STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

GUIDELINE 630G1: Biometric Authentication

VERSION NUMBER	Guideline 630G1-01
VERSION DATE	August 10, 2018
GUIDELINE TITLE	Biometric Authentication
GOVERNING POLICY	This guideline is governed by Policy 630: Identification and Authentication, regardless of revision.

OBJECTIVE

The objective of this guideline is to provide recommended best-practices for the implementation and use of biometric data (which includes fingerprints, palm prints, DNA, iris, and facial recognition) used in multi-factor authentication to verify the identity of individuals.

SUPPORTING DOCUMENTS

The following documents support this guideline:

- Policy 630: Identification and Authentication
- Standard 630S1: Authenticator Management

The following special publications (SP) of the National Institute of Standards and Technology (NIST) support this guideline and may aid in its implementation:

- NIST SP 800-76-2: Biometric Specifications for Personal Identity Verification

GUIDELINE

A biometric system is an automated system capable of capturing a biometric sample from an end user, extracting biometric data from the sample, comparing the biometric data with that contained in one or more reference templates, deciding how well they match, and indicating whether verification of identity has been achieved. Depending upon the biometric technology and the risk environment, using biometrics to supplement other authentication factors will likely enhance security. Where biometric authentication is used (as a factor in multi-factor authentication), the following security controls should be implemented.

MANAGEMENT CONTROLS

IT Managers should ensure that individuals are assigned to the following administrative roles:

- Enrollment Administrator – the individual who verifies the identity of new users and guides them through the creation of their associated biometric reference templates using the biometric capture device.
- Security Administrator – the individual who establishes and modifies the values of configuration parameters in the biometric software.
- Audit Administrator – the individual who reviews audit logs for security violations and related suspicious behavior.

IT Managers should maintain lists of individuals authorized to perform each of the following functions: enroll or re-enroll users; modify the security configuration; and review and manage audit logs.

IT Managers should ensure the following functions are restricted to authorized Administrators:

- Creation or modification of authentication rules
- Creation, installation, modification or revocation of cryptographic keys
- Startup and shutdown of the biometric service

IT Managers should ensure that only authorized Enrollment Administrators are permitted to create user biometric templates.

IT Managers should ensure that only authorized Audit Administrators can clear the audit log or modify any of its entries.

IT Managers should ensure that all Administrators must authenticate to the biometric system to perform administrative functions and that this authentication must include a factor outside of the biometric verification the system supports for other users.

ENROLLMENT CONTROLS

The strength of the authentication required in the enrollment process should never be less than the strength of authentication required during the verification process. This could lead to an attack on the enrollment process.

IT Managers should ensure that the enrollment process is conducted by an authorized Enrollment Administrator who will at a minimum check that the enrollee has submitted all required documentation used to authorize access to the system for which the biometric system supports authentication, and ensure the enrollee presents a valid photo ID.

IT Managers should ensure that users cannot self-enroll biometric information (i.e., enroll outside of the presence of an authorized Enrollment Administrator).

Potential enrollees who do not have the physical characteristics needed to provide the intended biometric sample should be offered an authentication alternative that does not pose an undue burden on the enrollee, nor creates an inherent weakness in the authentication process that could be easily impersonated or exploited.

To protect against the threat of a poor biometric template, there must be some form of quality control during the initial capture process. Good biometric software will prohibit the creation of clearly inadequately specified templates, however, there is a possibility of a marginal template entering the system (i.e., just good enough to pass quality criteria, but still noisy enough to be susceptible to a sophisticated attack).

IT Managers should ensure that Enrollment Administrators receive appropriate training that covers, at a minimum:

- The user identification and authorization requirements
- How to use the biometric software and capture device to obtain an acceptable user template
- How to identify when a template is unacceptable and needs to be recreated

Enrollment Administrators should re-create templates when there is an indication that a template has not been properly captured.

The Security Administrator should configure the system to search for matches between the enrolled template and previously existing templates and reject enrollment when a match is discovered. If this process cannot be automated, the Enrollment Administrator should enforce this requirement manually.

VERIFICATION CONTROLS

Verification is the process that supports routine user authentication. A user seeking physical or logical entry presents a live biometric sample to a capture device, which extracts a digital representation of the sample and transfers it to a comparator.

False Acceptance and False Rejection:

The central risk of the verification process is that the technology will mistakenly verify a user’s identity when that person is actually someone else – known as *false acceptance*. Human beings are constantly changing (we age, gain and lose weight, sustain injuries, modify behavior, etc.) therefore biometric systems must have some tolerance for error or common everyday changes in individuals would lead to *false rejection.*

There is a tradeoff between the *false acceptance rate* (FAR) and *false rejection rate* (FRR). A high FAR means that security may be unacceptably weak; a high FRR means that the technology is likely to be a significant nuisance to falsely rejected users.

- The Security Administrator should set the FAR to be no greater than 1 in 100,000.
- The Security Administrator should set the FRR to be no greater than 5 in 100.

Inevitably, there will be some false rejections that require intervention to allow proper access (e.g., the recently injured user). IT Managers should designate personnel who have the authority to override false rejections and ensure that they receive proper training in how to implement the fallback protocol and verify a user’s identity.

Liveness Checks:

Most leading biometric solutions have “liveness” checks that take some action to validate that the sample is coming from a live human being and not a facsimile. The Security Administrator should activate at least one of the available “liveness” checks.

IT Managers should document alternative identification and authentication procedures for users that are unable to present the required live biometric sample (such as when a user has a disability or injury).

Failure to Match:

The Security Administrator should configure the biometric system to:

- Prohibit the identical biometric sample from being used in consecutive authentication attempts
- Not reveal to a user any information related to how close the live sample supplied is to the corresponding biometric template

Exact Matches:

An "exact match" occurs when the digital representation of the live sample extracted from the capture device is identical to the stored biometric template to which it is compared. In most applications, an exact match is a good thing, but in biometrics, it is cause for suspicion. There is inherent variability in the sample capture process that makes exact matches unlikely for many biometric technologies. When one occurs, it may be indicative that someone has improperly obtained the biometric template and is staging a replay attack.

To mitigate the risk of bypass and replay, IT Managers should ensure that there is adequate physical security, encryption of transmitted data, monitoring, and rejection of "exact matches".

IT Managers should ensure that the physical connections between the following biometric system components are adequately secured:

- The connection between the capture device and the comparator.
- The connection between the comparator and the biometric-supported access control system.

FALLBACK CONTROLS

Fallback is the condition that occurs when the biometric system is not in use. In some cases, the biometric technology provides partial fallback mechanisms within the system itself. These approaches should be employed whenever feasible.

IT Managers should ensure that any override of the biometric system is accompanied by a photo ID check of the user and documentation of the following:

- The name of the user who was granted entry with the override
- The time the override occurred
- The reason for the false rejection

IT Managers should establish adequate identification and authentication procedures that must be followed whenever the biometric system is unavailable.

TECHNICAL CONTROLS

The Security Administrator should ensure biometric templates are protected by operating system permissions.

The Security Administrator should ensure that no user ID has access to the files other than those required for running the biometric application software.

Encryption:

The Security Administrator should:

- Ensure the biometric system is encrypted in accordance with state standards.
- Ensure that only the process running biometric software is able to read relevant private or shared secret keys (with the exception of key super-session events during which the Security Administrator may temporarily have the ability to replace the key [e.g., to modify the key file]).

The Security Administrator should configure the biometric system to:

- Encrypt and digitally sign all biometric data before it is transmitted from one physical device to another.
- Encrypt all biometric data resident on non-volatile memory or storage media.

Monitoring and Auditing:

IT Managers should ensure that the file permissions and storage scheme for biometric audit logs is no less secure than the scheme for the system audit logs of the operating system on which the biometric software resides.

The Security Administrator should configure the biometric system to audit the following transactions:

- All “exact match” verification transactions
- All failed identification or authentication attempts
- All start and stop events for the biometric service

EFFECTIVE DATE

This guideline shall be effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.

SUPERSEDES

This is the initial guideline and does not supersede a previous version.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this guideline to be adopted as of the 28 day of August, 2018.

Jim Purcell
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
630G1-01	08/10/2018	Initial version