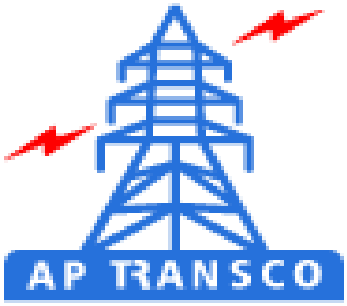

Transmission Corporation of Andhra Pradesh Limited

Event Log Monitoring Process

Confidentiality Statement

This Event log monitoring process document is strictly private, confidential and it is only for use by the Internal. This document shall not be used, disclosed, copied, published, distributed or reproduced in whole or in part without the prior written consent of APTRANSCO.

Document Control

Version	Date	Prepared by	Reviewed by	Approve by	Change Description
V1.0	23 /02 /2024	GICU	CISO	APTRANSCO	Initial Release

1. Purpose

This document outlines the Process for monitoring logical and physical event logs to ensure the security, compliance, and effective management of the organization's systems and facilities.

2. Scope

This policy applies to all employees, contractors, and third parties with access to the organization's systems or facilities. It covers all logical systems (e.g., servers, applications, networks) and physical access points (e.g., entry doors, restricted areas).

3. Responsibilities

- **IT Department:** Responsible for configuring, maintaining, and reviewing logical event logs.
- **Substation Team**: Responsible for monitoring physical event logs, OT Operations logs and coordinating responses to Corporate Office team / SLDC team.
- **Employees**: Report anomalies or unauthorized access attempts.

4. Logging Requirements

Logical Logs

Logical event logs must capture the following activities:

- User login attempts (successful and failed).
- Changes to system configurations.
- File and data access activities.
- Privileged account usage.
- System startup, shutdown, and errors.

Physical Logs

Physical event logs must record:

- Entry and exit of individuals from secure areas.
- Badge scans or biometric authentication attempts.
- Manual log entries for visitors.
- Security alarm activations.

5. Reporting and Escalation

- Document all incidents and investigations.
- Escalate critical issues to the Security Team or Compliance Officer immediately.
- Prepare monthly reports summarizing log reviews, findings, and corrective actions.
- Report should be done in format given in Annexture-I

ANNEXTURE-I

EVENT OVERVIEW		
Event Name		
Event Date		Event Time
Event Location		
Event Description		

EVENT COORDINATOR INFORMATION		
Coordinator Name		
Coordinator Organization		
Telephone		Email Address
Add. Contact Name		
Contact Details		

EVENT SCOPE	
Target Audience	
Messaging	
Objective	
Risk Management	
Identified Risk	**Risk Mitigation**