

# Original Provisioning RFP Questions

## Identity Administration and Provisioning

Students and employees: Describe how the current system provisions accounts and access, including subsequent data/attribute changes.

Contractors and affiliates: Describe how the current system provides for account creation and management for users who do not have records in the authoritative source for students or employees.

Guest accounts: Describe how the current solution provides for creation and management of guest (temporary) accounts.

What are the major systems that are integrated with the current system (ex: MS Active Directory, ADFS, OUD, ODBC databases, LDAP V3, Google, Windows Azure)

Can the current system suggest access rights based on an analysis of similar identities?

How are changes to identity attributes authorized, requested and validated?

Describe how/when users are de-activated or de-provisioned.

Can the current system integrate with external Security Incident and Event Management (SIEM) tools (or other monitoring) to automatically de-activate users who demonstrate suspicious activity?

Describe how the proposed solution assigns user IDs within its own database/source and within other downstream systems.

## Password and Credential Management

Describe all tools and communications media that can be used to reset passwords (include notifications for upcoming expiration warnings). Are notifications customizable (e.g. in the case of email, HTML, etc.)?

Describe how passwords are propagated to multiple downstream systems.

Does the current system provide for temporary/one-time passwords?

Describe how the current system intercepts password changes (e.g. on a user's desktop), and how those password changes are propagated to other credential stores or downstream systems..

How do you resolve differences between credential stores and any downstream password policies?

Describe available options for password policies supported (such as number of bad attempts allowed, password complexity, lockout timeframes for excessive reset attempts, etc.).

## Access Request and Approval Management

Describe the different options or workflows that are available for access requests, including any self-service functionality and types of devices /methodologies that can be used by end users (e.g. mobile options).

Do all access requests/changes require human approval, or can select requests be configured such that approval occurs automatically?

Can multiple approvers can be assigned to a single account/access request?

Describe options for requests that have non-responsive approvers. For instance, are there email reminders? Can the request be escalated from a non-responder to a different access approver?

Can approval authority be temporarily delegated to others (e.g. for approvers who are out of office, etc.)?

Can requests be approved via email and/or mobile devices?

Can life-cycle (people joining, moving and leaving the organization) events be configured for automatic access provisioning?

Does the current system provide visibility to access changes initiated through automated change events (e.g. new hire, promotion, termination)?

Can the current system request additional information from users involved in the access request process (e.g. requester, approver, application/data owners)?

What metrics are available for access requests?

## **Group and role management**

Describe how roles are created and/or managed within the current system, and if/how RBAC and/or ABAC can be performed.

What analytics or capabilities are available for groups/roles to perform tasks such as aggregation or de-duplication.

Can the current system support attributes for memberships of a role (e.g.department, location)?

Describe account or access reviews and reconciliation processes for access.

Can reviews be automated to occur on pre-determined intervals and/or in a manual ad-hoc manner?

## **Enterprise Authorization Reporting**

What reports are available (including descriptions of each report's purpose). Please describe any warehousing methodologies/integration that may be required or may be available. Indicate whether third-party, or extra-cost reporting tools are required or recommended (e.g. Crystal Reports, etc.).

Risk-based security controls and assurance level management

Does the solution support the ability to define and enforce access policy, including Separation of Duty policies?

Can risk-based policies be created in the current system to support notification/ alerting when user risk profiles change?