Identity University of Pittsburgh
Identity Theft Prevention (Red Flag) Policy Committee Charter

I. Preamble

This body is called the Identity Theft Prevention Policy Committee (Committee). It is authorized by the Chancellor and will serve at the Chancellor's discretion. The Chancellor has authorized the Senior Vice Chancellor and Chief Financial Officer (SVC/CFO) 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 new University Policy and supporting documents (e.g., procedures or standards) which will establish requirements and guidance relevant to the implementation of the University's Identity Theft Prevention Program.

III. Background

The University is required by federal regulations issued by the Federal Trade Commission (FTC) to implement an identity theft program (Red Flags Program), which identifies, detects, and responds to warning signs of identity theft (i.e., Red Flags), as well as prevent and mitigate identity theft. Currently, the University has various privacy practices in place to identify potential threats of identity theft, but those practices are currently decentralized and not formalized through University Policy. Federal regulation also requires that the University have a written policy governing that organization's identify theft program. This Committee is charged with developing a policy that meets that requirement and provides the responsibilities and processes that will be used in the University's identity theft program, including identifying covered accounts, detecting Red Flags, and describing the response to those Red Flags.

IV. Scope and Authority

The Committee will recommend a new Identity Theft Prevention Policy and supporting documents. In doing so, the Committee's deliberations must address the following topics:

- Scope. Identify the accounts that are subject to Policy and the Red Flags Program, including a definition of a covered account.

- Financial Impact. Determine whether any proposed changes to the current practices will potentially increase costs or provide cost savings.
- Establish Oversight. Identify which unit(s) will be responsible for conducting oversight of the Red Flags Program.
- Unit Responsibilities. Articulate Unit's responsibilities to stay in compliance with the Program, including any reporting requirements.
- Compliance. Address all statutory and regulatory requirements associated with the Red Flags Program, including those under the FTC's Red Flags Rule.
- Clarity. Consider users of the Policy and the use of terms so that the Policy and supporting documents are clear and concise.
- Third Party Servicers. Consider how this Policy impacts the University's third-party payment processors.

V. Responsibilities

As provided above, the Committee is created to propose a new Policy that will govern the Red Flags Program. To perform this function, the Committee has the responsibility to:

- Incorporate or address applicable federal and state requirements in the proposed Policy and procedure;
- Examine best practices in higher education, as well as those used by other local employers, when considering how this Policy can aid in the University's efforts to prevent identity theft;
- In accordance with the terms of this Charter, discuss proposals with interested stakeholders as needed;
- Review the current privacy practices in place to identify potential threats of identity theft, and consult with offices implementing those practices;
- 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 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 **Laurel Gift, Assistant Vice Chancellor, Office of Compliance, Investigations, and Ethics** and **John Duska, Chief Information Security Officer.** The Committee will include the following members:

1. **Mark Anderson,** Executive Director, Enterprise Risk Management
2. **David Basile,** Commander of Investigations, University Police Department
3. **Ericha Geppert,** Compliance Analyst, Compliance, Investigations, and Ethics
4. **Carolyn Hoyt,** Vice Chancellor for Advancement Operations
5. **Aynsley Jimenez,** Compliance Specialist, Human Resources
6. **Roseanne Johnston,** HIPPA Security Officer, Health Sciences IT
7. **Carolyn Kaikaka,** Associate Vice Chancellor, Student Financial Services
8. **Klaus Libertus,** Senate Computing & Information Technology Committee Member
9. **John McIntyre,** Security Analyst, Pitt IT
10. **Jill McLinden,** Chief Financial Analyst, School of Dental Medicine
11. **Gretchen Natter,** Assistant Dean of Students, Student Affairs

Tony Graham, 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 and associated procedures will be submitted to the SVC/CFO no later than the beginning of the 2024 Fall semester. The SVC/CFO may ask for interim status reports.

After the SVC/CFO'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;
- University Senate's Senate Computing & Information Technology Committee;
- Faculty Assembly;
- Staff Council;
- University Senate Council;
- Academic Leadership Team; 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 the Identity Theft Prevention, unless otherwise directed by the Chancellor.