THE UNIVERSITY OF UTAH®

Title: Sanctions Matrix Guidelines
Number: G4-004S
Responsible Office: Information Security and Privacy Office (ISPO)
Last Revision: January 2011
Owner: Director, ISPO. 801-587-9241 it_policy@utah.edu

I. OVERVIEW

A. This guideline is meant to provide procedures, standards, and other guidance for the implementation of University Policy 4-004: The University of Utah Information Security Policy – Section S: Sanctions and Violations.

II. GUIDELINES

A. In an effort to assign a more appropriate severity of sanction to the level of severity of a violation, the Information Security and Privacy Office has developed this 3-tiered system of sanctions. This was accomplished after much research and consideration of models of sanction from other academic institutions. The model presented here does not mandate a particular penalty; rather, it allows the supervisor and Human Resource specialist for Staff and Non-Faculty Academic Employees (or cognizant authority for Faculty or Students) to choose from an appropriate menu of options.

B. The Information Security and Privacy Office has submitted the matrix to leadership as recommended tiered guidance for imposing sanctions for confirmed privacy and security violations.

C. The guidance should be not be used as a hard and fast rule, it merely provides some structure for case-by-case decision makers to work with as the totality of circumstances must be considered, and decisions must be made within the framework of all applicable University Regulations (including the Student Code 6-400 for actions involving students, and the Faculty Code 6-316 for actions involving Faculty).

Potential Actions in Response to Privacy & Security Violations by University Employees (including Faculty, Staff, & Non-Faculty Academic Employees (all as defined in Policy 5-001)), and Volunteers			
Level of Violation	**Cause or Motivation / Type of Violation**	**Examples of Violations**	**Potential Actions (One or more)**
<u>Level I</u> Errors in handling restricted or sensitive information or in maintaining security measures	• Unintentional • Lack of training • Inexperience • Poor judgment • Poor process • Clerical Error • Process Error • Technical Error • Judgment Error	• Leaving an active computer screen with access to PHI/PII unattended • Leaving PHI/PII, in any format, unattended in public areas. • Disclosing PHI/PII without identity verification • Discussing PHI/PII in public or other inappropriate areas • Sending PHI/PII to wrong postal, FAX, or e-mail address • Failure to address vulnerability scans. • Failure to implement security best practices as defined by policy, procedures, and guidelines.	**For all categories of Employees:** • Letter of expectations, including provisions for mitigation, if appropriate • Inclusion of expectations/mitigation steps on performance evaluation • Repeat of Privacy & Security Training • Discussion of policy and procedures • Verbal warning or oral reprimand • New Confidentiality Agreement signed • Repeat of IT Security Training
<u>Level II</u> Breach in the terms of the Confidentiality Agreement and/or University policies concerning use and disclosure of restricted or sensitive information or in maintaining security measures.	• Intentional, but non-malicious • Curiosity • Concern • Compassion • Carelessness • Compulsiveness • Unauthorized • Non-job related • Stealth	• Failure to properly dispose of paper and electronic media appropriately. • Failure to implement appropriate safeguards for electronic PHI/PII. • Failure to complete required Security and Privacy Training and/or to sign appropriate Confidentiality Agreements • Accessing the record of any person, including co-workers, friends, or family, without a professional need-to-know • Using someone else's computer account • Installing unauthorized software with potential to harm systems • Adding, deleting, or altering electronic information without authorization • Failure to report a security or privacy violation • Failure to establish a Business Associate Agreement • Failure to follow Special Restriction for Out-of-Pocket Payment for Services • Repeated Level I violations	**For Staff & Non-Faculty Academic Employees** • Final written warning, requiring written corrective action plan in response; ineligible for transfer or promotion for up to 12 months • Suspension of information system user privileges • Suspension of employment • Suspension of research projects • Inability to participate in Research for up to 12 months. **For Faculty:** • Referral to Cognizant Senior Vice President for review of violation of Faculty Code;
<u>Level III</u> Breach in the terms of the Confidentiality Agreement and/or University Policies concerning use and disclosure of restricted or sensitive information, for personal gain or to affect harm on another person.	• Malicious intent • Financial gain • Revenge • Protest • Gross Negligence • Theft, including identity theft • Malicious actions: i.e., alteration or deletion of data; making systems inaccessible	• Access and unauthorized disclosure of PHI/PII for personal gain or to affect harm on another person • Unauthorized access of celebrity or VIP PHI/PII for any reason • Malicious alteration, deletion or removal of PHI/PII, from University facilities • Unauthorized publication or broadcasting of PHI/PII • A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline • Repeated Level I or II Violations	**For Staff & Non-Faculty Academic Employees** • Suspension of employment; • Suspension of Research Projects; • Termination of information system user privileges; • Revocation of Medical Staff privileges; • Termination of employment; ineligible for rehire and future information systems access. **For Faculty:** • Referral to Sr VP as violation of Faculty Code.

Potential Actions in Response to Privacy & Security Violations by Students			
Level of Violation	**Cause or Motivation / Type of Violation**	**Examples of Violations**	**Recommended Actions (One or more) (and see Student Code—University Policy 6-400 for further guidance)**
<u>Level I</u> Errors in handling restricted or sensitive information or in maintaining security measures.	• Unintentional • Lack of training • Inexperience • Poor judgment • Poor process • Clerical Error • Process Error • Technical Error • Judgment Error	• Leaving an active computer screen with access to PHI/PII unattended • Leaving PHI/PII, in any format, unattended in public areas. • Disclosing PHI/PII without identity verification • Discussing PHI/PII in public or other inappropriate areas • DMCA violations • Sending PHI/PII to wrong postal, FAX, or e-mail address	• Letter of expectations, including provisions for mitigation, if appropriate; • Retraining and reevaluation; • Specialized training and evaluation; • Discussion of policy and procedures; • New Confidentiality Agreement signed; • Community Service, as appropriate;
<u>Level II</u> Breach in the terms of the Confidentiality Agreement and/or University policies concerning use and disclosure of restricted or sensitive information or in maintaining security measures.	• Intentional, but non-malicious • Curiosity • Concern • Compassion • Carelessness • Compulsiveness • Unauthorized • Non-job related • Stealth	• Placing non-shredded documents in inappropriate waste receptacles; • Failure to complete required Security and Privacy Training and/or to sign appropriate Confidentiality Agreements; • Accessing the record of any person, including co-workers, friends, or family, without an authorized need-to-know; • Using someone else's computer account; • Installing unauthorized software with potential to harm systems; • Adding, deleting, or altering electronic information without authorization; • Failure to report a security or privacy violation; • Repeated Level I violations;	• Letter of reprimand, requiring written corrective action plan & acknowledgement of consequences of subsequent infractions; i.e., expulsion, and obligation to make restitution, as appropriate; • Temporary loss of University privileges, including use of University library, parking, computers, and athletic/entertainment functions; • Conduct suspension; • Contract of restitution
<u>Level III</u> Breach in the terms of the Confidentiality Agreement and/or University Policies concerning use and disclosure of restricted or sensitive information, for personal gain or to affect harm on another person.	• Malicious intent • Financial gain • Revenge • Protest • Gross Negligence • Theft, including identity theft • Malicious actions: i.e., alteration or deletion of data; making systems inaccessible	• Access and unauthorized disclosure of PHI/PII for personal gain or to affect harm on another person; • Unauthorized access of celebrity or VIP PHI/PII for any reason; • Malicious alteration, deletion or removal of PHI/PII, from University facilities; • Unauthorized publication or broadcasting of PHI/PII; • A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline; • Repeated Level I or II Violations.	• Expulsion without opportunity to continue at the University of Utah in any status, and ineligible for University privileges, including use of University library, parking, and entertainment/athletic functions; • Contract of Restitution.