INCIDENT RESPONSE POLICY

For

ACML Capital Markets Limited

Version:1.0

Document Classification: Internal

Document Control

Document Name	INCIDENT RESPONSE POLICY
Abstract	This document describes about the INCIDENT RESPONSE POLICY
Security Classification	Internal

Authorization		
Document Owner	Reviewed by	Authorized by
ACML Capital Markets Limited	Samir Shah	Vipul Patel

Amendment Log				
Version	**Modification Date DD MMM YYYY**	**Section**	**A/M/D**	**Brief description of change**
1.0	16-MAY-2024	Initial	A	Initial

1. Document Purpose

1.1. This document defines the policy for addressing Security Incidents through appropriate Incident Response.

1.2. This document applies to all Personnel and supersedes all other policies relating to thematters set forth herein.

1.3. The purpose of this document is to define the Incident Response procedures in the event of a Security Incident. This document is a step-by-step guide ofthe measures Personnel are required to take to manage the lifecycle of Security Incidents from initial Security Incident recognition to restoring normal operations. This process will ensure that all such Security Incidents are detected, analyzed, contained and eradicated, that measures are taken to prevent any further Security Incidents, and, where necessary or appropriate, that notice is provided to law enforcement authorities, Personnel, and/or affected parties.

2. Scope

The objective of this policy is to ensure a consistent and effective approach to the management of Security Incidents, including the identification and communication of Security Events and Security Weaknesses.

The Incident Response process is considered complete once Information confidentiality, integrity,and/or availability are restored to normal and verification has occurred.

3. Incident Response Policy

The Incident Response policy is as follows:

- Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to Security Incidents.

- The objectives for Security Incident management should be agreed upon with management, and it should be ensured that those responsible for Security Incident management understand the organization's priorities for handling Security Incidents.

- Security Events should be reported through appropriate management channels as quicklyas possible.

- Personnel and contractors using the organization's information systems and services arerequired to note and report any observed or suspected Security Weakness in systems orservices.

- Security Events should be assessed and it should be decided if they are to be classified as Security Incidents.

- Security Incidents should be responded to in accordance with documented Incident Response procedures.

- Knowledge gained from analyzing and resolving Security Incidents should be used to reduce the likelihood or impact of future incidents.

- Procedures should be defined and applied for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

- Awareness should be provided on topics such as:

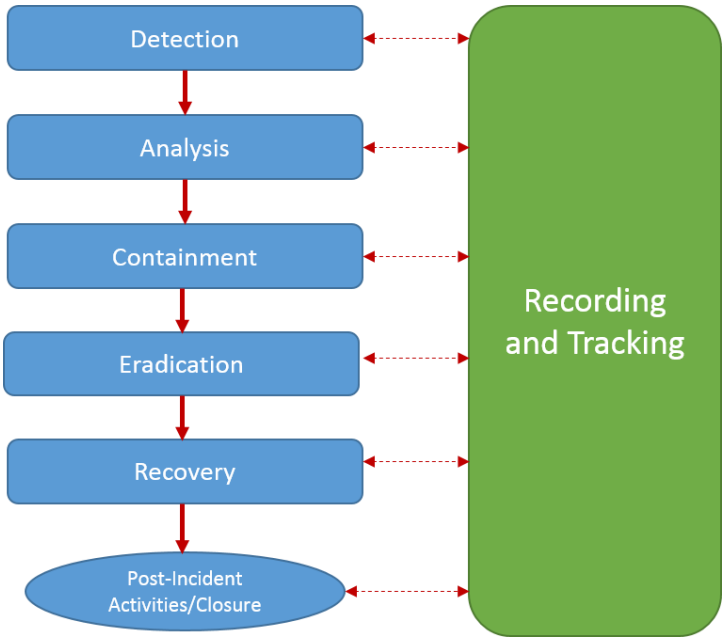
    - The benefits of a formal, consistent approach to Incident Management (personaland organizational);
    - How the program works, expectations;
    - How to report Security Incidents, who to contact;
    - Constraints imposed by non-disclosure agreements.

- Communication channels should be established well in advance of a Security Incident. Include all necessary parties in relevant communication:

    - Security Incident Response Team members
    - Senior Management

- In the event a Security Incident, Data Controllers, government bodies and other necessaryparties should be notified in a reasonable time frame, and in compliance with regulatory and other applicable requirements and guidance.

4. PROCESS


Detection
Analysis
Containment
Eradication
Recovery
Post-Incident Activities/Closure
Recording and Tracking

5. OVERVIEW

5.1. Roles and Responsibilities

Individuals needed and responsible for responding to a Security Incident make up the Security Incident Response Team.Core members will include the following:

- Director, Company
- Compliance Officer
- Chief Information Security Officer (CISO)
- Security team staff
- Information owner

Other groups and/or individuals that may be needed include:

- Senior management
- General Counsel's Office (GCO)
- Human Resources (Talent)
- End User Support
- Building and/or facilities management staff
- Other Personnel involved in the Security Incident or needed for resolution

To implement the above framework, a Internal Technology Committee is formed comprising of following person: Priyank Jhaveri, Vipul Patel and Samir Shah.