DOMAIN: INFORMATION SECURITY & PRIVACY GOVERNANCE SUBCOMMITTEE (ISP GC) - CHARGE

Summary

The Information Security and Privacy Governance Subcommittee (ISP GC) has been established to ensure that the information security and privacy programs are aligned with UO academic, research, and administrative objectives. The committee covers the protection of information systems, data confidentiality, integrity and availability. The ISP GC is expected to meet at least quarterly.

Last Updated - version: March 20, 2023

Purpose and Scope:

Sponsored by the Information Technology Steering Committee (ITSC), the Information Security and Privacy Governance sub-Committee (ISP GC) has been established to ensure that the information security and privacy programs are aligned with UO academic, research, and administrative objectives, and are consistent with university policies, state and federal laws. This subcommittee is charged to:

- Establish and maintain accountability for the UO Information Security and privacy programs by providing input and feedback to the ITSC, and oversight of university information security and privacy programs
- Provide oversight for resource allocation related to information security and privacy initiatives including requesting new funding, service addition, and use of pre-existing funding sources for improvements up to $100 thousand
- Mediate conflicting risks or competing information security and privacy requirements
- Provide assurance oversight relating to information security and privacy policies

The committee addresses information security which covers the protection of information systems, data confidentiality, integrity and availability[1]. Additionally, the committee has oversight responsibility for privacy, and the safety and reliability relating to operational technology (OT) and the internet of things (IoT) that integrate with traditional information technology.

Procedural Guidelines:

- *Meetings*: The ISP GC is expected to meet at least quarterly. The expectation is that additional committee work will be performed via "virtual" means and asynchronously, given the predicted challenges with scheduling additional face-to-face meetings. Chairs are responsible for ensuring visibility of the meeting on the global governance calendar Sharepoint site. Chairs will assign the meeting scheduling and logistics activities to a meeting participant such as an executive assistant or co-chair.

[1] Confidentiality, integrity and availability, commonly referred to as the CIA-triad refers to controls to limit data access to authorized individuals with need to know (confidentiality); ensuring that data is not modified in an unauthorized manner (integrity); and is always there when needed (availability).

- *Recommendations and Report*s: The committee will submit recommendations, comments, and ideas to the ITSC, as needed. Discussion to obtain consensus on recommendations and ideas will be the prevailing procedure used at meetings. If consensus cannot be obtained, a minority report may be prepared.
- *Minutes*: Summary minutes of each meeting will be kept. Copies will be sent to the ITSC as soon as possible after each meeting. Copies of the minutes will be made accessible to the University's IT and other stakeholders. Chairs are responsible for ensuring meeting minutes are taken, assigning the task to a meeting participant such as an executive assistant or co-chair.
- *Amendment of Charge*: Amendments to the charge may be made by the CISO with approval by the CIO and the ITSC, as necessary.

Tasks and Agenda

Following are examples of tasks and agenda items expected to be addressed by the committee:

- Reviewing and endorsing policies, strategies and major projects or initiatives based on security and privacy requirements (e.g., HIPAA, FERPA, GLBA, GDPR, PCI DSS)
- Tracking the progress of information (or OT) security risk remediation
- Reviewing information (or OT) security status metrics or requesting new metrics when needed
- Reviewing and approving or rejecting requests for policy exemptions from business units or projects
- Establishing ad hoc temporary working groups (including inviting subject matter experts) to investigate and report back on topics of interest

Membership

Members are appointed by and serve at the discretion of the CIO. All members must have a broad campus perspective and demonstrated interest in the strategic direction of information security and privacy in support of the University's mission. Members with term limits can have up to two consecutive appointments. Membership will include:

1. Chair: Chief Information Security Officer
2. Director of Institutional Research
3. University Registrar
4. Office of the Provost
5. Chief Human Resource Officer (CHRO)
6. Chief Resilience Officer (CRO)
7. University Records Manager
8. University HIPAA and Privacy Officer
9. Director of Research High Performance Computing Facility
10. One representative from the Office of the Vice President for Research & Innovation (Assistant Vice President or higher)
11. Vice President of University Communications
12. Associate Vice President of Business Affairs and Controller
13. One member from the Office of General Counsel

14. One senior member from the UO Libraries (two-year appointment)
15. One Senior member from Information Services (two-year appointment)
16. Two members from the Non-IS IT Directors group (two-year appointment)
17. One Academic Department Head (two-year appointment)
18. Two faculty members (two-year appointment)
19. The University of Oregon Senate (two-year appointment)
20. Audit (non-voting)
21. Subject matter experts will be invited to meetings as needed

Authorization:

_____ _____

Abhijit Pandit, Vice-President for Information Services and CIO Date