STATE OF ALABAMA

Information Technology Policy

POLICY 623-02: AUTHENTICATION

Users must uniquely identify themselves to a system or network resource and verify that identity with one or more authentication factors. Authentication factors include something a person *knows* (password, pass-phrase, PIN, etc.), something a person *has* (token, access card, etc.), or something a person *is* (biometric such as a fingerprint, retina scan, etc). Information Services Division (ISD) uses two-factor authentication (2FA), password plus token, for authentication to its major information system points of entry (i.e. VPN, mainframe/RACF, Outlook Web Access, etc.).

OBJECTIVES:

This policy defines the minimum requirements for authenticated access to State information systems and provides the requirements for:

- Password implementation, safeguard, and use
- Two-factor authentication token implementation, safeguard, and use
- Biometric authentication implementation and use

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

Identification and Authentication: All organizations operating information systems shall:

- Ensure information systems uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).
- Ensure information systems uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).
- Ensure every user is assigned a unique user identification and authentication mechanism (e.g., user ID and password) so all activities on a system or network are traceable to a specific user.
- Document system-specific identification and authentication requirements in system operating procedures.
- Ensure information system users are advised on protecting identifiers and the corresponding authentication mechanisms.

GENERAL SECURITY REQUIREMENTS

The following general security requirements apply to all types of authentication factors and/or processes:

- Authentication factors must never be shared, cached, stored in any readable form, or kept in locations where unauthorized persons might discover them.
- Ensure systems obscure feedback of authentication information during the authentication process.

PASSWORD REQUIREMENTS

PASSWORD POLICY SETTINGS

Enterprise client systems shall be configured by group policy at the domain level.

The following password policy settings control the complexity and lifetime of passwords.

Table: Password Policy Settings

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 day
Minimum password length	8 characters *
Password must meet complexity requirements **	Enabled
Store password using reversible encryption for all users in the domain	Disabled

* For privileged accounts (such as Domain Administrator accounts), the minimum password length is 15 characters (unless covered by two-factor authentication or password vaulting/one-time password).

** Complexity Requirements (Windows): Passwords shall use a combination of upper and lowercase characters, numbers, and special characters (e.g., punctuation symbols such as ?!@#$%&*). At least three of the four character types are required.

Complexity Requirements (RACF): Passwords shall be alphanumeric and shall include at least one of the following special (National) characters: @ # or $.

PASSWORD SELECTION

The individual user is responsible for selecting a complex password (or pass-phrase) that is not easily guessed. Password selection shall comply with the following requirements:

- Passwords shall not be a word found in a dictionary in any language or any slang in common use (because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds).
- Passwords shall not be names (do not use names of actors, characters from stories or movies, names from religious text, or names related to the user).
- Users shall employ different passwords on each of the systems to which they have been granted access (for example, do not use the same password for both RACF and VPN access.

PASSWORD STORAGE AND CONTROL

Passwords shall not be written down nor stored where they can be viewed by others.

Passwords must never be cached. Never use the “Remember Password” feature of any application (e.g., Outlook, Outlook Express, or Outlook Web Access) or any web site login.

Passwords must never be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, or in computers without access control.

Passwords shall only be stored and transmitted in an encrypted format.

Keep passwords secure and do not share accounts. Do not reveal your account password to anyone or allow use of your account by others.

TWO-FACTOR AUTHENTICATION (2FA) REQUIREMENTS

APPLICATION

All Virtual Private Network (VPN) access shall require 2FA utilizing a user-defined password with an assigned hard or soft token.

Currently, users of Outlook Web Access (OWA) may utilize a 2FA token, in addition to a password, when additional security is required (or desired) for remote e-mail access. Eventually, all users of OWA will utilize 2FA with hard or soft token and password for remote e-mail access.

Mainframe users will require a hard token for 2FA access through RACF.

If a user requires a hard token for mainframe access, that same token may also be used to access VPN, OWA, or other 2FA-enabled systems.

Users shall NOT be issued multiple tokens or both a hard token and a soft token for access to the same system(s); however, users may utilize a soft token for access to one system (e.g., network resource) and a hard token to access another system (e.g., mainframe resource) though it is neither necessary nor recommended.

All in-bound connection requests shall be routed through the token authentication server. If the user (requester) has been issued a token they will be required to present the token code for 2FA.

At the request of the Agency's IT Manager or their designee, contractors and vendors shall be issued temporary (maximum 90-day) tokens. If a longer period of use is required, the token may be renewed. Exception: This requirement need not be applied if the contractor's period of performance is expected to be 1 year or more.

TOKEN ADMINISTRATION AND REGISTRATION

Agencies with workgroup, domain or organizational unit (OU) administrative personnel, shall designate a Token Administrator who will act as the token registration authority for their organization. For all other organizations, ISD will serve as the token registration authority. Agencies shall inform ISD who their Token Administrator is.

The Token Administrator shall be responsible for managing, inventorying and tracking token assignments.

Agency Token Administrators shall submit a request to the ISD Help Desk for initial and additional allotments of tokens for their agency (unless the agency acquires their own tokens).

Agency Token Administrators may return any unassigned tokens or over-allocation of tokens to ISD by contacting the ISD Help Desk and arranging the token transfer back to ISD.

Agency Token Administrators shall utilize the Active Roles administration server to register, activate, and deactivate tokens.

The Token Administrator shall validate the token recipient's identity prior to issuing an authentication token to that person. The registration process to receive a token shall (whenever possible) be carried out in person before a designated registration authority authorized by organizational management.

If it is necessary to mail a token (when the token recipient cannot appear in person), the following requirements apply:

- Only non-activated tokens may be mailed.
- Tokens shall be de-activated before mailing them back to the Agency Token Administrator or to ISD; token-holders shall contact the Agency Token Administrator or the ISD Help Desk for token deactivation before placing the token in the mail.

- Mail tokens with a confirmation of receipt or some form of delivery acknowledgement.

When e-mailing token activation codes, the activation code shall be set to expire after no more than 1 day. If the token is not activated within the allowed time, the token-holder will need to contact their Agency Token Administrator or the ISD Help Desk for a new activation code.

TOKEN SAFEGUARD AND USE

Tokens are individually assigned and are authorized for use by the assigned token-holder only.

Do not share your token with another person. It is linked to your unique user name (User ID) and password. Reminder: user accounts and passwords must never be shared.

Do not leave your token where others can access it. If someone learns your system user ID and password and also has your token, they can log in as you on that system.

Tokens are not transferable and until returned are the responsibility of the person to whom issued.

Token Holders shall maintain accountability for their token(s) at all times; protect from loss, theft, or damage.

If a token is lost, the token holder shall immediately notify their Agency Token Administrator, Agency IT Manager or their designee, or the ISD Help Desk.

Token Holders shall notify their Agency Token Administrator, Agency IT Manager or their designee, or the ISD Help Desk of any changes in access requirements (such as when a token is no longer required or needs to be deactivated for any reason).

Soft Tokens:

Soft tokens require a smart phone or similar portable computing device. Users shall identify the device type prior to token issuance to ensure the proper instructions are provided.

Smart phones or other devices used to render a soft token shall utilize a PIN or other protection mechanism to prevent unauthorized access.

Soft token applications (on smart phones or similar devices) shall be uninstalled prior to device replacement or discontinuance of use or upon changes in employment (transfer, resignation, retirement, termination, etc.).

If the token-rendering device is lost, stolen, or in an unusable state, notify the ISD Help Desk. If possible, ISD administrators will perform a remote data wipe to clear the device memory.

Hard Tokens:

Hard Tokens, when no longer required (e.g., change of duties or employment status) or when no longer usable (e.g., battery has drained), shall be returned to ISD.

If a hard token becomes unusable, and it was not rendered unusable by user negligence, it will be replaced by ISD at no additional charge to the agency.

Lost, stolen, or damaged (unusable) hard tokens are subject to a $25 replacement fee.

Billing:

ISD shall bill/invoice agencies on a per month basis for each token issued to the agency, (billable amount will not be prorated). Agencies will continue to be billed as applicable until hard tokens are turned in or until ISD has been notified to deactivate a soft token.

Information Services Division (ISD) Responsibilities:

The ISD Help Desk shall securely store all unassigned hard tokens.

ISD Customer Service, the ISD Server Group, and the ISD Mainframe System Software Support Unit shall jointly ensure 2FA User Guides are available and up to date.

On the first business day of each month, the ISD 2FA Administrator shall provide a summary report of token usage for the preceding month (email report to cyber.security@isd.alabama.gov).

The ISD 2FA Administrator shall check at least monthly the last logon date for tokens and disable/revoke any tokens that have not been used for more than 60 days.

Document all 2FA-related processes describing the actions that need to be taken internal to ISD including (but not limited to) token request to delivery, token license receipt to retirement, token troubleshooting and incident handling, etc. The respective business units shall be responsible for documenting their respective processes/procedures.

BIOMETRIC AUTHENTICATION REQUIREMENTS

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 or not 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.

As a general rule, a biometric may not be used for identification or to verify an identity in single factor authentication. A biometric may be used for authentication only as a component of two or three factor authentication. Where biometric authentication is used, the following security controls shall be implemented:

MANAGEMENT CONTROLS

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

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

IT Managers shall 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

In no case shall the strength of the authentication required in the enrollment process be less than the strength of authentication required during the verification process because this begs for an attack on the enrollment process.

IT Managers shall 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 shall 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 shall 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 shall 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 shall re-create templates when there is an indication that a template has not been properly captured.

The Security Administrator shall 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 shall 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 shall set the FAR to be no greater than 1 in 100,000.
- The Security Administrator shall 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 shall 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 shall activate at least one of the available "liveness" checks.
- IT Managers shall 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 shall 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 he or she supplies 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 shall ensure that there is adequate physical security, encryption of transmitted data, monitoring, and rejection of "exact matches".

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

TECHNICAL CONTROLS

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

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

Encryption:

The Security Administrator shall:

- Ensure that 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 shall 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 shall 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 shall 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

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
620-03	3/9/2006	Original document
620-03_A	1/12/2007	Added biometric policy and user guidance statements.
620-03_B	10/28/2008	Added authenticator feedback requirement; moved biometric requirement to Standard 620-03S2: Authentication-Biometrics.
623-00	09/01/2011	New document number and format
623-01	05/23/2013	Merges Policy 623 with Standards 623S1 and 623S2 and adds requirements for two-factor authentication; aforementioned Standards are hereby rescinded.
623-02	07/01/2013	Requires maximum password age be set to 60 days (or less)