V.K. INFORMATION SYSTEMS SECURITY INCIDENT RESPONSE POLICY

(Source: Vice President for Information Systems and Computing and Associate Vice President for Audit, Compliance and Privacy, Almanac, January 16, 2007 *(*https://almanac.upenn.edu/archive/volumes/v53/n18/or.html*))*

This policy defines the steps that personnel must use to ensure that security incidents are identified, contained, investigated and remedied. It also provides a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. Finally, it establishes responsibility and accountability for all steps in the process of addressing computer security incidents.

Without an effective incident response process, corrective action may be delayed and harmful effects unnecessarily exacerbated. Further, proper communication allows the University key learning opportunities to improve the security of data and networks. Individuals who fail to comply are subject to sanctions as appropriate under University policies.

This policy applies to all users. It applies to any computing devices owned or leased by the University of Pennsylvania that experience a Computer Security Incident. It also applies to any computing device regardless of ownership, which either is used to store Confidential University Data, or which, if lost, stolen, or compromised, and based on its privileged access, could lead to the unauthorized disclosure of Confidential University Data. Examples of systems in scope include, but are not limited to, a User's personally owned home computer that is used to store Confidential University Data, or that contains passwords that would give access to Confidential University Data.

This policy does not cover incidents involving the University of Pennsylvania Health System (UPHS) information systems, which has a separate incident response policy. ISC Information Security will coordinate with UPHS as appropriate when UPHS computing devices, data, or personnel are involved.

For information on identifying and reporting computer security incidents, the process for handling incidents and documentation, a list of best practices, compliance, and related University policies see: www.upenn.edu/almanac/volumes/v53/n18/or.html (http://www.upenn.edu/almanac/volumes/v53/n18/or.html).