Proposed or Revised Policy Title:
The following revised policies are being proposed:

- ISO-100 Information Security Program
- ISO-200 Information Security Risk Management
- ISO-300 Identity and Access Management
- ISO-400 Information Classification and Determination
- ISO-500 Information Security Awareness Training
- ISO-600 Information Security Incident Reporting and Response
- ISO-700 Acceptable Use of Computers and Networks
- ISO-800 Privileged Access
- ISO-900 Contingency Planning
- ISO-1000 Device and Media Protection
- ISO-1100 Audit, Accountability, and Activity Review
- ISO-1200 Network, Server, and Transmission Security
- ISO-1300 Secure Application Development and Administration
- ISO-1400 Secure Facility Access Control
- ISO-1500 Vendor and Contract Security
- ISO-1600 Vulnerability and Patch Management

Policy Sponsor:
Collette, Lanita - (lcollette) – Chief Information Security Officer

Executive Leadership Review Dates:

Publication Dates:
(UAnnounce/other)

Policy description:
University information security policies have the following frequency of review requirements formalized in each policy: “The CISO must review information security policies and procedures annually, at minimum. This policy is subject to revision based upon findings of these reviews.”

This revised policy package includes the revisions from annual review and discussion with the Information Security Office Policy Working Group which is open to all University employees.

Reason for new policy or revision:
The landscape of information security threats and vulnerabilities change constantly. Furthermore, constant changes at the University create the potential for different information security business impacts if a threat actor can exploit a vulnerability. Therefore, annual discussion and revision of University information security policy is needed to create balance between the University’s information security risk tolerance and the University’s actual information security risk. Additionally, for the University to continue to maintain Cyber Risk Insurance Policy coverage at industry standard premiums, several policy revisions were identified as being essential.

Major impacts to University and potential stakeholders:
The most substantial change to University information security policies this year is a
simplification to how the University classifies information. The classification levels“Confidential” and “Regulated” were collapsed into a single classification “Restricted.” This change simplifies University decision making and avoids creating excess regulatory compliance risk through its classification process. The change requires a major refactoring of many policies.

The smaller changes were focused on creating additional specifications related to the increase in remote work to aid the institution in making information security risk-informed decisions related to work process changes necessitated by the COVID-19 pandemic.

**Anticipated concerns or objections:**
None.

**Describe the communication plan for sharing this new policy or revision:**
This package of policy revisions has already been reviewed and discussed by the ISO Policy Working Group. The most substantial changes were discussed with the IT Directors Council.

Updates to University information security policy are representative of updates to information security strategy for the institution. The primary mechanism for University Units to make information security risk-informed decisions and align with institutional information security strategy is the Information Security Risk Management Program. After the revised policy package is published, corresponding revisions will be made to the Risk Assessment required as part of participation in the program, enabling University Units to understand changes to strategy and update Unit information security practices through Risk Analysis and Security Planning also delivered through the program.

University Senior Leadership will be provided an updated University-wide Security Plan at the end of each fiscal year information security risk management cycle with performance measures to report progress towards information strategy formalized as University information security policy requirements.

**Estimate and description of financial cost to implement, if any:**
None.

**Will the policy affect any of the following?**

<table>
<thead>
<tr>
<th>Existing UA Procedure</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance with law/regulation</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Existing Board Policy</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Public</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Describe any item checked “yes”:**

Where new policy requirements differ from previous policy requirements, University Units will need to change their existing procedures to account for these changes. As the primary
mechanism to assist Units in updating procedures, the Information Security Office provides an Information Security Risk Management Program which guides Units through self-assessing against University information security strategy and developing Unit-specific Security Plans to address any discovered gaps.

rev. 7/2021