**Company Identity Security Policy**

Digital Identity

Pinion, Daniel A.

CYBR 3126: Client Server Security

Professor Joseph Odyn

Fall 2022

Purpose and Benefits:

This policy establishes a framework for issuing and managing trusted identity credentials to allow company internal employees to conduct company business (not personal business) online at the behest of the company. A Trusted Identity Credential (TIC) is one the company is absolutely confident that the identity credential presented, represents the real living person that is named in it, and whose photograph and other Personally Identifying Information (PII) is associated with said presented credential.

This policy is designed to benefit users of company systems, regardless if they be locally and/or remotely accessed and utilized, by providing a framework that creates and issues company internal Electronic Trusted Identity Credentials (E-TIC) that can be universally regarded as trustworthy, by closely following the National Institute of Standards and Technology (NIST) *Digital Identity Guidelines* (NIST SP 800-63 Suite; Version 3 & Sections A/B/C). This will help company efficiency and productivity as company internal employees (hereafter known simply as “employees”) will be able to utilize shared identity solutions, single-sing-on, and reduce the need to operate, manage, and remember multiple E-TIC credentials across an ungainly mass of multiple credential software programs. This will result in the company seeing reduced costs of maintaining multiple authentication services and make it more simple and streamlined for employees to gain secure access to the company’s systems.

Authority:

Under the authority of the executive employees of this company, following all legal Federal, State, and Local laws, as well as applying NIST document *Digital Identity Guidelines* (NIST SP 800-63 Suite; Version 3 & Sections A/B/C) this company has authorized the creation and establishment of this digital security identity policy. This policy provides the *Chief Information Officer* and *Chief Information Security Officer* with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols, and standards for the company and the company’s business, including hardware, software, security, business engineering, and business re-engineering.

Scope:

This policy applies to all employees and third parties (such as consultants, vendors, and contractors) of this company; regardless of position, seniority, or tenure; as well as to, of, and within any and all property of this company. This property includes the physical land upon which this company stands, the workstations our employees operate for the task of conducting company business, the servers the company uses for data storage and processing, and all of the networking equipment that is owned and operated by this company.

This policy applies to use and access of any company Information Technology (IT) or Information Security (IS) systems managed and/or hosted by the company and/or by third parties working on behalf of the company. While a third party may adopt a different policy, such a policy must include the requirements set forth in this policy. This policy also applies to any online or remote services and products provided by the company and/or our third-party associates. All systems within this company’s spaces of operation require user authentication to access, function, or to be operated. This includes all systems for which any employee or third-party partner may have administrative responsibility, including those managed or hosted by our third-party partners (hereafter simply known as “partners”). There are no exceptions to this policy.

Information Statement:

This policy requires that company and partner information owners complete digital identity requirements assessments during system design to determine the appropriate Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), and Federation Assurance Level (FAL) for all information technology (IT) systems that will require user authentication and contain or process company and/or partner data. The assessments focus on:

* whether the person seeking to access the system is who they claim to be and the potential impact to the confidentiality and integrity of the data and/or system if that person is not who they claim to be;
* whether the person accessing the service today is the same person who accessed the service using the same authenticator previously; and
* how to convey the results of authentication processes and relevant identity information to other applications.

Completion of the assessments provides a system specific company issued numerical IAL, AAL, and FAL. Assessments must be documented and kept with other system documentation and must be used to guide system design and functions which impact identity, authentication, and/or federation services for the company and our partners. All digital identity assurance processes will be managed using the NIST *Digital Identity Guidelines* (NIST SP 800-63 Suite; Version 3 & Sections A/B/C) regulations and standards.

CONUS vs OCONUS:

The particular wording of this policy applies to employees and partners that are accessing company and partner data systems directly, from within the physical property of the company or its partners, as well as to employees accessing said data remotely, from within the Continental United States of America (CONUS), not including Alaska, Hawaii, and/or USA territories. All access to such data from any foreign nation or from any Non-Continental State or Territory (OCONUS) by any entity is hereby expressly forbidden and will be subsequently blocked under all circumstances. At no time are any employees allowed to access company or partner data from outside the United States of America (OCONUS). Employees may only access such data from within the Continental USA national borders (CONUS).

Signed:

Company Chief Policy Authority (CPA) – Daniel Pinion

Company Chief Information Officer (CIO) – John Smith

Company Chief Information Security Officer (CISO) – Jane Doe

Policy

Password Rotation:

All employees will change their single-sign-on password(s), authenticator access password(s), and any other necessary passwords at minimum once per fiscal quarter. This means that at least once every three months all employees will change and update their company passwords. There are no exceptions to this policy, and this policy rule will be digitally enforced by the password change forcing mechanism built into the company’s data security systems. Users will either change their passwords when they feel it is necessary, or every three months by digitally enforced mandate, whichever is shorter. If any credential’s security is compromised, the user **must** change said credential immediately. Failure to do so is in violation of this policy, has the potential to expose the company’s data to unauthorized parties, and will result in termination if the issue is not addressed in an acceptably timely manner. Each new password must be unique from the previous one, must include at least 2 capital characters, 2 lower case characters, 2 symbols, and 2 numbers. Passwords may not include dictionary searchable words spelled out in plain letters, commonly used password combinations, nor sequential strings of numbers more than 4 numbers long. For example password, 1234, 123456, EarlyRiser1234!!, and P@ssW0rd1122!! are all unacceptable as passwords, but Er@1yR!$er30 is an example of an acceptable password.

Vetting User Identity:

A company or partner system’s IAL determines the correct Assurance Level any user trying to access it must have in order to gain access to that system. The strength of evidence and the vetting processes used, establish a level of certainty in the identity of the user requesting a TIC. These levels are used to establish a user’s TIC and E-TIC.

|  |  |
| --- | --- |
| Identity Assurance Level (IAL) | |
| IAL Charlie | There are no requirements to link the presented individual user to any specific real-life identity for access to systems that require this level of security. Any attributes, affirmations, or claims of identification credentials provided by the user with the authentication process are self-asserted or should be treated as such.  This is the lowest level of IAL and is used **ONLY** in systems of Security Level Non-Critical. Any system that is of Security Level Confidential or higher may **not** use this level of IAL for any form of user identity vetting, under any circumstance. There are no exceptions, except for using a higher level of vetting. |
| IAL Bravo | Presented evidence supports that the claimed identity of the user is an identifiable and verifiable real-world existing person and verifies that the individual user is actually appropriately associated with this real-world identity. Identity vetting can occur either remotely or in-person in accordance with this security policy and the NIST *Digital Identity Guidelines* (NIST SP 800-63 Suite; Version 3 & Sections A/B/C) regulations and standards. Our credentialing service or a partner’s credential service provider is allowed to validate the identity assurance level to the company or partner party that is reliant on the user’s vetting, while only providing basic identifying information of the user. This information includes name, company employing them, position within the company or partner, and reason for access.  This is the medium level of IAL and is primarily used in systems of Security Level Confidential or higher as necessary for a given system. Any system that is of Security Level Non-Critical **may** use this higher level of IAL for any form of user identity vetting, as it is more secure than IAL Charlie. |
| IAL Alpha | The individual user’s physical presence on company and/or partner property land is required for proofing the user’s identity to vet them into a given system of this level. Identifying attributes are **absolutely required** to be verified by an authorized and trained security identification verification technician of the company and/or partner. All Identifying information of the user **must** be provided to the company or partner party that is reliant on that user’s vetting, by the company credentialing service or the partner’s credential service provider.  This is the highest level of IAL and is primarily used in systems of Security Level Business Critical. Any system that is of Security Level Non-Critical or Confidential **may** use this, the highest level of IAL, for any form of user identity vetting, as it is the most secure IAL level. |

**No** business system of the company or any partner may **ever** use a level of IAL that is lower than the security level of the system that is being utilized. **Any** business system **may always and at any time** use an IAL level that is higher than the security level of the system that is being utilized.

Not properly vetting users has the potential of resulting in extremely dire consequences for the company, our partners, clients, and customers. The company’s and/or partner’s information owner, CIO, and CISO must all be included in any assurance assessments, to assist processing them and to guide any discussions regarding any final determinations of any assurance assessments. The specific owner of specific information (the information’s information owner) is the one responsible for assigning the correct IAL Security Level to any given system the company or our partners own and operate. Failure to do this process correctly can result in adverse business conditions ranging from simple inconvenience to total system failure. Such failures will not be tolerated. Any violation of this policy will be met with immediate termination and possible arrest if it is determined that any employee and/or partner violated any law(s).

Determination of the required IAL and the corresponding authentication technology used by the company and/or a partner will be addressed in the follow-on policy outlining this process. This follow-on policy will be used to examine data within a given system and determine the risks associated with improperly validating access which might result in a security breach and may cause company data to be exposed to those who are not authorized to access that data.

(The follow-on policy will be determined at a later date and will be disseminated with an update of this policy herein.)

Determining User Authentication:

Successfully authenticating a user provides risk-based assurance to the party that needs that authentication, that the user attempting to access a system and/or service of the company and/or our partners is indeed the same user that legitimately gained access to that same service or system before, using the same authenticator(s). The assurance strength level is called an Authenticator Assurance Level (AAL). There are three levels. AAL’s define the requirement of what is a correct authentication, based on the company’s and/or partner’s risk tolerance (aka “risk appetite”). This is defined by assessing how much damage or harm can be caused to the company and its partners by unauthorized users accessing systems they are not supposed to access. This includes company and partner employees, as well as external bad actors such as hackers.

|  |  |
| --- | --- |
| Authenticator Assurance Level (AAL) | |
| AAL Charlie | This gives assurance that the user being authenticated is the one authorized to possess the TIC bound to their account and they are using the authenticators they are authorized to use. This level only requires Single-Factor Authentication (SFA) such as simple log-in credentials like a username and password, smart company ID Card, or pre-established biometric log-in credentials. This level of authentication requires the user to prove they are in possession of and have control of their TIC/E-TIC Authenticator, and that they are authorized to use the authenticator they are using. Proof may be obtained simply by the user utilizing the authentication protocol assigned to them.  This is the lowest level of AAL and is **only** to be used in systems of Security Level Non-Critical. Any system that is of Security Level Confidential or higher may **not** use this level of AAL for any form of user identity authentication, under any circumstance. There are no exceptions, except for using a higher level of authentication. |
| AAL Bravo | This AAL Level gives high confidence that the user executing an authentication of their TIC/E-TIC is in possession and accountable control of a TIC/E-TIC Authenticator, they are who they are claiming to be, and that the Authenticator they are using is indeed connected to and bound to their TIC/E-TIC Account. This level of authentication requires **at least** two distinct authentication factors. This is commonly known as Two-Factor or Multi-Factor Authentication. These distinct factors could include any combination of factors such as a username & password credential, biometric log-in credentials, an RSA SecurID Token, smartcard, a code from an authenticator app, a code sent to an encrypted and passcode secured mobile device via text message or push notification, a code sent to a secure encrypted email, or many other possibilities that cannot all be listed here. The primary purpose of this is that two **distinct** factors are chosen and used for authentication. These factors should be distinct in the way they follow the principles of “something you know” (like a password), “something you have” (smartcard badge, cryptokey fob), and “something you are” (biometrics, voice print).  This is the medium level of AAL and is primarily used in systems of Security Level Confidential or higher as necessary for a given system. Any system that is of Security Level Non-Critical **may** use this higher level of AAL for any form of user identity authentication, as it is more secure than AAL Charlie. |
| AAL Alpha | This AAL Level gives a very high confidence that the user executing an authentication of their TIC/E-TIC is in possession and accountable control of a TIC/E-TIC Authenticator, they are who they are claiming to be, and that the Authenticator they are using is indeed connected to and bound to their TIC/E-TIC Account. This level of authentication requires all the same factors and parameters as AAL Bravo, but with the additional requirement of a **physical verification** of the user's possession and accountability of their TIC/E-TIC and their authorized authenticators.  Along with the same requirements as AAL Bravo, the user **must** verify this possession and accountability by presenting themselves and their credentials for secondary verification by trained security identification verification technicians. This may be accomplished via photographic means for employees who are remotely accessing the system, or by physically being verified into the system by being present in the company or partner building for visual verification by said technicians. This level of authentication also requires that two distinct factors and two distinct authenticators be used for authentication, using approved cryptographic protocols.  One of these cryptographic authenticators must be hardware based, and one or both must be officially rated as *impersonation resistant* by the company/partner Information Security (IS) department. A single device may be used for both authentications; however two distinct authenticators need to be used on the device, both must be encrypted, and both must be secured behind separate and distinct access credentials to open user access into them. The access credentials for accessing these distinct authenticators on the same device are solely the responsibility of the device's operator to maintain and keep secure from unauthorized persons or programs.  This is the highest level of AAL and is primarily used in systems of Security Level Business Critical. Any system that is of Security Level Non-Critical or Confidential **may** use this, the highest level of AAL, for any form of user identity authentication, as it is the most secure AAL level. |

**No** business system of the company or any partner may **ever** use a level of AAL that is lower than the security level of the system that is being utilized. **Any** business system **may always and at any time** use an AAL level that is higher than the security level of the system that is being utilized.

Improper validation, validation of false credentials, or validating using a false or unsecure authenticator or authentication protocol is a highly dangerous risk to the company and our partners. This risk can cause a potential exposure of company, partner, client, and customer data to unauthorized people or entities, such as hackers. The specific owner of specific information (the information’s information owner) is the one responsible for assigning the correct AAL Security Level to any given system the company or our partners own and operate. Failure to do this process correctly can result in adverse business conditions ranging from simple inconvenience to total system failure. Such failures will not be tolerated. Any violation of this policy will be met with immediate termination and possible arrest if it is determined that any employee and/or partner violated any law(s).

Determination of the required AAL and the corresponding authentication technology used by the company and/or a partner will be addressed in the follow-on policy outlining this process. This follow-on policy will be used to examine data within a given system and determine the risks associated with improperly validating access which might result in a security breach and may cause company data to be exposed to those who are not authorized to access that data.

(The follow-on policy will be determined at a later date and will be disseminated with an update of this policy herein.)

Federation and Assertions:

Federation means to link a user's same identity credentials between multiple systems. This allows the results of authorized authentication processes and user identity information to be trusted and to be shared amongst all the company and partner's various systems, programs, and applications. This is accomplished with Assertions. An Assertion is declared by an Identity Provider and that information is recorded and sent to the company or partner party that holds that identification information about the federated user.

If a user must be identified in any way for access to any company system, security systems and technicians are required to collect the minimum amount of personal information required for that level of security and must pass along that minimum information as part of the Assertion, to the company or partner party responsible for verification and authentication and who hold the federated user's identification information. Federation Assurance Levels (FAL) give all parties involved in a federation transaction, the minimum company and partner standard of options based on an assessment of company and partner risk tolerance, against the potential harm any unauthorized access by an attacker (a hacker for example) who takes control of a given federated transaction.

|  |  |
| --- | --- |
| Federation Assurance Level (FAL) | |
| FAL Charlie | This level of FAL allows any company or partner system to access Identity Assertions from an Identity Provider that is administrated separately from the company and its partners **and** is contracted by the company and its partners. The company and/or partner system(s) accessing the requested Assertion **may** inherently trust that the 3rd-party system has properly identified and authenticated the user up to the level of security the user has requested access through. If the trust of such a transaction is in doubt however, all involved security employees **must** immediately verify that the transaction’s trust is valid before completing the Federation Process.  FAL Charlie maps Assertions to the relevant Assertion Verification Profiles (such as Security Assertion Markup Language [SAML], OpenID Connect, Single-Sign-On, etcetera) without requiring any other Assertion Verification Features. Basic encryption may be used for this level of FAL, and is highly recommended to be used, but is not required in all situations or for all systems of this security FAL level.  This is the lowest level of FAL and is **only** to be used in systems of Security Level Non-Critical. Any system that is of Security Level Confidential or higher may **not** use this level of FAL for any form of user identity Federation, under any circumstance. There are no exceptions, except for using a higher level of Federation. |
| FAL Bravo | This level uses the same rules as FAL Charlie, but **also requires assertions to be encrypted** using company/partner “known-good” **authorized** cryptographic technologies. At this FAL Level the system of the company or partner that is requesting the Federation is the **only** system allowed to be used to decrypt the Federation results they receive. This gives the involved parties a strong assurance that the confidentiality and privacy of the Federation Assertion is valid.  At this level the results of the Federation Assertion **must** be encrypted with a public key provided by the company or by the company’s partner that is requesting the Assertion results.  This is the medium level of FAL and is primarily used in systems of Security Level Confidential or higher as necessary for a given system. Any system that is of Security Level Non-Critical **may** use this higher level of FAL for any form of user identity Federation, as it is more secure than FAL Charlie. |
| FAL Alpha | This level of FAL utilizes **all** of the same rules from FAL Bravo and Charlie but adds additional requirements on top of those. These requirements are that the user requesting an Identity Federation Assertion **must** prove they are in possession and have accountability of their assigned cryptographic key(s) that is/are connected to and referenced in the Assertion Record(s).  This **may** be done remotely via camera, by the user and this information being verified as present and accounted for by trained security identification verification technicians. This **may** also be done in person, on company/partner land property, by same said technicians visually verifying the same. The Assertion that is encrypted and sent to the involved company/partner party **will be** signed and encrypted by the Identity Provider utilizing company/partner authorized cryptographic technologies.  This is the highest level of FAL and is primarily used in systems of Security Level Business Critical. Any system that is of Security Level Non-Critical or Confidential **may** use this, the highest level of FAL, for any form of user identity Federation, as it is the most secure FAL level. |

**No** business system of the company or any partner may **ever** use a level of FAL that is lower than the security level of the system that is being utilized. **Any** business system **may always and at any time** use an FAL level that is higher than the security level of the system that is being utilized.

The Federation Process is a vital part of the process of authenticating a user is who they say they are and that they are the one who should be in possession of the credentials they are presenting. The process of Federation and Assertion of a user’s identity is used as the company and its partners have examined the data within our system(s) and identified and weighed the risks associated with not properly verifying and validating a user’s access to a system, and the potential problems this could cause for the company and out partners. Failure to do this process correctly can result in adverse business conditions ranging from simple inconvenience to total system failure. Such failures will not be tolerated. Any violation of this policy will be met with immediate termination and possible arrest if it is determined that any employee and/or partner violated any law(s).

Determination of the required FAL and the corresponding authentication technology used by the company and/or a partner will be addressed in the follow-on policy outlining this process. This follow-on policy will be used to examine data within a given system and determine the risks associated with improperly validating access which might result in a security breach and may cause company data to be exposed to those who are not authorized to access that data.

(The follow-on policy will be determined at a later date and will be disseminated with an update of this policy herein.)

Compliance:

This policy takes affect at the moment of publication. Compliance is not only expected but is mandatory by all employees and partners. There is no exception. Failure or refusal to comply will be met with swift and impartial reprimanding and possible termination. If any laws are broken by the one refusing or failing to comply with this policy, legal action may be taken, up to and including the arrest of that individual. The company and its partners reserve the right to amend any and all policies, rules, regulations, and standards at any time without prior notice. If any change in any company and/or partner policies, rules, regulations, and/or standards is made, notice(s) of such changes will be disseminated to any and all employees of both the company and **all** of its partners. There is no exception to this. **All** parties of the company and its partners **must** be made aware of any and all changes to any policies, rules, regulations, and standards; if not prior to the change being implemented; then directly after such a change is made.

**EXCEPTION CLAUSE:** If in the event that compliance with this policy is in some way not feasible, not technically possible, or compliance with this policy may cause a danger of physical harm to employees; or if deviation from this policy is **absolutely necessary** to support the continued function of the company and its partners’ business; then an exception to this policy **must** be documented to, requested of, and approved by the Chief Information Security Officer. If the Chief Information Security Officer is not available or is in some way incapable of reviewing and approving, or if the danger of imminent bodily harm is present, then the situation **must** be documented as best as possible, the record of the dire incident filed, and the involved parties in such a situation must utilize their best judgement in the moment of the incident. This clause is placed here with the intention of exceeding Disaster Preparedness and Recovery industry standards and best practices, while also maintaining the utmost standards of data security possible. If in doubt, document the problem, and use your best judgement. If you are in danger, evacuate the danger zone as best as possible, document the situation as best you can, and get to a safer location. **This company and its partners are not worth your life.** Stay safe, operate with common sense, operate with a security minded sense of urgency, and document as you go.

Contact Information:

**Chief Information Security Office**

**The Company**

**(The company’s address.)**

**(The company’s telephone number.)**

**(The CISO’s e-Mail address.)**

Revision History:

This policy **must** be reviewed, at minimum, once every year to ensure it stays relevant to the company and its partners’ business needs and requirements, as well as to ensure compliance with Federal, State, and Local laws, regulations, and standards.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer(s)** |
| 10/27/2022 | Original Policy Created, Published, and Disseminated. | Daniel Pinion – CPA  John Smith – CIO  Jane Doe – CISO |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |