# Logging and Monitoring Standard

**CWB Financial Group – Information Security Office**

**Document Version: Version 1.0**

**June 15, 2020**

CWB Financial Group

# Contents

# Document Summary

## Introduction

CWB Financial Group (herein referred to as CWBFG) requires a centralized log management service to support near real-time analysis of security events captured in audit logs. Log data aggregation and correlation from multiple log sources set the foundation for automated monitoring, which is capable of generating alerts on information security incidents. (SI-4)

CWBFG reserves the right to log all access to and activities performed on CWBFG information technology assets, for the purpose of:

- supporting internal investigation activities, such as:
  - detecting and preventing the inappropriate use of CWBFG information technology services;
  - detecting breaches to CWBFG Information Security policy or security standards; and
  - performing forensic analysis of unauthorized access or unauthorized activities.
- establishing baselines of what constitutes normal application use case patterns.
- complying with fiduciary, legal, regulatory and contractual obligations.

As per the CWBFG ***Information Security Logical Architecture***, this standard supports the following principles:

- Zero Trust
- Defense in Depth
- Access Control
- Defense Against Threats
- Defense Against Fraud

## Purpose

This standard documents logging and monitoring requirements and focuses on managing log data deemed important to CWBFG in terms of information security.

## Scope

This standard applies to all individuals who use, provision, and support CWBFG's technology assets, regardless of where these assets are located (e.g. Corporate or Cloud Service Providers). This also applies to authorized third parties who use or provide services, manage, or support CWBFG's technology assets.

As a cloud service customer, this standard also applies to the methods used to log and monitor for security events within the cloud based services our business engages with.

The ***Information Classification Standard*** provides guidance on the classification levels assigned to information, based on its value to CWBFG. The log management system can include logs from a variety of systems representing all classification levels (Confidential, Restricted, Internal and Public). Mandatory logging and monitoring must be implemented on systems housing data classified as 'Confidential' and 'Restricted', and/or services deemed to be 'Critical' and/or 'Security' systems.

## Out of Scope

This standard will not include operational logging and monitoring requirements for systems and network infrastructure where state, health and performance information of computer systems is monitored, using a combination of operational monitoring systems such as: System Center Operations Manager (SCOM), SolarWinds and Quest Foglight.

# Standard Statements

## Security Information and Event Management (SIEM)

Logging and the resultant log data assist in identifying compliance on the part of users and is critical in collecting evidence for performance management, incident identification and response, forensic activities or potential legal purposes. Without appropriate security logging, a threat actor or an unauthorized user's activities can go undetected, and the evidence required to determine whether an incident led to a breach can be inconclusive.

- CWBFG has established a centralized log management service (also known as Elastic) that must be leveraged to aggregate logs from multiple sources including:
  - All core Security services;
  - Servers and network devices;
  - Operating Systems, which capture:
    - System Events - containing operational actions performed by OS components, such as shutting down the system or starting a service;
    - Security Events - containing audit records such as successful and failed authentication attempts, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges;
    - Network traffic logs; and
    - Database audit logs.
  - Applications which generate their own log data, and capture:
    - Client requests and server responses;
    - Account information, such as successful and failed authentication attempts, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges;
    - Usage information, such as the number of transactions occurring in a certain period (e.g., minute, hour) and the size of transactions (e.g., email message size, file transfer size; and
    - Significant operational actions such as application start up and shutdown, application failures, and major application configuration changes.

## General Requirements

- Information Owner and/or Information Custodians must:
  - enable logging on information technology assets, applications and databases (AU-13) to:
    - identify unauthorized access attempts, malicious or unauthorized activities for all assets classified as 'Confidential' or 'Restricted' or categorized as 'Critical' or 'Security' systems;
    - ensure the collection of relevant log data to help with investigations of reported unauthorized access and unauthorized information disclosure;
    - ensure for each information technology asset type, basic attributes are captured in the log data to ensure meaningful recording of security events (e.g. username, source and destination IP addresses, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked). Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred); (AU-3)
    - ensure client or originating IP addresses are captured in logs when a reverse proxy, proxy, or load balancer are used, as these devices translate the source IP address to an internal IP addresses and do not typically log the originating IP addresses, making it more difficult to track the true source; and
    - ensure alert notifications are generated when security event thresholds have been triggered. Engage the Information Security Office – Security Operations Team to help determine the appropriate threshold assignments. (SI-4)
  - ensure logs are not added or stored anywhere else than the originating system or the centralized log management system.
  - ensure the use of secure protocols for transmission of logs, as defined in the ***Data Protection Standard*** and the ***Cryptographic Security Standard***.
  - ensure Infrastructure Operations has enabled operational components and standards around infrastructure monitoring technologies, which is out of scope for this standard, other than a requirement for operational teams to report all potential security events occurring in these logs to Security Operations.
  - log third party service provider and Business Partner access to CWBFG's information technology assets. (SI-4)
  - include in the baseline configuration for all information technology asset types logging requirements, including:
    - ensuring those assets generating logs and/or being centrally monitored use a trusted time source to generate time stamps for audit records; and (AU-8; SI-4)
    - enabling time synchronization, by:
      - mapping internal system clocks to the CWBFG trusted time sources (e.g. ntp.cwb.local); and
      - ensuring external hosted services use a trusted time source, confirmed via the Master Agreement with the vendor, or via the risk assessment performed by GRC.

## Data to Exclude in Logs

- The following attributes/fields must be removed, masked, sanitized, hashed, tokenized or encrypted and not recorded in clear text within log data:
  - cryptographic keys which can assist a threat actor in decrypting protected data;
  - passwords;
  - sensitive information (e.g. Personally Identifiable Information (PII)) or transactional information that has business value;
  - database connection strings; and/or
  - application source code and logic.

### Protection of Log Data

- Log data must be protected from misuse, such as tampering in transit, and unauthorized access, modification and deletion once stored. (AU-9; SI-4)
- Physical security safeguards must be utilized, including situating logging facilities within a secure zone with physical access controls.
- For systems categorized as 'Critical' or 'Security' and/or information systems classified as 'Confidential' or 'Restricted', the following additional protective controls must be considered:
  - leveraging multi-factor authentication (step up authentication) to restrict access to sensitive log data, via Role Based Access Control (RBAC) configuration and CWBFG Identity and Access Management system;
  - archiving audit logs in real time to a centralized secure repository to remain within storage capacity and prevent log data from being overwritten on the source system;
  - enabling cryptographic signatures to maintain integrity and to assist in detecting alteration or data corruption, where technically feasible; and
  - preventing privileged accounts from erasing or de-activating logging of their own activities. (SI-4)
- Sharing log data or alerts originating from 'Confidential' or 'Restricted' classified systems or from 'Critical' or 'Security' services with any external stakeholders and/or third parties (to meet contractual obligations or to adhere with regulation requirements) requires the Chief Information Security Officer's approval. (AC-21; SI-5)
  - Log data and/or alert information is considered 'Confidential' information and must be protected from unauthorized disclosure or alteration when transmitted to or stored within the external party's systems; and
  - Administrators must use secure communication methods to send log copies to support vendors and must avoid using email, instant messaging tools, or web meetings to share logs.

### Monitoring User Activities

- All requests to provide a report of an individual's activities must be requested by the individual's management team and authorized by Human Resources. Information discovered may be used to support disciplinary actions and therefore the confidentiality of this information must be preserved.
  - The SIEM must provide the capability for authorized individuals to investigate user activity and select a user session. Session auditing activities are developed, integrated, and used in consultation with Security Operations, in accordance with applicable federal laws, regulations, or CWBFG policies and standards. (AU-11)

## Security Operations – Incident Response

- The Information Security Office – Security Operations Team is responsible for ensuring timely response to reported security incidents. This includes:
  - deploying logging and monitoring services on:
    - the core security services (e.g. firewalls, web application firewalls, threat protection systems, identity and access management systems, load balancers, vulnerability management services, secure file transfer systems, cryptographic services, privileged access management systems, etc.); (SI-4 & AU-13)
    - web servers, Linux servers, email systems, etc.;
    - applications and/or databases classified as 'Confidential' or 'Restricted''; and
    - core network switches.
  - developing standard processes for performing log management, including:
    - defining logging requirements and goals for log generation, transmission, storage, analysis, retention, and disposal;

    - configuring log sources, performing log analysis, initiating responses to identified events, and managing long-term storage;
    - requiring logging and analyzing the data that is of greatest importance, and also have non-mandatory recommendations for other sources of data should be logged and analyzed if time and resources permit; and
    - addressing the preservation of original logs, for those cases where logs may be needed as evidence, by determining storage requirements or different processes which restrict access to the records.
- ensuring log data is:
    - aggregated and stored in one central location; (SI-4)
    - capable of real-time correlation and analysis across log sources;
    - encrypted when transmitted and stored;
    - retained for an appropriate period of time: (AU-11; SI-4)
        - three (3) months of hot index data;
        - nine (9) months of cold index snapshots, totalling 12 months retained log data; and
        - external cloud service providers that maintain a CWBFG instance should also retain logs for the same period of time, where possible.
    - securely dispose of, once the one-year retention period has been reached.
- enabling alerting if log capture has been disabled to ensure continual log collection. (SI-4)
- maintaining an incident response process used to respond to potential security incidents, including preparation, detection, analysis, containment, eradication, and recovery sub processes, including: (IR-4)
    - leveraging external third party security breach experts (e.g. Mandiant) for major incidents;
    - identifying and evaluating security events discovered through the monitoring of logs and generated alerts (AU-6; SI-4);
    - responding to alerts indicating a major incident, by leading the Cyber Security Incident Response Team's (CSIRT) response, as per the ***Incident Response Playbook***; and (IR-8; SI-4)
    - monitoring log data for new indicators of compromise. (SI-4 (24))
- performing continuous monitoring activities to facilitate ongoing awareness of threats, and vulnerabilities to support information security risk management decisions. (CA-7)
- providing logging and monitoring advice to Information Owners and/or Information Custodian, as required.

# Exceptions

All exceptions to this standard must be documented and approved by both the information owner and the Chief Information Security Officer. Exceptions to this standard must be documented and registered as a risk as per the Information Security Governance, Risk, and Compliance processes. Identified risks must be assessed by the CWBFG Information Security Office and mitigated in partnership with the business owner and third-party service providers.

# Enforcement

Failure to comply with this standard may impact the business and reputation of CWBFG. Depending on the circumstances, CWBFG will act to correct violations of this standard through training, counselling, disciplinary action, termination of employment, civil action or criminal prosecution.

It is the policy of CWBFG to handle information security incidents so as to minimize their impact on the confidentiality, integrity, and availability of CWB information systems, applications, and data. An information data breach incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information that interferes with information technology operations. All such incidents must be reported to the CWBFG Information Security Office.

# Roles and Responsibilities

| Role | Responsibility |
|---|---|
| Chief Information Security Officer | • Accountable for the creation, maintenance, and implementation of this standard where applicable.<br>• Accountable to have and maintain written standards and procedures necessary to ensure implementation of and compliance to this standard.<br>• Accountable to provide appropriate support and guidance to assist employees to fulfill their responsibilities of complying with this standard. |
| Sr. Manager, Information Security Program Management | • Responsible for the creation and maintenance of this standard and supporting policy where applicable.<br>• Responsible to have and maintain written standards and procedures necessary to ensure implementation of and compliance to this standard.<br>• Responsible to provide support and guidance to assist employees to fulfill their responsibilities of complying with this standard.<br>• Consulting with Sr. Manager, Security Governance, Risk and Compliance and Sr. Manager, Security Operations, as required. |
| CWB's Executive Leadership Team, Senior Leadership Team, Directors, and Managers | • Understand and comply with this standard and supporting policy in its entirety.<br>• Responsible to create and maintain processes and procedures to support this standard and supporting policy.<br>• Responsible to ensure that all appropriate personnel are aware of and comply with this this standard and supporting policy.<br>• Responsible for the creation of appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this standard and supporting policy. |
| CWB employees, contractors, third-party service provider, etc. | • Understand and comply with this standard and supporting policy in its entirety.<br>• Implement this standard with supporting processes and procedures.<br>• Report vulnerabilities and breaches. |

# Appendix A – Document Control

**Document Status**

| | |
|---|---|
| **Document Name** | Logging and Monitoring Standard |
| **Document Owner** | Chief Information Security Officer |
| **Version** | Final Version 1.0 |
| **Publication Date** | |
| **Information Classification** | Internal Use |
| **Revision Status** | Final |
| **Custodian** | Sr. Manager, Information Security Program Management |
| **Organization** | CWBFG Information Security Office |
| **Retention Period** | Retain for ongoing use |
| **Master Storage Location** | |

**Revision History**

| Version | Author | Contributor | Description of Changes |
|---|---|---|---|
| Draft 1.0 | Joanne Pearson | Michael Thompson<br>Prince Anthonysamy<br>Vikram Singh | Document creation, and initial review of content. Prepare draft for review. |
| Draft 2.0 | Joanne Pearson | Thomas Matthews | Revised Draft based on review. Ready draft for CISO review. |
| Final 1.0 | Joanne Pearson<br>Vikram Singh | Cory Gould | Finalize standard and publish in Keylight |

# Appendix B – Definitions

The following table highlight key definitions used in this Standard.

| | |
|---|---|
| **Alert** | A brief, usually human-readable, technical notification regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note. |
| **CISO** | Chief Information Security Officer |
| **'Critical' Services** | Systems whose function is critical to CWB success, such as:<br>• Data Center facilities are deemed critical. A facility, if damaged or destroyed would have the potential to disrupt or significantly reduce required service or deliverability.<br>• Core Banking systems<br>• HR systems<br>• Strategic Business Planning systems<br>Compromise of assets can result in a shutdown of system and/or significant commercial impact (including legal consequences such as regulatory non-compliance or violation of contractual terms and conditions) due to a related security tenet. |
| **CWBFG** | Canadian Western Bank Financial Group |
| **Incident** | An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. |
| **Incident Response** | A predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious security attacks against an organization's information systems(s). |
| **Log Data** | A record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. |
| **Security Information and Event Mgmt system (SIEM)** | A centralized system used for generating, transmitting, storing, analyzing, and disposing of log data. |
| **'Security' Service** | Systems whose function is to provide a level of protection/security to information, facilities or systems, such as the following core security services (as defined in the ***Enterprise Security Architecture – Logical Architecture***)<br>• Information Flow Control Services<br>• Identity and Access Management<br>• Integrity Services<br>• Logging and Monitoring Service<br>• Cryptographic Services<br>Compromise of asset results in (process or personal) safety risk due to related security tenet. All assets that perform key security functions are in this category by default. |