# Audit Log Review Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The aim of this policy is to ensure that processes are in place across all designated [Company Name] systems to ensure that designated audit logs are reviewed daily and following a security incident. Designated audit logs are outlined below. Any exceptions identified are followed up and reported to management. The overall goals of audit log review are to detect unusual or unauthorized events, investigate causal factors for identified events, reconstruct the course of events before and after an event, and identify the account associated with a specific event.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This policy applies to all of the following logs within the [Name of the specified environment or system]:

* + Operating System Logs
	+ Database Audit Logs
	+ Unusual or unauthorized Detection System Logs

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. Review of logs is to be carried out by means of [Company Name’s] network monitoring system [Name of System].
* Reviews should be conducted daily and following a security incident.
* The following individuals are the only individuals permitted access to log files: [List of Roles or Individuals]
* The network monitoring system software, [Name of System], is designed to alert [Individual Name/Role] to any event deemed to be potentially unusual or unauthorized. Alerts are designed as follows: [List of Alerts Mechanisms].
1. The following operating system events are logged:
	* Any additions, modifications, or deletions of user accounts.
	* Any failed or unauthorized attempt at user logon.
	* Any modification to system files.
	* Any access to the server or applications running on the server.
	* All actions taken by individuals with administrative privileges.
	* All access to audit logs.

The process for restoring logs for analysis is as follows: [Document the process].

1. The following database system events are logged, and are monitored by the [Name of system]:
	* Any failed user access attempts to log in to the database.
	* Any login that has been added or removed as a user.
	* Any login that has been added or removed from a role.
	* Any database role that has been added or removed from a database.
	* Any password that has been changed for a role.
	* Any action taken by an individual with administrative privileges.
	* All access to audit logs.

The process for restoring logs for analysis is as follows: [Document the process].

1. The following unusual or unauthorized detection events are logged, and are monitored by the [Name of System]:
	* Any listed vulnerabilities in the [Name of database].
	* Any generic attack not listed.
	* Any denial of service attack.
	* Any authentication failure that might indicate an attack.
	* Any traffic typical of known attacks.

The process for restoring logs for analysis is as follows: [Document the process].

1. For any unusual or unauthorized event confirmed, the following must be recorded in [Form Name] and [Individual or Role Name] must be informed.
	* User ID
	* Date & Time
	* Event type
	* IP Address of Origin
	* System and data affected

The process for restoring logs for analysis is as follows: [Document the process].

1. Logs must be retained for a period of a year, unless otherwise stated.
* Log disposal procedures are outlined within the [Name of related policy].

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.