GLOBAL EVENT AND AUDIT LOG MANAGEMENT

Revised: 10-31-2016

1.0 Purpose

Audit trails are used to accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis. The purpose of this policy is to establish standards for the configuration of audit trails for systems that store, process or transmit sensitive information

2.0 Scope

This policy applies to all PCI environment system components, including but not limited to computer hardware and devices, applications, network, and Internet connections. Additionally, this includes system components managed by third parties.
Exceptions to this policy must be reviewed and approved by the appropriate regional Security Exceptions process.

3.0 Policy

Crawford & Co. must record and review all significant activity on systems that store, process or transmit sensitive information.

3.1 Audit Trail Protection Standards

3.1.1 Centralized Log Management

System logs must be recorded on the involved system and a central log host that is not directly Internet-accessible.

3.1.2 Automation of Log Monitoring

Automated mechanisms must be employed to integrate audit monitoring analysis and reporting into an overall process for investigation and response to suspicious activities.

3.1.3 Authorized Viewing

Audit logs must be secured such that they cannot be modified and can be viewed only by authorized personnel.

3.1.4 Clock Synchronization

The clocks of all relevant systems must be synchronized with trusted time source, as part of protecting the accuracy of audit trail information.

3.1.5 Integrity

Audit trails must be protected with integrity monitoring controls and monitored for sudden decreases in size, failures of digital signatures, and gaps in log entry sequence.

*3.2 **Audit Entry Requirements***

Systems that store, process or transmit sensitive information must securely log all significant security events. System audit trails must be configured to capture the maximum amount of events described below.

*3.3 **General Requirements***

- Machine startup and shutdown; startup and shutdown of audit function;
- Successful/unsuccessful login and logout of users; denial of service events.
- Add, modify, and delete actions on all data/files/objects; plus read/view actions on data classified as confidential or restricted;
- Use of all privileged accounts and utilities;
- Changes to user accounts or privileges (creation, modification, deletion);
- Switching to another user's access or privileges after logging in;
- Software or hardware modification;
- All access to security files, attributes, or parameters.

3.3.1 Operational Requirements

- Login attempts with failed identification or authentication;
- Changes of the time or date of the system clock;
- Detection of a virus;
- Detectable hardware and software errors;
- Log failure and restart events;
- Changes to log files (creation, deletion, and configuration).

3.3.2 Communication Requirements

- Network link failures;
- Failed connection attempts;
- Network and device connections dropped;
- Data integrity verification failure for information transmitted over a network;
- Message authentication failure for information transmitted over a network;
- Overrides of network abnormality alarms and alerts;
- IP addresses of successful and unsuccessful connections;

- Changes to network security configuration (e.g. firewalls).

3.3.3 Audit Trail Entry Requirements

- Date, time, type, and any applicable error condition of event;
- The ID of the user who caused the event;
- The event success or failure;
- The application that created the audit event;
- The application(s) responsible for executing the event.

*3.4 **Continuous Monitoring***

Audit trails for system components that store, process or transmit sensitive information must be reviewed daily. All alerts from the Intrusion Protection System (IPS) or the Security Incident Event Management System (SIEM) must be reviewed promptly and resolved using the appropriate Incident Response procedures.

*3.5 **Audit Log Retention***

Copies of all audit trails from systems that store, process or transmit sensitive information must be retained in accordance with all applicable laws and regulations.

Policy Name	Event and Audit Log Management
Policy Number	Global_IS Policy 00004
Effective Date	10-31-2016
Approved By	Gretchen Hiley, Chief Technology Risk Officer
Last Approval Date	10-31-2016