Guideline on Personally Identifiable SAML Attribute Release

Objective

UW-Milwaukee has, and will continue, to license services and applications in the cloud. To manage the user accounts and provide authentication services for these providers, UW-Milwaukee will be using a Security Assertion Markup Language (SAML) based authentication framework. A SAML based framework enables authentication and authorization services used in federated identity management (FIAM). FIAM allows the service provider to "trust" another organization’s identities and credentials for access to the service. The goal of SAML based authentication and authorization is to protect personal privacy, minimize the excessive creation of individual credentials, and ensure institutional control over 3rd party management of its user’s identities.

Assumptions and Known Issues

1. At present, the handling of privacy assertions for students holding a student employment contract with UW-Milwaukee is not articulated well and is implemented in a non-uniform manner. This guideline makes the assumption that students holding a student employment contract have the same privacy rights as a student that is not employed under contract with UW-Milwaukee. It is also assumed that privacy assertions for students holding a non-student employment contract with UW-Milwaukee will be handled in the same way as other staff that are currently not a student of UW-Milwaukee.

2. At present, the handling of privacy assertions for handling affiliations other than students and employees have not been articulated. This guideline makes the assumption that other affiliations do not have the right to assert privacy over their given name, surname, email address and electronic identifier (ePantherID).

Attribute Data Classification

The exchange of attributes related to an individuals identity is foundational to the operation of the SAML service. To manage the risks associated with release of these attributes, a procedure based on data classification will be used. Attributes will be classified using UW-Milwaukee’s “Data Classification and Criticality Standards”. A copy of the standards may be referenced at [https://pantherfile.uwm.edu/groups/uits/security/Audit/Standards08/final/4DataClassif.doc](https://pantherfile.uwm.edu/groups/uits/security/Audit/Standards08/final/4DataClassif.doc).

Directory Information

Personal directory information is singled out because the data classification can depend on an individual’s affiliation with the institution and if the individual has asserted any privacy restrictions.

Students

For individuals holding a student affiliation, directory information is defined by the notification of FERPA
rights maintained by the Division of Enrollment Services and published at https://www4.uwm.edu/
current_students/records_grades/ferpa_students.cfm [https://www4.uwm.edu/current_students/records_grades
/ferpa_students.cfm]. The following attributes are designated as directory information.

- Given Name
- Surname
- Email address
- ePantherID
- Home Address of Record
- Home Telephone Number of Record

The data classification for student directory information will be modified by privacy assertions as follows:

1. If the student has asserted a FERPA privacy hold and does not hold a non-student employment contract with UWM, the student's directory information is confidential data.
2. If the student has asserted a directory privacy hold and does not hold a non-student employment contract with UWM, the student's directory information is sensitive data.
3. If the student has not asserted a privacy hold and does not hold a non-student employment contract with UWM, the student's directory information is unclassified data.

**NOTE** - While Date of Birth is designated as directory information for students via the notification of FERPA rights, the date of birth attribute is assumed to be confidential personally identifiable information (PII) for the entire community to simplify procedures. Should a service only need date of birth for students, that will be handled as a special case.

**Staff including Faculty**

For individuals holding a staff or faculty affiliation, a non-student employment contract is assumed. In the absence of policy, the following attributes are considered directory information by current usage.

- Given Name
- Surname
- Email address
- ePantherID
- Department and Office Location
- Office Telephone Number
- Home Address of Record
- Home Telephone Number of Record

If the staff or faculty person has asserted a directory privacy hold the home address of record and the home telephone number of record are considered sensitive data.

**Holders of Dual Student/Staff Affiliation**

Holders of dual student/staff affiliation assume the staff definition of directory information. In these situation, the staff directory privacy hold takes precedence.
Holders of Affiliations other than Student, Staff or Faculty

For individuals holding an affiliation other than Student, Staff or Faculty, the following attributes are considered directory information by current usage.

- Given Name
- Surname
- Email address
- ePantherID

Holders of affiliations other than Student, Staff or Faculty may not assert directory privacy holds.

Confidential Data

Attributes classified as confidential will only be released to registered service providers. Before release, a security assessment must be performed and the UWM Security Office must approve the release. If the service provider is an external entity, a contract addressing the handling of confidential data must be in place.

Sensitive Data

Attributes classified as sensitive will only be released to registered service providers. UWM Security Office must approve the release and may require a security assessment before approval. If the service provider is an external entity, a contract addressing the handling of confidential data must be in place.

Unclassified Data

Unclassified data may be released to registered and non-registered service providers without the need for a security assessment or contract protections. The IAM Program Manager has the authority to establish which unclassified data is made available to service providers.

Registered Service Providers (SPs)

At this time, all service providers (SPs) that wish to use UW-Milwaukee’s SAML framework must explicitly register to access the service. During the registration process, a service provider’s attribute requirements are determined, attribute data classification evaluated, proper institutional approval obtained, and a dedicated release profile established. To request registration, an email to UWM's Enterprise Single Sign-On support may be sent to “uits-esso-help@uwm.edu”.

Non-Registered Service Providers (SPs)

At this time, UW-Milwaukee does not allow service providers (SPs) to utilize the SAML framework without pre-registration. See the section on registered service providers for details.

In the future, UW-Milwaukee may allow service providers to access a default set of attributes without
pre-registration. It is likely that the default profile would consist only of the following:

- **EduPersonTargetedID** - This is a persistent opaque identifier that is unique for each end application and user. Processes would need to be defined to populate and maintain the service specific values needed for this to be useful.
- **EduPersonAffiliation** - This indicates whether a person is member, student, staff, or affiliate.

**Data Access by SAML Identity Provider (IdP)**

To enable the SAML framework to function, the SAML Identity Provider (IdP) service must have access to an inclusive set of all attributes that are to be released to any SP. These attributes will be sourced from the UITS OpenLDAP directory service and the IAM Program Manager is authorized to approve the release of any attributes present in the UITS OpenLDAP directory to the SAML IdP. The UWM Security Office will be notified of the release of any attributes holding a confidential data classification as a courtesy. A list of attributes released to the IdP may be audited upon request.

**History**

- **Original Draft** - RANKM - 20101029
- **Feedback from BRUNO** - RANKM - 20101207
- **Final draft submitted to IAAM Steering Committee** - RANKM - 20110201
- **Approved by IAAM Steering Committee via email poll** - RANKM - 20110211
- **Published on IAM Website** - RANKM - 20110404