Implementing Procedures for the Information Security Policy to Report Regulated Information to Compliance and Privacy Office

I. Introduction and Purpose

The Information Security Policy requires schools and divisions to report to the Compliance and Privacy Office if they have the following types of Regulated information:

- Government-issued identification numbers, including social security numbers, driver's license numbers, and passport numbers;
- Financial account numbers, including credit card numbers and bank account; and
- Personal health or medical information.

Regulated information is information that is protected by local, national, or international statute or regulation mandating certain restrictions.

These procedures provide guidance to schools and divisions to report Regulated information in accordance with the Information Security Policy by identifying Regulated information by conducting an inventory and determining who should have access to it, how access is provided, how this information is being stored, and how the information is disposed of in accordance with the Records Management Policy and the retention periods established in the Records Management Policy Implementing Procedures.

Schools and divisions are responsible for reviewing and determining the kinds of non-public information in their custody.

II. Inventory and Reporting Process

To determine if a school or division has Regulated information, it should conduct an inventory to review and classify the non-public information it has in its custody. The inventory process begins with a meeting with a member of the staff of the Compliance and Privacy Office to discuss and answer the inventory questions outlined at the end of these procedures.

Subsequently, the Compliance and Privacy Office will review the responses to the inventory questions. If the school or division has Regulated information that is not maintained in accordance with Information Security Policy and other applicable policies, the Compliance and Privacy Office will advise

the school or division of the steps necessary to maintain its Regulated information to meet such requirements.

If a school or division official has questions on how specific information should be classified or on the inventory process, they should contact the Compliance and Privacy Office (202-994-3386 or comply@gwu.edu).

III. Annual Review

Schools and divisions must review the inventory questions on an annual basis to determine if there have been any material changes (for example, changes to whom may have access to information or what information is in its custody).

Schools and divisions must inform the Compliance and Privacy Office if there are interim changes **within 30 days of such changes**.

Inventory Questions

1. **Please identify individuals in your school of division who can address any follow-up questions.**

   Please provide your name, phone number, and e-mail address for yourself and for a secondary point of contact for any future inquiries regarding Regulated information.

2. **Please describe the Regulated information in the custody of your school or division.**

   Please provide a detailed description of any the information in your custody that fits within the following categories:

   - Government-issued identification numbers, including social security numbers, driver's license numbers, and passport numbers;
   - Financial account numbers, including credit card numbers and bank account; and
   - Personal health or medical information.

3. **Please describe the business need for retaining this Regulated information.**

   Please indicate the specific requirement and duration this information is needed (e.g., mission critical for a certain duration with specific requirements outlined).

4. Who currently has access to this Regulated information and/or who needs to access this Regulated information?

Is this information shared internally? If so, with who is it shared? Is this data shared externally? If so, with who is it shared?

5. How is this Regulated information shared and stored?

Please describe the manner in which the Regulated information (identified in question 2) is shared and stored (e.g., paper, email, network drive, third party service).

Please describe any safeguards in place to ensure the information is protected when the employment of staff terminates, data sharing agreements terminate or expire, or contracts with third parties terminate or expire.

6. What is the process for disposing of any Regulated information?

Please describe the procedures that are currently in place to destroy information upon expiration of its established retention period(s) in accordance with the Records Management Policy and the Records Management Policy Implementing Procedures.