**LOGGING AND MONITORING POLICY**

R R Chokhani Stock Brokers Pvt. Ltd.



**May 5, 2020**

|  |  |
| --- | --- |
| **Author:** | Vishal Ayre |
| **Owner:** | Ramakant R Chokhani |
| **Organization:** | R R Chokhani Stock Brokers Pvt. Ltd. |
| **Version No:** | 1.0 |
| **Date:** |  05-May-2020 |

**Document Control**

**Document Title** Logging and Monitoring Policy

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version No.** | **Version Date** | **Author** | **Summary of Changes** |
| 1.0 |  05-May-2020 | Vishal Ayre | NA |

**Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Date of Approval** | **Version No** |
| Anand R Chokhani | Baselining ProcedureDocument |  05-May-2020 | 1.0 |

**Distribution**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Date of Issue** | **Version No** |
| NA | NA | 05-May-2020 | NA |

# Logging and Monitoring Policy

## Purpose

* IT infrastructure components forms a crucial part of R R Chokhani Stock Brokers Pvt. Ltd. operations. IT assets are constantly under threat from malicious users 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.

## Scope

This policy applies to:

* All staff and non-employees, stakeholders (interns, contractors, consultants, suppliers, vendors etc.) of *R R Chokhani Stock Brokers Pvt. Ltd.* and other individuals, entities or organizations that have access to and use *R R Chokhani Stock Brokers Pvt. Ltd.’s* information processing systems and card holder 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.

## Policy Statements

Logging shall be enabled on all information processing assets. All access to critical applications and *R R Chokhani Stock Brokers Pvt. Ltd.’s* network shall be logged and monitored for suspicious activities or security breaches and adequate response mechanism shall be setup for controlling security breaches.

### Log Monitoring

* Logging shall be enabled for all the critical devices including application servers, network devices and security devices.
* The logs of the applications shall be monitored periodically to ensure proper functioning and policy compliance.
* Some of the following activities and parameters shall be logged and monitored, but not limited to:
	+ Access to all audit trails
	+ Initialization of audit logs
	+ Stopping or pausing of audit logs
	+ Remote access activities of vendors
	+ All individual access to cardholder data
	+ Actions taken by any individual with root or administrative privileges
	+ Invalid logical access attempt
	+ Identification and authentication mechanisms
	+ Creation and deletion of system level objects
* Parameters related to audit trails:
	+ Ensure user identification is included in log entries
	+ Ensure type of event is included in log entries
	+ Ensure date and time stamp is included in log entries
	+ Ensure success or failure indication is included in log entries
	+ Ensure that audit trails are enabled and active for system components
	+ Ensure ONLY individuals who have a job related need, can view audit trail files. Access to audit trail files shall be monitored regularly
	+ Ensure current audit trail files are promptly backed up to a centralized server or media that is difficult to alter
* The logs shall be analysed for the following:
	+ Unauthorized access
	+ Configuration changes
	+ Abnormalities in mail routing events
	+ Failed logins
	+ Denial of service attempts

### Incident Reporting

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

### Backup

* Logs in the centralized server shall be backed up on a periodic basis.
* The backup logs shall be protected from unauthorized access.
* 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.