**Business Impact analysis**

Purpose:

The purpose of this policy is to define the process for conducting a business impact analysis (BIA) to identify critical business processes and prioritize their recovery in the event of a disruption.

Scope:

This policy applies to all business units and functions within the firm.

Policy:

1. Business Impact Analysis Process:
   1. The BIA process will be conducted by the team in collaboration with all business units and functions.
   2. The BIA process will include the following steps: i. Identification of critical business processes and their dependencies on IT systems. ii. Evaluation of the potential impact of disruptions to critical business processes. iii. Identification of recovery time objectives (RTOs) for critical business processes. iv. Identification of resource requirements to achieve RTOs for critical business processes. c. The BIA process will be reviewed and updated at least annually or as significant changes occur within the organization.
2. Roles and Responsibilities: a. IT team:
   1. Lead the BIA process.
      1. Identify and prioritize critical business processes.
      2. Define RTOs and resource requirements for critical business processes.
   2. Business units and functions: i. Provide input into the identification of critical business processes and their dependencies on IT systems. ii. Provide input into the evaluation of the potential impact of disruptions to critical business processes.
3. Reporting:
   1. The results of the BIA process will be documented in a report that includes:   
      i. Executive summary of the BIA process and results.   
      ii. Identification of critical business processes.   
      iii. Potential impact of disruptions to critical business processes.   
      iv. RTOs and resource requirements for critical business processes.   
      v. Summary of findings and recommendations.
   2. The BIA report will be reviewed and updated at least annually, or as significant changes occur within the organization.
4. Exceptions: a. Any exceptions to this policy must be approved by the IT Director.

Enforcement: Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or termination of contract.