



Case Files Professional

Illustrated Operations Manual

Commercial Edition

Installation | Casework | Field operations | Reports
Research | Billing | Client delivery | Recovery

A practical guide for administrators, case managers,
investigators, accounting staff and clients

Version 3.4.0

Includes the October 15 2026 packaged review fixes

Illustrations use fictional records

Contents

Select a chapter title or use the PDF bookmarks.

01 How to use this manual	4
02 Administrator quick start	5
03 Case manager quick start	6
04 Investigator quick start	7
05 Client quick start	8
06 Navigate the workspace	9
07 Use the current case tab order	10
08 Roles and access boundaries	11
09 Companies contacts and account lifecycle	12
10 Agency identity login and security	13
11 Prepare a new installation	14
12 Install and verify the scheduler	15
13 Create a case and review conflicts	16
14 Review public requests and case activity notes	17
15 Manage status closure and reopened efforts	18
16 Assign people and protect contact access	19
17 Record subjects people and vehicles	20
18 Schedule tasks and update task status	21
19 Use the Investigation Workspace	22
20 Plan investigations and keep field logs	23
21 Record findings and interviews	24
22 Request client scope authorization	25
23 Set safety check-ins and respond to alerts	26
24 Review the case timeline and quality checks	27
25 Upload documents and control client release	28
26 Configure Case Cloud and Dropbox paths	29
27 Register evidence and document custody	30
28 Preserve originals create copies and apply holds	31
29 Manage legal claims and IME records	32

Contents continued

Select a chapter title or use the PDF bookmarks.

30 Create review and attach scene diagrams	33
31 Draft reports and add daily observations	34
32 Approve release combine and export reports	35
33 Release final videos and create client delivery links	36
34 Prepare selected case packages	37
35 Use AI draft assistance and maps	38
36 Run and review Public Background Research	39
37 Use Training and Development	40
38 Enter time expenses and corrections	41
39 Manage pay rates payroll records and metrics	42
40 Configure invoice identity and delivery	43
41 Create invoices with or without a case	44
42 Issue edit and delete invoices	45
43 Send invoice notices and reminders	46
44 Write readable invoice email templates	47
45 Record payments and issue receipts	48
46 Review client invoices and payment links	49
47 Review budgets and accountant registers	50
48 Configure notifications and SMS rules	51
49 Publish personnel verification carefully	52
50 Create verify and retain backups	53
51 Import and restore an archive	54
52 Recover an interrupted operation or host	55
53 Apply updates and manage the domain license	56
54 Troubleshoot records mail and payments	57
55 Troubleshoot files diagrams and recovery	58
56 Agency maintenance checklist	59
57 Limits states and terms at a glance	60
58 Document maintenance and support	61

01 OPERATING PROCEDURE

How to use this manual

All users

Case Files Professional organizes agency work around case assignments, controlled records, reviewed deliverables and a financial audit trail. This manual covers the Commercial installation of version ^{3.4.0} with the packaged code review fixes dated October 15, 2026. Instructions refer to the application as packaged; your saved agency settings and user permissions determine the controls you see.

Read by role

Start with the role quick start, then follow the chapter for the work you need to perform. Administrators should also read installation, integrations, backups and recovery. An investigator does not need administrator access to carry out assigned field work. Clients should use their own quick start and the client invoice instructions.

Conventions

The location beneath each chapter title shows where to open the feature. Button names in procedures refer to application controls. Screen illustrations use fictional names and records; they explain control placement and workflow rather than reproducing a live client account. The PDF contents and bookmarks open chapters directly.

Record handling

Save changes before leaving a form. If a changed record warning appears, reload and compare the latest version before reapplying an edit. Do not bypass a protection message by changing database rows. Dates display as MM/DD/YYYY, while browser date pickers may follow device locale. Read timezone labels whenever entering or reviewing times.

What the manual does not promise

A saved credential is not a verified connection. Queued is not delivered, approved is not released, and a downloaded backup is not a proven restore. Verify the outcome named in each procedure. Legal references and research findings require source and identity review; the application does not determine their correctness or applicability.

Manual area	What you will find
Getting started	Installation role quick starts agency setup and access controls.
Daily operations	Cases field work evidence reports research time and billing.
Administration	Notifications protection updates recovery and troubleshooting.

02 OPERATING PROCEDURE

Administrator quick start

Agency Administration and Users and Permissions

An administrator establishes the agency environment, protects access and verifies that background services run. Use the full installer for a new empty environment and the appropriate patch or supported update process for an existing installation.

First session

1. Confirm the correct edition and domain. Set the agency identity, timezone, report branding and your own account security.
2. Configure agency SMTP in Agency Setup > Integrations and send a test. Password reset and operational emails depend on this delivery path.
3. Create staff users and client companies with their individual contacts. Assign the minimum roles needed; each contact receives an independent login.
4. Check Scheduler / Cron for both registration and a recent execution heartbeat. Correct the absolute PHP and application paths if the site moved.
5. Choose protected server storage or connect Case Cloud. Test a real transfer, retrieval and integrity result before relying on Dropbox.
6. Set up invoice branding, billing email delivery and any payment gateway separately from agency email. Test payments in the provider sandbox.
7. Create a fictional test case, assign a manager and investigator, and verify the client's view from a separate session.

Before operational use

Make and verify a full backup and store the private recovery material outside the server. Rehearse restore on an isolated environment with external payment and notification effects controlled. Verify protected application directories are not publicly readable.

Daily control

Review failed jobs, uncertain payment events, safety alerts, outbound errors and backup outcomes. A healthy dashboard does not establish that every external integration succeeded. Retain enough information to diagnose a failure without circulating credentials or private case files.

03 OPERATING PROCEDURE

Case manager quick start

Case Management and Field Operations

Case managers coordinate work on directly assigned cases. Administrator agency-wide visibility does not extend automatically to managers.

Open and assign

- 1. Review a Case Request or create a new case. Confirm the subject, client file, case type, requested scope and deadline. Check conflicts before operational work.
- 2. Assign the exact client contact, investigator and other staff who need access. Contacts sharing a company do not share case access automatically.
- 3. Create an Investigation Plan for the objectives and restrictions. Create Tasks & Schedule entries for appointments and field assignments; plans do not create calendar tasks automatically.
- 4. If additional work needs client approval, create a Client Scope & Authorization request addressed to the specific assigned contact.

Supervise and review

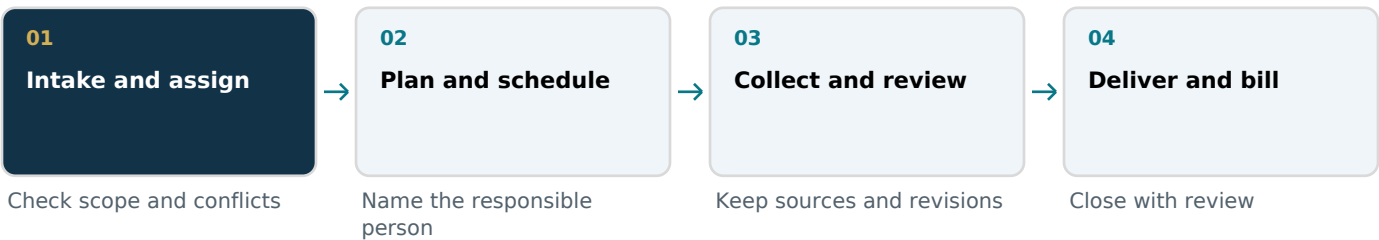
Review field logs, findings, evidence, interview records and safety deadlines. Follow up on missed safety check-ins directly. Acknowledge an alert only after reviewing it; acknowledgement is not the investigator checking in. Review submitted reports and timesheets. Return incomplete work with a clear correction reason. Approve reports when ready, then release explicitly when the client may see them. Select reviewed legal-record and diagram snapshots for reports rather than copying uncertain working notes.

Deliver and bill

Prepare only the intended client deliverables. Check final video links and report files using the client's permitted view. Create or review the invoice; issuing and sending are separate actions. Record only payments actually received and reconcile provider events before marking financial work resolved.

Close the effort

Use Closure Review to address incomplete tasks, reports, evidence disposition, integrity, time and finance checks. Save checklist progress while working. A closed effort remains locked. Reopening creates a separate suffixed effort and preserves the original; review the new assignments and deadline before continuing.



Illustrated example Case manager quick start

04 OPERATING PROCEDURE

Investigator quick start

Field Operations and assigned cases

Investigators work within their current case assignments. Some historical case material may be readable through an authorized later effort, but historical visibility does not make the earlier effort writable.

Before field work

1. Open the assigned case and read the current instructions, subject details, vehicles, location and restrictions. Confirm the active effort number.
2. Review the task start and end times and their timezone. Set or review a Safety Check-in schedule using the agency's escalation instructions.
3. Prepare the investigation plan or interview questions. Use Training & Development for the available field guides and blank forms.

During and after work

Record observations in Surveillance Field Log with actual event times and locations. Separate direct observations from reported information and conclusions. Add sources and limitations to findings. Record witness contact attempts, attributed statements and follow-up questions in the interview section. Upload files to the correct case. An uploaded document is internal unless management releases it. Store evidence through the evidence workflow and record custody changes; uploading a file alone does not document every custody event. Create the report for the correct investigation date. Review the chronology, photographs and references, then submit for management review. Enter actual field and travel hours and expenses in the timesheet and submit separately. Completing a task does not submit a report or timesheet for you.

Editing and deletion

The workspace permits edits to records you created or are assigned, subject to record and case locks. Scope requests, legal holds and conflict decisions require case management. Delete removes eligible workspace records from active lists while retaining signed prior revisions. An active hold can block deletion.

Finish safely

Check in or complete the safety schedule when work is finished. A phone losing connectivity does not notify a supervisor that you are safe. Use the direct escalation procedure when the application or email is unavailable.

05 OPERATING PROCEDURE

Client quick start

My assigned cases Scope Approvals and My Invoices

Each client contact has an independent account. Belonging to the same company as another contact does not expose that person's cases, invoices or authorization requests.

Sign in and review

1. Use the agency's Case Files address and your own login. If needed, use the password reset page; a reset email depends on the agency's configured mail service.
2. Open an assigned case. Reports and documents appear only after the agency releases the appropriate record. Internal drafts, evidence registers and investigative workspaces are not client areas.
3. Open Scope Approvals when the agency requests approval. Review every field, the requested budget, restrictions and agreement reference.
4. Confirm your authority and enter a decision note before approving or declining. The decision is recorded with your identity, time and version. Additional work may require a new request.

Invoices and payments

Use My Invoices from the dashboard header or Invoices & Payments. Open invoices can offer Pay Online when the agency enabled a gateway. Paid / Settled and Void are separate filters. The payment page is hosted by the selected processor; do not send card details in a case note or email. A browser returning from checkout is not by itself proof of payment. Check the posted balance and receipt after verification. If a result is uncertain, contact the agency with the invoice number and processor reference before trying again.

Shared video links

A separate delivery URL may have its own password and expiry. That password is distinct from your login password. A delivery-link visitor is not necessarily an authenticated client account. Only the files permitted on that link are available.

Access changes

Inactive accounts and inactive companies lose access. Contact the agency if a case or document you expected is unavailable. Do not use a colleague's account to bypass the assignment process.

06 OPERATING PROCEDURE

Navigate the workspace

Dashboard left menu and case folder tabs

The left menu groups agency-wide modules. Case folder tabs keep the current case context while moving between subjects, reports, documents, tasks, invoices and the Investigation Workspace. A logo click returns to the dashboard.

Find a case

Use the header case search for a case number, a partial case number, or a claimant or subject name. For example, 1003 can match a case number containing those digits. Search is restricted to case numbers and claimant or subject names; it is not a general phone, address or document-content search. Results remain limited to your authorized cases.

Read the case header

Confirm case number, effort suffix, case type, status and priority before entering work. The return button in the main header opens the case overview. Redundant return links beneath the tabs have been removed from the updated case-record pages. Legal, Claims & IME uses its own record-category tabs below the case navigation.

Small screens

Open or close the sidebar with the menu button. Scroll inside the menu to reach lower items. On a phone, forms and action groups wrap; wide tables may scroll horizontally within their container. Check the complete row before choosing an action. Do not assume a partly visible column is empty.

Dates and save results

Display dates use MM/DD/YYYY. Native date controls may visually follow the device locale; saved values retain their required internal format. Times may use the selected user or agency timezone as labelled. Read the label instead of assuming all screens use the phone's timezone. Save confirmations refer to the action just completed. A changed-record warning means another version was saved; reload before editing again. Confirmation dialogs offer Confirm Delete and Cancel. Deletion behavior depends on the module and can preserve audit records or reject protected records.

CASE FILES PROFESSIONAL Search Cases

Sample User

Dashboard

Calendar

Case Management

Field Operations

Finance & Billing

2026-1003 | Sample subject

Overview

Reports

Documents

Workspace

Confirm case and effort before entering work

Use the left menu for modules and folder tabs for this case

Illustrated example Navigate the workspace

07 OPERATING PROCEDURE

Use the current case tab order

Case folder navigation

The full internal case navigation follows the order below. Role and case permissions still determine the subset visible to each person. Client-specific Scope Approvals and Shared Documents labels remain appropriate to the client view.

Move between modules

Open the intended case and confirm its number and effort suffix before selecting a tab. Changing tabs retains the case context. Some pages have a second row of category tabs such as Criminal Matters and Civil Matters; those categories do not change this main case sequence.

Visibility and layout

Managers and administrators see the controls permitted by their role and assignment. Investigators, accounting users and clients see fewer items. On narrower screens the row wraps; read left to right, then continue on the next row. The menu and folder-tab styling remain unchanged.

Position	Case tab
01	Overview
02	Subjects
03	Tasks & Schedule
04	Vehicles
05	Legal, Claims & IME
06	Evidence
07	Scene Diagrams
08	Research & AI
09	Case Documents
10	Reports
11	Timesheets
12	Notifications
13	Assignments
14	Billing
15	Client Videos
16	Activity
17	Investigation Workspace
18	Closure Review

08 OPERATING PROCEDURE

Roles and access boundaries

Users and Permissions

Roles determine the kinds of actions available. Assignments determine which cases and records a user can reach. Share only the assignments needed for the work; a company relationship is a billing and contact structure rather than a blanket access grant.

Operating rules

Administrators can manage agency configuration and cases across the installation. Case managers coordinate their assigned cases. Investigators use assigned field and reporting functions, with additional ownership restrictions on some drafts. Accounting handles authorized financial work without becoming an investigator. Clients receive assigned and explicitly released material.

Company and record checks

The exact billed client owns the registered-client invoice view. Another contact at the same company does not inherit it. Client authorization requests name a specific assigned contact. Public delivery URLs grant only their permitted content and do not create a client account. Remove obsolete assignments when work ends. Deactivate accounts when access should stop. Closing a case locks its operational records; it does not mean the data was deleted. Investigators cannot use a historical relationship as permission to change a closed effort.

Check access with a second session

Create a fictional case and verify the intended view as a manager, investigator and client. Confirm that the client cannot open internal documents or draft reports and cannot see a colleague's case. Test real account deactivation and company status controls on sample accounts before relying on them.

Role	Typical responsibilities	Important boundary
Administrator	Agency setup users protection and system controls	Manage agency configuration protection users and cases across this installation.
Case Manager	Assigned case planning review release and supervision	Does not automatically see every agency case.
Investigator	Assigned observations reports evidence and own time	Scope holds and conflict decisions require management.
Accounting	Authorized invoices payments approved time and accounting	No internal Investigation Workspace access.
Client	Assigned released deliverables invoices and own approvals	No drafts or other company contacts records.

09 OPERATING PROCEDURE

Companies contacts and account lifecycle

Clients and Companies and Users

Create one company for an organization, then create or attach its individual client contacts. Each person keeps a separate username, password, account status and case assignments.

Create the structure

- 1. Open Clients & Companies and add the company. Enter its shared company and billing identity and address.
- 2. Add a new client contact from the company or link an existing client account. Verify the person's email and active status.
- 3. Use the company selector to narrow the client contact choices when assigning a case or creating an invoice. Save the exact contact doing business with the agency.
- 4. Confirm the contact on the resulting case and invoice. Company selection does not substitute for a case assignment.

Make a company inactive

An administrator can use Make Inactive on the company. All linked client accounts become inactive, existing sessions are invalidated and pending client notifications are cancelled. Cases, invoices and assignments remain recorded. A contact linked later to an inactive company also becomes inactive.

Reactivate deliberately

Activate Company activates every linked client account, including contacts previously inactive on their own, clears their separation dates and invalidates old sessions. Previously cancelled messages are not automatically restarted. Review the contact list after reactivation and individually deactivate anyone who should remain inactive.

Staff accounts

Users separates Administrators, Case Managers, Investigators, Clients and Accounting. Maintain role, employee or vendor identifiers and lifecycle dates where used. Security changes can invalidate existing sessions. An inactive user needs the required separation information. A Personnel profile is separate from a login account and does not create one automatically.



One company record | Independent logins | Explicit case assignments

Illustrated example Companies contacts and account lifecycle

10 OPERATING PROCEDURE

Agency identity login and security

Agency Setup and My Account

Agency Profile controls the agency name, contact information, website, address, timezone and uploaded logo. Print & Report Branding controls the report letterhead, signature image, signer, title and license line. Invoice branding has its own settings.

Configure identity

1. Save the agency profile and verify the header and login page. The login uses the Case Files logo unless an agency logo is configured. Review the login and reset page after saving a new logo.
2. Upload suitable report letterhead and signature images and verify a real report export. Images have format and size checks; the agency logo and output images accept the displayed limits, normally up to 2 MB.
3. Review invoice branding separately. Editing the agency profile does not intentionally rewrite branding frozen into earlier approved reports or issued invoice snapshots.

Login protection

Use the CAPTCHA provider options in Agency Setup > Security. The available choices include Google reCAPTCHA and Cloudflare Turnstile. Choose the correct provider and its matching site and secret keys; keys from one service do not work with another. Register the actual serving domain and test login and password reset after saving.

Account protection

If authenticator enrollment is enabled, enroll through My Account and store the single-use recovery codes securely. Enabling the enrollment option does not automatically require every user to enroll. An administrator can use the account controls to reset a lost enrollment.

Session and password handling

Use unique account credentials and sign out on a shared device. Password reset depends on valid agency SMTP settings and the saved recipient email. Do not replace the database password hash to work around a missing reset message. First verify mail delivery, spam filtering and the account status. The copyright year updates dynamically. Copyright website links open in a new tab. Confirm the configured identity on the actual login and reset pages before operational use.

11 OPERATING PROCEDURE

Prepare a new installation

Hosting and the full installer

A full installer creates a new installation. It is not a migration tool and should not be run over an existing working database. Use a separate HTTPS test domain or subdomain and a new empty database when validating a new deployment.

Choose the package

Use the Commercial full installer for a fresh installation. It includes the Investigation Workspace and the packaged fixes. No separate patch is needed for a new installation. For an existing application, use its supported update procedure; do not run the clean installer over the working database.

Prepare hosting

The application requires 64-bit PHP 8.3 or newer and compatible MySQL or MariaDB hosting. Required PHP capabilities include PDO MySQL, OpenSSL, cURL, Fileinfo, mbstring, ZIP, DOM, XMLWriter, GD, iconv and ctype. The installer checks requirements; resolve failed checks before continuing. Use a dedicated database and user with the required schema and record privileges. Keep config and storage writable by the hosting account with restricted permissions. Allow enough disk space for local files, encrypted archives, staging and safety snapshots, not just the ZIP size.

Protect private paths

Apache must enforce the supplied .htaccess rules. Other web servers need equivalent restrictions for app, config, database, storage, vendor, docs and cron, and for sensitive configuration, SQL, log and archive files. Test that protected files return a denial rather than their contents.

Keep recovery available

Retain an independent hosting backup before changing an existing domain. Keep LicenseHub product and activation details available. Do not copy production credentials into a different installation merely to make a test site open; licensing, domain identity and encryption keys are installation-specific controls.

Material	Use
Commercial full install	Fresh installation with the normal installer and a new empty database.
Review notes and tests	Reference material only; do not upload to the live application.
This manual	Reading training and operational reference; it does not install software.

12 OPERATING PROCEDURE

Install and verify the scheduler

Installer and Agency Setup > Scheduler / Cron

Upload the chosen full package with its directory structure intact. Open the installer on the intended HTTPS domain. The serving domain and installation path must match the installation identity.

Run the wizard

1. Enter the actual domain, product key and one-time activation code. The installation folder is detected. There are no default login accounts.
2. Choose manual database credentials or supported cPanel provisioning. Use complete prefixed database and user names where your host requires them.
3. Enter agency identity, timezone and the first administrator. Use a password satisfying the displayed requirements, at least 12 characters.
4. Set the actual PHP CLI binary when needed. The installer attempts scheduler registration without replacing unrelated cron jobs.
5. Finish and sign in. Test SMTP, save branding and confirm the edition before creating operational cases.

Verify cron execution

Open Scheduler / Cron and inspect registration and heartbeat separately. An installed entry is not proof that its command ran. Use the exact command shown by this installation; the binary and application paths depend on the hosting account. The regular dispatcher runs every five minutes and handles due work, notifications and protection tasks.

If installation is interrupted

Follow the displayed recovery instructions. A nonempty database is rejected intentionally. If cPanel provisioning fails before schema or activation, the wizard may permit switching to manual credentials through its recovery path. Do not delete database contents, journals or installation state simply to retry.

Existing installations

Back up first, replace the files named by the appropriate patch in the existing application root, and complete any prompted Database Upgrade. The protected upgrade workflow makes its safety backup before adding required tables. Preserve installed.php, storage, keys and credentials. Do not extract into a separate nested folder and expect the live application to change.

13 OPERATING PROCEDURE

Create a case and review conflicts

Case Management > Case Overview > New Case

A case records the investigation type, requested work, subject and client context. Verify the intended matter before saving because numbering and effort identity are controlled records.

Intake procedure

1. Review a public Case Request if one exists. Confirm the requesting person's authority, contact details and requested service using the agency's intake process.
2. Use Check Conflicts Before Opening a Case. Search names, aliases, client names and organizations. An administrator can search across the agency; a case manager's results are limited to directly assigned cases.
3. Select the case type and enter its required intake fields, subject or claimant, client file, deadline, priority and instructions. Verify spelling and dates.
4. Choose the correct company and individual client contact where offered. Save the case and record its generated number.
5. Review the case overview, then add the necessary staff and client assignments. Confirm that the investigator can open the active effort.

Conflict decisions

A zero search result does not establish that there is no conflict. A case manager cannot clear an agency-wide conflict solely from a scoped result. Record the names checked, review decision and restrictions under Investigation Workspace > Conflict Reviews. Restrict operational work according to the documented decision.

Numbers and types

Annual case numbering begins at YEAR-1000 and is allocated by the system. Do not reuse or manually change an existing number. Case-type definitions are saved with the case so later catalog changes do not silently replace the recorded intake definition.

14 OPERATING PROCEDURE

Review public requests and case activity notes

Case Management > Case Requests and case activity controls

The public request page collects an inquiry. It does not automatically create an active case, grant a client login or establish that work has been accepted.

Handle a request

1. Publish the supported Public request link from Agency Setup where the agency wants inquiries. Verify the destination before linking it from an external website.
2. Open Case Requests as an administrator or case manager. Read the submitted details and verify the requesting person's authority and contact information through the agency's intake process.
3. Mark the request New, Reviewed or Closed as appropriate. Create the actual case through the normal intake workflow after acceptance, conflict review and verification.
4. Delete an unwanted request into Trash using confirmation. Restore returns it as New. Do not confuse a request status with the status of a separately created case.

Use case notes

The case's Add Activity / Note quick action opens the internal case-note workflow. Record the narrative in the correct case with an appropriate title and timing. A note is not automatically a released report or a client message. Follow the page's edit, review and case-state restrictions.

Read the audit activity

The case Activity view lists the latest one hundred case events with local time, actor and action. It does not reproduce private notes or complete narratives in the event details. Open the underlying record for its content. Use the Investigation Workspace timeline when comparing operational records across sources.

Verify meaning

An audit event records an application action; it does not independently establish that an external observation or communication occurred. A submitted public inquiry is source information needing review. Preserve the original context and create the proper case, task or report rather than treating an intake or audit row as a completed investigation.

15 OPERATING PROCEDURE

Manage status closure and reopened efforts

Case Overview and Closure Review

New, Active / Working, On Hold, Closed and Cancelled describe different stages of an effort. They are not interchangeable deletion commands. Closed and cancelled operational facts remain locked.

Update a live effort

Review the latest record before changing status or instructions. Save the intended reason and review any triggered notification choices. An On Hold case is distinct from a legal preservation hold: the latter is an administrative deletion and disposition protection in Investigation Workspace.

Close with review

1. Open Closure Review and inspect each reported issue. Resolve incomplete report review or release, evidence integrity and disposition, open tasks, outstanding time or expenses, and applicable financial gates.
2. Save checklist progress if the review is not finished. Saving a checklist does not close the case.
3. Complete the required attestations and close from the case status controls when the gates permit it. Confirm the final status and audit event.

Cancel carefully

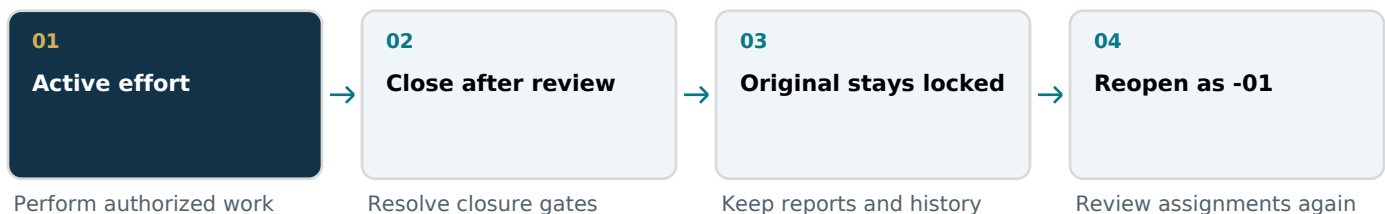
Cancellation requires an explanation and resolution or voiding of unfinished time entries. The workflow cancels unfinished tasks and applicable pending case messages. It preserves the case and its history. Resolve financial consequences separately; a case cancellation does not refund a processor transaction.

Reopen as another effort

Reopening creates a new suffix such as -01 or -02 while keeping the closed original. Review copied people, vehicles and reusable reference records. Reports, evidence, operational logs, timesheets and tasks are not simply duplicated as new work. Investigators require new assignments; active non-investigator assignments may carry forward. Enter and confirm the new deadline.

Preservation

Administrators and managers can add or release an administrative legal hold even on a closed or cancelled case, with the required reason. This exception does not unlock ordinary investigative facts or erase prior records.



Illustrated example Manage status closure and reopened efforts

16 OPERATING PROCEDURE

Assign people and protect contact access

Case > Assignments

Assignments are the main boundary for case access. A user role permits a kind of work, while an assignment establishes the user's relationship to this effort.

Assign the team

1. Open the correct active case and Assignments. Choose active accounts for the roles needed on that effort.
2. Select the responsible manager and investigator. Add accounting only when financial access is needed.
3. Select the client company and the exact contact. Do not assume adding one contact adds everyone in that company.
4. Save and verify the resulting list. Check notification choices and the investigator's active account and SMS preferences before expecting an assignment text.

Revise assignments

Remove obsolete assignments when responsibilities change. The application rechecks active assignment on later requests and delivery paths. A removed assignment can also remove inherited history access through that relationship. Review outstanding tasks and scope requests so their assigned person remains appropriate.

Historical access

Authorized users can sometimes read earlier efforts through a later assigned effort or supported case relationship. Earlier efforts remain read-only. The Investigation Workspace requires direct access to the selected case, not merely inherited visibility into another effort's history.

Company and billing separation

An invoice has its own billed contact. A registered-client invoice must remain within that exact client's authorized context. Company identity can supply a shared bill-to address, but it does not create a shared login. If several contacts need one case, assign those contacts explicitly through the supported assignment controls.

Verify the result

Use a separate session for a test client and investigator. Confirm that the expected case opens and that another company's or colleague's records do not appear. If a case is unavailable, first check account activity, company status, role and current assignment before changing permissions more broadly.

17 OPERATING PROCEDURE

Record subjects people and vehicles

Case > Subjects and Vehicles

Subjects & People stores claimants, subjects, witnesses, attorneys and other contacts associated with a case. Use the appropriate involvement type and identify the source of the details entered.

People procedure

1. Enter the person's name, aliases and available identifying details accurately. Add DOB only when supported by the case information.
2. Save address, phone, email and descriptive details in their intended fields. Review similar names before linking a witness or research request.
3. Upload the appropriate protected photo if available. A photo can support human review; it is not sent for automatic facial identification.
4. Review the saved row. Age displays in completed years from the saved date of birth; it is not a separate verified identifier or a substitute for DOB.

Vehicles

Enter vehicle details manually or use the supported VIN lookup. Review the decoded fields against the actual source. A partial decode does not establish ownership or the identity of the person driving. Optional licensed vehicle images are representative reference images, not photographs of the claimant's actual vehicle.

Use in other modules

Interviews can link a related person on the same case. Public Background Research lets you choose which saved identifiers to send after authorization; private notes, case documents, case number and the local photo are excluded from that request. Saving research does not silently replace the person's profile.

Correction and deletion

Use Edit to correct the record when authorized and the case is writable. Subject deletion and related upload deletion can be blocked by preservation rules or an active legal hold. Do not remove a source record merely because a name was corrected; preserve the relationship and document the correction through the permitted workflow.

18 OPERATING PROCEDURE

Schedule tasks and update task status

Case > Tasks & Schedule and left menu Calendar

The case task area uses records with Add Task, Edit and Delete controls. The left menu calendar displays the same task schedule; it is not a second independent record to update.

Create and review

- 1. Choose Add Task on the correct case. Select an eligible active assigned investigator.
- 2. Enter location, start, end, instructions and priority. The task label follows the case type. Confirm the selected timezone. End must follow start and the duration cannot exceed seven days.
- 3. Choose email or SMS notifications deliberately. Save and confirm the task row and calendar placement.
- 4. Use Edit to revise permitted fields and the status. New tasks begin as Scheduled. Completion or cancellation changes require the displayed note.

Work the assignment

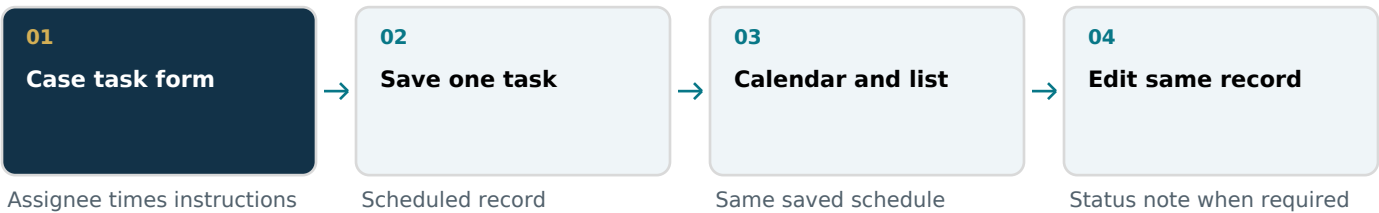
Scheduled work can move to In Progress or Completed through its permitted controls. Cancellation requires management where the workflow restricts it. Record what was done in the completion note. Report submission, timesheet submission and evidence entry remain separate actions.

Delete and calendar use

Authorized managers can delete an eligible task using Confirm Delete. This removes it from active scheduling and cancels its pending task messages while retaining its record and audit context. An active legal hold can block deletion. Closed or cancelled cases keep their normal write restrictions. Use calendar month controls or the schedule list to review timing. An ICS download exports an event; importing it into a device calendar may disclose its contents to that calendar service. It does not create a two-way sync, send invitations or update itself after a later case edit.

Appointment-derived tasks

A legal or IME record can provide an appointment task draft. Review and save it. Later changes to the source appointment do not silently move the task; update the saved task intentionally.



Illustrated example Schedule tasks and update task status

19 OPERATING PROCEDURE

Use the Investigation Workspace

Case > Investigation Workspace

The workspace groups internal planning, observations, sources, interviews, approvals, safety and preservation. It is included in both editions. It does not replace Tasks & Schedule, reports, the evidence register or invoices.

Common record procedure

1. Choose the required tab and Add the named record. Enter a meaningful title, narrative, state, assigned team member and relevant timestamps.
2. Complete the section-specific fields. Select same-case source files, evidence, reports or other workspace entries where useful.
3. Save and inspect the resulting record and version. The list provides row-level Edit and Delete actions according to permission and state.
4. Use Edit for a correction. An update preserves the prior signed revision. If a stale-version warning appears, reload before applying the intended change.

Deletion and immutable decisions

Delete archives an eligible entry from active lists rather than erasing its signed history. Safety deletion resolves its associated active alerts. Scope deletion invalidates obsolete pending decisions and notifications through state/version checks. An approved or declined client decision is not editable; additional authorized work uses a new request. An active legal hold prevents deletion until properly released.

Access

Administrators retain agency-wide access. Managers and investigators need direct case assignment. Investigators can edit only records they created or are assigned, and cannot manage scope, holds or conflict decisions. Accounting does not gain access. Clients only receive their own assigned scope requests.

Choose the right record

Use a plan for objectives, a task for a scheduled assignment, a log for an event, a finding for a supported proposition and a report for reviewed delivery. Completing one does not automatically complete or publish the others.

Tab	Record focus
Investigation Plans	Objectives steps restrictions and progress
Surveillance Field Log	Arrival observation lost contact break and departure
Findings & Sources	Basis confidence limitations and linked support
Witnesses & Interviews	Contact attempts attributed statements and follow-up
Client Scope & Authorization	Exact contact budget restrictions and decision
Safety Check-ins	Next deadline instructions and optional location
Legal Holds	Preservation duty and documented release
Conflict Reviews	Search terms decision and restrictions

20 OPERATING PROCEDURE

Plan investigations and keep field logs

Investigation Workspace > Plans and Surveillance Field Log

Plans describe what to establish and how to approach the work. Field logs describe what happened. Keep the two records distinct so an intended step cannot be mistaken for a completed observation.

Investigation Plans

Create a plan with the objective, unanswered questions, investigative steps and completion criteria, restrictions and due date. Assign an active team member when appropriate. Use Open, In progress, Completed or Cancelled to track the plan. Create separate plan records for independently assigned objectives. A plan does not automatically create a calendar task. If a step needs a scheduled appointment or field assignment, create a task and verify its assignee and schedule separately. Update the plan when the objective is completed or changed.

Surveillance Field Log

1. Choose Arrival, Observation, Lost Contact, Break or Departure, or add a field-log entry from the tab.
2. Enter the actual observation time and location. Review end time when an interval is recorded; it cannot precede start.
3. Describe activity, vehicle or direction and weather or conditions as appropriate. Distinguish what was seen from what was inferred.
4. Attach supporting material or cite authorized source records from this case. Save and confirm the chronological placement in Case Timeline.

Time and narrative checks

Entries use the signed-in user's selected timezone as labelled and store UTC internally. Record event time rather than relying on the save time. Quality checks can flag overlapping non-break field-log intervals and activity outside a report date, but they cannot establish what occurred.

Report use

Internal logs do not automatically publish to clients or overwrite report narratives. Use them to prepare an accurate report, verify chronology and cite support. Correct an error through Edit so the prior revision remains available; do not create a contradictory duplicate merely to conceal the earlier entry.

21 OPERATING PROCEDURE

Record findings and interviews

Investigation Workspace > Findings & Sources and Witnesses & Interviews

A finding is a proposition supported by identified material. An interview record preserves contact attempts, preparation, attributed information and follow-up. Neither should turn uncertain information into an established fact by changing its wording alone.

Findings procedure

- 1. Choose the appropriate state: Observed, Reported, Corroborated, Disputed or Unverified.
- 2. Describe the finding and its basis, corroboration or contradictory information. Explain confidence and limitations.
- 3. Select the same-case sources that support it. The system rechecks report and file access and rejects cross-case source IDs.
- 4. Save and review every linked source. Changing a source selection later does not erase the older revision's file reference or make the retained file disposable.

Interview procedure

Choose a related witness or person saved on this case. Record contact attempts, planned questions, the attributed statement, discrepancies and follow-up. The person's name is snapshotted with the interview so later profile changes do not silently rewrite that reference. Upload a supported recording or document where appropriate. Interview audio or video requires an entered recording consent or authority note. The application records that note; it does not determine whether the recording was authorized. No automatic transcription is included. Use Add Follow-up Task to open the normal task form, then save that task separately.

Files and corrections

Normal document upload limits apply, normally 25 MB and any lower hosting limit. Supported media include MP3, WAV, M4A, OGG, MP4 and WebM when their actual MIME type matches. Client Videos has a different final-delivery workflow and limit. Edit the record when permitted and review the retained history. Avoid saving conclusions merely because a source has a matching name. State conflicting identifiers and leave a finding unverified until it is supported.



Illustrated example Record findings and interviews

22 OPERATING PROCEDURE

Request client scope authorization

Investigation Workspace > Client Scope & Authorization

Scope requests document an exact client's decision about the proposed work and budget. They do not automatically change an invoice, billing rate or case budget.

Manager procedure

1. Add a scope request with the requested objectives, budget limit, restrictions and agreement or written-instruction reference.
2. Choose the exact active assigned client contact. All fields in this request are visible to that person, including its narrative and source note. Keep confidential internal strategy in another section.
3. Set Awaiting client approval and save. The request queues an agency email to the named contact, subject to current account, assignment and delivery checks.
4. Review the recorded decision. Use Review Billing Budget if approved work needs a deliberate update to the separate financial controls.

Client procedure

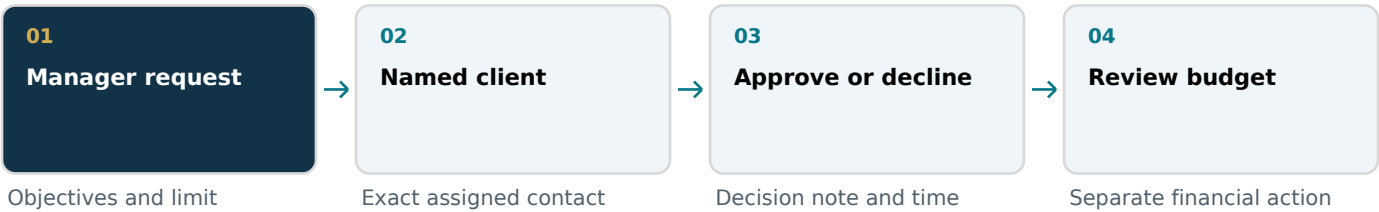
The assigned contact opens Scope Approvals, reviews the complete request, confirms authority and enters a decision note. Approve or Decline records the contact, time, version and note. The decision also queues a message to active administrators and assigned case managers.

Preserve decisions

Approved and declined requests cannot be edited into a different authorization. Create a new request for additional work or changed terms. Management can delete an eligible request from active lists while retaining its signed history; an active legal hold can block that action. A deleted or changed request invalidates obsolete approval notifications through its state and version.

Verify delivery and access

Another person at the same company cannot approve the request merely because of company membership. Inactive parent companies and removed assignments block the relevant delivery path. An email accepted by the SMTP service is not proof the client opened it or approved anything. Confirm the decision in the case record before treating requested work as authorized.



Illustrated example Request client scope authorization

23 OPERATING PROCEDURE

Set safety check-ins and respond to alerts

Investigation Workspace > Safety Check-ins

Safety schedules are an operational aid for the case team. They depend on the application, cron, connectivity and email. They are not emergency dispatch or continuous location tracking.

Set a schedule

1. Add a Safety Schedule on the assigned active case. Choose the responsible team member and a future check-in deadline.
2. Record supervisor contact and escalation instructions, plus a meeting point or location note where needed.
3. Save and verify the deadline and timezone. Confirm the supervisor knows the direct escalation procedure if the system is unavailable.

Check in and finish

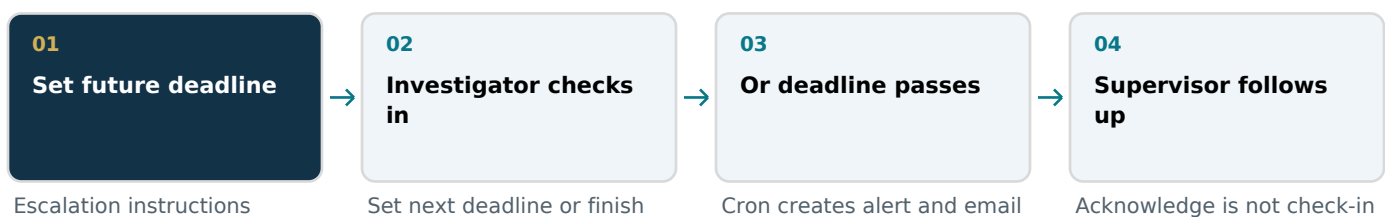
Use Check In & Set Next Deadline to record a check-in and move the next required deadline forward. Complete the schedule when safely finished. Acknowledging an alert as a supervisor does not itself record the investigator's check-in. Deleting an eligible safety entry archives the record and resolves its open or acknowledged alerts.

Optional location

Share My Current Location Once requests browser permission only after the user clicks it. The coordinates are entered into the form and sent to the case team only when the form is saved with the required consent. HTTPS and browser location permission are needed. There is no background tracking or automatic facial identification.

Missed deadline

On a later scheduler run, the system creates an in-app alert and queues agency emails to active administrators and assigned case managers. Duplicate notices for the same deadline are suppressed. New check-ins make earlier notices obsolete; closed or cancelled cases do not generate new safety messages. Review the last scheduler check and any error shown. Act on a missed check-in through the documented escalation instructions rather than waiting for repeated email. The workspace adds no separate automatic safety SMS rule; existing task and case SMS settings are a different system.



Illustrated example Set safety check-ins and respond to alerts

24 OPERATING PROCEDURE

Review the case timeline and quality checks

Investigation Workspace > Case Timeline and Report Quality

The unified timeline links observations and work records to their source. It combines workspace entries, report observations, reports, tasks, evidence and case audit events within the user's permitted view.

Use the timeline

1. Open the correct case and choose Case Timeline. Apply From and To dates when narrowing an effort.
2. Read the timestamp, record type, title or observation and state. Open the source record for the underlying facts and attachments.
3. Compare field-log times with task schedules and report activity. A scheduled task time is not proof the activity happened.
4. Use pagination for older entries. Date-only report records remain dates rather than shifting to the previous day through timezone conversion.

Run report quality review

Use the case-wide Report Quality tab or the report's Review & Release area. Checks flag missing narrative, dates or activity, possible name spelling inconsistencies, observations outside the report date, overlapping non-break field logs, attachment references without attachments and disputed or unverified findings needing review.

Resolve a flag

Read the actual source before changing anything. Correct an error in the editable source, or explain the limitation and follow the applicable report revision workflow. Do not remove an accurate uncertainty merely to clear a warning. Quality flags do not establish truth, completeness, legal sufficiency or that every inconsistency was found.

Visibility

Investigator report author restrictions remain in effect. A timeline link does not grant access to a source that is otherwise restricted. Closed or cancelled efforts remain read-only, and signed history remains part of the source record after a permitted correction or archival deletion.

25 OPERATING PROCEDURE

Upload documents and control client release

Case > Case Documents

Case Documents stores the actual file in protected server storage and, when configured, transfers it to Dropbox with a protected local mirror. Access and storage are separate concepts: Internal describes who may see it, not whether it is stored in the cloud.

Upload and review

1. Open the correct case, enter the document title and choose the actual file. Normal documents are limited to 25 MB, subject to a lower hosting limit.
2. Upload and inspect the saved row, storage result and actual file. An accepted upload is not proof of completed Dropbox transfer.
3. Keep working documents internal. An assigned manager or administrator can use Release to Client after reviewing the content.
4. Check the client's permitted view before delivery. Use the withdrawal control when future client access should stop.

Formats

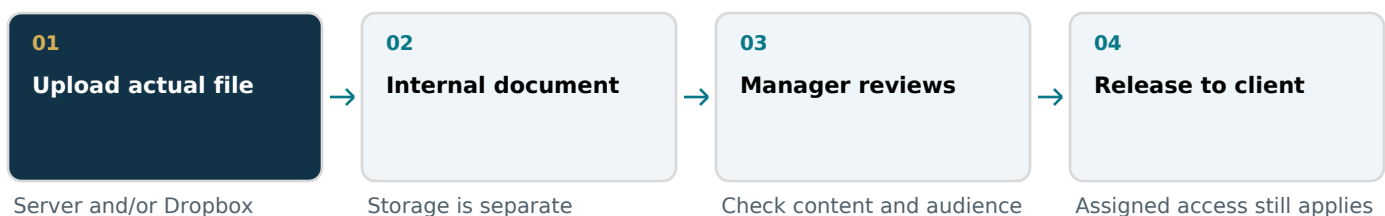
The general document workflow accepts supported PDF, DOCX, text, CSV, image and audio or video formats with matching content checks. A renamed extension does not make an executable or invalid image acceptable. Other upload areas, such as training and final videos, have their own supported formats and limits.

Delete with care

Delete appears beside the appropriate upload actions and uses Confirm Delete or Cancel. The server rechecks the user's authority, case state, legal holds and retained references. Evidence files, cited investigation sources, copy provenance, reviewed report associations and other retained relationships can prevent deletion. A permitted deletion is not a reason to erase source provenance outside the application.

Downloaded copies

Withdrawing a document or revoking future access does not recall a file already downloaded. Do not distribute a public server storage path. Use the authorized file route or the supported delivery workflow so the access checks remain active.



Illustrated example Upload documents and control client release

26 OPERATING PROCEDURE

Configure Case Cloud and Dropbox paths

Agency Administration > Case Cloud Connection

Case Cloud uses the agency's Dropbox application and authorization. It does not relocate historical files merely because the destination setting changes.

Connect and test

1. Configure the agency-owned Dropbox app and its authorization through the connection page. Use credentials and permissions matching that app.
2. Enter the desired folder with forward slashes, such as /Test or /Agency Case Files. Do not use Windows backslashes. Follow the displayed path and length validation.
3. Save, then perform the actual transfer test. Confirm upload, retrieval and hash verification rather than assuming a saved token is connected.
4. Review pending or failed transfers. Retain the local copy and retry through the supported action after correcting authorization or permissions.

App folder versus full account

With Dropbox App Folder access, API paths are relative to that app's assigned folder. If the app lives under /Apps/Case Files, entering /Apps/Test can produce a visible path beneath /Apps/Case Files/Apps/Test. To request a child called Test within that scope, use /Test. Reusing an older app does not turn an App Folder token into full-account access.

Existing file relationships

Changing the configured folder affects destination selection for new work; it is not a case migration and does not rewrite every stored remote path. Existing remote files and backup archives must be managed with the original account and recorded paths. Do not move them manually before planning how their stored relationships will be preserved.

Operational checks

Pending transfers keep private local mirrors. Storage availability and access visibility are reported separately. Backups have their own managed archive workflow. If a remote path is not found, preserve the local copy and inspect the stored account/path relationship before deleting or recreating records.

Dropbox App Folder scope

Visible Dropbox app root: /Apps/Case Files

Entered /Test Resolves under the app root as /Test

Entered /Apps/Test Adds Apps/Test inside that same root

Destination settings do not migrate recorded historical paths

Illustrated example Configure Case Cloud and Dropbox paths

27 OPERATING PROCEDURE

Register evidence and document custody

Case > Evidence

The evidence register records items associated with the case. The agency-wide Evidence Management list shows cases that have evidence entered. A register entry does not replace physical handling, collection notes or original source records.

Register the item

- 1. Add the reference, evidence type, custodian, storage location and collection time. Confirm the case number and subject.
- 2. For digital evidence, attach the preserved file through the supported workflow. Review the file identity and recorded hash.
- 3. Save and inspect the row. The list includes Reference, Custodian, Location, Disposition and Actions, with the case context.

Custody events

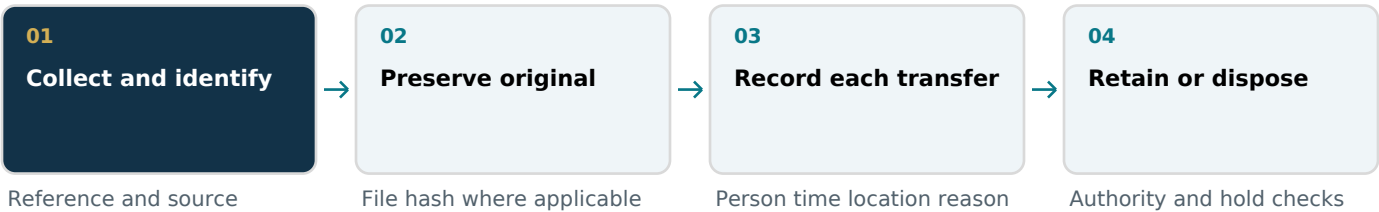
Record each transfer with the person responsible, time, location and authority or reason. Do not backfill a transfer as if it were contemporaneous without explaining the source of the entry. Use the existing custody controls so the signed chain remains linked to the item. Management records retention or final disposition when authorized. An active legal hold blocks final return, release or destruction, while documented retention and transfers remain available. Do not use upload deletion as a substitute for a custody disposition.

Integrity review

The application checks its keyed custody chain and preserved file integrity. A successful hash check means the checked bytes match the stored reference; it does not establish who created the original content or prove the underlying event occurred. A mismatch or unavailable result needs investigation and preservation of relevant storage and logs.

Client delivery and deletion

Internal evidence is not automatically published to clients. Use reviewed report attachments or an authorized selected package when disclosing appropriate material. Delete or removal controls can retain history and are blocked by preservation rules. Do not erase physical evidence or remote originals merely because a list entry was archived.



Illustrated example Register evidence and document custody

28 OPERATING PROCEDURE

Preserve originals create copies and apply holds

Investigation Workspace > Evidence Preservation and Legal Holds

Keep originals separate from working or redacted copies. Copy provenance and retained source relationships help explain what was used without overwriting the original file.

Verify and create a copy

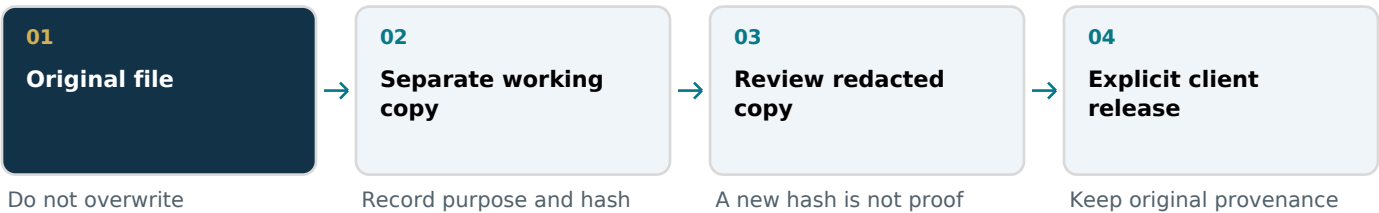
- 1. Open Evidence Preservation and inspect the recorded SHA-256 and latest result. Verify Now checks actual file bytes and size against the stored reference.
- 2. Choose an original, a copy type and a purpose or change note. A working copy can be created from the original; a modified or redacted copy must be prepared separately and uploaded.
- 3. Inspect the resulting internal case document. Review the content before client release. A changed hash proves different bytes, not complete redaction.

Scheduled integrity checks

The rolling sweep is enabled by default, checks up to two files per scheduler run and revisits due files after seven days or the next completed sweep. A large collection can take longer than a week. Cloud-only verification may download bytes and consume network resources. Administrators may disable the sweep while manual verification remains available. An unavailable result can reflect a missing file, transfer failure, connectivity or mismatched bytes. Do not label every failed check as tampering without inspecting the result.

Legal hold procedure

A manager or administrator creates an active hold with its preservation reason. It blocks covered record and upload deletions and final evidence disposal. To release, edit the hold and document the release reason. Prior revisions remain preserved. Holds can be administered on closed or cancelled cases without unlocking investigative facts. The hold protects supported application actions. It cannot prevent someone with direct hosting or Dropbox access from deleting bytes outside the system, and it does not replace the separate backup retention policy.



Illustrated example Preserve originals create copies and apply holds

29 OPERATING PROCEDURE

Manage legal claims and IME records

Case > Legal, Claims & IME

This shared case module records Criminal Matters, Civil Matters, Claims & Insurance, Independent Medical Exams and Attorneys & Case Contacts.

Create and review

1. Choose the record category and Add Record. Enter the related subject, source or document reference and the category-specific details.
2. For criminal matters, record allegations or charges as entered with jurisdiction and court details. For civil matters, record the claim or matter and its source. Preserve the difference between an allegation and an adjudicated outcome.
3. For IME work, review the appointment, deadlines, report and follow-up requirements. Use a supported appointment task draft only after verifying the proposed schedule.
4. Save the draft and submit or review through the category's controls. The agency-wide list shows only cases with relevant records.

Lists and corrections

Rows show Record, Status, Review / Revision, Dates and Actions, with the case number. Use Edit on editable records and the amendment process for reviewed material. Source review locks should not be bypassed by changing rows directly. Delete is available when authority, state and retention rules permit it. Prior report snapshots and audit context remain preserved. An active legal hold or a closed effort can block the action.

Use in reports

Select reviewed records explicitly when preparing a client report. The report keeps a snapshot rather than automatically following every later source change. Review the selected revision and client-facing caption before approval.

30 OPERATING PROCEDURE

Create review and attach scene diagrams

Case > Scene Diagrams

Scene Diagrams records the working illustration and its revisions. The agency-wide scene diagram list shows cases with saved diagrams, with Diagram, Revision, Status and Actions under the case context.

Build a diagram

1. Choose Add Diagram on the correct case. Give it a clear title describing the scene or purpose.
2. Use the available drawing, object, label and measurement tools. Record actual measurements and assumptions accurately; a diagram created from estimates should be described as illustrative.
3. Save and inspect the drawing at its intended output size. Check label spelling, orientation, references and any scale statement.
4. Submit and review through the available workflow. Management can approve or release the revision required for report use.

Attach to a report

Select the reviewed diagram revision and write a client-facing caption that explains what it shows. The report references that revision. Later working edits do not silently change a diagram already attached to a report.

Revision and deletion

Use Edit for permitted working changes and the revision workflow for corrections to reviewed work. Use Delete only when the diagram is eligible; Confirm Delete is a confirmation, not an override of a legal hold or preservation requirement. Existing report snapshots and review history remain significant even if an active list entry is removed.

Check the export

Preview or export the diagram independently before combining it with a report. Confirm that labels remain readable and that the diagram communicates the intended relationships. The application cannot verify that a measurement reflects a physical survey or that a symbol's placement is factually correct.

31 OPERATING PROCEDURE

Draft reports and add daily observations

Case > Reports > Create Report

Create the report on the correct case and effort, using its investigation date and type-specific profile. The agency-wide report area shows cases with saved reports rather than an empty report listing for every case.

Draft procedure

1. Choose Create Report. Verify the report date, title, subject, client references and profile.
2. Complete factual scope and narrative sections. For surveillance, enter the daily summary, video duration and chronological observations using actual times.
3. Add photographs and captions. Surveillance summaries support up to four photographs; each activity entry supports up to two. Check orientation and what each image actually depicts.
4. Select reviewed case-record and scene-diagram snapshots when needed. Inspect their selected versions and write appropriate captions.
5. Save the draft and preview it. Use the quality checks, verify chronology and resolve unsupported statements before submitting.

Daily reporting

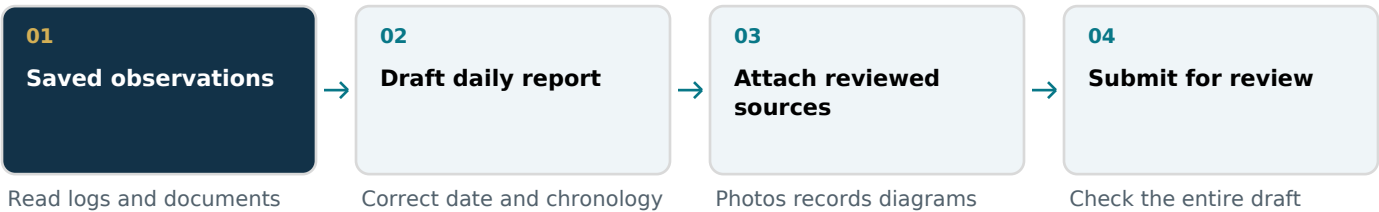
A report's date is a date-only record. Observation timestamps have timezone context. If saved daily entries exist, changing the report date may be blocked to keep the chronology consistent; create a new daily report when the work belongs to another date. Management-only first-date content stays with the primary report or revision chain.

Editing boundaries

Investigators prepare their own drafts within authorized cases. A manager can review and correct where permitted. Approved or released work uses a new draft revision rather than silently rewriting the approved report. Case closure and preservation controls still apply.

Narrative and uploads

Internal field logs and saved research are source material, not automatically approved report content. Review facts and attribution before transferring them into a narrative. Uploading a photo or selecting an attachment does not itself establish identity, accuracy or client release.



Illustrated example Draft reports and add daily observations

32 OPERATING PROCEDURE

Approve release combine and export reports

Report > Review & Release and case Reports

Save, Submit, Approve and Release are separate stages. Approval records management review; client visibility follows explicit release and the client's case permissions.

Review and release

- 1. Read the complete report, not only its summary. Verify names, dates, times, observations, photographs, captions, source snapshots and branding.
- 2. Return incomplete submitted work with a correction reason, or approve when ready. Resolve any quality flags with a source check.
- 3. Release the client version explicitly. Test that the assigned client can reach only the intended report and attachments.
- 4. For a correction after approval or release, create the supported draft revision, review it and release the correction deliberately.

Combine investigation dates

From the case Reports area, select the desired dates. Combine only reports from the same case and compatible profile. Choose the supported full or surveillance summary output and preview before downloading. Combining reports does not merge their independent source histories or make draft content client-visible.

Export formats

Use the supported Print, PDF and native Word controls. Exports follow the saved report data, selected revisions and branding context. Internal SIU analysis is excluded from public outputs where the profile marks it internal. Word, PDF and browser print can paginate differently.

Final output check

Inspect the actual downloaded file for page breaks, letterhead, signature, readable photographs, correct date order, omitted blank references and the intended report revision. Check a long report and real letterhead on the target host before regular use. The application preserving a snapshot does not mean every later correction has been delivered to recipients of an older downloaded copy.



Illustrated example Approve release combine and export reports

33 OPERATING PROCEDURE

Release final videos and create client delivery links

Case > Client Videos

Client Videos is the final delivery workflow. Original evidence and separate VideoPro processing remain distinct from the released client copy.

Prepare and release

1. As an authorized manager, upload the final MP4 with a client-facing title and description. The normal limit is 128 MB and lower hosting limits can apply. H.264 video with AAC audio is a suitable compatibility target.
2. Preview the actual saved file, including playback and seeking. Review content, storage and transfer state before release.
3. Use the release control with its required reason. Release does not itself send a delivery message.
4. Create a link for the exact active assigned client. Choose expiry, optional separate password, download permission and notes. Include only a released same-case report and an issued invoice for that client when attaching them.

Test and send deliberately

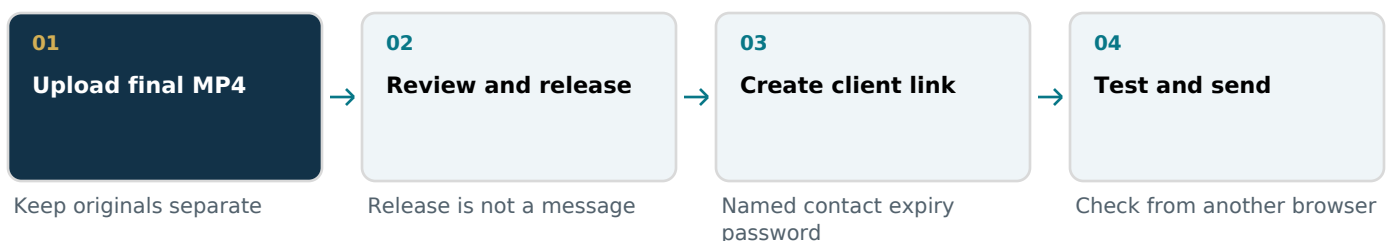
Open the unique link in a separate browser. Test password, expiry behavior, video playback, permitted downloads, report/invoice attachments and notes. Copy and send the URL through the agency's chosen channel; creating or copying it does not automatically email it. Send a delivery password separately from the link. A viewer note is shared with the case team but does not establish authenticated client identity. Viewer grants last thirty minutes; the visitor can reopen the original link afterward when it remains valid.

Revoke and protect

Revoke a link or withdraw the video to stop new access. Expiry, client activity, parent company status, assignment and related record state are rechecked. Already downloaded copies and in-flight transfers cannot be recalled. Keep original evidence under its preservation workflow rather than replacing it with a compressed delivery copy.

If playback fails

Check codec, file integrity, host upload/post limits, protected local mirror and the actual target browser. A completed cloud transfer is not proof that a particular device supports the encoding.



Illustrated example Release final videos and create client delivery links

34 OPERATING PROCEDURE

Prepare selected case packages

Investigation Workspace > Case Packages

Case Packages builds a ZIP of explicitly selected material for internal preparation or a named client audience. Package creation does not send the file or grant access to it.

Build a package

1. Choose Internal / counsel preparation or Selected client. For a client package, select the exact active assigned contact.
2. Select up to ten reports and thirty files, subject to the 200 MB total uncompressed limit. Select only what the recipient should receive.
3. For an internal package, optionally include evidence and custody indexes or workspace records with verified revision histories. Client packages reject those private indexes.
4. Confirm the selection and build the download. The system checks access and reads back ZIP contents before returning it.

Contents and integrity

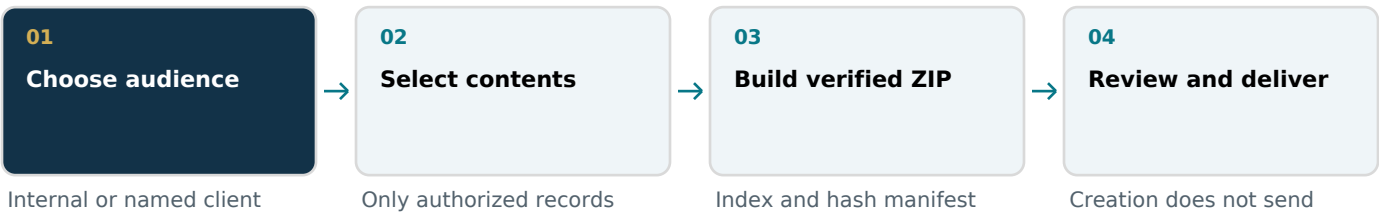
The ZIP includes selected report PDFs and files, a dated index, a SHA-256 manifest and a server HMAC manifest signature. The index identifies selected material; it does not imply every underlying exhibit is included. The HMAC is a server-side integrity record, not a public-key certificate or a guarantee of admissibility.

Review before disclosure

Open the ZIP privately and inspect every included item and the named audience. A client package uses that client's released-report and file permissions. It should not contain internal notes merely because the preparing manager can see them. Send through the agency's authorized channel only after human review.

If package generation fails

Check the selected records, file size, storage availability, integrity result and export requirements. A failure should not be worked around by copying an entire private storage directory. Narrow the selection or correct the underlying availability issue, then build again.



Illustrated example Prepare selected case packages

35 OPERATING PROCEDURE

Use AI draft assistance and maps

Case > Research & AI

Research & AI combines Public Background Research, AI Draft Assistance, Location & Directions and Research History. The left-menu research area shows saved case results within the viewer's permissions. AI generation buttons are intended for case and report work, not invoices or invoice settings.

Enable and request assistance

An administrator configures the agency's OpenAI credential, enables AI and chooses the exact model ID available to that account. A missing or disabled credential or model can make Generate AI unavailable. Saving a key alone does not prove the request can run.

1. Choose the task, such as drafting from supplied facts, summarizing, proofreading or reviewing a report. Review the text selected for transmission.
2. Confirm the required acknowledgment and submit once. Draft assistance sends entered text; case files and subject photos are not automatically attached.
3. Read the suggestion, verify factual content and choose Accept or Discard. Resolve a pending suggestion before saving where the form requires it.
4. If the source changes, obtain a fresh suggestion rather than applying stale text. Requests and results remain in authorized encrypted research history.

Maps and directions

Use the appropriate saved or entered location and review it before opening directions. Optional embedded maps or geocoding require the configured browser and server keys with suitable restrictions. Provider results do not silently correct the case address or establish occupancy or ownership.

Human review

AI text is a draft. Check names, times, figures, attribution, uncertainty and source support. Do not use generated prose to imply that an investigator observed something or performed a search that did not occur. Provider fees and availability belong to the configured agency account.

36 OPERATING PROCEDURE

Run and review Public Background Research

Research & AI > Public Background Research

This feature uses the configured OpenAI Responses API web search capability. It is not a Skopenow replacement, restricted database subscription or automatic facial-identification service.

Run the search

- 1. Select the saved subject or claimant from the case. Review name, aliases, DOB, calculated age, address, phone, email and identifying details.
- 2. Choose which identifiers to include and the research scopes: Court & Public Records, Business Affiliations, News and Public Social Media. A saved name is required.
- 3. Review the exact information being sent and authorize the request. When DOB is absent, a known approximate age can be supplied for this search.
- 4. Submit once and inspect the result. Private notes, case documents, case number and local photo are excluded from the provider request.

Review identity and sources

Every finding starts as Possible Match. Open the source URL, compare corroborating identifiers and contradictions, and enter reviewer notes. Use Confirmed by Reviewer only after a supported review, or Not Relevant when the item does not belong to this subject. A shared name or city is not enough. Public social research can find accessible profiles and posts but cannot guarantee every platform or record. Private, sign-in-only and restricted sources are outside that promise. Only source-linked findings supported by provider source metadata are shown.

Save to the case

Save individual findings, a selection or the draft summary. Not Relevant items cannot remain saved. Saved findings retain source links, dates, match state and reviewer notes in the encrypted case research record. They do not automatically change a subject profile or publish into a client report.

Uncertain results

Timed-out or uncertain requests are not automatically retried. Check provider usage and the record state before initiating another billed request. No findings does not establish no records. Review allegations separately from adjudicated outcomes.

Sample subject | Selected identifiers

Name

DOB

Address

Phone

Review what is sent

Possible Match

Review source

Record notes

Save to case

Public sources only | No automatic facial identification | Human identity review

Illustrated example Run and review Public Background Research

37 OPERATING PROCEDURE

Use Training and Development

Training & Development > Investigator Field Guide

Training & Development is available to administrators, case managers and investigators. Clients and accounting users do not receive the guide page, forms or downloads.

Read and download

1. Search for a topic or choose a guide category. Read the current guide and its reference links.
2. Open a video or reading link as appropriate. External availability can change; a stored reference is not a guarantee the provider still hosts it.
3. Download a blank form or sample report for the intended purpose. Print / Save PDF and editable Word downloads are available where offered.

Maintain the guide

Administrators and case managers can add or edit guides, reading links and video links and upload files. Investigators have read and download access. Only administrators can delete guides or files. Review a published edit and its attachments after saving; use the shared confirmation dialog for a permitted deletion.

Files

Guide uploads allow the displayed training formats, including PDF, DOC/DOCX, TXT, CSV, XLSX, PPTX and images. The limit is 15 MB per file and thirty files per guide. These are training-specific limits rather than the general case-document limits. Files are private on the server and mirrored to configured Dropbox storage. A failed transfer retains the server copy and provides Retry Dropbox upload. Full backups include private training files.

Included material and limits

The recovered field guide includes 32 original topics, 23 YouTube references and eight original blank forms or fictional sample reports. The supplied original backups did not contain every separate live-only training page or later attachment. The system does not claim to have recreated material that was absent from those sources. Keep agency-specific procedures current and verify external reading and videos before assigning training.

38 OPERATING PROCEDURE

Enter time expenses and corrections

Timesheets & Expenses and case Timesheets

Time records separate actual field hours, travel hours, mileage and expenses. They support approval, billing and payroll estimates; saving a time record does not pay a worker or charge a client.

Enter and submit

1. Open the correct case and work date. Enter field and travel hours to the required decimal precision, plus mileage and applicable meals, tolls, parking or other expenses.
2. Describe activity and work notes. Attach the appropriate receipt when available. Expense-only entries have zero hours.
3. If start, end and unpaid breaks are entered, reconcile them with declared hours. Combined active daily hours across cases cannot exceed 24.
4. Save Draft or Save & Submit for Approval. Confirm the saved state and responsible person.

Review and correct

Management approves or disapproves with a correction reason. Correct a returned record and resubmit. Managers can correct permitted nonapproved records while retaining ownership and history. Approved records require an audited correction draft; reconcile any invoice reservation before amendment. The application prevents duplicate active records for the same person, case and date. Superseded and voided records do not add to active totals. Do not create another active entry to bypass a correction or duplicate warning.

Export approved work

Use Approved Work Summary and the authorized person and date filters for Print, PDF, Word or financial CSV. Investigators see their own entries; accounting sees approved work within assigned case scope. Verify totals and receipts before using an export for billing or payroll.

Rates and status

Pay rates are separate from client billing rates. Approval makes work eligible for later financial workflows; it does not prove money moved. A case cannot be treated as financially complete solely because its field task was marked Completed.

39 OPERATING PROCEDURE

Manage pay rates payroll records and metrics

Work & Supervision > Payroll & Payments and Investigator Metrics

Payroll & Payments contains Pay Rates, Approved Work Estimate and Payment Ledger. Estimates and payment records have different purposes.

Set rates and estimate

Authorized administrators, managers and accounting users manage pay rates and ledger records. Set the worker's Employee or Vendor type where relevant. Approved-work estimates remain case-scoped even when rate management is agency-wide. Check approved hours, mileage and reimbursements before relying on an estimate. Pay rates do not change invoice billing rates automatically. Review the date range and worker before preparing a payment outside the system.

Record an actual payment

1. Choose the worker and enter the period, payment date, method, reference and amounts actually paid.
2. For employees, enter withholding or deductions manually where supported. Employee net uses gross plus reimbursements less those deductions.
3. For vendor 1099 records, review the gross paid amount; it excludes the employee-style extra amounts.
4. Save and verify the ledger. The application does not transmit payroll funds, compute every tax obligation or file tax forms.

Correct and review

Void an incorrect payment with a reason rather than deleting its history. Voided values are excluded from active totals. Investigators can review their own payment records but cannot post, void or change pay rates.

Metrics

Investigator Metrics uses approved recorded measurements and shows observation, video or usable-footage measures, task timeliness and optional review-score denominators. Review what is counted and the date/person filters. A high percentage is not an automatic quality judgment, and absent measurements should not be treated as proof of poor performance.

40 OPERATING PROCEDURE

Configure invoice identity and delivery

Finance & Billing > Invoice Setup & Settings

Invoice setup is separate from Agency Setup. It allows an invoice-specific logo, company identity, address, phone, email, website, tagline, contact details, terms and payment instructions. Accounting can view settings; administrators change them.

Set the invoice presentation

- 1. Open Invoice Setup and save the invoice identity and logo. Change or blank Invoice tagline to control the separate line under the agency name. Text embedded in a logo image must be changed in that image.
- 2. Review General & Terms and Numbering. Choose the supported payment terms, number format and next counter. Counters cannot simply move backward into used numbers.
- 3. Edit payment instructions as text. A statement about a fee does not automatically add that fee to the invoice calculation.
- 4. Check the resulting invoice before issuing. Earlier issued branding remains a saved snapshot; changing global defaults does not automatically rewrite it.

Use dedicated billing email

Billing Email Delivery controls the invoice From name, From address, Reply-To and optional separate SMTP transport. This can be different from Agency Setup email. Test the actual sender and delivery; a mailbox address alone is not SMTP authorization.

Templates and gateways

Configure Email Templates, Reminders, Overdue Emails and Receipts for their respective messages. Payment Options is the single editor for Stripe or Authorize.net credentials and webhook instructions; Agency Setup links there rather than requiring a second independent setup.

Initial defaults

The installer includes editable generic invoice, reminder, overdue and receipt templates. Set the billing contact name, email and phone before sending. Payment credentials are not bundled; enter the agency gateway credentials separately.

SAMPLE AGENCY

Invoice-specific logo address and contact details

INVOICE INV-2026-1003

Service	Quantity	Rate	Amount
Investigation services	4.00	100.00	400.00
Blank Case # or Client File # fields are omitted			

Illustrated example Configure invoice identity and delivery

41 OPERATING PROCEDURE

Create invoices with or without a case

Invoices & Payments > Create New Invoice

An invoice can belong to a case or stand alone. It can bill an existing client contact or use an email-only recipient without creating a login account.

Create the draft

1. Choose the case if applicable. Select the company and exact client contact, or No client.
2. For No client, enter the recipient in the displayed To email field. CC and BCC are available both with and without an existing client. A draft can be saved without a recipient, but Send requires a valid delivery address.
3. Review invoice and due dates, subject, client file and bill-to identity. Add service lines or supported approved work, then check quantities, rates, expenses, taxes, discounts and notes.
4. Save and preview the actual invoice details. Case-specific Billing shows the invoice list directly; the global invoice area retains its dashboard.

Approved work and numbering

Importing approved work reserves the source against duplicate billing. Exact decimal field and travel totals are used. Resolve existing reservations before trying to import or amend the same work again. Invoice numbers are controlled; deleting a record does not reset or reuse one.

Blank references

Case # and Client File # are omitted from the custom invoice when blank. Their separate optional lines are also omitted in supported outgoing email formatting. A standalone invoice does not need a fabricated case number just to make the template render.

Recipient access

A registered contact receives their authorized portal context. An email-only invoice uses a random private link restricted to that invoice and its receipts. Changing the email-only recipient replaces that private link. Treat it as confidential. CC/BCC copies do not give recipients a registered client's account or access to the rest of the portal.

42 OPERATING PROCEDURE

Issue edit and delete invoices

Invoice overview and invoice list Actions

Issue makes a reviewed draft an issued financial record. Send Invoice is a separate communication action. Issuing alone does not send the invoice email.

Issue after review

Review client identity, line items, tax, discount, total, dates, references, branding and payment instructions. Issue when those details are ready. The issued invoice retains its client and agency snapshot and its controlled number.

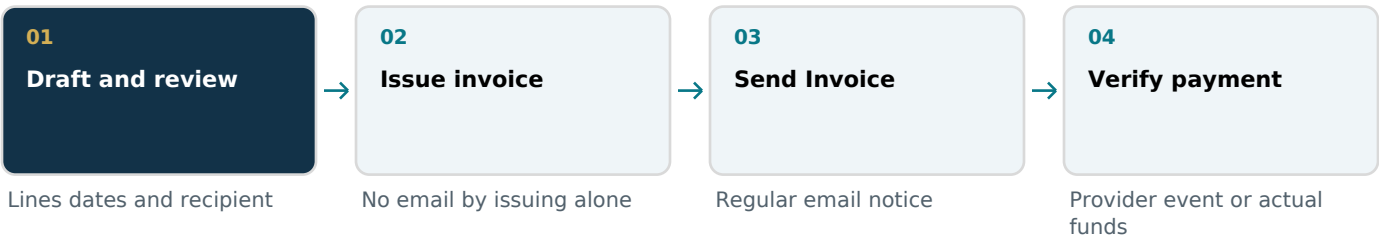
Explicit issued invoice editing

- 1. Choose Edit from the invoice list to open the issued invoice in explicit edit mode. Normal View remains read-only for those details and lines.
- 2. Change permitted dates, subject or client references, notes, discounts and manual line details. The invoice number, issued state and payment/credit ledger remain.
- 3. Resolve open or uncertain checkout attempts before editing. The revised total must stay positive and cannot fall below posted payments plus credits.
- 4. Save and choose Finish Editing. The system retains an encrypted pre-edit snapshot and audit event, and reminder dates follow the revised due date.

Editing does not email the invoice. Send the intended notice explicitly after review.

Delete eligibility

Authorized financial staff see View, Edit and Delete. Confirm Delete archives an eligible invoice from active lists and links, marks it void, cancels pending emails and disables recurring schedules while retaining audit records. It is not available to clients. Invoices with payments, credits or unresolved checkout attempts cannot be deleted. Reconcile the transaction rather than changing database rows to bypass the protection. Void and Paid / Settled have distinct meanings; case closure or company inactivation does not automatically erase either financial record.



Illustrated example Issue edit and delete invoices

43 OPERATING PROCEDURE

Send invoice notices and reminders

Invoice > Email & Recurring

Send Invoice uses the regular invoice email template even when the invoice is already overdue. The dedicated reminder buttons choose the corresponding reminder or overdue template.

Choose the intended action

- 1. Confirm an issued invoice, recipient, balance and due date. Review CC/BCC and the billing sender.
- 2. Use Send Invoice for the ordinary invoice notice. It attempts delivery after the transaction commits, with the scheduler as fallback.
- 3. Use Send Upcoming Invoice for an unpaid invoice with a future due date. Use Send Overdue Invoice for an unpaid invoice past its due date. Ineligible buttons remain disabled with an explanation.
- 4. Inspect the notification outcome and recipient delivery as appropriate. Accepted by SMTP does not establish inbox delivery or that the client read the email.

Automatic reminders

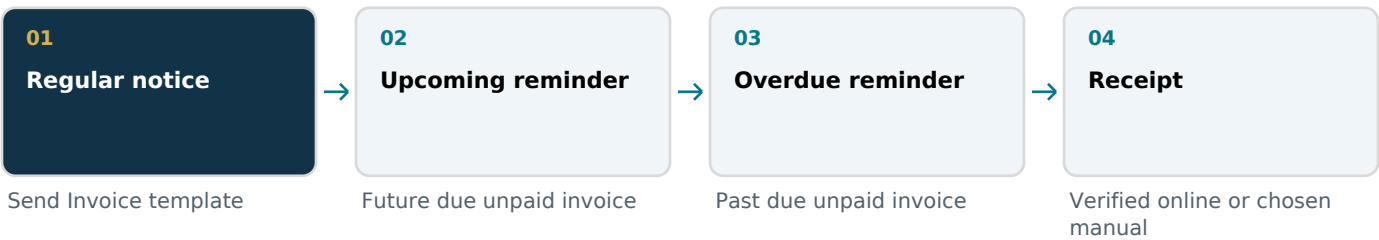
Configure the automatic reminder and overdue switches, offsets and templates in Invoice Setup. Reminders begin from a sent invoice workflow rather than merely issuing a draft. Current balance, invoice state, recipient preferences and due date are checked before dispatch. Paid or void records stop applicable future reminders. Manual reminder sends work independently of the automatic enable switches but still respect the client's email opt-out and server-side eligibility checks. Avoid repeatedly sending a notice simply because a recipient has not replied.

Recurring work

Use the available recurring controls deliberately and verify recipient and schedule. Deleting an eligible invoice disables its recurrence. After restore, outbound work is paused for reconciliation; a snapshot cannot undo a message already accepted by an external mail service.

Timing

An immediate send means an attempted post-commit dispatch, not a guarantee of instant delivery. Future reminders wait until their due time and scheduler processing. Safety notices and source imports also use scheduled work, so check the execution heartbeat before diagnosing a missing email as a template problem.



Illustrated example Send invoice notices and reminders

44 OPERATING PROCEDURE

Write readable invoice email templates

Invoice Setup > Email Templates Reminders Overdue Emails and Receipts

Templates are editable plain text with supported placeholders. The system creates safe HTML and a plain-text alternative; arbitrary PHP or Blade template code is not executed.

Format the message

Use real blank lines between paragraphs to create space blocks. Put Invoice #, Case #, Client File #, Subject, Amount Due and Due Date on their own lines. Separate optional references so the empty line can be omitted cleanly when no case or client file exists. Use {invoice_url} where the View Invoice & Pay button should appear in the HTML email. The full URL remains in the plain-text version. This link uses the installation's configured domain and subdirectory; do not paste an old FusionInvoice address. A receipt URL remains a receipt download link rather than becoming an invoice payment button.

Detail colors

The invoice detail section uses green when more than three days remain, amber during the last three days including the due date, and red after the due date. The calculation uses the agency timezone and invoice due date when sent. Delivered emails do not later change color as time passes.

Sender and templates

Templates use general billing contact placeholders. Set the contact name, email and phone in Invoice Setup to populate them. Replace defaults when agency details change. Global template edits do not automatically overwrite saved client-specific overrides.

Verify a sample

Send test invoices for a case invoice, a standalone invoice, a reminder and an overdue notice. Inspect both HTML and plain text, blank optional references, the payment link, sender, Reply-To and CC/BCC behavior. Do not include a real recipient in a test unless a deliberate message is intended.

Token group	Supported examples
Invoice and amount	{invoice_number} {issue_date} {due_date} {total} {balance} {days_overdue}
Matter and contact	{case_number} {client_file} {subject_name} {client_name} {agency_name}
Billing contact	{billing_contact_name} {billing_contact_email} {billing_contact_phone}
Links and instructions	{invoice_url} {portal_url} {case_url} {payment_instructions}
Receipt fields	{payment_amount} {payment_method} {payment_reference} {payment_kind} {receipt_url}

45 OPERATING PROCEDURE

Record payments and issue receipts

Invoice payment controls and Payment Options

Manual payment methods describe how money was received. Selecting Zelle, Bill.com or another method does not initiate a transfer through that service.

Record manual funds

1. Confirm the invoice, amount, date, actual method and reference. Enter only funds actually received, or the supported refund record when appropriate.
2. Choose whether to email the receipt for this manual payment. The master receipt setting and client email preferences still apply.
3. Save and review the posted payment and outstanding balance. Keep the external bank or remittance reference for reconciliation.
4. If an entry or provider result is uncertain, reconcile it before another posting rather than resetting the database.

Online payments

Stripe or Authorize.net uses hosted checkout when enabled. Case Files does not collect a card number or CVV. Signed events and provider verification, including invoice, amount and currency checks, drive posting. A browser return URL alone never marks an invoice paid. Verified online payments can queue receipts when receipt delivery is enabled. Repeated provider events are deduplicated. That protection does not make it safe to repeatedly start a new charge after an uncertain result.

Gateway setup

Configure the enabled gateway and webhook instructions under Invoice Setup > Payment Options. Use your own provider account and sandbox credentials first. Verify webhook reachability, a test payment, a duplicate event, a partial payment and the receipt before accepting live transactions.

Refunds credits and settlement

Use supported refund and credit controls with the appropriate authority. An external refund, dispute or processor adjustment needs reconciliation with its recorded event and invoice. Do not confuse processor gross payment with net bank settlement or a credit note with a cash refund.

Available manual methods	Meaning
Cash Credit Card Debit Card Online Payment	Records the selected method; online capture still needs provider verification.
Paper Check Cashiers Check eCheck via DPX	Records actual funds and the remittance reference.
Direct Deposit Wire Transfer	Records a bank movement that occurred outside the system.
Bill.com Zelle Melio Venmo	Records receipt through that service; does not start a transfer.

46 OPERATING PROCEDURE

Review client invoices and payment links

Client dashboard > My Invoices

Clients review their own invoices through the portal. An email-only recipient uses the private link for that single invoice without a new client login.

Client workflow

1. Open My Invoices or Invoices & Payments. Filter Open, Overdue, Paid / Settled or Void as needed.
2. Open the invoice and verify its agency identity, number, dates, services, total and outstanding balance.
3. Choose Pay Online when an enabled gateway is offered on an open invoice. Complete the processor's hosted checkout.
4. After returning, verify the payment result and receipt. A delayed or uncertain result should be investigated before another attempt.

Access boundaries

Unissued drafts are not client invoices. One company contact cannot see another contact's invoice just because they share an employer. Email CC/BCC recipients do not gain the billed contact's portal account. Changing an email-only recipient replaces that invoice's private capability link.

Invoice links in other deliveries

A video delivery can attach an issued invoice for the selected client and case. The delivery link does not authorize unrelated invoices. Test the link from a separate browser before sending it and review its expiry or password where present.

Questions and errors

Keep the invoice number and any processor reference when contacting the agency. Do not send card numbers, CVV, account passwords or private recovery codes in a case message. A paid invoice remains a financial record; it is not a deleted case. Void is a separate state and does not by itself prove a previous payment was returned.

47 OPERATING PROCEDURE

Review budgets and accountant registers

Case Budget and Finance & Billing > Accountant Workspace

Case budgets distinguish approved cost estimates from pending work. The accountant workspace separates invoice activity, recorded payments, credits, receivables, approved expenses and payroll records for review.

Case budget

Set the authorized budget, hourly cost rate, mileage cost and alert threshold. These cost estimates are distinct from client billing rates. Review approved and pending estimates before authorizing additional work. Where closure gates require an over-budget authorization, document it in the supported override field. An approved scope request does not automatically update these values. Use Review Billing Budget deliberately after the client decision and preserve the authorization reference.

Accountant procedure

1. Open Accountant Workspace as Administrator or Accounting. Select a valid reporting period of up to 366 days.
2. Review Invoice Register, Payments & Settlements, Credit Register, Current Receivables, Approved Expenses and Payroll Register separately.
3. Investigate Exceptions and record supported statement settlement matches. Distinguish gross receipts, processor fees, refunds and net settlements.
4. Record Period Review and produce CPA Exports when the period has been checked. Source transactions remain available for authorized work.

Interpretation and limits

The registers support review and import into other accounting software. They are not a complete general ledger, tax calculation or independent proof of bank reconciliation. A report is bounded to 5,000 rows; narrow the period or scope when it exceeds that limit. Compare the export with processor and bank records. A restore can return application transactions to an earlier point while the bank activity still happened. Reconcile external activity before resuming postings, and do not mark a review complete merely because a report downloaded successfully.

48 OPERATING PROCEDURE

Configure notifications and SMS rules

Agency Setup > Integrations and Agency Administration > SMS Rules

Agency SMTP handles operational and account email. Invoice messages can use dedicated billing SMTP. SMS requires the configured Twilio service, an active eligible recipient and that recipient's SMS settings.

Configure and verify

1. Save agency SMTP and send the test message. Confirm the sender and actual arrival, not only saved settings.
2. Configure Twilio credentials through the encrypted integration settings. Save eligible investigators' international-format phone numbers and SMS preference.
3. Open SMS Rules and edit the supported events and templates. SMS rule templates start unfilled and disabled. Enter the agency wording and enable only the events intended for use.
4. Save a small fictional workflow and inspect the queue/provider result before relying on automatic operational messages.

Rule events

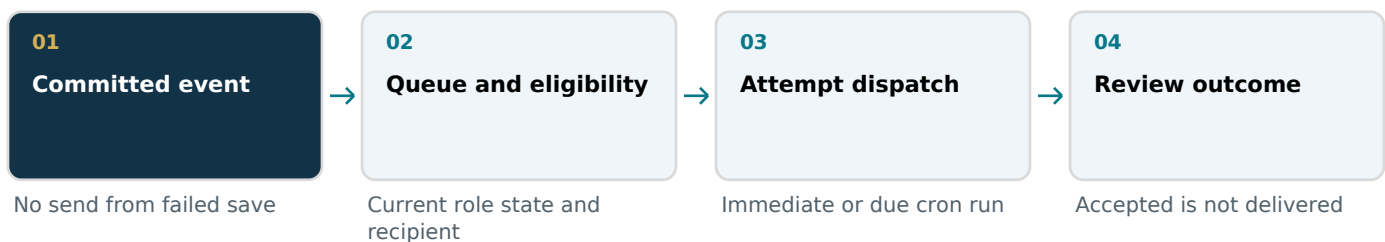
Supported SMS rules include case activation or investigator assignment, case closure, task scheduling or update, a task reminder one day before, task completion and report submission for review. These messages are directed to eligible assigned investigators; they are not a general broadcast to every role. Task-related choices and recipient eligibility still apply.

Shortcodes

Use only supported placeholders. Common values include {agency}, {case_number}, {case_type}, {case_link}, {task_id}, {task_link}, {start}, {end}, {location}, {actor}, {subject}, {instructions} and {hours}. Review message length and whether the text exposes more case information than necessary. SMS bodies are limited by the application and the service may split messages for billing.

Immediate and scheduled delivery

Immediate events attempt dispatch after a committed change, with cron fallback. Future reminders wait for their scheduled due time. Current assignment, account status and task or invoice state are rechecked. Accepted by SMTP or Twilio is not proof of recipient delivery. Reconcile uncertain sends before retrying to avoid duplicates.



Illustrated example Configure notifications and SMS rules

49 OPERATING PROCEDURE

Publish personnel verification carefully

Users & Permissions > Personnel & Verification

Personnel profiles and login accounts are separate. Creating a profile does not create an application user. Public verification is opt-in and publishes only the reviewed fields allowed by that feature.

Prepare a profile

1. Create or review the personnel record as an administrator. Confirm the display name, role, portrait, employee or vendor ID and lifecycle dates.
2. Link a user account where appropriate without assuming a profile grants case permissions. Assign roles and cases through Users and Assignments.
3. Review the public display fields before enabling publication. Keep sensitive internal details out of the public profile.
4. Test the public lookup with the intended ID and exact normalized surname. CAPTCHA and rate limits apply.

Interpret a lookup

A published verification result identifies the agency's published profile and status. It does not reveal case assignments and does not authenticate the person physically presenting an ID. Use the agency's direct verification procedures where identity matters.

Maintain status

Update lifecycle and inactive status promptly through the supported controls. Keep account activity and profile publication consistent with the agency's decision, while recognizing that they are different records. An employee or vendor's payroll type also remains a separate financial designation.

Files and public exposure

Use an appropriate reviewed portrait, not a case subject photograph. Uploaded images are normalized by the supported workflow. Do not assume a private upload becomes public merely because it was saved; publication requires the feature's intended control. Conversely, inspect the public page after publication to confirm only the intended fields appear.

50 OPERATING PROCEDURE

Create verify and retain backups

Agency Administration > Backup & Recovery

Database backups protect records. Full backups protect captured application and local files together with records. Neither replaces independent hosting disaster recovery or a rehearsed restore.

Create and verify

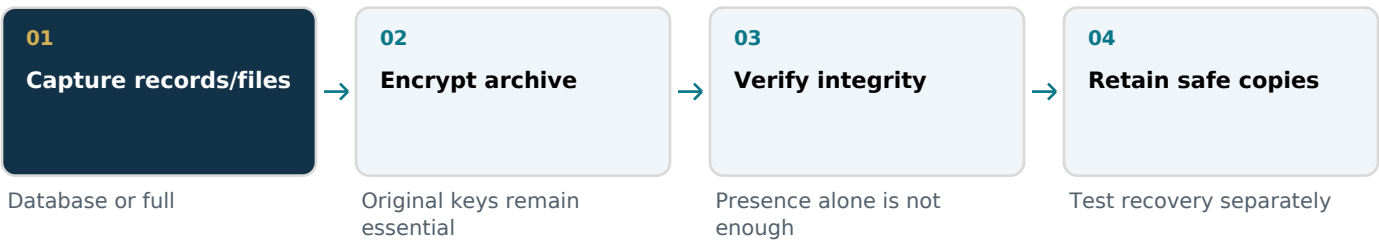
1. Open Protection & Schedule and review prerequisites, available storage and scheduler execution.
2. Choose the appropriate database or full capture. Follow progress through the retained operation rather than starting a duplicate job.
3. Inspect Archives & Restore for the result and destination. File presence and size are availability checks, not full integrity verification.
4. Run Verify Integrity to authenticate the encrypted archive and entry hashes. Retain the result and obtain an off-server copy as appropriate.

Policy and safety sets

Daily database backups retain four; full backups every fourteen days retain two. Confirm your saved schedule. Successful update safety snapshots are deleted automatically; failed-update and restore snapshots stay protected. Failed scheduled captures wait until the next scheduled day; manual retries remain available. Recovery uses encrypted .cfpb archives and original recovery keys. Dropbox also receives readable .sql database exports or .zip full backups; these exports are unencrypted. Deletion and retention remove both managed cloud formats together. Keep recovery keys securely outside the server.

Delete or cancel

Regular archive deletion requires the displayed DELETE confirmation, administrator password and a reason. It removes managed copies through their recorded storage relationship; partial failures remain visible. Protected safety sets cannot be deleted through that ordinary action. Capture cancellation is cooperative before a complete copy is retained. Retained-copy finalization and restore or update replacement cannot simply be cancelled. Preserve journals and safety material after an interrupted operation.



Illustrated example Create verify and retain backups

51 OPERATING PROCEDURE

Import and restore an archive

Backup & Recovery > Archives & Restore

A restore replaces records and potentially files with the chosen snapshot. Verify the intended archive and have a tested recovery path before starting.

Restore procedure

1. Verify archive integrity and identity. In-place restore requires the same installation, domain, edition, original keys and exact application version.
2. Review the archive type and timestamp. A database-only restore requires its referenced file bytes to be present and valid; a full archive can restore captured bytes.
3. Enter RESTORE and the administrator password as required. The worker creates a verified protected full safety snapshot before replacement.
4. Let the retained progress operation finish. On success sessions are invalidated; sign in again and complete reconciliation before resuming normal external effects.

Import is not restore

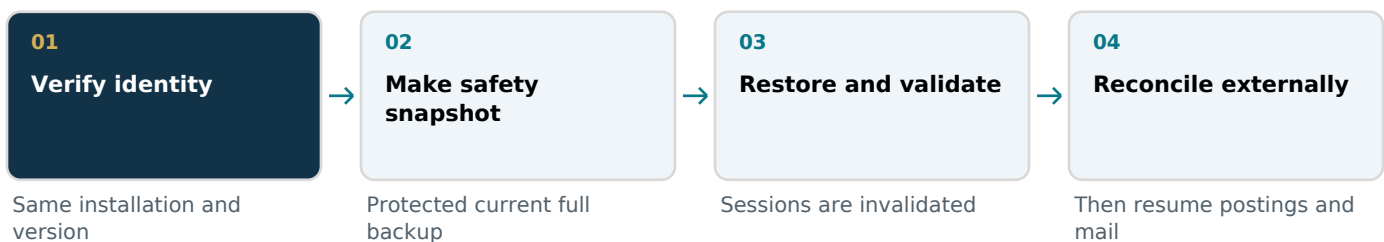
Uploading an archive and verifying it only makes it available for a later permitted restore. The large-file workflow uses ordered 2 MB chunks subject to hosting limits, with a total import limit of 8 GB and adequate staging space. Unfinished uploads can expire; finalized import material remains protected by its workflow.

What changes

Database audit returns to the snapshot's point in time. Full restore can remove application or upload files added after that snapshot while retaining rollback material during the operation. Current connection configuration, license and scheduler settings are preserved by the supported in-place process.

External effects remain real

A snapshot cannot reverse a bank payment, processor refund, payroll transfer or accepted email. Historical pending, sending and uncertain messages are cancelled, and financial posting and outbound dispatch pause until password-confirmed reconciliation. Review provider records and rebuild missing legitimate ledger entries before releasing that pause. Do not clear a maintenance flag manually to force the site open. Use the documented recovery process if the worker was interrupted.



Illustrated example Import and restore an archive

52 OPERATING PROCEDURE

Recover an interrupted operation or host

Administrator recovery procedures

Use the operation's recorded recovery material. A missing progress session or a long-running operation is not proof the worker has stopped.

Interrupted backup or restore

Preserve the maintenance state, work directory, journals and protected safety archive. The supported CLI recovery helper checks the worker mutex and commit markers before deciding whether to roll back or complete the operation. It refuses to interrupt a live worker. If recovery cannot establish a safe state, it leaves protection in place for administrator assistance.

CLI example

Use your actual PHP CLI binary and application path. For backup recovery, the documented form is `/absolute/path/to/php /absolute/path/to/application/cron/backup-recovery.php`. The placeholder paths are not commands to copy unchanged. An interrupted update with a broken bootstrap may require the preserved operation-specific recovery runtime described by that update.

Cold host recovery

1. Prepare private staging outside the web root. Keep the original encrypted archive and private recovery bundle together only for the controlled recovery work.
2. Use the documented backup-unpack helper to authenticate, decrypt and verify into a new private directory. It does not import SQL or activate an installation for you.
3. Rebuild compatible hosting for the original domain and identity, provision the intended empty database and import only the verified database export. Preserve original encryption and audit keys and license identity.
4. Restore directory protection and permissions, recreate cron for the new absolute paths, keep reconciliation required and review external activity before normal use.

Acceptance

Cold recovery is a hosting procedure requiring rehearsal. Remove private plaintext staging after acceptance while keeping required recovery and safety material. Do not publish recovery JSON, SQL dumps, keys or unencrypted files in the site's public directory. Independent hosting backups remain useful if the entire application account is lost.

53 OPERATING PROCEDURE

Apply updates and manage the domain license

Agency Administration > Update Center and System & Security

Update Center supports entitled LicenseHub releases and supported manual update packages. A full clean-install ZIP is not automatically a valid Update Center package.

Update procedure

1. Review entitlement, edition, runtime requirements, release notes and disk capacity. Create or confirm a recoverable backup first.
2. Use the supported update action with UPDATE and the administrator password. For a manual Update Center upload, provide the published release SHA-256 when required.
3. Allow validation, the protected full safety snapshot, file and additive schema changes and post-update verification to complete.
4. Sign in again if sessions were invalidated. Inspect the outcome and history before resuming work. Complete any prompted Database Upgrade.

Patch file delivery

When a separately supplied compatible update instructs direct file replacement, upload all its contents into the existing application root and overwrite matching files. Preserve installed.php, storage and credentials. Replacing only a stylesheet or creating a nested patch folder will not apply the complete change. Do not use the clean installer on the existing database.

Failure and recovery

Preserve journals and runtime after an uncertain result. Successful update safety snapshots are removed on the next page load or scheduler run; failed-update and restore snapshots remain protected. Cleanup is audited.

License state

The application verifies signed activation, domain and current entitlement. A copied installation is not a supported way to license another domain. Confirmed revocation blocks access until the license becomes active again. Use the displayed license status and Refresh License Status controls when diagnosing a legitimate domain. Network or TLS problems require investigation; changing database flags is not a licensing repair.

54 OPERATING PROCEDURE

Troubleshoot records mail and payments

Application messages and System & Security

Begin with the exact page, role, case or invoice number, action and time. Preserve the visible diagnostic reference. Do not send passwords, API secrets, card data or entire private databases in an ordinary support message.

Case or page unavailable

Check active account, role, company activity and current assignment. For a missing new page, verify that its PHP file, route map and menu file were replaced in the actual serving root. Clear PHP OPcache through hosting controls if it is serving old code after a verified replacement. Refreshing a browser alone may not clear server-side code caching.

Changed or protected record

Reload after a stale-version warning and compare the latest saved record. A legal hold, reviewed snapshot, closed effort or retained source can intentionally block deletion or editing. Use the applicable revision or release workflow rather than forcing a database update.

Mail or SMS not received

Confirm the correct agency or billing SMTP path, recipient address, active account, opt-in settings, queue state, cron heartbeat and provider outcome. An accepted submission is not proof of delivery. Do not repeatedly send uncertain work before checking the provider.

Invoice creation or payment errors

Retain the Diagnostic stage, SQLSTATE, numeric code and reference shown by the application. Complete a prompted Database Upgrade. Check client/case selection and invoice numbering, and use provider records to reconcile an uncertain payment. A checkout return page is not payment verification.

AI unavailable

Confirm the feature switches, exact model ID, configured account access and outbound connectivity. Verify the provider account usage and recorded research state before retrying an uncertain request. A stored key alone does not prove the request succeeded.

55 OPERATING PROCEDURE

Troubleshoot files diagrams and recovery

Case Cloud exports and Backup & Recovery

Use the recorded file identity and operation outcome. Preserve originals and private recovery material while diagnosing the issue.

Dropbox path or transfer

Check the Dropbox account, app access scope and entered folder. App Folder paths are relative to the app's own folder. A new destination setting does not automatically move old files or update stored historical paths. A failed transfer can leave a valid local mirror; inspect it before trying a deletion.

Missing or unavailable file

Check the record's state, access visibility, source relationship and recorded storage location. An Internal label describes visibility even when Dropbox stores the file. A hash or size failure means the available bytes did not verify; a network or storage availability error is not automatically proof of tampering.

Report or diagram output

Open the correct saved revision and verify the selected snapshots, fonts, branding, photographs and host PHP limits. Check the exported file rather than assuming the browser preview has identical pagination. A reviewed diagram attached earlier does not follow later working edits automatically.

Mobile display

Confirm the latest assets were replaced with the PHP files. Use the sidebar's own scroll region and horizontal table scroll where offered. Check a phone in both orientations and a tablet with the actual case text and browser zoom. Avoid reducing device text size simply to hide a layout defect.

Maintenance page

Backup or restore in progress protects the workspace while an operation owns maintenance. Reconnect only through the progress capability offered to the original authorized session. If interrupted, preserve journals and use the documented recovery helper. Do not delete locks or safety archives to make the page disappear.

Supply useful evidence

Provide the page name, action, role, timestamp, displayed error and reference, plus a narrowly cropped screenshot without secrets or unnecessary personal data. Keep the original evidence or recovery files unchanged until the issue is understood.

56 OPERATING PROCEDURE

Agency maintenance checklist

Administrator daily weekly and release review

Use this checklist as a repeatable operating routine. Assign a responsible person and record the actual outcome rather than treating an enabled switch as completion.

Daily

1. Review safety alerts and overdue operational work. Confirm that active schedules have the right supervisor instructions.
2. Check notification failures and uncertain payment events. Reconcile before retrying an external effect.
3. Confirm recent scheduler execution and expected backup outcomes. Review storage capacity if captures or transfers are failing.
4. Review newly submitted reports, time and client scope decisions within the agency's normal service process.

Weekly

Review user and company activity, departed staff and obsolete case assignments. Verify a sample backup and off-server availability. Check failed Dropbox transfers and integrity exceptions. Review invoice aging, manual remittance references and unreconciled processor activity. Confirm that client-facing delivery links and expiry periods remain appropriate.

Monthly

Review training links and resource access, invoice sender details, template wording and client overrides. Compare application and hosting capacity with retention and staging needs.

Before a release or hosting change

Test a fictional case as manager, investigator and client; verify search, task scheduling, report release, a document download, invoice creation and the client invoice view. Test the configured sandbox gateways and mail path deliberately. Create and verify a full backup and keep recovery material available.

After restore

Reconcile external payments, refunds, payroll and accepted messages. Recreate cron if paths changed, verify directory protection, test the original license identity and record the required reconciliation before resuming outbound work. A restore rehearsal is complete only after the restored application and its referenced files are usable.

Control	Evidence to retain
Scheduler	Recent heartbeat and a due job outcome
Backup	Archive identity integrity result and tested recovery route
Payments	Invoice ledger processor reference and settlement reconciliation
Access	Role/company/assignment review and separate-session checks

57 OPERATING PROCEDURE

Limits states and terms at a glance

Quick reference

These limits describe the packaged workflows. Lower PHP, proxy, account or hosting limits can take precedence. Use the actual form's current validation message when a request is rejected.

Important state distinctions

Internal is a visibility label; Local, Pending and Dropbox describe storage or transfer. Submitted is awaiting review; Approved is not automatically Released. Issued is a financial state; Sent describes an email action or accepted notice. Paid / Settled and Void are distinct invoice views. Queued is waiting for processing; Accepted indicates a provider accepted a submission, not that a person read it. A saved research item remains subject to identity/source review. An archived workspace entry retains history rather than being physically erased.

Read outcomes carefully

Verify Integrity checks the recorded archive or file bytes, not the truth of its content. A private invoice or video link is a limited capability and should be protected like confidential correspondence.

Workflow	Packaged limit or rule
Case document upload	Normally 25 MB; validated supported formats and host limits.
Final client video	MP4 up to 128 MB, subject to host limits and browser compatibility.
Training attachment	15 MB each and thirty files per guide.
Case package	Ten reports thirty files and 200 MB total uncompressed.
Public research requests	Shared thirty AI requests per hour agency limit.
Task interval	End after start with duration no more than seven days.
Accounting report	Period up to 366 days and bounded to 5,000 rows.
Backup import	Up to 8 GB with available staging space; chunked requests 2 MB.

58 OPERATING PROCEDURE

Document maintenance and support

Manual reference

This manual describes the Commercial installation of Case Files Professional version 3.4.0 with the packaged review fixes and revised case tab order. Use the applicable release notes when a later build changes labels, permissions or limits.

Feature scope

The manual covers companies and separate client contacts; case assignments, subjects, vehicles and tasks; the Investigation Workspace; internal documents and release; evidence and custody; legal, claims and IME case records; diagrams and reports; Research & AI and Public Background Research; training; timesheets and payroll records; invoices, payments and notifications; and protection, recovery and update workflows. The Investigation Workspace is included in this installation. Generic invoice templates can be customized to the agency. SMS templates remain unfilled and disabled until configured. Optional integrations require agency-owned accounts and deliberate setup.

Maintain procedures

When updating a procedure verify the exact page, role, record state, source and expected outcome against the deployed build. Retest the client view after changes to release or company controls. Keep illustrations fictional and remove credentials and private client information from training materials.

Built-in help

Use Help & Guides and the setup documents supplied with the application for operation-specific CLI recovery and integration details. The built-in handbook download may be an earlier packaged guide. Keep this manual with the applicable release notes. Do not upload the separate code-review tests into the live application.

Operational acceptance

Local code checks do not establish live SMTP/SMS delivery, processor settlement, Dropbox transfer, native database behavior or a successful disaster recovery. Verify those on the intended host and record remaining limitations. This manual is an operating reference rather than a certification that every deployment or stored conclusion is error-free.

Public policies and integration setup

Public agency policy pages

Terms of Use and Privacy Policy are available without signing in. Their URLs use the actual licensed installation domain and folder: /terms and /privacy beneath the application path. Do not enter the example domain from a different installation.

Agency Setup > Public Policies

Both documents are prefilled. Edit the wording and public contact email to match the agency's actual practices. Use {agency_name} and {contact_email} for dynamic fields; ## begins a heading and blank lines separate paragraphs. Text is displayed as escaped plain text. Saving updates the effective date. Review these agency policies before relying on them.

Agency Setup > Maps & Vehicle Images

The Terms of Use and Privacy Policy URL fields are prefilled automatically. Existing custom URLs remain unchanged by an update. You can retain links to your agency's external policies. Enable Maps only after saving appropriate API credentials and reviewing the public pages. Embedded maps and address lookup send relevant information to Google; the public pages include Google service policy links.

Invoice Settings > Payment Options

For Authorize.net, register the dedicated /authorize-webhook.php endpoint shown in Payment Options. Do not append a provider query string. Enter the matching API Login ID, Transaction Key and Signature Key. Choose Live or Sandbox for the matching account. Hosted checkout can remain disabled while its credentials stay stored. Stripe remains independent.

Backups and successful updates

Dropbox receives readable SQL database exports or ZIP full backups alongside encrypted recovery copies. Standard exports are unencrypted. Normal deletion and retention manage both cloud copies. Safety snapshots tied to completed successful updates are removed automatically after the worker finishes, on the next page load or scheduler run. Failed-update and restore recovery snapshots remain protected, and cleanup is audited.

Send an SMS connection test

Administrators: open Agency Setup > Notifications. Save the Twilio sender and credentials first. Enter a test recipient with country code and click Send SMS Test. One fixed message is submitted immediately without waiting for CRON. Twilio acceptance and the message SID appear on the result page; check the phone to confirm receipt. A rejection shows an error. Trial accounts require verified recipients. Charges apply. Refreshing does not resend the message. Do not repeat an uncertain request until you check Twilio logs. Tests are limited to five per administrator per ten minutes and are audited without case details.