| | | |
|---|---|---|
| Standard: GP0007.01 | Category: General Provisions | Version Date: 09/02/2009 |
| Title **Obtaining Approval of Policies and Standards** | | Effective Date: 10/15/2007 |
| Originating Unit: Security Program for the Information and Computing Environment | | Last Review: 06/23/2009 |
| Reviewer: HSC Chief, Information Security | | Next Review: 06/23/2012 |

## Purpose:

The purpose of this standard is to identify stakeholders (by role), vetting and approval requirements for SPICE Policies and Standards.

## Reference(s):

1. Policy GP0007: SPICE Policy and Standard Authority

## Standard:

1. The general steps for making SPICE policies and standards are:
   a. Propose – suggest content for SPICE policy and standard to the HSC Security Office
   b. Develop – research and write draft policy and standard statements in SPICE policy and standard format.
   c. Comment – read and provide feedback which will be taken into consideration prior to final policy or standard draft.
   d. Recommend – read and provide required changes that must be included prior to recommending for approval. Comments may also be provided.
   e. Approve – Allow draft policy and standard statements to be committed to HSC policy and standard applicable to all Units of the HSC.
   f. Inform – communicate the approved policy or standard to those affected.
2. Propose - Any faculty, staff member or student may propose a SPICE policy or standard. Proposals can be submitted *via* email to security@health.ufl.edu and should contain the following information:
   a. Category (General Provision, Physical Security, Technical Security, Incident Response, Contingency Planning), or suggested new category.
   b. Title of the policy or standard to change or suggested new title.
   c. Purpose of the suggested policy or standard statement.
   d. Policy or standard statement(s) or description of what the submitter would like to see as policy or standard.
   e. Contact information of submitter.
3. Develop - The UF HSC Security Office triages HSC SPICE policy and standard proposals and determines the viability of the proposal for the HSC. The UF HSC Security Office or a SPICE Council appointed task force will research and draft

policies or standards from viable proposals. College or Unit-specific information security policy is developed and proposed by the Unit ISA and ISM.

4. Comment, Recommend and Approve - The table below depicts the stakeholders and their responsibility for SPICE policy and standard making in the HSC.

| | MATERIALITY | | | | |
|---|---|---|---|---|---|
| **Stakeholder Group** | A. Funding impact across HSC | B. Change impacts users across HSC | C. Funding or change impact to specific operations across HSC * | D. College or Unit-specific change impact ** | E. Definitions, usability, structure, corrections of HSC SPICE |
| 1. SVPHA | Approve | Approve | Approve | | |
| 2. HSC Deans & Institute Directors | Recommend | Recommend | | | |
| 3. Affected Dean, Director & Dept Chair | | | Recommend | Approve | |
| 4. ISAC or relevant ISAC sub-committee | Recommend (Technology related) | Recommend (Technology related) | Recommend (Technology related) | | |
| 5. SPICE Council | Determine Materiality, Recommend | Determine Materiality, Recommend | Determine Materiality, Recommend | Determine Materiality | Comment |
| 6. ISAs/ISMs | Comment | Comment | Comment | Develop | |
| 7. HSC Security Office or SPICE Council appointed task force. | Develop | Develop | Develop | Comment (for purposes of identifying conflict with SPICE Policy) | Develop, Approve |

* For example, credit card handling policy affects specific operations in the HSC and a small population of people, but nearly every College generates revenue via credit cards. In this case, a credit card handling policy would target the specific credit card handling operations in an HSC College, Center, Institute or Affiliate.

** Colleges and Units may augment the SPICE body of information security policy whenever SPICE policies are not restrictive enough. However, added restrictions should be considered College or Unit information security policy and not SPICE program policy. SPICE program information security policy applies to all Colleges, Centers, Institutes and Affiliates in the HSC and must be approved by the SVPHA.

5. The SPICE Council determines the materiality of draft HSC SPICE and Unit-specific information security policy or standard.

6. The HSC Security Office, with consultation from SPICE Council, determines the communication plan for the approved HSC SPICE policy or standard. Any

stakeholder group may be requested to participate in the communication plan in order to effectively reach the affected HSC faculty, staff and students.

7. Approved HSC SPICE policies and standards will be accessible from the HSC SPICE web site (https://security.health.ufl.edu/).