Logo Placeholder

TITLE **Risk Management & Risk Treatment**	POLICY APPLIES TO Entire Organization	REVISION DATE
POLICY # 101	POLICY REFERENCE	EFFECTIVE DATE
AREA	BOARD APPROVAL DATE	LAST REVIEWED DATE
ORIGINATOR	AUTHORIZED BY:	

Purpose:

This policy is established to formally acknowledge our commitment to risk management. Through this policy, we aim to achieve the following objectives:

- ensure all possible efforts to manage risk within the organization and minimize risk-associated adversity
- identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- maximize potential opportunities in organizational activities.

Scope:

The policy applies to all processes and activities involved in normal operations of [Organization Name]. All employees of [Organization Name] are liable to identify, analyze, assess, monitor, control and communicate risks linked to any activity or process within the scope of their authority and responsibility.

Policy:

[Organization Name] holds strong commitment to identify and manage risks which may arise during the provision of services and the overall organizational management.

To ensure this, we shall carry out the following action plan:

1. Assessing Security Risks

At a minimum, risk assessment shall consider risks in each relevant area of our operations. The term “risk assessment” has no single definition as it widely differs in terms of methodology and scope. The core aim, however, is the same: to assess risk associated with information assets of the organization.

According to a definition by NIST Risk Management Guide, risk assessment is ‘‘the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.’’

Security Risk Assessment shall be the first step of our risk management process. It will allow us to

analyze present security controls being operated on organizational assets and to determine the probability of occurrence of loss to those assets. Through our security risk assessment, we shall review our organization's threat landscape, the worth of assets, vulnerabilities in the security controls, impact of anticipated losses; and recommend any additional controls required to minimize risk to an acceptable level.

Security Risk Assessments shall serve the following purposes within [Organization Name]:

- Fulfill the requirement of various information security standards and frameworks such as ISO 17799, GLBA, HIPAA, COBIT 5, EDM03, OMB A-130, FERC, etc.
- Fulfill requirement 12.2 of PCI DSS i.e. "Implement a risk assessment process that is performed at least annually and upon significant changes to the environment that identifies critical assets, threats, and vulnerabilities, and results in a formal assessment."
- Maintain a check and balance on the present status of the security of information assets.
- Review information security program periodically to assess its effectiveness and update it according to the evolving threats such as advanced technology, skill acquisition by intruders, and promulgation of information.
- Allocate resources according to risk faced by information assets as opposed to allocation on the basis of convenience or personal interest in a skill or device.
- Measure the security posture of [Organization Name] to allow for comparison with past and anticipated future results.

To carry out the security risk assessment, [Organization Name] shall conduct the following activities:

- Review the appropriateness of current security guidelines, standards, policies and procedures
- Analyze assets, vulnerabilities and threats, along with their likelihood and impact
- Assess the physical security of our computer systems and network components
- Review and analyze network architecture, components and protocols and ensure that they are in accordance with our security policies
- Review and analyze configuration, usage and implementation of remote access systems, firewalls, servers and external network connections
- Review all authentication mechanisms
- Review agreements of products or services from our contractors and vendors
- Evaluate the effectiveness of employee security awareness training program by
    - Interviewing employees and key staff
    - Checking perimeter controls
    - Carrying social engineering experiments
    - Inspecting physical security checkpoints

Our risk assessment will conclude with list of risk to organizational assets. We shall give practical recommendations for addressing identified vulnerabilities and reducing security risk levels. The security risk assessment team shall also formally compare our security program with similar organizations to estimate how we stand in comparison to our competitors.

2. Treating Security Risks

The risks identified in the risk assessment process will now need to be mitigated. To reduce the identified risks, the security risk assessment team makes certain recommendations known as safeguards. Senior management shall make risk-based decisions to either develop and implement new security controls or improve existing ones; and to select and compile safeguards, justify their implementation, and establish

risk parameters that control the approval of recommended safeguards.
Our risk treatment shall have the following action plan:

- Distinguish the root causes of risks identified in the risk assessment process
- Select the right mix of safeguards. This will be done by determining optimal set of safeguard costs, effectiveness and acceptable residual risk. The right mix of safeguards shall be selected from the following categories:
    - People - such as competent and trustworthy individuals.
    - Processes - such as information security awareness trainings, change management, etc.
    - Technology – such as intrusion detection system, SPAM filters, multi-factor authentication, etc.
- Choose one of the options for handling risk mitigation:
    - Accept Risk – acknowledge that a particular risk exists and decide to accept it as it is
    - Avoid – eliminate the cause of risk and adjust requirements accordingly
    - Control – implement the right set of recommended safeguards to reduce or minimize risk likelihood and ensure risk optimization
    - Transfer – reallocate responsibility and authority to another stakeholder that is prepared to accept the risk

  These decisions shall me made keeping in view the potential impact and probability of the risks.
- Ascertain different risk treatment methods, tools and strategies for all major risks
- Evaluate and prioritize the methods, tools and strategies
- Select alternatives for each risk and allocate the resources
- Communicate the risk mitigation plan to all involved parties

3. Schedule of Assessments

All assessed and treated security risks shall be recorded in a risk register which will provide a complete schedule of all assessments.

The schedule of assessments shall have the following entities:

- Risk ID (A unique identification code)
- Risk Description (A brief description of the assessed risk)
- Risk Rating (Low, Moderate or High)
- Impact of Occurrence (Impact in case a potential risk turns into a real threat)
- Risk Likelihood (Probability of Occurrence)
- Existing Controls (Actual risk controls already in practice)
- Responsibilities (Who holds the responsibility of dealing with the risk)
- Risk Treatment Plan (How a particular risk will be treated)
- Residual Risk (Remaining risk after treatment)

Responsibilities:

Senior Management

The senior management shall be responsible for annually reviewing the risk management process and conducting periodic reviews of progress. They will manage operations and make strategic decisions with a risk-conscious mindset.

IT Staff

This policy applies to all IT staff responsible for managing, scheduling and remediating findings from internal and external assessments.

Managers

All line managers shall have the responsibility to ensure that risks for each of the activities under their control are identified, documented, assessed and managed. Any new risks identified as a result of change in business environment shall also be documented. Risk records shall be maintained regularly to reflect the occurrence of any changes.

All Employees

All employees shall have the responsibility to identify risks relevant to their scope of responsibility and report their line managers.

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.

[Organization Name] shall carry out risk management activities in compliance with the following frameworks:

- **ISO 27002:2007 – Section 4.1 & 4.2** (Assessing Security Risks & Treating Security Risks)
- **COBIT 5** – EDM03– Ensure Risk Optimization & DSS01 Manage Operations
- **GLBA** – Part 314 Standards for Safeguarding NPI: § 314.4 (b) Internal & External Risks to security - Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations.
- **PCI** – PCI DSS: 12.2 Annual Risk Assessment

Procedure(s):

Procedures go here (will always reference procedure documentation, will never be a part of the policy)

Form(s):

No known forms at this time

References:

- Landoll, J.D. (2005). The Security Risk Assessment Handbook. Auerbach Publications.
- Scarfone, K., et al. (2008). Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115.
- Risk Assessment Special Interest Group. (2012). PCI DSS Risk Assessment Guidelines. PCI Security Standards Council.
- ISACA. Cobit 5 for Risk: An ISACA Framework. [online] Available at: http://www.isaca.org/cobit/documents/cobit-5-for-risk-preview_res_eng_0913.pdf

Contact:

Chief Compliance Officer
1234 Mail Street
Cheyenne, WY 82001
(217) 555-6624
compliance@customer.org

Policy History:

Effective date:

Policy created:
June 1st, 2019