IT Security Advisory Board Charter

PURPOSE

The IT Security Advisory Board (hereinafter referred to as “the Board”) is a deliberative body charged to provide guidance and oversight at the direction of the Information Technology Strategy Council (ITSC). The purpose of this charter is to outline responsibilities, composition and operating guidelines.

Our foremost priority is to diligently assess and mitigate cyber risks, ensuring the resilience and integrity of our digital infrastructure. We are steadfast in safeguarding sensitive information, recognizing the paramount importance of securing data such as social security numbers, which serve as the cornerstone of personal identity protection. Moreover, our dedication extends to the formulation and enforcement of robust information security policies, exemplified by adherence to standards such as IS3 and IS12. Additionally, we are committed to upholding general compliance requirements mandated by regulations such as GLBA, Title IX, HIPAA, and PCI, demonstrating our unwavering commitment to regulatory adherence and the preservation of trust within our organization and beyond.

RESPONSIBILITIES

The Board is an advisory body with the following responsibilities:

1. Champion strategic direction with Campus partners.
    a. Set and oversee policies and procedures for balancing privacy and security.
    b. Set and oversee policies and procedures for accepting information risk.
    c. Broad oversight of the Campus information security and privacy programs.
    d. Discuss cybersecurity topics and their implications for the University's security posture.
2. Engage with internal and external stakeholders, including senior management, and IT staff, to gather insight and perspective.
3. Evaluate (with recommendation to endorse or reject) IT investment requests and projects based on strategic security objectives.

4. Review (with a recommendation to endorse or reject) security-related product roadmaps.
5. Review (with recommendation to endorse or reject) the priority of projects related to the security enterprise.
6. Be informed of significant project developments and challenges, and provide guidance as needed.
7. Report regularly Board activities, findings, and recommendations to the ITSC.
8. Review and make recommendations about IT governance policies, standards, and procedures to ensure alignment with strategic objectives and best practices.
9. Promote IT governance awareness and foster a culture of accountability.

COMPOSITION

The Board will consist of a diverse group of staff and faculty with the necessary expertise and experience in IT/governance.

Roles

1. **Chair:** A permanent ITS staff member appointed by the ITS CIO. Their responsibilities include regular attendance of the IT Security Advisory Board, setting meeting agendas, presiding over meetings, and ensuring the effective operation of the board. Provides recommendations to the Chief Information Officer (CIO) of Information Technology Services (ITS) regarding modifications to board membership.
2. **Co-Chair:** A rotating member serving a two-year term, with eligibility for a two-year renewal. Their responsibilities include regular attendance of the IT Security Advisory Board, aiding the Chair in preparing meeting agendas, and jointly presiding over the meetings.
3. **Members:** Participates in discussions and decisions, represent constituents across Campus units, and provides context on justification and prioritization of work. Membership will rotate based upon a staggered two-year term assignment.

The Board shall consist of the following representatives: *IT Security Advisory Board Membership*.

OPERATING GUIDELINES

Meeting Procedures

1. **Frequency:** The Board shall meet at least quarterly or as deemed necessary by the Chair.
2. **Agendas:** Topics for the meeting will be collected by the Chair. The meeting agenda and supporting reference materials are to be circulated to members in advance of the meeting.
3. **Member Preparation:** In addition to the scheduled meetings, members should expect to spend time accessing and reviewing relevant materials in advance to fulfill their responsibilities.
4. **Member Participation:** Each member is expected to attend and actively participate in Board meetings. Their responsibility is two-way: to bring input and perspective from his or her constituency to the Board and to report back issues and results widely. Board members shall maintain the confidentiality of all sensitive and proprietary information discussed during Board meetings.
5. **Decision-Making:**
    a. **Decisions are made within the meeting** upon agreement of a simple majority of voting members; one vote per person (regardless of how many areas they represent). For more routine matters, decisions may be made outside of a meeting via electronic methods (e.g. poll).
    b. **Off-cycle decisions** may be necessary due to unforeseen circumstances. Being flexible and responsive to changing needs is crucial for effective governance.
        i. Chairs have the authority to approve operational and non-major work requests.
        ii. Chairs must communicate off-cycle decisions and rationale behind them at the beginning of the next board meeting, setting the stage for transparency.
6. **Guests:** The Chair may invite other appropriate individuals (i.e. Subject Matter Experts) to participate in specific projects or agenda items.
7. **Minutes:** Minutes shall be recorded for each meeting, documenting decisions, recommendations, and any assigned actions. Minutes will be published in the IT Security Advisory Board - Meeting Agenda & Minutes folder.

8. **Documentation:** Agendas, reference materials, presentations, and minutes from each meeting are to be made available on the Board's corresponding folder on the ITS Governance Google Drive in a method that aligns with the governance values of transparency, accountability, stewardship, collaboration, and agility.
9. **Communication:** Key findings, recommendations, and decisions will be communicated to the Information Technology Strategy Council (ITSC) and the IT Senate Committee. Not all decisions or updates may be relevant to all parties, so communication may be selective and targeted based on the nature of the information. Information may flow through channels in a specific order, ensuring that key individuals or groups are informed before broader communication is initiated.

REVIEW

1. The Charter shall be reviewed and updated at least once every year or as necessary to ensure alignment with organizational needs and industry best practices.
2. Amendments to the Charter require approval by the Board.

APPROVAL

This charter is hereby approved and adopted by the IT Security Advisory Board on *3/26/2025*.

Dewight Kramer
Advisory Board Chair