

# Risk Analysis Policy

Policy #: ECP-202

Version #: 10.1

Approved By: Julie Parker, CEO

Effective Date: March 3, 2010

## Purpose:

The purpose is to conduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information held by the organization.

## Scope:

This policy applies to <<Organization Name>> in its entirety, including all facilities and systems that process sensitive information. Such risk analysis activities will be conducted at least once a year and must result in a comprehensive Risk Analysis Report that summarizes the risks, vulnerabilities to the confidentiality, integrity and availability of sensitive information. This report must also identify recommended safeguards and prioritize all such risks and vulnerabilities.

## Policy:

Risk is defined as the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence.

<<Organization Name>> will conduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information held by <<Organization Name>>.

All risk analysis activities that are to be implemented are organized into three phases. These phases are:

- Phase I: Documentation Phase
- Phase II: Risk Assessment Phase
- Phase III: Safeguards Determination Phase

The activities that <<Organization Name>> will conduct in each phase are as follows:

### **Phase I: Documentation Phase**

- Identify systems with sensitive information
- Document the purpose of these systems
- Document the flow of sensitive information

### **Phase II: Risk Assessment Phase**

- Identify vulnerabilities and threats to sensitive information
- Describe the risks
- Identify controls
- Describe the level of risk

### **Phase III: Safeguards Determination Phase**

- Recommend safeguards for sensitive information
- Determine residual risk to sensitive information

The results of all identified risk analysis activities along with the safeguard and other recommendations must be summarized with supporting documentation in a Risk Analysis Report.

Responsibilities:

The Security Officer is responsible for coordinating all activities associated with risk analysis. All involved employees who assist with risk analysis activities will be trained in appropriate security compliance requirements and <<Organization Name>>'s security policies with the objective that they understand their responsibilities and duties to reduce the risk of security violations.

Compliance:

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Procedure(s): None

Form(s):

Forms related to the risk analysis policy include:

- Risk Assessment Survey

References:

- International Standards Organization (ISO 27002).
- HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services: <http://www.cms.hhs.gov/securitystandard/downloads/securityfinalrule.pdf> February 20, 2003
- American Reinvestment and Recovery Act of 2009 (ARRA)/ (HITECH) [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111\\_cong\\_bills&docid=f:h1enr.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf)  
*(The HITECH Act begins at H.R. 1-112 through 1-165 (pp. 112 through 165 in the document). The security and privacy provisions are found at Subtitle D Privacy, beginning H.R. 1-144 (p. 144))*

Contact:

John Doe, Security Officer  
1234 Anystreet  
Anywhere, IL 55555

E: John.doe@anywhere.com

P: 555.555.5555

F: 777.777.7777

Policy History: Initial effective date: March 3, 2010