Potential Amendments to the Proposal for the Establishment of a University Privacy Policy (Senate Document #20-21-15)

The Information Technology (IT) Council's recommendation associated with the University of Maryland Privacy Policy can be found here.

The following amendments to the proposed Privacy Policy have been submitted for consideration at the Senate meeting and must be formally proposed by the Senators who submitted them, discussed, and voted on at the meeting. The amendments are being sent to Senators so that they can review them in advance of the meeting.

In the following amendments, text in **blue and bold** indicates an addition; text in ~~red and strikethrough~~ indicates a removal. Text in green indicates moved text.

Amendment #1

VI. Policy Violations

A. **Suspected violations of this Policy will undergo a standard University review in accordance with relevant University policies to determine responsibility.**

~~A~~**B**.University employees or students who are found responsible for violating this Policy and/or the associated Privacy Standards and Guidelines may be subject to disciplinary action in accordance with relevant University policies. Furthermore, certain violations may result in civil penalties and/or criminal prosecution.

~~B~~**C**.Unit Heads who are found responsible for knowingly or intentionally violating this Policy and/or the associated Privacy Standards and Guidelines, where such violations lead to, or are responsible for, a reportable security incident or other penalties imposed by government regulators or agencies, may obligate the responsible unit to cover a portion or all of the University remediation costs and/or externally imposed penalties associated with the violation.

Amendment #2

V. Implementation

A. This Policy, the associated Privacy Standards and Guidelines, and the implementation of those instruments are overseen by the University's Chief Data Privacy Officer (umd-privacy@umd.edu).

B. The Division of Information Technology (DIT) is responsible for supporting Units with the implementation of this Policy by providing effective tools, appropriate resources, and training aimed at minimizing potential costs and workload burdens imposed on Units.

~~B~~**C**. Standards and Guidelines

1. This Policy is supplemented by Privacy Standards and Guidelines that are developed in coordination with appropriate stakeholders and the University IT Council and maintained by the Chief Data Privacy Officer. These Standards and Guidelines address the operationalization of the privacy Principles identified in Section IV.A, including but not limited to access to specified data types, vendor engagement, incident response, and the exceptions process.

2. The Vice President for Information Technology & Chief Information Officer (VPIT & CIO) or designee may issue, amend, or rescind such Privacy Standards and Guidelines as required to comply with legal obligations and University policy, or to meet the needs of the University Community.

~~C~~**D**.Exceptions

1. Where a legitimate need has been demonstrated, such as a novel use of an existing data set for health and safety purposes, the VPIT & CIO or designee, in X-15.00(A) page 5 consultation with appropriate stakeholders, may grant exceptions to this Policy and its Standards and Guidelines.

2. When considering requests for exceptions, the VPIT & CIO or designee, in consultation with appropriate University stakeholders, will evaluate the documented purpose for the exception and the privacy risks to the individuals affected.

3. Subject to the University's legal obligations or circumstances that necessitate immediate access, the University may provide advance notification to an individual prior to the use of the individual's PII pursuant to an exception request. In certain instances, individuals may be unavailable to receive such advance notification, or such notification may not be reasonably practicable. In such cases use may occur without notification, consistent with applicable law.

Amendment #3

V. Implementation

A. This Policy, the associated Privacy Standards and Guidelines, and the implementation of those instruments are overseen by the University's Chief Data Privacy Officer (umd-privacy@umd.edu).

B. Standards and Guidelines

1. This Policy is supplemented by Privacy Standards and Guidelines that are developed in coordination with appropriate stakeholders and the University IT Council and maintained by the Chief Data Privacy Officer. These Standards and Guidelines address the operationalization of the privacy Principles identified in Section IV.A, including but not limited to access to specified data types, vendor engagement, incident response, and the exceptions process.

2. The Vice President for Information Technology & Chief Information Officer (VPIT & CIO) or designee may issue, amend, or rescind such Privacy Standards and Guidelines as required to comply with legal obligations and University policy~~, or to meet the needs of the University Community~~.

Amendment #4

II. Definitions

A. "Personally Identifiable Information" means information that is created, received, processed, stored, or transmitted by or on behalf of the University that, alone or in combination with other information, enables the identification of an individual. PII includes but is not limited to a person's:

1. Full name**, including legal name or preferred name**;
2. Social Security Number;
3. Driver's License or other State Identification Number;
4. Passport Number;
5. Biometric information including physiological, biological, or behavioral characteristics, including an individual's DNA, that can be used alone or in combination with other identifying data to establish an individual's identity;
6. Geolocation Data;

7. Internet or network activity, including browsing history, search history, and information regarding an identifiable individual's interaction with an internet website, application, or advertisement;

8. Financial account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account; and

9. Identifiable health information, including disability status, related to the past, present, or future physical or mental health or condition of an individual.