Identity and Access Management (IAM)
Minimum Application Security Controls
Draft – 10/30/2015

Preamble

The security controls and data classifications described in this document are provided as a guideline. Individual campuses may have adopted a different or more stringent set of data classifications and security controls. Before using this document, please validate with your campus IT Security office or Chief Information Officer regarding data classifications and security controls in use on your campus.

Minimum Security Controls[1]

1. Data Security Controls

1.1. Provider must not store UWS Non-public, Confidential or Restricted information in a persistent format (to disk or other long-term storage) unless persistent storage is essential to critical operation of the application. Functions that do not require persistent storage of UWS Non-public, Confidential or Restricted Information for essential operation should not commit this information to persistent storage.

1.2. UWS Non-public, Confidential or Restricted Information must be encrypted in transit by an encryption technology that has been tested and documented by the National Institute of Standards and Technology[2]. Web and application servers must use a minimum of TLSv1.1 for all web access. For non-web applications, a minimum of TLSv1.1 or equivalent encryption should be used.

1.3. UWS Confidential Information should be stored in an encrypted form, or at the very least hidden when viewed from outside the application by unprivileged application users. Plain text storage of UWS Confidential Information is strongly discouraged and should be supplemented by industry-recognized compensating controls that prevent the unauthorized release of this data in the event of a compromised host.

1.4. UWS Restricted Information must be stored in an encrypted form. Plain text storage of UWS Restricted Information is not allowed.

2. Server / Network Security Controls

2.1. Physical access to servers containing UWS Non-public, Confidential or Restricted Information should be restricted to those employees or agents of the Provider that are directly involved in the delivery of services to UWS. Physical access should be logged and audited according to best industry practices for physical access to areas containing Non-public, Confidential or Restricted, sensitive or restricted data.

2.2. Servers, databases and network components must be patched regularly to address vulnerabilities in operating systems and application software.

2.3. Application and data storage software must run current anti-virus and other threat mitigation, and this software must be regularly updated with current signatures and definitions.

2.4. Application and data storage servers must be protected by appropriate firewalls that deny all traffic from untrusted networks, prohibit all direct public access to the data store, and restrict traffic between the application server and all other publicly accessible hosts and the data store to channels require for application functions. Ports that are not require for the application server's data access should be blocked.

2.5. Communication between the application server and data storage must be secured by encryption software such as IPSec, SCP, SSL, TLS or other industry recognized transport encryption. Software must use an encryption algorithm that is free of known security flaws. Such communication, even when encrypted, should not be routed over the open Internet.

---

[1] This document represents the minimum security standards that are likely to apply in most data-sharing arrangements with cloud providers. The most comprehensive framework of security principles available to assist cloud customers in assessing the overall risk of a cloud provider can be found at the Cloud Security Alliance, Cloud Controls Matrix (CCM) Version 3.0 at https://cloudsecurityalliance.org/group/cloud-controls-matrix/

[2] http://csrc.nist.gov/groups/STM/cavp/standards.html

2.6. Shell or command access to application servers and data storage servers must be limited to system administrators and application developers. Such access must also be restricted to known locations or via an authenticated VPN.
2.7. Shell or command access to all servers should be appropriately encrypted using IPSec, SCP, SSL, TLS or other industry recognized transport encryption that is free of known security flaws.
2.8. Shell or command traffic to and from the servers must not be routed over the open internet without the use of an authenticated VPN.
2.9. Access logs must be maintained in accordance with the institution's applicable IT policies, and should be audited for inappropriate access on a scheduled basis.
2.10. Server login accounts must be unique for each developer and administrator, and servers should apply a password strength policy requiring that passwords meet generally accepted security standards. Level of access should be appropriately restricted to the lowest level of privileges required for access, and any need for elevated privileges should be met by privilege changing software like "sudo" or similar tools. Servers must maintain an audit log of all changes in privilege level exercised through this method.

3. Logging / Auditing Controls

3.1. In addition to transactional logging, the data store must maintain an audit log of data updates, which upon request must be made available to the university. Every read access to restricted data should also be logged in the audit log.
3.2. Intrusion detection or prevention software must be run at the host and/or network level, and logs must be reviewed on a regular basis.
3.3. Provider should have in place a program for regularly assessing and remediating vulnerabilities in its server, network and application environment.
3.4. Provider must ensure that any third party, including but not limited to agents, contractors, hosting providers or other service providers that store or maintain UW Non-public, Confidential or Restricted Data adhere to all of the guidelines above.

4. User Authentication and Authorization Controls

4.1. Access to UWS data and applications must use the access control services designated by campus policy and must comply with appropriate use standards for the institutionally managed credentials.
4.2. Applications should integrate with institutionally managed access control services in a manner that refers the user to the institutionally managed login service. Strong preference is given to integration technologies such as SAML that do not allow an application to handle a user's password.
4.3. Computer systems and applications must not encourage the use of the user's institutionally managed password in combination with any other identifier.
4.4. Computer systems and applications must not store the password associated with an institutionally managed identifier. Only the institutionally managed access control system may store this password.
4.5. The service must provide access control solutions that limit access based on business or technical function.

5. Application Privacy Controls

5.1. Applications should be capable of restricting display of information for users that have elected that their data remain private from others via FERPA or other institutionally recognized means. Election of FERPA or other privacy hold should not prevent users from being able to access an application.
5.2. Applications should make known to users the manner in which their data is used and made available to others through publication of privacy policies.
5.3. Applications should provider users the opportunity to express or withhold their consent when their data is asserted to an external application or third party service provider.

6. Provisioning and Data Delivery

6.1. Wherever possible, user data should be delivered to applications by SAML assertion or other attribute delivery means at user login. Where this is not possible, preferred approaches include directory or web services integration that query data only as needed.

6.2. Applications should provide a means of provisioning users on first use of an application. Where this is not possible, applications should provide a programmatic means for provisioning users.

6.3. Applications should provide a means of deprovisioning users, either programmatically or through an expiration process.

6.4. Once deprovisioned, unnecessary user data should be purged from the application.

7. Federation Metadata Consumption

7.1. Applications that integrate with institutionally managed access control systems must also integrate with institutionally managed systems for integrity monitoring. For SAML-based applications, this includes automated publication and consumption of federation metadata.

8. Contractual Requirements for External Providers

8.1. Contracts established with external service providers must provide the following protections for UW System institutions:

8.1.1. Provider must perform independent 3rd party audits against an industry recognized security standard (e.g. NIST 800-53, ISO 27000, PCI-DSS or comparable).

8.1.2. Provider should achieve and maintain product certification through a recognized 3rd party security certification process such as CSA STAR[3] or FedRamp[4].

8.1.3. Provider must not disclose Non-public, Confidential or Restricted information to 3rd party without explicit written approval from UWSA.

8.1.4. Provider must inform UWSA of any request by 3rd party for Non-public, Confidential or Restricted information.

8.1.5. Provider must refer request for data to UWS unless compelled by lawful subpoena, in which case provider must notify UWS.

8.1.6. Provider must apply with all applicable regulations based on the nature of the data (HIPAA, GLBA, PCI, etc.).

8.1.7. With regard to information covered under the Family Educational Rights and Privacy Act (FERPA), Provider must commit to maintaining best practices identified by the US Department of Education's Privacy Technical Assistance Center (PTAC)'s *Responsibilities of Third Party Service Providers under FERPA*[5] and the PTAC's Data Security Checklist[6].

8.1.8. Provider must apply security best practices in accordance with NIST, FISMA/FIPS, ISO/IEC, COBIT or other recognized industry security standard to protect UWS Non-public, Confidential or Restricted information.

8.1.9. Provider must notify UWS immediately of any unauthorized disclosure of UWS Non-public, Confidential or Restricted data.

8.1.10. Provider should provide remedy for breach of UWS data held by provider through cyber liability insurance or other means, including reimbursement of UWS financial cost related to breach.

8.1.11. On termination of contract, provider must make available to UWSA all Non-public, Confidential or Restricted UWSA data in Provider's possession and must destroy all copies of UWSA Non-public, Confidential or Restricted data.

---

[3] https://cloudsecurityalliance.org/star/certification/
[4] https://www.fedramp.gov/
[5] http://ptac.ed.gov/sites/default/files/Vendor%20FAQ.pdf
[6] http://ptac.ed.gov/sites/default/files/ptac-data-security-checklist.pdf

8.1.12. In the event of bankruptcy or other cessation of operation, Provider must notify UWS and make arrangements to transfer data to UWS. UWS will be provided a minimum of 30 days to retrieve or migrate data. Unauthorized destruction or abandonment of UWSA data should constitute a material breach and UWS should be provided a right of action for actual damages.

8.1.13. Provider must disclose to UWS any internal uses of UWS data that are not for the purpose of providing services to UWSA. This includes data mining and analysis of UWS data and user behavior.

Appendix A – UW-TISC Data Classification Framework

Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). For each classification, several data handling requirements are defined to appropriately safeguard the information.

A. **Level I: Low Sensitivity/Public Data:**
Access to Level I institutional data is targeted for general public use and may be granted to any requester or may be published with no restrictions. Level I data is specifically defined as public in local, state, or federal law, or data whose original purpose was for public disclosure.

Examples of Level I (low sensitivity) institutional data:
- published "white pages" directory information
- maps
- university websites intended for public use
- course catalogs and schedules of classes (timetables)
- campus newspapers, magazines, or newsletters
- press releases
- campus brochures

B. **Level III: Moderate Sensitivity/Internal & Confidental Data:**
Access to Level III institutional data is authorized for all employees for business purposes unless restricted by a data steward. Access to data of this level is generally not available to parties outside the university community and must be requested from, and authorized by, the data steward who is responsible for the data.

Examples of Level III (moderate sensitivity) institutional data:
- project information
- official university records such as final grades, financial aid awards, financial reports, etc.
- human resources information
- some research data
- unofficial student records
- budget information

C. **Level V: High Sensitivity/Restricted Data:**
Access to Level V institutional data must be controlled from creation to destruction, and will be granted only to those authorized persons who require such access in order to perform their job, or to those individuals permitted by law. Access to Level V data must be individually requested and then authorized by the data steward who is responsible for the data. Level V data is highly sensitive and access to this data is restricted by laws such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights & Privacy Act (FERPA), Code of Federal Regulations Title 45, the Wisconsin Notification Act 138, and any other applicable federal or state laws. In law, Level V data elements are usually restricted due to a direct relationship to an individual's identity (such as name); however this policy requires restriction of the data elements themselves regardless of any link to an individual's identity.

Examples of Level V (high sensitivity) institutional data:
- social security numbers

- credit card numbers
- passwords
- individual health information or financial account information
- driver's license numbers or state identification numbers
- survey or research data covered by the Institutional Research Board (IRB) as defined by the appropriate data steward
- research and/or classes that deal with "personally identifiable information" as defined by the appropriate data steward
- any information containing biometric data that can identify an individual, such as DNA profile, fingerprint, voice print, retina or iris image, or unique physical characteristic

1.1. Data Handling

The following chart specifies security precautions needed to safeguard and protect institutional data for the three data classifications. The level of control in the following data handling areas depends on the classification of data.

Data Handling and Control Areas	Level 1 Low Sensitivity (Public Data)	Level III Moderate Sensitivity (Non-Public/Internal Data)	Level V High Sensitivity (Confidential/Restricted Data)
Printed Reports	No controls	May be sent via campus mail; no labels required	Individually authorized, with a confidentiality agreement. Must be delivered via confidential courier; reports must be marked "confidential"
Electronic Access	No controls	Role-based authorization	Individually authorized, with a confidentiality agreement
Secondary Use	Authorization by data steward recommended	As authorized by data steward	Prohibited
Physical Data/Media Storage	No controls	Access is controlled	Access is controlled, monitored, and logged
External Data Sharing	No controls	As allowed by Wisconsin Open Records Law; FERPA restrictions	As allowed by Federal regulations; Wisconsin Open Records Law; FERPA restrictions; and *Business Associate Agreement* for Protected Health Information (PHI)
Electronic Communication / Transmission	No controls	*Encryption* recommended	Encryption required

Data Tracking	No controls	No controls	Social security numbers, credit cards, and PHI locations must be registered
Data Disposal	No controls	Recycle reports; wipe/erase media	Shred reports; *Department of Defense Level Wipe* or destruction of electronic media
Auditing	No controls	No controls	Audit logins and changes in access
Mobile Devices	No controls	Password protection recommended; locked when not in use recommended	Password protected; locked when not in use; encryption used for the Level V data
Personally Owned Devices	No controls	Password protection recommended; locked when not in use recommended; up-to-date virus protection and patches required	Prohibited

Printed Reports – A requirement for the heading on a printed report to contain a label indicating that the information is confidential, and/or a cover page indicating the information is confidential is affixed to reports.

Electronic Access – How authorizations to information in each classification are granted.

Secondary Use – Indicates whether an authorized user of the information may repurpose the information for another reason or for a new application.

Physical Data/Media Storage – The protections required for storage of physical media that contain the information. This includes, but is not limited to: workstations, servers, CD/DVD, tape, USB Flash drives, laptops, and PDAs.

External Data Sharing – Restrictions on appropriate sharing of the information outside of the host University.

Electronic Communication / Transmission – Requirements for the protection of data as transmitted over telecommunications networks.

Data Tracking – Requirements to centrally report the location (storage and use) of information with particular privacy considerations.

Data Disposal - Requirements for the proper destruction or erasure of information when decommissioned.

Auditing – Requirements for recording and preserving information accesses and/or changes, and who makes them. Audit records will be kept and reviews by appropriate staff.

Mobile Devices – Requirements for the protection of information stored locally on mobile devices. This includes, but is not limited to: laptops, tablet computers, PDAs, cell phones, and USB flash drives.

Personally Owned Devices – Requirements for the protection of information stored locally on devices owned by faculty or staff. This includes, but is not limited to: desktop computers, laptops, tablet computers, PDAs, cell phones, and USB flash drives.