



Information Security
Governance Committee Charter
Updated as of August 2019

PURPOSE

The Information Security Governance Committee's (ISGC) primary purpose shall be to act on behalf of the University's Executive Leadership Team (ELT) in fulfilling the University's oversight responsibility with respect to the University's information technology use and protection, including but not limited to data governance, privacy, compliance, and cybersecurity.

The ISGC is tasked with enterprise-wide oversight of Columbus State University's electronic information footprint. To be successful, the ISGC will align and coordinate resources with the various schools, colleges, and departments across the University. These coordinated security efforts will be vetted by all impacted parties through an agreed-upon governance process.

The ISGC will be as forward-thinking as possible. Therefore, it commits to:

- Certifying the clarity of the cyber-risk management programs
- Expressing confidence in the adequacy of the overall program
- Confirming trust and confidence in the information the stakeholders receive
- Continually challenging the effectiveness of existing cyber-risk management programs
- Supporting cyber-risk initiatives as they continue to evolve
- Promoting a risk-aware culture through continuous communication to the CSU community
- Developing a holistic risk management strategy
- Ensuring systems are adequate to protect against security breach and effectively safeguard the University's infrastructure, assets, intellectual property and data
- Striking a balance between the cost of the program and the value that it provides to reflect its sensitivity to the impact its actions will have on the University budget.



COMPOSITION

The Information Security Governance Committee shall consist of the following current roles at Columbus State University. The Committee shall appoint Committee members, fill vacancies occurring on the Committee, and designate the Chair of the Committee:

Interim Chief Information Officer (CIO)	Theodore Laskaris
Interim Chief Information Security Officer (CISO)	Loretta Marshall
Human Resources Director	Carole Clerie
Enterprise Risk Management	Richard Barrow
General Counsel	Craig Burgess
Assistant Vice President of Business and Finance	Jeffery Davis
Director of TSYS Cyber Security Center	Michael Barker
Department Chair/Professor of Computer Science	Shamim Khan
Interim Executive Director for Operations & Infrastructure Services	Valerie Alexander
Executive Director of IT Services	Mary Covington
Assistant Dean of Students	Dana Larkin
Assistant Chief of Police	Laura Bennett

MEETINGS AND MINUTES

The Committee shall hold such regular and/or special meetings as its members shall deem necessary or appropriate. The minutes of each meeting of the Committee shall be prepared and distributed to each Committee member. The Chair, in consultation with the other committee members, shall determine



the length of the committee meetings and shall set the agendas for Committee meetings. The Chair of the Committee shall report to the ELT from time to time or whenever so requested by the ELT.

The Chair (or in their absence, a member designated by the Chair) shall preside at each meeting of the Committee. The Committee shall have the authority to establish its own rules and procedures for notice and conduct of its meetings so long as they are not inconsistent with any provisions of the University's bylaws that are applicable to the Committee.

AUTHORITY

The ISGC has the authority to conduct assessments and review processes to evaluate the adequacy and completeness of the information security plan and the information security governance structure within the context of the institution's strategic priorities and goals and within the context of the regulatory environment.

In fulfilling its responsibilities, the Committee shall be entitled to delegate any or all of its responsibilities to a subcommittee of the Committee.

RESPONSIBILITIES

The Committee shall be responsible for the following:

1. Data Governance - To provide oversight of policies, procedures, standards, guidelines, plans, and execution intended to provide security, confidentiality, availability, and integrity of the information.
2. Disaster Recovery - To review periodically the University's disaster recovery/business continuity capabilities.
3. Compliance Risks and Information Security Audits - To oversee the University's management of risks related to its information technology systems and processes, including privacy, network security, data security, and any audits of such systems and processes.



4. Periodic and Annual Reports - To review and oversee the preparation of the University's disclosures in its reports filed relating to the University's information technology systems, including privacy, network security, and data security.
5. Advisory Role - To review the University's information technology strategy or programs relating to new technologies, applications, and systems.
6. Annual CISO Report - Review annually, the CISO's assessment of the effectiveness of the University's risk management and data security programs measured against the University's cybersecurity threat landscape, including the following program components: cybersecurity risk monitoring, effectiveness testing, integrity of information security systems and controls, adequacy of resources, security awareness training and cybersecurity insurance coverage.
7. Regulatory Landscape - Review and discuss key legislative and regulatory developments that could materially impact the University's cybersecurity risk exposure.
8. Incident Response Plan - Assess annually the effectiveness of the University's data breach incident response plan as presented by the CISO, including disclosure, investigation, remediation and post-breach security measures.
9. ISGC Performance Review - The Committee shall evaluate the Committee's performance and the performance of its members on an annual basis, including the Committee's compliance with this Charter, and provide the ELT with any recommendations for changes in procedures or policies governing the Committee. The Committee shall conduct such evaluation and review in such manner as it deems appropriate.
10. ISGC Charter Review - The Committee shall review and reassess this Charter, including the Committee's purpose and oversight role, at least annually and submit any recommended changes to the ELT for its consideration.