State of Oklahoma 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 – Data collected from an individual unique to their person. Common biometric data include fingerprint, retina scan, voiceprint, hand scan and facial patterns.

Biometric identifier – Physical human characteristics used to digitally identify a person to grant access to systems, devices or data. Examples are retina 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 collection, used or stored in health care treatment.

Biometric information – Any information, regardless of how it is captured, converted, stored or shared, based on an individual's biometric identifier used to identify them. Biometric information does not include the excluded items listed in the biometric identifier definition.

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 – Credentials used to access controlled facilities and information systems at the appropriate security level. PIV credentials have certificates and key pairs, PINs, biometrics like fingerprints and retina scans and other unique identifiers. It provides the capability to implement multifactor authentication for networks, applications and buildings.

Standard

1. 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 policy, biometrics data includes biometric identifiers and biometric information.
2. Biometric data is 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.

Disclosure and Authorization

1. 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:
    a. Details regarding the collection, storage and use of such biometric data.

    b. Specific purpose and length of time for which the biometric data is collected, stored and used.
2. 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 individuals' biometric identifier or biometric information unless:
    a. The subject of the biometric identifier or biometric information consents to the disclosure or redisclosure.
    b. Disclosure or redisclosure is required by state or federal law or municipal ordinance.
    c. Disclosure is required under a valid warrant or subpoena issued by a court.

Security

1. 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.
2. 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.
3. 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. Please see NIST FIPS 140-2 – Security Requirements for Cryptographic Modules for encryption standards.
4. Data should be protected by strong passwords that are changed regularly and never shared among employees. Password requirements must be consistent with the State of Oklahoma Information Security Policy, Procedures, Guidelines policy. The password requirements policy is found in section 2.1.4.
5. Biometric hashes are considered restricted data and must be handled accordingly.

Data Retention

1. The agency retains biometric data until one of the following occurs:
    a. Employment is terminated or employee moves to a different role or position where biometrics are not used.
    b. Individual consents to such disclosure or dissemination.
    c. Agency no longer uses the biometric information.
    d. The data retention period is exceeded.
2. Biometric data shall be destroyed consistent with the Disposal of Media policy found in the State of Oklahoma Information Security Policy, Procedures, Guidelines. The Disposal of Media policy is found in Appendix E, Section 3.

References

1. State of Oklahoma Information Security Policy, Procedures, Guidelines.
2. 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	**Last Reviewed:** 08/12/2021
Revision Date: 08/12/2021	**Review Cycle:** Annual
Approved by: Jerry Moore, Chief Information Officer	