Report from the Faculty Senate HOP Committee
Comments on HOP 8.14 to 8.18 regarding information security.
Feb 13, 2014

The Senate HOP committee met on Feb 5, 2014 and discussed each policy in detail and has a number of general concerns regarding the policies. We recommend that the Senate HOP committee continues to work with Jesse Zapata and Ken Pierce to address these concerns before the policy is returned to the University HOP committee for a vote to send to Legal Affairs. The Senate HOP Committee does not support the policies as they are currently written.

Our concerns are as follows:

The language in the policies needs to be reworked to increase clarity so that the language is understandable to a wide range of users. The current language appears to be largely extracted from UTS165. For example, 8.14, p. 3, Definitions: "Information Owner- The manager or agent responsible for the business function that is supported by the information resource or the individual upon whom responsibility rests for carrying out the program that uses the resources."

Concepts such as "data", "information resources", etc. are so broadly defined theoughout all of the policies that it is difficult to determine what information and personnel the policies are targeting. For example the term "data", as defined in 8.14, would appear to apply to all information (see below). Definitional precision is of particular concern with respect to research related information. Clearly some data requires different levels of protection than other research data. We advise that the three types of data be carefully defined and that the policies be crafted around those data types. Note that "Confidential Data" is not defined, except as that exempt from disclosure; what data is exempt from disclosure? Also Restricted Use Data is not defined. (see 8.14, p. 2, VII, B. Protected Data).

> **Data -** Recorded data, regardless of form or media in which it may be recorded, which constitute the original data necessary to support the business of UT System or original observations and methods of a study and the analyses of such original data that are necessary to support Research activities and validate Research findings. Data may include but is not limited to: printed records, observations and notes; electronic data; video and audio records, photographs and negatives, etc. There are three types of data that require special consideration:
>
> A. **Confidential Data:** Data that is exempt from disclosure under the provisions of the Texas Public Information Act or other applicable state and federal laws.
> B. **Protected Data:** Data, such as Confidential or Restricted Use Data, which must be protected by a higher level of security.
> C. **Sensitive Data:** Digital Data maintained by an Entity that requires higher than normal security measures to protect it from unauthorized access, modification or deletion. Sensitive Data may be either public or confidential and is defined by each Entity based on compliance with applicable federal or state law or on the demonstrated need to (a) document the integrity of that Digital Data (i.e., that the Data had not been altered by either intent or accident), (b) restrict and document

individuals with access to that Digital Data, and (c) ensure appropriate backup and retention of that Digital Data.

Also ensure that all definitions are exactly the same among the policies, currently some policies use somewhat different wording than other policies.

8.18. Clarify who is in a Position of Special Trust. The way it is currently written it is not clear.

8.16 appears to be particularly burdensome and difficult to implement. For example, "Risk assessments, strategy reports, and information security administrators" are not sufficiently defined so that they can be applied. Guidance needs to be provided regarding scope, application, and frequencies of activities such as risk assessments and strategy reports. This policy needs substantial reconsideration with clear definitions while giving careful concern for the costs and challenges of operationalizing the policy.

Consideration needs to be given to the burdens of operationalizing all of these polices.