TO: Andrew Leavitt, Chancellor

FROM: John Koker, Provost and Vice Chancellor

DATE: December 9, 2019

RE: UW System Administration Policy 1032, Information Security: Awareness

On the recommendations of the Faculty Senate, Senate of Academic Staff, University Staff Senate, and Oshkosh Student Association Senate, I am recommending your approval of the UW System Administration Policy 1032, Information Security: Awareness.

I have attached the policy for your review. Please contact me if you have questions regarding the proposal.

JK/eh
Attachment

☐ Approve

☐ Do not approve

Signature

12/16/2019
Date
Policy 1032
Information Security: Awareness

1. PURPOSE
The purpose of this policy is to ensure that all employees and students that access University of Wisconsin (UW) System information technology assets are exposed to information security awareness materials commensurate with their role within the UW System.

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

3. SCOPE
This policy applies to authorized users who are issued digital credentials to access non-public information technology (IT) digital resources under the control of the University of Wisconsin (UW) System including but not limited to: currently enrolled students, employees, authorized contractors, vendors, volunteers, and other authorized users as determined by UW institutions.

4. BACKGROUND
The President of the University of Wisconsin System is empowered to establish information security polices under Regent Policy Document 25-5, Information Technology: Information Security. The UW System is committed to a secure information technology environment in support of its mission. The information security awareness training described within this policy is designed to help ensure satisfactory and consistent information security awareness throughout all UW System institutions.

5. DEFINITIONS
Digital Credentials: A user’s identification and authentication information, typically a username and password.

Employee: Faculty, staff, or students who are employed by an institution, whether compensated or voluntary.

Institutions: All research and comprehensive UW System universities and associated branch campuses, UW Shared Services, and UW System Administration.

Non-public information technology resources: Any information technology resource that is not intended to be accessed by the general public and requires authentication of the user using digital credentials.
6. POLICY STATEMENT

All employees shall:

   a. Upon hire and annually thereafter, review Regent Policy Document 25-3, Acceptable Use of Information Technology Resources and any supplemental institution acceptable use policies, if applicable.

   b. Every fiscal year, complete information security awareness training that provides information security best practices and the individual's role in protecting the university's systems and data. All newly hired employees are required to complete information security awareness training within 30 days of their initial hire date.

Students shall on an annual basis:


   b. Be provided access to information security awareness training that includes information security best practices and their role in protecting the university’s systems and data.

The UW System AVP for Information Security shall make available to institutions systemwide information security awareness training which promotes information security as an integral part of day-to-day activities. Institutions may supplement the systemwide information security awareness training, as appropriate, for systems or data sets that have specific regulatory requirements or data security needs.

Institutions are responsible for ensuring that employees have access to, and have completed, information security training each fiscal year. Institutions may take appropriate action, including but not limited to the removal of access to UW System information assets for those who have not completed training requirements.

Employees who are concurrently employed at more than one UW institution, or who have transferred from one UW institution to another UW institution, are only obligated to complete security awareness training at one UW institution, of their choosing, in a given fiscal year. Institutions may require employees to provide proof that security awareness training has been completed at another UW institution, within a given fiscal year, to satisfy compliance with this policy.

Institutions shall foster additional broad-based information security awareness activities as they deem necessary through methods such as:

- Websites
- Email
- Social media
- In-person or online training sessions
- Conferences or events
- New employee or student orientations
- Social engineering campaigns
7. RELATED DOCUMENTS

Regent Policy Document 25-3, Acceptable Use of Information Technology Resources and Computing Devices


UW System Administrative Policy 1031, Information Security: Data Classification and Protection

8. HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/14/2016</td>
<td>First Approved</td>
</tr>
<tr>
<td>09/13/2018</td>
<td>Original Issuance Date</td>
</tr>
<tr>
<td>03/29/2019</td>
<td>Revision 1</td>
</tr>
<tr>
<td>05/14/2019</td>
<td>Faculty Senate</td>
</tr>
<tr>
<td>05/16/2019</td>
<td>Senate of Academic Staff</td>
</tr>
<tr>
<td>06/12/2019</td>
<td>Oshkosh Student Association Senate</td>
</tr>
<tr>
<td>10/30/2019</td>
<td>University Staff Senate</td>
</tr>
<tr>
<td></td>
<td>Chancellor</td>
</tr>
<tr>
<td>04/2021</td>
<td>Scheduled Review</td>
</tr>
</tbody>
</table>

9. CHANCELLOR’S APPROVAL

[Signature]

Chancellor’s Signature

12/16/2019

Date