IAM Security Guideline

1. Introduction

**1.1 Purpose**

The Identity and Access Management (“IAM”) Standard mandates that Larggg1 Inc establish access control capabilities to appropriately govern, manage, and secure user access to data, applications, systems, networks, and computing devices.

This assures that only authorized individuals gain access to Larggg1 Inc’ data, applications, systems, networks, and computing devices. Additionally, this assures individual accountability to provide authorized users with access **privileges** that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

**1.2 Scope**

This Standard applies to all Larggg1 Inc Personnel and Group Companies.

The scope of this document covers:

* Larggg1 Inc owned and/or managed hardware, operating systems (o/s), applications, and databases, that are deployed on or connected to the Larggg1 Inc network, either physical or virtual.
* End user devices on the Larggg1 Inc network.
* All Larggg1 Inc regular or temporary employees, contractors, consultants, and any other agent acting on behalf of the Company.
* All production environments including non-production environments that contain highly restricted / restricted production data (forward looking control – refer to Appendix C).
* Controls related to privileged access accounts (including break-glass, JIT access, vaulting, and privileged session monitoring) will be defined in the Privileged Access Management Standard. This IAM Standard applies to general user accounts and non-privileged access.

**1.3 Control Applicability**

* The Security Priority Scorecard (SPS) is used to evaluate and categorize applications in terms of cyber security risk so that a commensurate level of protection can be applied. Based on the answers to key questions, a security priority score is calculated as defined in the SPS Guideline.
* An application is then assigned a Security Priority Level based on their score.
* The control requirements outlined in this standard are allocated based on the Security Priority Level of an application:
* Level 4: Minimum Security Requirements (CIA score < = 30%)
* Level 3: Additional Security Requirements (CIA score > 30%)
* Level 2: Enhanced Security Requirements (CIA score > 50%)
* Level 1: Critical Security Requirements (CIA score > 70%)



**1.4 Intended Audience**

The controls outlined in this standard must be reviewed and understood by all members.

**1.4 Glossary/Terms**

A glossary of defined terms is attached in Appendix A. Terms defined in the glossary appear in bold when they first appear in the text of this Standard.  Additional defined terms can be found in the Master Enterprise Glossary.

1. Requirements

**2.1 Identity Proofing**

2.1.1 User IDs

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM-IP-01 | All users must be assigned a unique identifier to access systems or data. | All Levels |
| IAM-IP-02 | IDs must not be reused until all previous access authorizations are removed and a period of at least seven (7) years has passed. | All Levels |
| IAM-IP-03 | Level 4 identity validation is required before initiating transactions that impact security, including password resets, token provisioning, or key generation. | All Levels |

2.1.2 Shared Accounts

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM-IP-04 | **Shared accounts** must be documented, assigned an owner, and regularly audited. | All Levels |
| IAM-IP-05 | Shared accounts should be traceable to individuals who use them. | All Levels |
| IAM-IP-06 | Shared accounts must be disabled when no longer needed. | All Levels |

2.1.3 Account Provisioning, Amendment and Deactivation

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM-IP-07 | The IAM lifecycle must align with the principle of **least privilege** including:   * Business requirement validation before account creation. * Identity verification before allocating accounts. * Timely deactivation of accounts. * Documentation and monitoring of IAM lifecycle changes. * Restriction of the creation, modification, and deactivation of user accounts to authorized administrators. | All Levels |

2.1.4 Authentication

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM-IP-08 | All users and administrators must authenticate using at least two factors:   * Something you know (e.g., password). * Something you have (e.g., token, smart card). * Something you are (e.g., biometric). | 1,2,3 |
| IAM-IP-09 | Single Sign-On (SSO) against the enterprise Active Directory/Azure Active Directory is the primary method of authentication (refer to section 2.5 Access to Systems and Applications Delivered by Third Parties). If SSO is not feasible due to technical limitations please contact Information Security for an alternative or risk control exception. | All Levels |

**2.2 Access Control**

2.2.1 Access Allocation, Modification and Removal

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM-AC-01 | All access to systems or data must be controlled based on the following:   * Where capability allows, fine grain authorization within applications should also align to Role Based Access Control (RBAC). * Least privilege principle. * Explicit deny of unauthorized access. * Revocation of unused access. | All Levels |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IAM-AC-02 | The allocation, modification, and removal of access control rights or privileges must be governed by the principle of least privilege and include the following:   * Access must be granted only as required for job functions. * Users joining, moving, or leaving (JML) must have their access reviewed and updated or revoked promptly.      |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | **Level 1** | **Level 2** | **Level 3** | **Level 4** | | **Joiners** | NA | NA | NA | NA | | **Transfers**  **(Movers)** | Within 10 business days | Within 15 business days | Within 20 business days | | | **Leavers** | Within 10 business days | Within 15 business days | Within 20 business days | |  * Authorization must be verified before granting access. * Accounts for systems that are intended to be accessed by all users are exempt from access reviews (e.g. email, intranet, internet). | All Levels |
| IAM-AC-03 | Before access privileges come into effect:   * Details of users must be recorded, including their identity, associated identifier (e.g., **credentials**) and access privileges to be granted. | All Levels |

2.2.2 Segregation of Duties (SOD)

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM-AC-04 | Access privileges must allow for the appropriate segregation of duties:   * Critical functions must be segregated to prevent misuse of privileges. * Clearly define roles, separate key functions so that no single role can control all aspects of a process, divide key roles among different users to reduce risk of errors and prevent misuse of privileges. * SODs must be established, implemented, and documented. * Audit functions must be separate from access administration. * Administrative roles must be strictly limited and aligned with operational needs. | 1All level 1s must go through a review to determine if SOD is required. |

2.2.3 Database and Data Stores Access

All access to any database containing data with a data protection categorization of **Restricted or Highly Restricted** (including access by applications, administrators, and all other users) must be restricted as follows:

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM-DB-01 | All user access to, user queries of and user actions on databases are conducted through **programmatic** **methods**. | All Levels |
| IAM-DB-02 | Restrict database management utilities to only authorized database administrators. | All Levels |
| IAM-DB-03 | Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). | All Levels |

**2.3 Remote Access & Third-Party Access**

2.3.1 Remote Access Controls

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM-RA-01 | Remote access must be performed using managed devices (devices that are registered or managed by Larggg1 Inc). | All Levels |
| IAM-RA-03 | All external access must be encrypted and authenticated via multi-factor authentication (MFA). | All Levels |
| IAM-RA-04 | Devices connecting remotely must comply with:   * Up-to-date system patches. * Current anti-virus protection. | All Levels |

2.3.2 Vendor Access (to LARGGG1 INC systems for support purposes)

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM-RA-05 | Application vendor accounts must only be enabled for the duration of the support engagement. only when needed. | All Levels |
| IAM-RA-06 | Application vendor access must be authenticated via MFA. | All Levels |
| IAM-RA-07 | Application vendor accounts must be disabled when no longer required. | All Levels |

**2.4 Access Reviews & Monitoring**

2.4.1 Periodic Access Reviews

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM-AR-01 | User access must be reviewed based on the security priority score.   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | **Level 1** | **Level 2** | **Level 3** | **Level 4** | | **Periodic access reviews** | Every 6 months | Every 12 months | Every 24 months | |  * Access reviews must validate that all access privileges are still required. * Unnecessary access privileges must be revoked. * Incomplete Level 1 user reviews will have access removed if not completed by the manager within the prescribed timelines. * **Note**: Application owners must ensure that access to applications that are not onboarded to the IGA platform are manually reviewed. | All Levels |

2.4.2 Account Disablement & Inactivity, Changes to Roles

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM- AR-02 | Departed employees' accounts must be deactivated:   * Active Directory accounts: within 12 hours. * **Emergency accounts**: within 24 hours. * Application access as defined in 2.2.1 Access Allocation, Modification and Removal. | All Levels |
| IAM- AR-03 | All accounts must be reviewed upon changes in user role (i.e. changes in Cost Center, to the user's business title OR changes to their physical work location) and in every access review cycle as follows:   * The review must validate and recertify that all access privileges are still needed and authorized. * The results of the review must be documented and unnecessary access privileges must be removed. * Accounts for systems that are intended to be accessed by all users are exempt from access reviews (e.g. email, intranet, internet). | All Levels |

**2.5 Password Management**

Applications managed by Larggg1 Inc must comply with the requirements below. Third-party/SaaS applications where LARGGG1 INC does not have control over password configurations are exempted from adhering to these requirements.

2.5.1 General Password Policies

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM- PM-01 | End-user passwords must:   * Be at least 12 characters long. * Contain uppercase, lowercase, numbers, and special characters * Expire every 90 days. * Not be reused within the next six password cycles. | All Levels |

2.5.2 First Time Passwords

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM- PM-02 | First-time use and reset passwords/phrases must be:   * Set to a unique value for each user. * Configured to be changed immediately after first use (if possible). * Not stored in the ticketing system and anywhere in cleartext. | All Levels |

2.5.3 Password Encryption

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM- PM-03 | All authentication credentials (such as passwords/phrases) must be encrypted during transmission and storage. | All Levels |

**2.6 Session Management**

2.6.1 Lockouts and Timeouts

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM- SM-01 | User accounts must lock after 3 failed login attempts. The accounts must remain locked for 15 minutes before they are automatically unlocked. | All Levels |
| IAM- SM-02 | Session timeouts must be enforced after 15 minutes of inactivity. This excludes systems provided by default to all colleagues. | All Levels |

**2.7 Access to Systems and Applications Delivered by Third Parties**

2.7.1 Access Controls

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Requirement** | **Applicable to Level #** |
| IAM- TP-01 | Access to SaaS or COTS systems and applications that create, acquire, process, exchange, or store Larggg1 Inc Highly Restricted, Restricted or Internal Information must be delivered by a Single Sign-On (SSO) solution that uses **approved Federated Identity and Access Management (FIAM) protocols** (e.g. SAML, WS-Federation). | All Levels |

1. Roles & Responsibilities

**HR** is responsible for providing timely and accurate authoritative user identity information throughout the user lifecycle: join, move, leave.

**Product Owners** are responsible for defining role-based access entitlements to the applications under their ownership. They are also responsible for reviewing and approving access that is considered privileged (privileged access controls (e.g., PAM tools and elevated session governance) are out of scope and covered separately).

For systems and applications that are considered rated as Level 1 or Level 2 critical or sensitive, Product Owners are responsible for reviewing and approving all access to their application.

**Application and Infrastructure Custodians** are responsible for implementation and maintenance of the required access controls. They are also responsible for providing accurate and timely data to the IAM platform for inclusion in the reviews, as well as to ensure the availability of the integration between their applications and IAM platform(s) for reviews and for automated provisioning, if such integration exists.

**People Managers** are responsible for managing user access privileges for their direct reports throughout the entire user lifecycle. This includes overseeing and reviewing access to **shared platforms** in line with this Standard. Specific responsibilities include regularly reviewing and updating access rights, especially during role changes and terminations; approving access requests; providing compliance attestations; and promptly reporting any access control-related incidents in accordance with the Incident Reporting Standard.

**Security Architecture and Engineering team i**s responsible for providing a technology platform to manage entitlements and to provide guidance and best practices for IAM process and controls.

**Active Directory Team** is responsible for enablement of access to real-time user and systems account information.

**Users** are responsible for compliance with all the elements stated in this standard.

1. Monitoring and Reporting

Identity and Access Management related reports must be made available on request for review, investigation, and audit.

1. Exceptions & Breaches

**5.1 Exceptions**

Requests for exceptions to this Standard must be submitted using the Technology Control Exception Form.

**5.2 Breaches**

All breaches of this Standard must be reported immediately in writing (email being sufficient) to the Document Custodian. The Document Custodian will consider the course of action, including reporting as per the Incident Reporting Standard.

1. Reference Documentation

The Identity and Access Management Standard should be read in conjunction with the accompanying documents referenced throughout and listed in [Appendix B](bookmark://_Appendix_B), which outline applicable controls.

1. Administration Information

**7.1 Ownership**

The Identity and Access Management Standard is owned by Information Security. For questions, issues, and suggestions, please contact:

|  |  |
| --- | --- |
| **Custodian** | **Contact Information** |
| Bob Smith | (555)-4577 |
|  |  |
|  |  |

**7.2 Document Revision**

The Identity and Access Management Standard shall be reviewed on an annual basis.

**7.3 Document History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Released** | **Summary of Changes** |
|  |  |  |
|  |  |  |
|  |  |  |

**7.4 Approval**

The Identity and Access Management Standard is hereby approved by John Smith.

Appendix A – Glossary

1. “**Shared account”** is an account that can be accessed by multiple individuals to accomplish a single shared function, such as supporting the functionality of a process, system, device, or application.
2. **“Shared platform”** is a centralized and collaboratively utilized system or digital environment that enables multiple authorized users, departments, or organizations to access, manage, and exchange data or services. Examples include SharePoint, Confluence, JIRA.
3. **“Credentials”** are a record within a system or application that allows access to information/functionality within the said system or application once the correct credentials (e.g., username/password) are provided. An individual may potentially hold multiple Credentials within a system or across multiple systems within Larggg1 Inc, but each Account must be owned by one individual.
4. **“Privilege”** is a set of user attributes that define how a user and/or an account can interact with a system or application.
5. “**Least Privilege**” All users of Larggg1 Inc’ systems, services and applications and data (employees, contingent workers, service providers, clients, affiliates) will be provided with only the access and privileges required to achieve their business objectives, accomplish their tasks, and discharge their duties to Larggg1 Inc. Similarly, all service accounts are provisioned with only the access and privileges required to achieve their tasks.
6. **“Programmatic methods”** refers to the use of programming language to access a database. Using a programming language to access a database enables the data to be used in more ways and is also safer than using direct access/manual access.
7. **“Emergency Account”** is an access account that is highly privileged, and not assigned to specificindividuals. Emergency access accounts are limited to emergency or "break glass"' scenarios where normal administrative accounts can't be used.
8. **“Approved FIAM Protocol”** includes the following:
9. Security Assertion Markup Language (SAML): SAML is a protocol that enables IdPs to send users’ login credentials to SPs. SAML enables users to be authenticated and authorized by simplifying the password management and identity process. It uses Extensible Markup Language (XML), a set of rules that encode documents to standardize communication between computers and systems. SAML is crucial to organizations' ability to store users’ identities across various identity management systems and use security tools like SSO.
10. Open Authorization (OAuth): OAuth is a framework that enables users to consent to applications sharing their login credentials. It uses access tokens to provide users with secure access to connected third-party services without revealing or exposing their login credentials. A common example of this is logging in to a website by using a Facebook or Google account rather than creating a username and password.
11. OpenID Connect (OIDC): OIDC is an authentication protocol from the OpenID Foundation. It verifies users’ identities when they attempt to access protected Hypertext Transfer Protocol Secure (HTTPS) websites. It works in conjunction with OAuth to provide an authentication layer to OAuth’s authentication layer.

Appendix B – Reference Documents

1. Acceptable Use Standard
2. Incident Reporting Standard

Appendix C – Forward Looking Controls

|  |  |  |
| --- | --- | --- |
| **Section #** | **Activation Date** | **Control** |
| 1.2 | Q1 F27 | All production environments **including non-production environments that contain highly restricted / restricted production data (forward looking control – refer to Appendix C)**.    **Forward looking control:** Applies to non-production environments that contain highly restricted / restricted production data. |