Title: Information Security: Data Protection Standard

1. PURPOSE OF PROCEDURES
This document describes the minimum data protection standards that must be met by University of Wisconsin System institutions.

2. RESPONSIBLE UW SYSTEM OFFICER
Associate Vice President (AVP) for Information Security

3. DEFINITIONS
The definitions for High, Moderate and Low Data can be found in UW System Administrative Policy 1031, Information Security: Data Classification and Protection.

- **Advance Threat Protection**: A category of security solutions that defend against sophisticated malware or hacking based attacks targeting sensitive data.

Please refer to the UW System Information Security Program glossary for the following definitions:
- Data Steward (Link)
- Access Control (Link)

4. PROCEDURES
A. Minimum Data Handling Requirements
The following table establishes the minimum standards for data handling.
<table>
<thead>
<tr>
<th>Access Controls (incl. Request for Data Access)</th>
<th>Access to view low risk data does not require authentication.</th>
<th>Access to view or modify is restricted to authorized individuals.</th>
<th>Access is limited to end users and administrators who have been designated by the appropriate Data Steward or similar position.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to modify low risk data must use authentication methods that meet the requirements of <strong>UW System Administrative Policy 1030, Information Security: Authentication</strong>, and its associated procedure.</td>
<td>Remote access by third party for technical support is limited to authenticated and authorized access via secure protocols.</td>
<td>Remote access by a third party for technical support is limited to authenticated and authorized access via secure protocols.</td>
<td></td>
</tr>
<tr>
<td><strong>Copying/Printing/Transmission</strong></td>
<td>No minimum standards.</td>
<td>Data distribution must be limited to individuals whose role requires access to the data set and who have authorization to access the data set.</td>
<td>Data distribution must be limited to as few individuals as feasible whose role requires access to the data domain and who have authorization to access the data set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hard copies must not be left unattended and must be stored in a secure location.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data must be encrypted in transit and at rest, and all parties must be authenticated.</td>
</tr>
</tbody>
</table>
| Network Security | No minimum standards. | Defense in depth must be used, including two of the three following controls:  
1. Network firewall protection, including port restriction, protocol restriction or IP address Access Control Lists (ACL).  
2. Single factor authentication, such as username/password.  
3. Comprehensive intrusion detection and intrusion prevention, including advanced logging of all attempted access to network resources, or Advanced Threat Protection (ATP). | In addition to the moderate controls, protection with a network firewall is required.  
Network access to a system or server hosting the data must be limited to the minimum necessary. |
| System Security | No minimum standards. | System administrators shall follow any system security procedures established by the institution as well as operating system-specific best practices for system management and security. | System administrators shall follow any system security procedures established by the institution as well as operating system-specific best practices for system management and security.  
Protection with a firewall is required. |
| Physical Security | No minimum standards. | Data must be masked from casual view to prevent unauthorized access.  
Hardcopy files must be properly marked and stored in a locked cabinet. | System must be locked or logged out when unattended.  
Storage must be in secured location. |
<table>
<thead>
<tr>
<th>Data Storage</th>
<th>No minimum standards.</th>
<th>Data must be stored in an institution or UW System provided cloud storage service or data center. Individuals and departments should not select storage providers or technologies without institution or UW System approval. If data is stored on individual workstations or mobile devices, encryption is required. Hard copies must not be left unattended and must be stored in a secure location.</th>
<th>Data must be stored in an institution or UW System provided cloud storage service or data center. Individuals and departments should not select storage providers or technologies without institution or UW System approval. If data is stored on individual workstations or mobile devices, encryption at rest is required. Hard copies must not be left unattended and must be stored in a secure location. All devices that access high risk data must be managed in an institution or UW System approved manner.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup/Disaster Recovery</td>
<td>No minimum standards.</td>
<td>Regular backup is required and recovery periodically tested. Backup media must be encrypted and stored in a secure location.</td>
<td>Regular backup is required and recovery periodically tested. Backup media must be encrypted and stored in a secure location or offline.</td>
</tr>
<tr>
<td>Media Sanitization and Disposal</td>
<td>No minimum standards.</td>
<td>Must securely destroy or use bonded disposal service.</td>
<td>Must securely destroy or use bonded disposal service.</td>
</tr>
<tr>
<td>Workstations and Mobile Devices (incl. personally owned devices)</td>
<td>No minimum standards.</td>
<td>Password protection and an inactivity auto-lock are required. Employees shall remove UW System data from their personally owned devices before the devices are discarded or replaced, or</td>
<td>Password protection and an inactivity auto-lock are required. Employees shall remove UW System data from their personally owned devices before the devices are discarded or replaced, or</td>
</tr>
</tbody>
</table>

SYS 1031.B - Information Security: Data Protections

4 of 5
before the individual is discharged from employment with the UW System.

5. RELATED DOCUMENTS

UW System Information Security Program
UW System Administrative Policy 1031, Information Security: Data Classification and Protection
UW System Administrative Policy 1031.A, Information Security: Data Classification Standard

6. HISTORY

Revision 2: December 9, 2019
Revision 1: January 9, 2019
First approved: July 31, 2017

APPROVED BY:

Robert G. Cramer
Vice President for Administration
University of Wisconsin System