UNIVERSITY of WISCONSIN
UWMILWAUKEE

UWM System Security Guidelines

Introduction

Per UW System Data Protections Procedure 1031.B

"All information shall be kept in a manner consistent with appropriate controls, and procedures commensurate with its data classification the protections outlined in UW System Administrative Procedure 1031.B, Information Security: Data Protections."

https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification-and-protection/information-security-data-protections/

The purpose of this document is to provide guidance on how to ensure the security of systems and data belonging to the University of Wisconsin - Milwaukee (UWM) and University of Wisconsin System and to maintain the ability to provide disaster recovery, management and monitoring of systems.

Scope

UWM systems and services (including but not limited to servers, computers, data storage, and associated software) and their related business processes.

Exceptions

Exceptions to this procedure may be requested from the UWM Information Security Office and/or UWM Chief Information Officer.

Requirements

1. Access Controls
   a. Authentication and Authorization is required to access all moderate and high-risk systems.
   b. Only Data Stewards or a similar position should authorize access to high-risk systems.
   c. Systems identified as High-risk must utilize Multi-factor authentication.
2. Data Copying/Printing/Transmission
   a. Data distribution must be limited to individuals whose role requires access to the data and who have authorization to access the data.
   b. Paper copies of system information must be stored securely and not left unattended.
   c. high-risk data must be encrypted in transit and at rest. Accordingly, systems that store or transmit high-risk data must utilize disk encryption.
   d. Secure protocols must be used for transmission and remote access.
3. Network Security
   a. All systems must be protected by a firewall.
   b. System firewalls must be configured to limit the ports and protocols to only those necessary for the service.
   c. Intrusion detection/prevention or Advanced Threat Protection systems must be utilized to monitor and protect systems with high-risk data.
4. System Security
   a. Systems must utilize a standard Operating System build or image.

    b. Systems must be managed and monitored by an IT management application. E.g. SCCM, JAMF, RH Satellite.
    c. Systems containing high-risk data must have a defined and justifiable patch window.
    d. Services with multiple servers or operating systems must create and maintain documentation containing dependency, network, and interaction specifications.
    e. Systems containing high-risk data must send log files to a central logging service.
    f. Major systems must have central monitoring and alerting.
    g. Systems containing high-risk data must have their system information recorded within CIO approved asset management systems.
    h. Operating Systems must be joined to a central credential store.

5. Physical Security
    a. Systems containing high-risk data must be located in secure locations.
    b. Systems should have their interactive user-sessions locked or logged-out when unattended.
6. Data Storage
    a. Systems containing high-risk data must be stored in an UWM CIO or UW-System Administration approved cloud service or data center.
    b. Individuals and departments must not select storage providers or technologies without institution or UW System approval.
    c. UWM systems containing high-risk data require Encryption.
7. Backup/Disaster Recovery for major high-risk systems
    a. Backups of systems must be made on a regular basis.
    b. Backups must be tested on a regular basis.
    c. Backup media for high-risk data must be encrypted and stored securely.
8. Disposal
    a. Systems that are beyond their securely-supportable lifetime should be removed from service.
    b. Systems that are removed from service must have their data securely destroyed on-site or through a bonded disposal service.

Definitions

- ***Access****: The physical or logical capability to interact with, or otherwise make use of information resources.*
- ***Approved****: Documented approval of UWM CIO or their delegate.*
- ***Authentication****: Is the process of validating a credential and associating the enclosed identity attributes with a session. A credential may contain a verifier, or it may require collecting a verifier at runtime. A runtime verifier may be single-factor or multi-factor. Single-factor is most commonly a secret key (a password), multi-factor requires use of at least two different methods for verification.*
- ***Authorization****: Is the technical step of allowing or denying access to resources based on business rules created by the service owner. The business rules are generally expressed as access control lists that leverage identity attributes that are defined and maintained by the enterprise. There is wide variety in the architecture and style of expressing, mixing, and optimizing identity attributes, roles, privilege, and access control lists (ACLs) for efficient management of authorization across the enterprise.*
- ***Backup****: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system failure.*
- ***Change****: Any addition, modification, update, or removal of an Information Resource that can potentially impact the operation, stability, or reliability of a UWM network or computing environment.*
- ***Computer****: An electronic device for storing and processing data. (Laptop, Desktop, Tablet, Server).*
- ***Control****: A safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.*
- ***Credential****: An object that is verified when presented during an authentication transaction. Credentials consist of one or two elements:*
    1. *Identity Attributes (required): most often just a single identifier (e.g. username) associated with the entity being authenticated. However, in many circumstances, other identity attributes may be required (e.g. assertion of a right to use license fora particular resource).*
    2. *Verifier (optional as part of the credential, may be provided separately from the identity attributes at authentication time).*
    3. *The identity attributes contained in the credential are no more reliable than the identification and registration processes that precede it. The relative confidence that may be placed in the information is generally indicated by the level of assurance for the credential.*
- ***Custodian****: An individual or entity responsible for implementing Owner-defined controls and access to an Information Resource. Custodians include Information Security Administrators, UWM information technology/systems departments, vendors, and any third party acting as an agent of or otherwise on behalf of the UWM.*
- ***Custodian of an Information Resource****: A person responsible for implementing the information owner-defined controls and access to an information resource. Custodians may include state employees, vendors, and any third party acting as an agent of, or otherwise on behalf of the UWM.*

- ***Data**: Recorded data, regardless of form or media in which it may be recorded, which constitute the original data necessary to support the business of the UWM or original observations and methods of a study and the analyses of such original data that are necessary to support Research activities and validate Research findings. Data may include but is not limited to: printed records, observations and notes; electronic data; video and audio records, photographs and negatives, etc.*
- ***Decentralized Areas**: UWM business units, departments, or programs outside of University Information Technology Services that manage or support their own information systems.*
- ***Digital Data**: The subset of Data (as defined above) that is transmitted by or maintained made available in, electronic media.*
- ***Encryption**: The conversion of plaintext information into a code or cipher text using a variable, called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.*
- ***Firewall**: A software or hardware device or system that filters communications between networks that have different security domains based on a defined set of rules. A firewall may be configured to deny, permit, encrypt, decrypt, or serve as an intermediary (proxy) for network traffic.*
- ***Information**: Data organized, formatted and presented in a way that facilitates decision making. All information is data.*
- ***Information Resources**: Any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDAs), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, itis the procedures, equipment, facilities, software, and Data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.*
- ***Information System**: The technology (hardware, software, networking and data) people, and processes that an organization uses to manage data.*
- ***Integrity**: The accuracy and completeness of information and assets and the authenticity of transactions.*
- ***Institution**: The University of Wisconsin – Milwaukee.*
- ***Major system**: For purposes of this exercise, a "major system" is one which is critical to the enterprise OR one in which a significant amount of protected data resides, so much so that a breach or compromise of the system would pose a major challenge to the University. Examples include: Student Information Systems (PAWS), Human Resource Systems (AIMS), or Medical Record Systems (Medicat).*
- ***Owner**: The manager or agent responsible for the business function that is supported by the information resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security and authorizing access to the information resource. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared.*
- ***Password**: A string of characters used to verify or "authenticate" a person's identity.*
- ***Research**: Systematic investigation designed to develop and contribute to knowledge and may include all stages of development, testing and evaluation.*

- ***Security Incident****: An event which results in unauthorized access, loss, disclosure, modification, disruption, destruction of information resources whether accidental or deliberate.*
- ***Secure Protocol****: A network communication protocol that provides authentication, encryption, and message integrity in a sounds fashion that is recognized by regulatory bodies.*
- ***Server****: A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.*
- ***Vendor****: Someone outside of the UWM who exchanges goods or services for money or other consideration.*

Approved by CIO: Robert J Beck
Date: 12/16/19