DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Accountability for Risks Associated with Exceptions to Information Security Standards
PAGE: 1 of 3	**REPLACES POLICY DATED:** 2/15/10, 12/1/14, 8/1/15
EFFECTIVE DATE: April 1, 2016	**REFERENCE NUMBER:** IP.SEC.009 (formerly IS.SEC.009)
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities, Company business units and all Corporate Departments.

PURPOSE: To establish procedures for business owners to request an exception to Information Security Standards and to assign financial accountability for those exceptions.

Background:

The Information Protection Department maintains and publishes (on Atlas) Information Security Standards which outline the minimum technical and procedural controls required to maintain the confidentiality, integrity, and availability of Company electronic data. All Company affiliated-facilities, business units, and Corporate departments are obligated to adhere to these Standards in order to comply with state and federal regulations (*e.g.*, HIPAA) and contractual obligations (*e.g.*, Payment Card Industry standard or PCI). These standards serve to protect the Company's network from exposure to malicious persons, software, and other threats that can damage systems, data and software; impact patient safety; or cause delays to patient care.

There are circumstances in which the prudent course of business means a department, facility, or business unit cannot comply with Information Security (IS) Standards for technical reasons, cost, or other needs. In these cases, it is incumbent on the business unit to document the business decision to make an exception, develop a plan to mitigate the exception, and accept the risks associated with not meeting the Information Security requirements, including the potential financial impact.

POLICY:

1. All Company-affiliated facilities, business units, and Corporate Departments must comply with IS Standards in order to reduce the impact of threats and vulnerabilities on Company data, systems, and networks.

2. When Company business units determine compliance with IS Standards is not possible or feasible for technical reasons, cost, or other reasons prudent for business operations, a Mitigating Control Plan (MCP) must be completed. The MCP must be implemented in order to mitigate the risk associated with making an exception to the IS Standard. The Information Protection Program will work with those business owners to identify potential compensating or mitigating controls that will help reduce the potential risk. However, the facility, Company Business Unit or Corporate Department will be held financially responsible for its decision to make an exception to an IS Standard.

3. When an exception to Information Security Policies and Standards results in harm to Company data, systems or networks resulting in recovery, breach notification, or other related activities, the non-compliant business will be responsible for those costs.

DEFINITION:

Financially Responsible Executive – the individual who is authorized to make financial decisions for a specific facility, Division, or Line of Business.

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Accountability for Risks Associated with Exceptions to Information Security Standards
PAGE: 2 of 3	**REPLACES POLICY DATED:** 2/15/10, 12/1/14, 8/1/15
EFFECTIVE DATE: April 1, 2016	**REFERENCE NUMBER:** IP.SEC.009 (formerly IS.SEC.009)
APPROVED BY: Ethics and Compliance Policy Committee	

PROCEDURE:

1. The Information Protection Program and appropriate Directors of Information Security Assurance (DISAs) will work with Company departments, facilities, or business units to develop approaches to implement IS Standards, as well as consult on risk and mitigation strategies when business requirements conflict with IS Standards. Enterprise security risk must be evaluated by the Information Protection Program and the Chief Information Security Officer to develop approaches to implement IS Standards and determine appropriate mitigation strategies when business requirements conflict with IS Standards.

2. A Company affiliated business unit, facility, or department must work with their DISA to document exceptions to the IS Standards and identify mitigating controls in an MCP. This documentation must be submitted and managed within the Company-provided Governance Risk and Compliance (GRC) tool.

3. If ePHI is involved with the exception to the IS Standards, the Facility Privacy Official (FPO) must be engaged per the Privacy Official Policy (IP.PRI.002) to ensure HIPAA compliance is addressed.

4. The Chief Information Officer (CIO), IT&S VP, or delegate must review the proposed MCP, agree it is an appropriate plan, accept responsibility for the risk mitigation activities, and submit the MCP to the Information Protection Program for approval.

5. Delegated members within the Information Protection Program will endorse the MCP with signature when there is agreement that the mitigating controls are appropriate and adequate for protection.

6. The Financially Responsible Executive (*e.g.*, CFO, CEO, etc.) must sign the MCP, acknowledging he or she has made a business decision to accept financial liability when there are consequences for making an exception to the IS Standard and he or she has reviewed and approved the MCP associated with the exception.

7. The documentation of the business decision in the MCP must include relevant details about the exception to IS Standards. Examples of what should be documented include:

    a. Information Security Standards that are in question;
    b. Specific details of the business decision made;
    c. Business justification, *e.g.*, cost, technical limitations;
    d. Compensating or mitigating controls;
    e. Data/systems/networks or procedures affected;
    f. Estimated risks and potential impact to the business;
    g. Likelihood of a threat and estimated cost if a threat occurred;
    h. Name of Financially Responsible Executive who is accepting financial liability for the risk associated with the exception

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Accountability for Risks Associated with Exceptions to Information Security Standards
PAGE: 3 of 3	**REPLACES POLICY DATED:** 2/15/10, 12/1/14, 8/1/15
EFFECTIVE DATE: April 1, 2016	**REFERENCE NUMBER:** IP.SEC.009 (formerly IS.SEC.009)
APPROVED BY: Ethics and Compliance Policy Committee	

i. Timeline to complete the MCP; and
j. Expiration date of the MCP.

8. The DISA, the Information Protection Program, Facility leadership, and the appropriate business unit will work jointly to implement mitigating controls and track remediation.

9. Company-affiliated business units, facilities, and departments who fail to document their exceptions and associated mitigating controls will still be held accountable for any consequences (*e.g.* breach or network impact) caused by making an exception to the IS Standards.

10. The Senior Vice President and Chief Ethics and Compliance Officer must be consulted regarding any requests for exceptions to Information Security Policies.

REFERENCES:

1. Information Security Program Requirements Policy, IP.SEC.001
2. Information Security Roles & Responsibilities Policy, IP.SEC.006
3. AM.IC.01 – Electronic Data Classification Standard
4. HHS – CMS HIPAA Security Series "Basics of Risk Analysis and Risk Management"