**LOGGING AND MONITORING POLICY**

**ISO 27001: 2013**

**XTRACAP FINTECH PRIVATE LIMITED**

**411, Vishal Tower, 10 District Centre, Janakpuri, Delhi, West Delhi, India - 110058**

**Document Summary**

|  |  |
| --- | --- |
| **Item** | **Value** |
| Document Name | Logging and Monitoring Policy |
| Classification | Internal |
| Distribution | ISMS Forum |

**Document Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Change Description** | **Prepared By** | **Approved By** |
| 07-09-2022 | 1.0 | Document creation | Anjaly TA | Inderjit Singh Bedi |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Contents

[**PURPOSE** 3](#_Toc457807261)

[**SCOPE** 3](#_Toc457807262)

[**POLICY** 3](#_Toc457807263)

# **PURPOSE**

The objective of this policy is to ensure that XTRACAP FINTECH PRIVATE LIMITED detects unauthorised activity, ensure that critical systems are monitored and information security events are recorded.

# **SCOPE**

This policy covers all information and associated IT infrastructure within XTRACAP FINTECH PRIVATE LIMITED.

# **POLICY**

1. XTRACAP FINTECH PRIVATE LIMITED critical network devices such as servers, Network devices and services shall be configured to monitor and logs recording of user activities, exceptions, and information security events shall be recorded, stored and produced when required.
2. XTRACAP FINTECH PRIVATE LIMITED IT Department shall ensure that audit logs recording exceptions and other security-relevant events are produced for critical systems and kept for an agreed period to assist in future investigations and access control monitoring.
3. XTRACAP FINTECH PRIVATE LIMITED IT Department shall ensure that procedures for monitoring use of information processing facilities are established, and the results of the monitoring activities are reviewed annually.
4. Current logs will be created application wise under application folder name

e.g. for API: fintech-api.log file will be created under api-logs folder

System will archive file in 3 cases

1. When logs file exceeds 50mb size
2. When a new day is started.
3. When application is restarted

The file will be archived in gz format with date and will be moved to the folder of the application under folder name as current year and month.

1. If there are multiple archives in a day file will be appended with numeric in suffix of the file name
2. The logs that are generated are backed up on the dr server and the s3 bucket. Jenkins is used for monitoring the application logs and any alerts are sent on Teams.  
   The Leadership group & IT Group has access to these logs.
3. All the monitored critical devices such as servers, firewalls, Routers etc. shall have their system clocks synchronized for consistent and meaningful logged information.
4. Monitoring and logging devices and software shall be protected from unauthorised use and other internal or external attacks that may deactivate the logging process and / or modify to delete the logs themselves.
5. Logging facility and Logs of monitored devices shall be protected from tampering and unauthorised access. The Logs should be securely stored to provide evidence during audits.
6. Annual audit and review of all logs generated by monitored devices shall be the responsibility of IT Department.
7. Current list of access privileges of each user for each information system and IT asset shall be securely retained.
8. All incidents that are found to have been repetitive shall be reported to Info Sec Manager for further action.