

Security Committee – Policy Review Impact Statement, Commentary, and Concerns

Purpose: This document serves the purpose of noting points of discussion regarding our review of policy proposals as they make their way before the SECCOMM Committee. Often comments and concerns are included as revisions to the actual policy as it makes its way towards final approval. In many cases, concerns related to a policy initiative cannot directly be addressed in the policy language itself but still merit recognition by others reviewing the policy at different approval and review levels. In some cases, the comments are merely a recognition that guidelines and protocols need to be established at lower levels in the organization so that the policy can have a legitimate chance of functioning in a beneficial manner for the betterment of the institution. Comments are organized by section and categorized as needed.

Policy: UGA PRIVACY POLICY

No.	Section	Comment	Response
1	2.0	Will there be a method for tracking 'authorized access' and disabling or removing such access when a person's employment is terminated or if they are removed from having such privileges? Ideally this would be tied to an account such as MyID, but there needs to be an exit protocol as well. Especially since MyIDs tend to stay active long after an employee is gone (Ex: Retired employees).	Need to establish a Best Practice statement related to De-Provisioning accounts. ID Management initiative may address some of these operational concerns.
2	2.0	Is there going to be a notification procedure for when personal information is divulged to entities not approved by the owner of the information? (Ex: court order requests the information; will the individual be notified?)	This is outside of the scope of the privacy policy.
3	2.0	How will we or what need is there to assure that we have documented who or what roles have authorization or access to private information?	This is a recognized 'blind spot'. Dealt with in procedurally different ways across campus organizations. It is said that the Main Frame is solid in management of this concern but other distributed or non frame systems vary greatly in addressing it. Can we address through education or role based security model?
4	2.0	What record of authorization will be required to prove an individual has granted proxy authority to someone other than themselves to receive private information?	These types of records should be maintained in accordance with the specific applicable regulatory requirement in question whether FERPA, HIPPA, or other.
5	2.0	What obligation are we under to communicate to an individual that a request by an official entity has been made or granted by an outside entity or representative?	This is outside of the scope of the privacy policy.

Security Committee – Policy Review Impact Statement, Commentary, and Concerns

6	4.0	Section should mention that communications need to be secured/encrypted. I wouldn't recommend assuming that it's understood from the previous sub-section.	We need to create best practice and a statement of minimum standards to reinforce secure/encrypted communications as an aspirant operational posture at both the unit and institutional levels.
7	4.0	Where can we point faculty, staff, and students to view the pertinent state regulations and can a summary be provided to ensure at least a minimum understanding of their obligations under the law?	Caroline Killens is the person responsible (Librarian III – Head of Acquisitions and Serial Services) for Retention Management questions. The references section will contain an indication of where to find this information and will note whether it is legal code oriented with the code identifier or whether it is simply a best practice that we wish to strive towards.
8	4.0	Do we have a list of systems that require the use of SSN in part or whole within UGA where interaction with that system is not through an encrypted mechanism?	We do not have this information but we aspire to understand the existence more fully over time.
9	5.0	How should violations be communicated to administration by unit management?	
10	5.1	<p>“This responsibility includes providing training and control systems for the responsible use of personal information that is accessible to its employees.” (2nd Paragraph)</p> <p>I'm very concerned that this sub-section only mentions the roles & responsibilities of Departments and/or units. It makes no mention of the enforcement body's (CIO/CISO)'s responsibilities. Current wording has the Departments developing and maintaining all of the training. Keep in mind that this policy is campus-level, not just at department-level. Since that's the case, the CISO/CIO should provide at least the framework of information for such training or training for campus-level systems and services.</p>	This point of concern is noted. This is explicitly listed as a responsibility of the CISO and CIO. The framework for achieving this is organized under security awareness and control systems training.

Security Committee – Policy Review Impact Statement, Commentary, and Concerns

11		<p><u>“...The University encourages all individuals to exercise caution in making available their own personal information to others. In particular, individuals should not give others access to their identification cards, passwords or personal identification number (PIN).” (2nd Paragraph)</u></p> <p>The underlined portion has little or no value to this section. It’s merely a blanket statement about how to approach the general storage and use of information. It may be better suited in a summary or overview section. Perhaps this should be a statement in the actual training.</p>	This is recognized but group felt it was OK to leave statement in the policy.
12	6.0	There is no mention of actual metrics (‘Measurement’) of the review process. In the vetted policy template, this section is broken into 6.1 – Review procedures, and 6.2 – Metrics explaining how to gauge the effectiveness and use of the policy.	This is a good question. We have no specific solutions to address it at present but we aspire to have a central metric tracking and reporting mechanism.
13	6.0	The Office of the CISO should make available statistics regarding the number and types of reported violations and subsequent actions taken to unit management in a manner that does not disclose the parties involved.	EITS will evaluate how to make this happen in practice.
14	GEN	<ul style="list-style-type: none"> - There should be direction to the enforcement procedure if it will not be spelled out directly in this document. - Framework for training. - How are violations reported, at a department-level? Is there a procedure? 	