# Audit Logging Policy

## Purpose

The purpose of this policy is to outline how systems generate log events for audit purposes, and how these logs are stored and processed to help detect security issues.

## Scope

This policy applies to all systems classified as Customer Confidential, and the logs that they generate.

## Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

## Policy Statement

### Centralized Logging

Applications and system logs are pushed to a central logging repository where possible. Access control to the central repository is enforced based on the Access Control policy. Logs are retained in compliance with applicable legal, regulatory, customer, and operational requirements.

<Company Name> uses a specialized logging service to store all audit logs. Using a logging service ensures that logs are shipped away from the system in which they were generated, and as such are further protected from users with privileged access to that system. In addition, storing logs in a single central location allows for easier access management , helping to ensure only authorized users with a business need can view logs. By default, logs are transmitted using channels encrypted with TLS or equivalent.

The retention period of audit logs is managed centrally on the logging service. The retention period is governed by applicable legal, regulatory, contractual and business requirements. Logs that go past their retention period are automatically deleted by the logging service.

If a very long retention period is required by business or legal reasons, audit logs older than a certain window may be archived to a low-cost storage location. Archived logs are typically

stored on the same cloud provider, with equivalent encryption strength and further restricted access control.

Retention periods for audit logs are specified in <Company Name>'s Data Retention Procedure.

## Security Event Logging

Security tools are deployed and system components are configured to monitor for security-related events.

Owners of systems classified as Customer Confidential should ensure that their components log security-related events, such as:

- User account creation
- Session creation attempts
- Modification of permission sets
- Privilege elevation (if applicable)
- User impersonation (if applicable)

In addition, system owners should work to identify other security-related events specific to their component, and ensure that the appropriate logging or alert mechanism is employed to record or communicate their occurrence.

When possible, <Company Name> uses automated tools to monitor for additional suspicious activity, such as changes in network traffic and data access patterns, requests from known malicious IP addresses, and requests with known malicious signatures. These tools are configured to send alerts, which are reviewed based on priority.

## Security Event Review

Security events are triaged and reviewed for unauthorized and malicious activity. High priority findings are treated as potential security incidents.

When possible, <Company Name> uses automated tools to escalate and triage security events in real-time. In addition to promptly reviewing high-priority alerts, [POLICY OWNER]

is responsible for periodically reviewing all security events generated by <Company Name> systems.

Any suspected malicious activity, or unauthorized or inadvertent disclosure, will be treated as a potential Security Incident, and managed as described in the Security Incident Management Policy.