Audit Trail Policy

Version: 1.00

This Audit Trail Policy is intended to ensure that computers and network devices have proper logging to detect, investigate, and remedy events that may be a security hazard or a threat to the organization or personnel.

1.0 Overview

This Audit Trail Policy is an internal IT policy which provides guidance about what events on computer systems should be logged, how long logs should be retained, who can access the logs, what kind of access to logs should be granted.

2.0 Purpose

This Audit Trail Policy is required to help ensure the security of servers and the network by providing guidance about the events to be logged, how long logs should be retained, and what access to logs should be granted.

3.0 Scope

This Audit Trail Policy applies to all servers, network devices, and network security devices which are capable of producing event logs. This policy is effective as of the issue date and does not expire unless superceded by another policy.

4.0 Audit Log Requirements

- Security related activity on all servers, firewalls, routers, and workstations must be logged. Examples include:
  - Unsuccessful login including details such as IP address where the login was attempted from.
  - Successful login including details such as IP address where the login was done from.
  - Account management events when accounts are added, modified, renamed, or deleted.
  - Changes to policy.
  - System shutdown, system startup, or other system security events.
  - User privilege use and attempted use of privileges not granted.
  - Object access.

If possible, the user name or ID should be recorded, time of the event, computer or IP address the action was performed from, and success or failure of the action or event.

- Audit logs must be retained on all firewalls, routers, and servers for a minimum of six months and recommended for one year. Where laws or regulations apply, logs may need to be retained longer. Business managers are responsible for informing IT management about any laws that apply to data stored on their servers. On workstations, audit logs should be allowed sufficient space to be retained six months if possible.
- Audit logs are normally reviewed daily as a part of normal maintenance on servers. This especially applies to firewalls, routers, and servers with sensitive data on them. Servers that have publically available data may be audited less often with permission but this is not recommended since any compromised server is a serious security threat.
- All suspicious activity found in logs shall trigger the incident response plan according to policy and shall be investigated.
- All activity that indicates violation of policy shall be investigated.
- Audit logs shall not be accessible to users and shall only be writeable by programs with valid reason to write to them. Where possible programs should be able to ammend the logs but not delete entries.
- Permissions on audit logs must be set to prevent unauthorized access to them. The distribution of audit files, in electronic form or printed form is limited to only those who require access and have clearance to view the information.
- Sensitive information such as social security numbers, credit card numbers, and passwords should either not be retained in logs or should be masked so they cannot be read.
- Where possible without reducing security, tools should be used to automate auditing and locate patterns in audit files which would point to something requiring attention.
- Only administrators of the systems and their management should be able to review logs. In the event of a security incident, investigators may be granted full or partial access. Auditors may also be granted access to logs.
- Sufficient storage must be made available to keep audit logs for the required times at the level of detail specified.
- All security events that should be invested are to be included in the audit log and include enough information to properly investigate the event including but not limited to the time of the event and the process associated with the event.

Audit logs must be sufficient to support investigations of inappropriate use, intrusions. or any security incidents. Auditing of printer access for forensic investigation of inappropriate use is recommended.

5.0 Enforcement

Since audit logs are important to check events that affect the security of the organizational network and prevent unauthorized data disclosure, employees that purposely violate this policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

6.0 Other Requirements

- Procedures for ensuring that automated tools comply with security requirements and auditing requirements must be developed.
- More detail about what is audited for each system type must be provided. This includes what system, security, and application events are logged on each type of server such as mail server, print server, file server, web server, and others.
- Additional detail about the level of access for the business need and based on system type and interoperability must be created.

Approval

Approved by: Sandeep Jindal Date: 04/02/2020