New and Revised Information Security Guidance and Framework Realignment

To: Deans, Directors, and Department Heads
From: Teresa E. Banks, Information Security Office
Date: November 13, 2012
Subject: New and Revised Information Security Guidance and Framework Realignment

The Information Security Office has been working with campus stakeholders to update several of our standards and guidelines so that they include appropriate HIPAA Security Rule requirements, as well as other compliance program requirements. These documents have been vetted by stakeholders, and approved by the Information Security Advisory Committee.

The revised documents are:

1. **Information Security Terms Guideline (IS-G100)** [1]: Revised to include additional terms for compliance programs
2. **Data Facility Physical Security Standard (IS-S501)** [2]: Revised to include requirement for data facility repairs and modifications must be documented, and that plans must be kept up to date.
3. **Server Security Standard (IS-S603)** [3]: Revised to include requirements for audit logs, access reports and incident tracking reports, and review of these documents on a regular basis, as indicated in the Information System Activity Review Guideline (IS-G603 â€" new guideline).

The new documents are:

1. **Compliance Program Documentation Standard (IS-S101)** [4]: Created to provide guidance on documentation requirements for units that have legal, regulatory, or contractual obligations related to any compliance program.
2. **Compliance Program Documentation Guideline (IS-G101)** [5]: Accompanying guideline to the above standard for specific compliance program documentation requirements.
3. **Information System Activity Review Guideline (IS-G603)** [6]: Guideline that accompanies Server Security Standard (IS-S603). This document provides guidelines for ensuring the regular review of information system activity, such as audit logs, access reports, and security incident tracking reports. This guideline is especially critical for all units, especially those that interact with Confidential University Data or data covered by regulatory or contractual requirements.

As well, we have worked to realign our standards, procedures and guidelines so that they better align with the ISO 27001 compliance standard that comprises best practices in information security. The remaining documents have not been changed, other than being renumbered to reflect the realignment. The old numbers have been included as a reference point.

We will be working with our campus stakeholders in the next few months in order to provide further documentation updates, and will announce the changes after they are thoroughly vetted and then approved.

If you have any questions, please contact the Information Security Office at 621-UISO (8476).

Source URL:https://uaatwork.arizona.edu/uannounce/new-and-revised-information-security-guidance-and-framework-realignment

Links
[1] http://security.arizona.edu/isg100 [2] http://security.arizona.edu/iss501 [3] http://security.arizona.edu/iss603 [4] http://security.arizona.edu/iss101 [5] http://security.arizona.edu/isg101 [6] http://security.arizona.edu/isg603