FIA Audit Log Schema and Redaction Rules

1.1 What Every Audit Log Entry Must Capture

Central File: ~/App_Data/auditLog.xml

Root Element: <auditLog version="1" retentionDays="1095"> … </auditLog>

Each audit log entry is stored as an <entry> element with the following fields and rules:

Field (XML)	Purpose / Example	Logged?	Redaction Rule / Note	Visible To	Retention
id (attribute)	Unique id for the log entry (GUID).	Store	No PII; just GUID.	Super Admin, University Admin	3 years
timestampUtc	When the action happened in UTC.	Store	Full ISO 8601 timestamp.	Super Admin, University Admin	3 years
actorUserId	Internal user id from users.xml.	Store	Internal id only; not shown to end users.	Super Admin only in UI	3 years
actorRole	Role of actor (SuperAdmin, UniversityAdmin, Helper, Participant, System).	Store	No redaction.	Super Admin, University Admin	3 years
actorEmail	Email address of actor.	Store	Shown only in admin UIs; never sent to participants.	Super Admin, University Admin	3 years
actorDisplayName	Short name for easier reading (e.g., "Jenna D.").	Store	No redaction.	Super Admin, Univers	3 years

				ity Admin	
actorUniversity	University of actor (e.g., "Arizona State University").	Store	No redaction.	Super Admin, University Admin (own)	3 years
category	High-level group (Auth, Consent, Catalog, Helper, Security, System).	Store	No redaction.	Super Admin, University Admin	3 years
actionType	Action key (e.g., ParticipantConsentAccepted, NewUniversityCreated).	Store	No redaction.	Super Admin, University Admin	3 years
targetType	What was touched (ParticipantAccount, HelperAccount, Event, Session, etc.).	Store	No redaction.	Super Admin, University Admin	3 years
targetId	Internal id of target (user id, event id, etc.).	Store	No redaction.	Super Admin, University Admin (own)	3 years
targetLabel	Friendly label (e.g., "Abby N. – Event #23").	Store	Keep non-identifying when possible (first name + initial).	Super Admin, University Admin	3 years
clientIp	IP address where action came from.	Store (truncated)	Store raw in file, but UIs show only truncated (e.g., 192.0.2.*,	Super Admin, University	1–3 years

			2001:db8:****:****).	Admin	
userAgentHash	Hash of user-agent string for device grouping.	Store (hashed)	Store SHA256 hash only; never full UA string.	Super Admin, University Admin	3 years
consentVersion	Version string when action relates to consent.	Store	No redaction.	Super Admin, University Admin	3 years
severity	Severity level (Info, Warning, Critical).	Store	No redaction.	Super Admin, University Admin	3 years
<notes>	Short human note explaining the action.	Store (short)	Max ~240 chars; never store message bodies, quiz answers, or sensitive content.	Super Admin, University Admin	3 years
<meta>/<item key>	Extra key/value pairs (non-sensitive).	Store (safe only)	Only store coarse info like counts, versions, IDs; no free-text from participants.	Super Admin, University Admin	1–3 years

1.2 Redaction Rules by Area

The table below describes which fields must be logged and which details must be excluded or redacted for each key area.

Area / Event Type	Log These Fields	Never Log / Must Redact
Participant consent (#158)	All actor fields; category=Consent; actionType=ParticipantConsentAccepted; consentVersion; clientIp; device hash in userAgentHash; meta count of checkboxes or coarse consent options.	Full consent form text; detailed explanations typed by participants; any free-text answers. Only store that consent exists and its version.
Login & impersonation (#158, #173)	All actor fields; category=Auth; actionType=LoginSuccess / LoginFailed; basic IP; UA hash; failure count or lockout count.	Passwords, password hashes, full JWT/session IDs, and full user-agent strings.
University switch (#158)	All actor fields; category=Auth; actionType=SuperAdminSwitchedUniversity; targetType=University; university IDs or codes.	Lists of participants or detailed user lists; keep only codes and IDs.
Course catalog changes (#163–166)	Who performed the change; role; action (CreateCourse, UpdateCourse, DeleteEvent, PublishCourse); target IDs and short titles.	Full course content text; syllabus details; entire lesson descriptions (not needed for audit).
Helper spot-checks (#168–169)	Who verified; helper id and optional name; which log (delivery/checkin/note); decision (Verified, Questioned); short admin note.	Full participant help note text; detailed one-to-one conversation content; anything that could identify sensitive situations.
Password resets & account lock (#160, #177)	Who triggered the reset or lock; target account (email, id); action; timestamp; IP; severity.	New password values; reset tokens; security answers; any

		credential-like data.
Monitoring & alerts (#173)	Counts of failed logins; spikes in denied access; impersonation attempt counts; links to related entries via IDs or correlation IDs.	Individual payloads; full URLs with query parameters; full error stack traces.
Session changes & notifications (#174)	Admin; event/session IDs; concise change summary (old vs. new time/room); counts of affected enrollments and waitlisted participants.	Individual participant names or emails in the audit row. Detailed per-recipient notification text belongs in messaging/notification XML if needed.

Retention Policy: The default retention is 3 years (1095 days), configured as *<auditLog retentionDays="1095">* with automated pruning on write. Critical security events can be tagged with *severity="Critical"* and optionally exempted from automatic pruning or archived separately.