Logging and Monitoring Policy

Purpose

The purpose of this logging and monitoring policy is to ensure that all logs are collected and monitored to detect any kind of suspicious activities, misuse of systems, and security incidents.

What to Log

User login and logout times and activities
Failed login attempts
Use of administrative privileges
Who is using critical and sensitive data and their activities
System errors and warnings
Start and stop events

Log Review Responsibility

Logs must be reviewed by the security team.
Authentication and security logs should be reviewed daily.
System logs should be reviewed periodically or during investigations.

Log Storage and Retention

Logs must be stored securely to prevent unauthorized access.
Logs must be protected from modification.
Logs should be retained for a minimum of 90 days or as required by organizational or compliance requirements.

Action on Suspicious Activity

Any suspicious activity identified in logs must be reported immediately.
The affected system found should be investigated by the security team.
Necessary actions such as account lock, password reset, or system isolation should be taken if suspicious activity takes place.
All incidents must be properly documented for future reference.

Conclusion

Effective logging and monitoring help the organization detect threats early, investigate incidents, and maintain compliance.