

	LOM 3.1 Forensic Advantage Access Rights, Security Auditing and Data Backup	
	Document #: 1321	Page 1 of 3
	Revision #: 1	Issued Date: 10/30/2017
	Document Manager: John Bowen	Approved By: Jeffrey Nye

3.1. Forensic Advantage Access Rights, Security Auditing, and Data Backup

The Laboratory Case Management System (LCMS) utilized by the Michigan State Police (MSP) Forensic Science Division (FSD) and the Biometrics and Identification Division (BID) is the Forensic Advantage (FA) product from The Computer Solution Company (TCSC). The system is managed and maintained internally by the FSD Technical Support Unit (TSU) and externally by the Michigan Department of Technology, Management and Budget (DTMB).

3.1.1 Creating New and Modifying Existing User Profiles

- Requests to add, modify, or remove existing accounts shall be made utilizing the FS-052 (Forensic Advantage Access/Change Request).
- Request for new accounts or modification to existing accounts of laboratory staff are required to be submitted through channels to the Lab Director. The Laboratory Director will forward the request to the TSU.
- Division Administration staff may also request new accounts or modification to existing accounts. These request will be made after consultation with the affected Laboratory Director(s).
- Requests for new users who will be authoring reports also require a signature image. The image should be scanned and e-mailed to the TSU at the same time as the FS-52.
- If access to multiple labs and/or sections is requested, the affected Lab Director(s) is contacted by TSU staff to confirm the requested access rights are approved. Approval by the affected Lab Director(s) must be documented.

3.1.2 Access Rights Authorization

- Users requiring access to the FA system must first have a valid network login ID (which requires meeting the MSP security restrictions) and also be a member of the 'FA_Analysts' group on the FA server network.
- The default level of access for all employees is 'Analyst' level access. Analyst level access is low-level with all permissions to units, exams and storage areas denied by default.
- Staff that are unit supervisors are specified as the supervisor for their subordinate staff from within the subordinate's user profile in FA. This ensures that they have supervisor privileges for their direct reports only.

3.1.3 Removing User Access from the System

- Requests to remove laboratory staff user privileges from the system are submitted by the Laboratory Director or Division Administration to the TSU utilizing the FS-52.
- If an employee's access is de-activated because the employee has left the FSD, the request to remove the employee's access should be made within 48 hours of the employee leaving.
- User accounts are de-activated by disabling the network account and removing all membership to laboratory entries in FA. The user account in FA is not deleted. This ensures any documentation associated with casework the analyst worked on remains accurate.

	LOM 3.1 Forensic Advantage Access Rights, Security Auditing and Data Backup	
	Document #: 1321	Page 2 of 3
	Revision #: 1	Issued Date: 10/30/2017
	Document Manager: John Bowen	Approved By: Jeffrey Nye

3.1.4 Auditing of User Accounts and Privileges

On a bi-annual basis, the FSD TSU will communicate to each Laboratory Director a list of personnel who have access to Forensic Advantage in their respective labs. The Laboratory Directors shall audit the list and communicate any needed changes to the FSD TSU via the FS-052 Forensic Advantage Access/Change Request form. The results of these audits shall be documented in a memo to the Division Director and subsequently uploaded to the FSD Documentation Management System.

3.1.4.1 Auditing of Privileged Users

On a biannual basis, the FSD Quality Assurance Manager will assure the completion of an audit of administrative overrides (data corrections/changes) completed by the privileged users (administrators) in Forensic Advantage.

3.1.5 Data backup and Retention

- **Redundancy:** The Forensic Advantage system consists of a main server at the DTMB Hosting Center, a delivery server which routes e-mail and fax delivery, a fax server, and a web server. A redundant copy of the database is maintained in near real-time, by DTMB and offsite.
- **Data backup:** DTMB provides backup of the main server in the hosting center. The file system receives a full backup every Sunday with incremental backups every other day of the week. The SQL database is fully backed up on Wednesdays with differential backups performed every other day of the week. Data is kept for 30 days at which time the backups are overwritten with new backups.

3.1.6 Requests for Changes

3.1.6.1 Requests for Changes in Forensic Advantage Settings

Requests for modification or enhancement of configurable areas of Forensic Advantage shall proceed as follows:

- All requests from FSD staff will be submitted first to the FSD TSU
- Depending on the nature of the request, FSD TSU staff will contact the relevant parties (Technical Leaders, Laboratory Directors, Division Administration) for approval and clarification of the change
- If the request is a local configuration change, FSD TSU staff might complete it themselves
- If the request requires vendor intervention, FSD TSU staff will serve as liaison with the vendor to see the work completed.
 - Upon completion, significant changes may be applied to the FA Training environment for testing and validation.
 - FSD TSU staff will involve appropriate staff (to include the original requestor) in testing and verifying the change is adequate
- Notifications to all staff (of significant changes) will be made via email

	LOM 3.1 Forensic Advantage Access Rights, Security Auditing and Data Backup	
	Document #: 1321	Page 3 of 3
	Revision #: 1	Issued Date: 10/30/2017
	Document Manager: John Bowen	Approved By: Jeffrey Nye

3.1.6.2 Requests for Administrative Overrides (data correction changes) in Forensic Advantage

Requests for corrections of administrative errors in Forensic Advantage shall be communicated to the FSD's Technical Services Unit (TSU) for remediation. TSU personnel shall document all relevant supporting data (source/content of the request, the action taken, dates of request, reason for request, etc.) as part of their corrective activity.

These Administrative Overrides will be audited according to section 3.1.4.1 of this document.