**Risk Management Process Policy**

**Purpose:**

This policy establishes the scope, objectives, and procedures of Trialomics, Inc information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

**Scope:**

The policy covers the administrative, physical, and technical processes that enable and govern PHI that is created, maintained, received, or transmitted by Trialomics, Inc.

**Policy:**

1. It is the policy of Trialomics, Inc to conduct thorough and timely risk assessments of potential threats to the confidentiality, integrity, and availability of PHI. This assessment will be carried out at least annually.
2. To develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the organization’s information security program.
3. Trialomics, Inc implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
   1. Ensure the confidentiality, integrity, and availability of all PHI the organization creates, receives, maintains, and/or transmits.
   2. Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.
   3. Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required.
   4. Ensure compliance by workforce.
4. All documentation of risk management efforts, including decisions made on controls to implement as well as those to not implement, are documented and maintained for six years in the Risk Analysis Result google doc and on the Risk Assessment tab in the Periodic Ledger worksheet.

**Procedures:**

1. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of Trialomics, Inc Information Security Officer.
2. The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.
   1. The probability and impact of occurrence for each identified risk will be assessed by the Trialomics Information Security Officer, with input from workforce using the following approach:
      1. Probability
         1. High – Greater than <70%> probability of occurrence
         2. Medium – Between <30%> and <70%> probability of occurrence
         3. Low – Below <30%> probability of occurrence
      2. Detectability
         1. High – Risk that is easy to detect
         2. Medium – Risk that requires specific actions to be detected
         3. Low – Risk that has is outside the sphere of influence of Trialomics or our customer
      3. Impact
         1. High – Risk that has the potential to greatly impact project cost, project schedule, or performance
         2. Medium – Risk that has the potential to slightly impact project cost, project schedule, or performance  
            Low – Risk that has relatively little impact on cost, schedule, or performance
   2. Risks that fall within the High Probability and High Impact will be deemed major and have risk response planning which may include a risk mitigation, detectability, and/or contingency plan.
3. Each risk will be assigned to the Information Security Officer for monitoring purposes to ensure that the risk will not “fall through the cracks”. If possible the monitoring will be automated and trigger alerts when appropriate.
   1. For each major risk, one of the following approaches will be selected to address it:
      1. Avoid – Eliminate the threat by eliminating the cause
      2. Mitigate – Identify ways to reduce the probability or the impact of the risk
      3. Accept – Nothing will be done
      4. Transfer – Make another party responsible for the risk (buy insurance, outsourcing, etc.)
   2. For each risk that will be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring.
4. The level of risk will be tracked, monitored, and reported throughout the project lifecycle. All project change requests will be analyzed for their possible impact to the project risks. Management will be notified of important changes to risk status as deemed necessary.