Information Security Program

Policy Number:
IV.06.01

Reason for Policy:

This policy will give the University of Oregon Information Security Office the authority to perform various security activities to protect the University's data, computers, networks, and users.

Responsible Office:

For questions about this policy, please contact the Chief Information Security Officer at 541-346-9700 or wlaney@uoregon.edu.

Enactment & Revision History:

Enacted as an emergency policy by Dr. Scott Coltrane, Interim President on June 25, 2015. This policy supersedes former OAR Chapter 580, Division 055.

Policy:

Summary
This policy grants authority to the University of Oregon Information Security Office, a unit within Information Services, to implement an Information Security Program to mitigate risk regarding information security. Responsibilities of the Information Security Program include, but are not limited to:

- Develop policies, procedures, and guidelines for securing University systems, networks, and data based on applicable laws, regulations, and best practices
- Consult with campus users and departments to investigate information security issues, perform risk assessments, and propose products and processes to mitigate risk discovered
- Monitor the University networks to identify malicious activity
- Provide incident response for information security incidents
- Increase campus awareness of information security through training and communication
- Use frameworks to ensure that information security is built into current and new systems.
- Identify risks to the security of information, systems, and users in order to mitigate these risks to levels acceptable by University Administration.

Scope
The University of Oregon Information Security Office will have information security

responsibilities over all University data, computers, and networks. Each member of the University community has a role in protecting the security of information including Faculty, Staff, Students, Vendors, and Contractors.

Policy Statement

The University of Oregon Information Security Office will implement an Information Security Program to mitigate risk regarding information security. There will be a number of duties performed by the University of Oregon Information Security Office to carry out the responsibilities of the Information Security Program. The Program will include, but is not limited to, the following activities:

1. **Development of Policies, Procedures, and Guidelines**
   The University of Oregon Information Security Office will draft policies, procedures, and guidelines related to information security. These may be overarching policies such as data classification polices or specific technical guidelines such as how to encrypt hard drives. The policies, procedures, and guidelines will be developed in conjunction with Campus IT Leadership to ensure that they will be effective in mitigating risk in the many diverse Campus units. Additional identified groups will also be included in the review to gather input. The policies, procedures, and guidelines will be developed based on state and federal laws and regulations by which the University is bound as well as best practices in the information security community. Changes in policy will be reviewed by the Policy Advisory Council. Changes in procedures will be reviewed by Campus IT Leadership.

2. **Perform Risk Assessments**
   The University of Oregon Information Security Office will perform risk assessments of central systems to determine gaps where additional security controls are needed. If gaps are discovered, recommendations will be made to mitigate potential risk. The University of Oregon Information Security Office will also work with Campus units who request a risk assessment of their systems. Occasional Campus-wide security assessments will be performed in conjunction with Campus IT Leadership.

3. **Operate Security Systems**

   The University of Oregon Information Security Office will operate systems that monitor the security of UO computers and networks. Examples of these types of systems include the campus-provided antivirus solution and our malware detection system

4. **Perform Network Monitoring**
   The University of Oregon Information Security Office will monitor the University networks for malicious activity. These can include, but are not limited to, the presence of viruses and malware, users transmitting or receiving larger than normal amounts of data, violations of the Acceptable Use Policy (http://it.uoregon.edu/acceptable-use-policy), systems being used to relay spam, and internal or external individuals attempting to break into University systems. The University of Oregon Information Security Office will use these network monitoring capabilities to notify individuals and University units of systems where problems are detected. By default the Information Security Office will not

investigate monitored data at the level of an individual user, but will investigate at the individual level when an appropriate triggering event occurs on its Security Systems (such as the antivirus system). Authorized investigators include Information Security Office staff and also IT Professionals in the units where an event is triggered."

5. **Data Retention Limits**
   Data (construed to include *all* personally-identifiable information in addition to other forms of retained data) from security systems and network monitoring systems will be maintained for a maximum of one year. The need for data retention up to this maximum limit will be reviewed on a periodic basis to determine if data can be retained for a shorter period of time. Any retention of data beyond the maximum of one year will require a revision to policy per the regular policy press.

6. **Lead Security Incident Response**
   The University of Oregon Information Security Office will provide security incident response in the event of breaches on University systems. This will include forming a Security Incident Response Team, performing forensics to gather relevant data, and providing a report on whether and how the system was compromised, what type of data was resident on the system, and if the data appears to have been viewed or exfiltrated by an unauthorized individual.

7. **Provide Security Awareness, Training, and Communication**
   The University of Oregon Information Security Office will raise the awareness of information security through awareness materials, website presence, and awareness talks at University meetings. The University of Oregon Information Security Office will also provide training for technical and non-technical Faculty, Staff, Students, Vendors, and Contractors on security tools that can be used to mitigate security risk. Finally, the University of Oregon Information Security Office will provide communications to Campus IT Leadership on how to remediate security vulnerabilities when they are discovered.

8. **Use Security Frameworks to Provide a Consistent Security Posture**
   The University of Oregon Information Security Office will use the *Framework for Improving Critical Infrastructure Cybersecurity* developed by the National Institute of Standards and Technology (http://www.nist.gov/cyberframework/) to address the security posture of the University. By standardizing on one framework the University of Oregon Information Security Office will be able to provide for consistent and repeatable security assessments and recommendations across all University systems, data, and networks.

Who Should Know This Policy

All University personnel and external parties involved with using, requesting, approving, or accessing UO information assets.