POLICY ON LOGGING AND MONITORING

Oneview Corporate Advisors Private Limited

CIN: U74999MH1976PTC407933

Registered Address:
619 & 620, 6th Floor,
The Summit Business Bay, 266/1-172, Gundavali, Andheri Kurla Road,
Andheri (East), Mumbai - 400 093

Correspondence Office:
18, Deshapriya Park Road, Kolkata - 700 026.

Table of Contents

Sr no.	Contents	Page
1	Introduction	1
2	Purpose	1
3	Scope	1
4	Policy Statements	1

1) INTRODUCTION

This Logging and Monitoring ("Policy") establishes the principles and guidelines for capturing, retaining, and analysing system and application logs across the organization. It aims to ensure that all relevant activities—particularly those related to financial transactions, client data, and critical systems—are adequately recorded and continuously monitored.

2) PURPOSE:

The IT infrastructure components forms a crucial part of Oneview Corporate Advisors Private Limited (herein referred to as "OCAPL or "the Company",) operations which are critical to the Organizations operations. IT assets are continuously under threat from malicious users, unauthorized access and misuse and as a result, needs to be monitored effectively on a continuous basis for any abnormal activities. This policy aims to establish effective system to centrally log and monitor information security controls.

3) SCOPE:

All Employees and non-employees, stakeholders (interns, contractors, consultants, suppliers, vendors, service providers etc.) of the company and other individuals, entities or organizations that have access to and use information processing systems and Cardholder data environment to perform their daily job-related responsibilities or meet their contractual obligations.

All Information assets involving data, applications, network, security devices, servers and other IT system",

4) POLICY STATEMENTS

Logging shall be enabled on all information processing assets. All access to critical applications and the company's network shall be logged and continuously monitored for suspicious activities or security breaches and adequate response mechanism shall be setup for controlling security breaches.

4.1 LOG MONITORING

i. Logging shall be enabled for all the critical devices including application servers, network devices and security devices, databases, and other systems supporting business operations.

ii. The logs of the applications shall be monitored periodically to ensure proper functioning and policy compliance with the regulatory requirements.

iii. Some of the following activities and parameters shall be logged and monitored, but not limited to:
   a) Access to all audit trails
   b) Initialization of audit logs
   c) Stopping or pausing of audit logs
   d) Remote access activities of vendors
   e) All individual access to cardholder data
   f) Actions taken by any individual with root or administrative privileges
   g) Invalid logical access attempt
   h) Identification and authentication mechanisms
   i) Creation and deletion of system level objects

iv. Parameters related to audit trails:

a) Ensure user identification is included in log entries
b) Ensure type of event is included in log entries
c) Ensure date and time stamp is included in log entries
d) Ensure success or failure indication is included in log entries
e) Ensure that audit trails are enabled and active for system components
f) Ensure only individuals who have a job-related need, can view audit trail files. Access to audit trail files shall be monitored regularly
g) Ensure current audit trail files are promptly backed up to a centralized server or media that is difficult to alter

v. The logs shall be analyzed for the following:

a) Unauthorized access
b) Configuration changes
c) Abnormalities in mail routing events
d) Failed logins
e) Denial of service attempts

4.2 INCIDENT REPORTING

i. Any incident shall immediately initiate the IT Incident Management Process as per the IT Incident Management Policy.
ii. Designated Officer shall prepare the "Log Analysis Report", post any event identified.

4.3 BACKUP

i. Logs in the centralized server shall be backed up on a periodic basis.
ii. The backup logs shall be protected from unauthorized access.
iii. The Retention period of the logs shall be decided by the Designated Officer. Though all logs shall be maintained for minimum period of 1 year.