Scope
This guideline applies to all University of Arizona units that have a legal, regulatory or contractual obligation related to any compliance program, i.e., Export Control, FERPA, FISMA, HIPAA, PCI DSS or any compliance area.

As stated in the Compliance Program Documentation Requirements Standard (IS-S101), units that are part of compliance programs shall maintain documentation, written or electronic, on implemented policies and procedures regarding compliance with the contractual or regulatory information security obligations. Additionally, if an action, activity or assessment is required, this also shall be documented and maintained. Units shall retain the documentation according to specific compliance requirements from the date of creation or the date when last in effect, whichever is later.

Following are the most common documentation requirements for units that must comply with certain regulatory and contractual compliance programs.

- Export Control Requirements
- FERPA Requirements
- FISMA Requirements
- HIPAA Regulatory Requirements
- PCI DSS Reporting Requirements

Export Control Requirements
If a project is export controlled, all export controlled project information, technical data or equipment must be protected from access by unauthorized foreign persons. Only those foreign national employees who have been authorized by a Department of State or Department of Commerce license or license exemption can have access to export controlled project information and equipment if required. A Technology Control Plan (TCP) must be in place to secure the project information, data, and equipment from unauthorized access prior to the start of the export-controlled project. The TCP template can be found on the Export Control Compliance website and must be approved by the University’s Export Controls Officer. Licenses and license exemptions must to be kept for five (5) years after the expiration of the license.

Family Educational Rights and Privacy Act of 1974 (FERPA) Requirements
The Office of the Registrar serves as the compliance office for FERPA for the University of Arizona. In compliance with this Act, the Office of the Registrar will provide such reporting and compliance data as the Federal Government may require. It also serves as the official records office for this Act and for forwarding complaints directly to the Department of Education, if necessary.
**Federal Information Security Management Act (FISMA) Requirements**
The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. As part of research and patient care the University’s has contracts with federal agencies that require compliance with this Act. Units that have such contracts must complete detailed documentation and assessments on IT resources used as part of the program that falls under FISMA compliance.

**HIPAA Regulatory Requirements**
REFERENCE: 45 CFR 164.316(b); 164.316(b)(i); 164.316(b)(ii); 164.316(b)(iii)
Units with HIPAA obligations must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule, and must periodically review and update documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI).
Units with HIPAA obligations must retain documentation required in 164.316(b)(i); of the HIPAA Security Rule for six (6) years from the date of creation or the date when they last were in effect, whichever is later. Documentation must be available to those persons responsible for implementing the procedures to which the documentation pertains.

**Payment Card Industry Data Security Standard (PCI DSS) Reporting Requirements**
The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Merchants processing credit cards are required to complete and pass an annual Self-Assessment Questionnaire (SAQ) self-validating PCI DSS compliance. There are different SAQ versions, each intended to address different modes/procedures/systems dependent on how the merchant stores, processes or transmits cardholder data.

In addition, annually, each merchant must also complete a Report on Compliance (ROC) documenting all areas on Report that are applicable to the merchant business method of processing credit cards. The ROC is part of the PCI-DSS standard, and must include the following elements:
1. Executive Summary: Description of entity’s business and high-level network diagram (either obtained from the entity or created by assessor) of the entity’s networking topography that includes:
   a) Connections into and out of the network
   b) Critical components within the cardholder data environment, including POS devices, systems, databases, and web servers, as applicable
   c) Other necessary payment components, as applicable
2. Description of Scope of Work and Approach Taken
3. Details about Reviewed Environment
4. Contact Information and Report Date
5. Quarterly Scan Results
6. Findings and Observations
7. Revalidation of Open Items
8. Completion Steps
The ROC and Attestation of Compliance must be completed and retained with PCI-DSS department documentation. The ROC and SAQ Certification plus all supporting documentation must be made available upon request to security assessors, campus banking liaisons or acquirer representatives and internal and external auditors. Supporting documentation would include but not limited to all applicable requirements such as evidence of a passing external public facing IP scans, audit logs, department security policy, copies of third party service provider agreements, process flow charts, network system maps and any other documentation to support the ROC requirements. For those entities that outsource storage, processing, or transmission of cardholder data to third-party service providers, the ROC must document the role of each service provider, clearly identifying which requirements apply to the assessed entity and which apply to the service provider.

**Related Guidance**
- Information Security Policy (IS-100)
- Information Security Terms Guideline (IS-G100)
- Compliance Program Documentation Requirements Standard (IS-S101)
- Information Security Policy Page
- NIST FISMA Implementation Webpage
- UA Office of the Registrar FERPA Webpage
- US HHS Guide on HIPAA Documentation Requirements
- UA Office for the Responsible Conduct of Research Export Control Compliance Webpage

All italicized terms used in this standard are defined in the Information Security Terms Guideline.

**Revision History**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>9/11/12</td>
</tr>
<tr>
<td>Effective Date</td>
<td>11/1/12</td>
</tr>
</tbody>
</table>