithm.

Personal Identity Verification (PIV) – Credentials used to access controlled facilities and information systems at the appropriate security level.

Standard
Biometrics refers to the science of measuring, recording and analyzing the unique physical attributes of a person. Biometric data is data collected from an individual that is unique to them. As used in this standard, biometric data includes biometric identifiers.

Biometric identifiers are used to create PIV credentials for an individual. These credentials are used to access controlled facilities and information systems. Once implemented at an agency, PIV provides security, authentication and identity attributes for employees and contractors. PIV credentials have certificates and key pairs such as PINs, biometrics like fingerprints and retinal scans or other unique identifiers. PIV provides the capability to implement multifactor authentication for networks, applications and buildings.

An individual's biometric data is not collected or otherwise obtained by an agency without prior consent. The consent informs the individual the reason the biometric information is being collected, as well as the following:

- Details regarding the collection, storage and use of such biometric data.
- Specific purpose and length of time for which the biometric data is collected, stored and used.

An agency shall not sell, lease, trade or otherwise profit from an individual's biometric data. An agency shall not disclose, redisclose or otherwise disseminate an individual's biometric identifier or biometric information unless:

- The subject of the biometric identifier or biometric information consents to the disclosure of redisclosure.
- Disclosure or redisclosure is required by applicable law, regulation or rule.
- Disclosure is required under a valid warrant or subpoena issued by a court of competent jurisdiction.

The following security requirements apply to biometric data:

- The agency shall minimize collection, storage and use of biometric data to the minimum amount necessary.
- The state agency uses a reasonable standard of care to store, transmit and protect from disclosing any electronic biometric data collected. Storage, transmission and protection from disclosure are performed in a manner that is the same as or more protective than how state agency stores, transmits and protects from disclosure other confidential and sensitive information used to uniquely identify an individual.
- A vendor can manage biometric identification devices, and the software required for the device. However, the collection, storage, handling and destruction of employee data shall be done by the agency.
- Encryption is required for all devices that may be used to store or access biometric data. Additionally, all transmissions of biometric data shall be encrypted at rest and in transit with controlled access. Reference NIST FIPS 140-2 – Security Requirements for Cryptographic Modules for encryption standards.
- Data should be protected by strong passwords that are changed regularly and never shared among employees. Password requirements must be consistent with the Password Requirements Standard.
- Biometric hashes are considered restricted data and must be handled accordingly.

The following data retention and disposal requirements apply to biometric data:

- Unless a longer retention period is required by applicable law, regulation or rule, the agency retains biometric data only for so long as the agency's use of the biometric data is necessary to accomplish the purpose for which it was collected. Biometric data shall be destroyed consistent with the Media Disposal Standard.

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

- Data Security Standard.
- Account Management Standard.
- NIST FIPS 140-2 – Security Requirements for Cryptographic Modules.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 08/12/2021	**Review cycle:** Annual
Last revised: 02/12/2025	**Last reviewed:** 07/17/2025
Approved by: Janet Morrow, Director of Risk, Assessment and Compliance	