University of Pittsburgh
Information Technology Security Policy Committee Charter

I. Preamble

This body is called the Information Technology (IT) Security Policy Committee (Committee). It is authorized by the Chancellor and will serve at the Chancellor's discretion. The Chancellor has authorized the Vice Chancellor and Chief Information Officer (VC/CIO) to direct the operations of this Committee, consistent with the terms of this Charter. This Charter outlines the purpose, relevant background, scope, responsibilities, composition, and operations of the Committee, as well as the review process for any proposals generated by this Committee.

This document should be read in conjunction with Policy AO 01, Establishing University Policies, and all other applicable University policies, protocols, and procedures.

II. Purpose

The Committee is created for the purpose of proposing a University IT Security Policy, as well as documents that will support its implementation, which will describe the University's security practices and responsibilities for protecting Controlled Unclassified Information in Nonfederal Systems and Organizations as described in NIST 800-171.

III. Background

The University is required to have IT security controls for the Controlled Unclassified Information it generates, stores, and shares. Controlled Unclassified Information is sensitive information that requires protection due to its importance to federal agencies or the government. NIST 800-171 provides security measures including user authentication, access controls, encryption, incident response planning, media handling procedures, and regular security assessments to safeguard controlled unclassified information. Development of this policy will: 1) establish an IT security framework based on standards including NIST 800-171 and other standards as appropriate; 2) provide responsibilities to Pitt IT and other relevant departments for IT control activities; and 3) create a more coordinated environment.

IV. Scope and Authority

The Committee will recommend an IT Security Policy and supporting documents. In doing so, the Committee's deliberations must address the following topics:

- **Authority and Responsibility**. Examine the NIST requirements and associated responsibilities and identify which components within the University are responsible for implementation.

- **Operational Impact.** Consider the operational impact on Units with access to covered information in implementing IT security controls necessary to meet NIST 800-171 requirements and determine what rules or processes can be established to lessen that impact.
- **Best Practices**. Assess best practices in higher education regarding the protection of Controlled Unclassified Information and determine applicability to the University.
- **Clarity**. Consider users of the Policy and the use of terms so that the Policy and supporting documents are clear and concise.
- **Alignment**. Identify University Policies that impact or will be impacted by the proposed policy, including research and human resources policies.
- **Non-Compliance.** Address how compliance will be monitored and enforced.
- **Interoperability**. Consider the impact establishing IT security controls will have on the University's third-party partners.

V. Responsibilities

As provided above, the Committee is created to propose a Policy on IT Security. To perform this function, the Committee has the responsibility to:

- Review NIST 800-171 for the framework and control activities to be implemented;
- Research and incorporate IT security requirements for research;
- Research and discuss best practices for IT Security policies, including benchmarking peer universities;
- Consistent with the terms of this Charter, consult with specific stakeholders in the University community that have access to Controlled Unclassified Information or other sensitive information potentially within the scope of this policy.
- Incorporate or address applicable federal and state requirements in the proposed Policy and procedure;
- Consistent with the terms of this Charter, consult with ITAC and its Information Security Subcommittee;
- Recommend a draft Policy for review pursuant to the process described in Section VIII below and consider feedback received during that review; and
- Recommend a draft procedure or supplemental guidance, if needed, for the effective and efficient implementation of the proposed Policy.

It is expected that the Committee will work in confidence in order to have a full and frank discussion of all options. Individual members should maintain the deliberations of the committee confidential and are expected to not discuss the content of the Committee's deliberations outside of the Committee, unless authorized to do so by the Committee. The broader community will

have an opportunity to consider the Committee's proposals pursuant to the process described in Section VIII below.

VI. Composition

This Committee will be chaired by **Brian Hart**, IT Policies and Special Projects, Pitt IT. The Committee will include the following members:

1. **Mark Anderson**, Executive Director, Enterprise Risk Management
2. **Robert Cunningham**, Vice Chancellor for Research Infrastructure
3. **John Duska**, Interim Chief Information Security Officer
4. **Robert J. Ellison**, Systems Architect, Computing, Telecommunications, and Media Services; and Adjunct Professor, Computer Information Systems & Technology at the University of Pittsburgh at Bradford & Titusville Campuses
5. **Luke Ferdinand,** Technology Support Services Manager, University Library System and Staff Council Representative
6. **Laurel Gift**, Assistant Vice Chancellor, Office of Compliance, Investigations, and Ethics
7. **Jay Graham,** Chief Enterprise Architect, Pitt IT
8. **Ryan Mahramas,** Associate University Registrar
9. **Ilia Murtazashvili**, Associate Professor in the Graduate School of Public and International Affairs, Associate Director of the Center for Governance and Markets, and Past Chairperson of the Faculty Senate's Computing and Information Technology Subcommittee.
10. **Uduak Ndoh,** Vice Chancellor and Deputy Chief Information Officer, Health Sciences
11. **Amy Wildman,** Director of Data Analytics and IT solutions, Kenneth P. Dietrich School of Arts & Sciences
12. **Bill Yates,** Vice Chancellor, Office of Research Protections, Professor of Otolaryngology, Professor of Neuroscience, Professor of Clinical and Translational Science, School of Medicine

Anthony Graham, Senior Policy Specialist, Policy Development and Management, will facilitate and support the Committee.

VII. Operations

The Committee will meet monthly or more frequently as circumstances dictate, until the work set forth above is complete. The Committee's proposed Policy on IT Security will be submitted to the VC/CIO no later than the beginning of the Fall term 2025. The VC/CIO may ask for interim status reports.

After the VC/CIO's review is complete, the draft Policy will be submitted to the Policy Office to coordinate its review consistent with Policy AO 01.

VIII. Policy Review Process

The review process for the Committee's recommended Policy will include:

- University comment period;
- Academic Leadership Team;
- University Senate's Computing and Information Technology Committee;
- Faculty Assembly;
- University Senate Council; and
- Administration Leadership.

The Committee will coordinate with the Policy Office to consider feedback provided throughout this process. Once this review process is complete, the proposed policy will be sent to the Policy Office for review and submission to the Chancellor in accordance with Policy AO 01.

IX. Amendment

Any amendments to this Charter must be made in accordance with Policy AO 01 and receive the approval of the Chancellor or designee.

This Committee shall expire on the publication of a new University Policy that governs IT Security, unless otherwise directed by the Chancellor.