Summary of Changes to Data Governance Policies

**EP 2.214, Security and Protection of Sensitive Information**

1. **Policy name change**
   - OLD: Security and Protection of Sensitive Information
   - NEW: Institutional Data Classification Categories and Technical Guidelines
2. **Philosophy** – removed since it exists in EP2.215, Institutional Data Governance
3. **Data classification categories** – expanded from two to four categories
   - Public – Institutional Data where access is not restricted and is subject to open records requests.
   - Restricted (new) – Institutional Data used for UH business only. Includes student contact information and UH ID numbers. Restricted data will not be distributed to external parties except under the terms of a written memorandum of agreement or contract.
   - Sensitive – Institutional Data subject to privacy or security considerations or any Institutional Data not designated as public, restricted, or regulated. Examples of sensitive data include the contents of a student’s record.
   - Regulated (new) – Institutional Data where inadvertent disclosure or inappropriate access requires a breach notification in accordance with HRS §487N or is subject to financial fines. Social Security Number (SSN) and personal financial information fall within this category.
4. **Roles and responsibilities** – removed since it exists in EP2.215, Institutional Data Governance
5. **Access** – removed; to be addressed in a separate policy at a later date
6. **Technical guidelines around use and storage** – to be revised and included as an ITS link
7. **Breaches** – removed; will become a new admin procedure
8. **Data security related measures** – retained in the policy
   - Data ITS authority to enforce technical measures to ensure data is protected, including requiring server registrations
   - ITS authority to require departments/units/programs to report on the data they manage
   - FTC Red Flags Identity Theft Prevention Program
9. **Personnel related actions** (terminations, violations, background checks) – retained in the policy
10. **Guidelines for reporting and dissemination of protected data** (e.g., recommended small cell size) – new addition as a link to the data governance website
1. A new principle on minimal access was added; an existing principle was moved to best practices

2. Addition of more best practices – minimal access, need to know, mandatory training and education (a new administrative procedure), student surveys, remote access

3. Addition of Student Data Oversight Committee (SDOC)

4. Reiteration of data security measures in EP2.214 added under the Chief Information Security Officer’s roles and responsibilities

5. Expansion of data users description to include mandatory training and education requirements when dealing with protected data

DGO: 3/22/17