SUBJECT: **ACES Audit Programme** NUMBER: **III-40**

DATE: June 2016

APPROVED BY:

Purpose

The purpose of this policy is to define the standard, routine auditing requirements and processes necessary both to safeguard the data stored in ACES and to protect the ACES system itself. This policy establishes the baseline requirements of the auditing programme; exceptional circumstances, such as a breach, could necessitate a more in-depth, specialized audit.

Procedures

Access Modes

ACES data can be accessed in only two ways.

The predominant mode of access to ACES, by far, is through the standard user interface (i.e., aces.kflaphi.ca). All end users, without exception, access ACES through the web interface. End users are designated persons, most often epidemiologists and infection control practitioners from the local public health agency and hospital respectively. The client application (i.e., aces.kflaphi.ca) retrieves data that users view in the tool through a middle-tier application that provides role-based authorization, resolves the user request to a database query, and coordinates that request with the database server. Database queries are not and cannot be submitted directly through the user interface. Instead, middle-tier REST endpoints broker requests between the front-end client application and the back-end database. Every endpoint to ACES is secured and every execution of an endpoint method is logged. This is the standard approach used to capture and record access by end users accessing ACES through the web interface. Both to provide an additional audit trail for those accessing ACES data through the client application and to provide an audit trail for project staff who access the database directly, auditing is also enabled at the database level.
The ACES DSA defines authorized persons and

A secondary mode of accessing ACES data is through database client query tools. As of this writing, SQL Server is used for data persistence in the data storage layer and so the ACES Project Team may use client tools—typically SQL Server Management Studio—for direct access to the database. The ACES Project Team would directly access the database to perform ad hoc maintenance (e.g., reindex a table), troubleshoot a problem, or they may execute custom queries (not available through the standard interface) in support of an epidemiological investigation.

Auditable Events

Through the ACES web interface, auditable events include:

1. logon
2. logoff

3. REST endpoint invocations (these capture the data requests required to populate each page a user visits on the website) When a user submits a request for information such as line listings or epicurves, the request is sent to an endpoint that facilitates communication between the user's web browser and the ACES Database server.
4. change password
5. account maintenance (e.g., change e-mail address)

Through database client tools, auditable events include:

1. logon
2. logoff
3. DDL and DML statements (including CREATE, DROP, EXEC, SELECT, UPDATE, INSERT, and DELETE)

Information Captured

Data captured varies by event type and mode of access. Where feasible, data will include:

1. date, time, and time zone of event
2. event type
3. originating IP address
4. originating hostname
5. authorization credentials
6. request (What information the USER was looking for such as line listings or epicurves and what parameters were specified)
7. results returned (The actual result set that was returned to the users interface or web browser)

Non-Repudiation Safeguards

Review, Analysis, and Reporting

Using these audit entries, a number of techniques are employed to detect suspicious activity. These include identifying multiple failed login attempts, unusual time-of-day and day-of-week access patterns, the attempted access of non-existent pages, or page accesses with unusual query parameters. Source IP addresses are reverse geocoded and the source geographies (cities, provinces, or countries) are reviewed for reasonableness. It may well be that an authorized user of ACES accesses the system whilst on vacation overseas but these should be very few and far between. These methods of detecting suspicious access are neither definitive nor hacker-proof but form part of the larger intrusion detection toolkit that collectively help to identify threats and mitigate overall risk.

Auditing Hierarchy

Additional to the automated intrusion detection methods enumerated below, periodic reviews of the access logs are conducted by KFL&A Public Health's Supervisor of Informatics with special attention given to direct accesses of the ACES database by project staff. These occur randomly

but at least quarterly. KFL&A Public Health's Associate Director of Knowledge Management, in turn, reviews access to ACES by all project staff, including the Supervisor of Informatics. All of these reviews are documented on the Knowledge Management Information and Security Practices (ISP) Register.

Storage and Archiving

Audit logs are written to host server storage and are simultaneously written to an independent secondary storage location. These secondary audit logs are encrypted, compressed, and stored off-site hourly. As of this writing, these secondary files are stored indefinitely whilst the audit files on the host server(s) are overwritten as required to reclaim disk space.