Physical Files and Assets Tracking Platform

Administrator and Asset Registrar Guide

ADMINISTRATOR / ASSET REGISTRAR GUIDE

Prepared by SPACE95

Release 2.0 | June 2026

Physical Files and Assets Tracking Platform

Document Control

Document Title	Administrator and Asset Registrar Guide
Prepared By	SPACE95
Document Type	User Guide / Operating Manual
Release	2.0
Date	June 2026
Platform	SPACE95 Physical Files and Assets Tracking Platform
Audience	Asset Registrar, Registry Officer, System Administrator, Auditor and Department Manager

Document Acceptance and Release Notice

This is a managed user guide. Changes should be issued as a complete document replacement with the release number incremented. The guide is intended for practical training, reference and audit support for the Physical Files and Assets Tracking Platform.

Release	Date	Affected Pages	Description of Changes
2.0	June 2026	All	Expanded practical operating manual with step-by-step procedures, USB RFID support and Electronic Documents tab guidance.
1.0	June 2026	All	Initial professional user guide release for the redesigned Asset Tracking Center.

About SPACE95

SPACE95 is a Seychelles-based Information Technology services company providing custom application development, technical support, enterprise systems, training, network infrastructure and business solution services. The platform described in this guide forms part of SPACE95's practical business systems capability for physical records, asset custody, file movement, reporting and decision-support.

Table of Contents

Introduction and Scope

This guide is written for administrators and asset registrars who configure and operate the SPACE95 Physical Files and Assets Tracking Platform. It is intentionally practical and procedure-based. It explains why each feature exists, when to use it and how to perform common registry operations step by step.

Registry objective

The registrar should be able to answer these questions at any time: Where is the file? Who is responsible for it? When did it move? Is it overdue? Is it confidential? Is there an electronic copy? Has it been archived, destroyed or reported missing?

Latest release features covered

- Resizable side-by-side panels and full-screen register/actions mode.
- USB barcode, QR, webcam and basic USB RFID scanning from the same scan area.
- RFID file profile fields and RFID assignment by USB reader.
- Electronic Documents tab for scanned copies and attachments.
- Reports, analytics, notifications, lifecycle and confidential access controls.

Core Concepts for New Users

File tracking is the discipline of knowing where each physical file is, who is responsible for it, when it moved, and what evidence exists for that movement. The system does not replace office procedure; it records and controls it.

Main principle

Every file should have one known custodian and one clear location. If a file is passed from one person to another, it must be scanned or recorded so the chain of custody remains reliable.

Term	Meaning	Why it matters
Physical file	The actual folder, box, document packet or asset being tracked.	This is what staff handle and move in the office.
File number	The official file reference printed on the label.	Users can search and identify files without opening the folder.
Barcode / QR	Machine-readable label printed for the file.	Allows quick scanning and reduces typing mistakes.
USB RFID tag	A tag read by a USB RFID reader at a desktop or laptop.	Allows fast identification by scanning the RFID tag like a keyboard input.
Custodian	The person currently responsible for the file.	Accountability depends on knowing who has the file.
In Transit	The file has been sent but receiver has not confirmed receipt.	Prevents silent handover and forces confirmation.
Electronic document	A scanned copy or attachment stored under the physical file profile.	Allows digital copies to be found with the physical file record.

Dashboard cards
Totals, waiting, in transit, overdue, alerts

Universal scanner/search
Barcode, QR, webcam, USB RFID, manual search

Actions
scan + operational tabs

Central Register
search results and clickable file cards

Selected File Profile
custody, RFID, documents, history, issues

Why the one-screen cockpit matters

The page is designed to avoid switching between old separate pages for check-out, check-in, request, register, movement history and reports. Users can search, scan, open a file profile, send, receive, print labels and upload electronic documents from one operational screen.

Roles, Permissions and Operating Responsibility

Role	Typical responsibilities	Important control point
System Administrator	Manage security, configuration, setup records and technical deployment.	Should not perform daily custody work unless required.
Registry Officer / Asset Registrar	Register files, print labels, assign RFID, manage check-out/check-in, audit storage and run reports.	Main control role for physical registry.
Department Manager	Monitor departmental files, review overdue files and approve/follow up requests.	Should use reports and dashboard, not bypass registry.
Auditor / Read Only	Review movement, view audit and lifecycle evidence.	Cannot change custody or configuration.
Normal User	Request, receive, send and return authorised files.	Must confirm receipt and send through system.

Step-by-step: verify your access before rollout

1. Log in as administrator.
2. Open the Security or Admin panel.
3. Confirm your role allows setup, file edit, move, audit and report actions.
4. Log in as a test registry user and confirm only registry operations are visible.
5. Log in as a normal test user and confirm admin-only actions are hidden or blocked.
6. Test a confidential file with a normal user to confirm masking/limited access works.

Pre-Go-Live Setup Checklist

Before users start scanning real files, the registry should complete the setup below. Skipping setup leads to poor file descriptions, wrong categories, weak reports and unreliable custody.

Go-live setup checklist

- [ ] Categories created.
- [ ] Classifications created.
- [ ] Content categories created.
- [ ] Locations and storage areas created.
- [ ] Movement reasons created.
- [ ] Statuses reviewed.
- [ ] Confidentiality levels reviewed.
- [ ] Retention policies seeded if lifecycle is used.
- [ ] Notification rules seeded.
- [ ] User roles assigned.
- [ ] Upload folder permissions checked.
- [ ] Scanner/barcode/RFID devices tested.
- [ ] Sample files registered and labels printed.

Setup area	Examples	Why it matters
Category	Employee File, Legal File, Finance File	Controls reporting and label grouping.
Classification	Active, Archive, Restricted, Case File	Helps staff understand file type.
Location	HR Registry, Payroll Office, Main Archive	Supports storage and audits.
Movement Reason	Review, Approval, Audit, Payroll Processing	Explains why files move.
Confidentiality	Normal, HR Confidential, Payroll Confidential	Protects sensitive files.

How to Search for and Open a File

Searching is the safest first step when you are unsure where a file is. You can search by file number, barcode, description, custodian, category, location, RFID tag, document title and other fields.

Step-by-step: search by file number or description

1. Go to the Central Register search box.
2. Type the file number, part of the name, description, barcode or RFID tag.
3. Click Search or press Enter.
4. Review the result cards. Check File No, Description, Current Custodian, Status and Expected Date.
5. Click Open on the correct file.
6. Read the file profile before requesting, receiving or sending the file.

Step-by-step: use filters

1. Use the All files dropdown to limit the register to files with you, waiting for you, in transit, overdue or requested.
2. Use the category dropdown to show only a selected file category such as Employee File or Legal File.
3. Use the location dropdown to show files for a location or registry area.
4. Click Search to refresh results.
5. Click Show All to remove narrow search text if you need the full register again.

What to check before acting on a file

Check	What to look for
Current Custodian	Who currently has the file or whether it is in transit.
Status	Whether the file is with a user, waiting receipt, archived, missing or destroyed.
Pending Requests	Whether someone else has requested it.
Confidentiality	Whether the file has restricted information.
Electronic Documents	Whether scanned copies or attachments are available.
Movement Timeline	Last send/receive action and who performed it.

Scanning Methods: Barcode, QR, Webcam and USB RFID

The system supports several scanning methods because different offices work differently. A registry desk may use a USB barcode scanner; a laptop user may type manually; a tablet user may use the camera; and offices with RFID tags may use a USB RFID reader. All of these methods use the same scanner/search area.

Scanner input choices

Barcode
USB scanner types barcode

QR Code
camera or QR label

USB RFID
reader types tag number

Manual
type file no or barcode

Method	How it works	Best used for
USB barcode scanner	The scanner types the barcode into the scan field and usually presses Enter automatically.	Fast daily check-in and check-out at a desktop.
QR code / webcam	The camera reads the QR/barcode printed on the label.	Tablet or mobile use where no USB scanner is available.
USB RFID reader	The reader types the RFID/EPC number into the active scan field.	Office clerks scanning files at a desktop/laptop using RFID tags.
Manual typing	User types file number, barcode, RFID or description into search.	Fallback when a label is damaged or no scanner is connected.

Step-by-step: prepare the scanner area

1. Click inside the Scan / type barcode, file no. or asset ID field.
2. Select Scan Mode. Use Auto Detect for normal work. Use RFID USB only when assigning or testing RFID tags.
3. Check the RFID workstation/reader name if the field is shown. Use a clear name such as HR Registry Counter PC or Payroll Laptop.
4. Scan the label or RFID tag. If the scanner does not press Enter automatically, press Enter.
5. Read the message shown by the system before taking the physical file to the next person.

How Auto Detect works

Scanned value looks like	System treats it as
ASSETID=...;FILENO=...;BARCODE=...	QR value containing multiple fields
Long hexadecimal/number value from USB RFID reader	RFID tag or EPC value
Known barcode or file number	Barcode/file number lookup
Plain text description	Universal search text

Important for USB RFID

The USB RFID reader is not a network device in this phase. It simply types the RFID value into the page like a keyboard. Keep the cursor in the scan field before scanning.

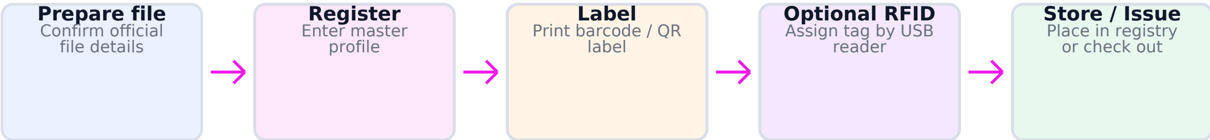
Common status colours and meanings

Green	Orange	Red
Completed or available	In transit or needs attention	Exception, issue or not found

Registering a New Physical File

Registration creates the master record for the physical folder or asset. A file should not be circulated before it is registered, labelled and assigned to the correct custodian or registry location.

New file registration workflow



Step-by-step: add a new file

1. Click Register in the Actions panel.
2. Enter File No / Asset Serial No using the official file reference.
3. Enter a clear Description. For employee files, include employee name or number if your policy allows it.
4. Select Category, Classification and Content Category.
5. Select Owner Department and Owner Employee if applicable.
6. Select Physical Location and structured storage fields such as Office, Room, Cabinet, Shelf, Box and File Position.
7. Select Confidentiality Level. Use a restricted level for HR, payroll, legal or executive files.
8. Enter retention/lifecycle details if available.
9. Save the file.
10. Open the new file profile and verify all details.
11. Print the barcode/QR label and attach it to the folder.
12. If RFID is used, assign the USB RFID tag.
13. Place the file in its storage location or check it out to the first custodian.

Required quality checks before saving

Check	Reason
File number is unique	Prevents two physical files sharing one identity.
Description is meaningful	Users can find the file without guessing.
Category and classification are correct	Reports and filters depend on them.
Location/storage is correct	Physical audits depend on it.
Confidentiality is correct	Wrong level may expose sensitive files.
Label printed clearly	Scanning depends on readable label.

Maintaining the File Profile

The file profile is the control record for the physical file. It contains identity, category, location, custody, RFID, photos, related files, electronic documents, requests, issues and movement history.

Step-by-step: edit file details

1. Search and open the file.
2. Review the current custodian and status before editing.
3. Click the edit/register/profile action available to your role.
4. Change only the fields that are genuinely incorrect or incomplete.
5. If changing location, confirm the physical file is actually moved to that location.
6. If changing confidentiality, confirm that access rules remain appropriate.
7. Save changes.
8. Re-open the file profile and verify the changes.
9. Record a comment or note if the correction affects audit history.

Fields the registrar should understand

Field group	Examples	Registrar note
Identity	File No, Barcode, Asset ID	Should rarely change after label is printed.
Classification	Category, Content Category, Classification	Used for search, reports and file type control.
Custody	Current User, Checkout To, Status	Normally changed by send/receive workflow.
Storage	Office, Room, Cabinet, Shelf, Box	Used for physical location audit.
RFID	RFID Tag No, EPC, Last Seen	Used only if USB RFID tags are deployed.
Electronic Documents	Scanned copies and attachments	Does not replace original custody unless office policy says so.

Barcode, QR and Label Printing

Labels are the bridge between the physical folder and the system record. A good label makes scanning fast and reduces errors.

Step-by-step: print a label for one file

1. Search or open the file.
2. Click Label or Labels / QR.
3. Review the label preview.
4. Confirm the file number, barcode/QR and description are correct.
5. Print on the approved label printer or paper.
6. Attach the label to a visible part of the folder.
7. Test by scanning the label in the scan field.
8. If the scan opens the correct file, the label is ready for use.

Step-by-step: print labels for a batch

1. Use the Central Register filters to find the batch, or open Bulk Operations.
2. Select the files requiring labels.
3. Choose Bulk Print Labels.
4. Review the print preview.
5. Print labels.
6. Attach labels carefully to the matching physical files.
7. Scan a few samples to validate that labels match files.

Label control rule

Never attach a label to a file without checking that the label file number matches the folder. A wrong label creates a serious custody and audit problem.

USB RFID Basic Operation

RFID support in this release is intentionally simple. The USB RFID reader behaves like a keyboard. When a tag is scanned, the number is typed into the scan field. There is no fixed antenna, no background device communication and no automatic door tracking.

RFID Item	Meaning
RFID Tag No	The RFID number assigned to the file.
RFID EPC Code	The electronic product code, often the same value as the tag number.
RFID Tag Type	Usually USB RFID or the model/type of tag.
RFID Tag Status	Assigned, replaced, inactive or other status.
Last RFID Seen Date	Last time the tag was scanned in the system.
Last RFID Seen Location	Office/counter where the scan happened.
Last RFID Reader	The workstation or reader name used during the scan.

Step-by-step: assign a USB RFID tag to a file

1. Open the file profile.
2. Confirm that this is the correct physical file by checking file number and description.
3. Place the cursor inside the Assign RFID Tag scan box.
4. Set Scan Mode to RFID USB if shown.
5. Scan the RFID tag with the USB reader.
6. Check that the RFID value appears in the field.
7. Enter or confirm RFID Tag Type, for example USB RFID.
8. Confirm the workstation/reader name and location.
9. Click Assign RFID To This File.
10. Wait for the success message.
11. Check the file profile now shows RFID Tag No, EPC, Assigned Date, Assigned By, Last Seen Date, Last Seen Location and Last Seen Reader.

Step-by-step: replace an incorrect RFID tag

1. Open the file profile and confirm the current RFID value.
2. Check that the replacement tag is not already assigned to another file.
3. Scan the new RFID tag in the assign box.
4. Save the new tag.
5. Attach the new physical RFID tag to the file/folder.
6. Mark or remove the old tag from the folder to avoid future confusion.
7. Review the movement/custody timeline for the RFID_ASSIGNED event.

> **RFID limitation in this phase**
>
> The system only knows about an RFID tag when a user scans it on the page. It does not automatically know that a file passed through a doorway or moved between rooms.

Sending, Receiving and Outbox Control

The registrar may send files one by one or in batches. The outbox is a staging area that lets the user scan several files and send them to one receiver together.

Step-by-step: send files from registry to an employee

1. Open or scan the first file.
2. Click Outbox or Add to Outbox.
3. Repeat for all files being sent to the same receiver.
4. Open the Outbox To Send panel.
5. Review the list and remove mistakes.
6. Select the receiver employee.
7. Select movement reason.
8. Enter expected return/check-in date if required.
9. Click Check OUT / Send.
10. Physically hand over or dispatch the files.
11. Advise receiver to scan/receive them immediately.

Step-by-step: receive returned files into registry

1. Click inside the scan field.
2. Scan the barcode, QR or USB RFID tag on the returned file.
3. If the system says the file is waiting for you or in transit to registry, click Receive / Check IN.
4. Confirm the success message.
5. Place the file into the correct cabinet/shelf/box.
6. If the location changed, update storage location or run location scan workflow.

Monitoring in-transit files

Condition	Registrar action
File in transit same day	Monitor normally.
File in transit past expected date	Contact receiver and sender.
Receiver says file not received	Use Report Issue: File not received.
Wrong receiver selected	Correct through registry process and record note/issue.

Request and Approval Workflow

The request workflow prevents informal file borrowing. Users can request a file from the current custodian, and the custodian can approve, reject or send later.

Step-by-step: respond to a file request as custodian/registrar

1. Open the Requested Files dashboard card or request section in the file profile.
2. Read the requester, reason, priority and needed-by date.
3. Check whether the file can be released.
4. If approved, click Approve & Send or prepare the file in outbox.
5. If not available, choose Send Later and enter a note/date if supported.
6. If the request is invalid, reject it and enter a clear reason.
7. Send the physical file only after the system movement is recorded.

Priority guide

Priority	Meaning	Expected handling
Normal	Routine office request.	Process in normal registry cycle.
Urgent	Required soon for operational work.	Review same day if possible.
Audit	Needed for audit/review.	Keep clean evidence and avoid informal transfer.
Legal	Related to legal/case work.	Check confidentiality and approval.
Payroll / HR	Sensitive employee data.	Confirm access and confidentiality before sending.

Location and Storage Control

Location control records the physical storage path of files. A good storage path lets a new registry officer find a file without asking the previous custodian.

Recommended storage structure

Level	Example
Office	HR Registry
Room	Records Room 1
Cabinet	Cabinet A
Shelf	Shelf 03
Box	Box 2026-EMP-01
File Position	Position 018

Step-by-step: assign/update storage location

1. Open the file profile.
2. Confirm the physical file is in your hand or at the storage location.
3. Open Storage / Audit or edit profile storage section.
4. Select storage location or enter office/room/cabinet/shelf/box/position.
5. If using storage barcode, scan the storage location barcode.
6. Save the location.
7. Physically place the file in the matching location.
8. Search the file again and verify that the location displayed is correct.

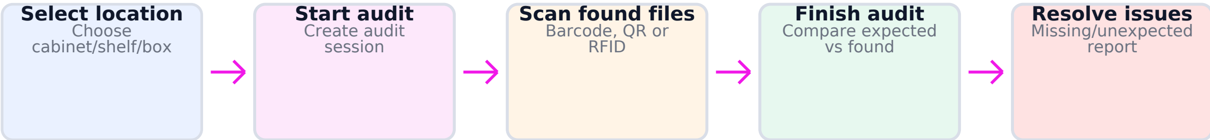
Step-by-step: location scan workflow

1. Click Storage / Audit.
2. Scan or select the storage location.
3. Scan each file placed in that location.
4. Review the scanned list.
5. Save the storage assignment.
6. Run a search/filter by location to confirm files now appear there.

File Audit by Location

A location audit compares what the system expects to be in a location with what the registrar physically finds there. It identifies missing, unexpected and misplaced files.

Physical audit workflow



Step-by-step: audit a cabinet/shelf/box

1. Click Storage / Audit.
2. Select the location to audit.
3. Click Start Audit.
4. Physically go to the cabinet/shelf/box.
5. Scan every file found there.
6. Do not skip files even if they look wrong.
7. Click Finish Audit.
8. Review Expected, Scanned, Missing and Unexpected lists.
9. Investigate missing files and update location or report issue where required.
10. Export or print audit exception report if needed.

Audit result	Meaning	Action
Expected and scanned	Correct file found in expected location.	No action.
Missing	System expected file there but it was not scanned.	Search, follow up custodian, report issue if needed.
Unexpected	File found there but system expected elsewhere.	Update location or investigate wrong filing.
Misplaced	File exists but in wrong location.	Move to correct location or update with reason.

Electronic Documents and Scanned Copies

The Electronic Documents tab allows the system to manage the physical folder and also store scanned copies or attachments linked to that folder. This is useful when staff need quick access to a scanned document but still need to know where the original physical file is.

Field	Purpose
Document Title	Clear name such as Employment Contract 2026 or Signed Request Form.
Document Type	Groups documents, for example Contract, Letter, Form, Certificate, Photo or Other.
Upload File	The scanned PDF, image, Word document or other attachment.
Document Date	The date of the actual document, not just the upload date.
Version No	Used when the same document is uploaded again as a later version.
Uploaded By / Uploaded Date	Audit evidence of who added it and when.
Confidentiality	Controls how sensitive the electronic copy is.
Notes	Short explanation of the document.

Step-by-step: view electronic documents

1. Search for the physical file and click Open.
2. Scroll to the Selected File Profile.
3. Find the Electronic Documents / Scanned Copies section.
4. Read the document title, type, version and upload details.
5. Click Open or the file link to view/download the attachment if your access allows it.
6. Close the document when finished and do not save copies locally unless your office policy allows it.

Step-by-step: upload a scanned copy or attachment

1. Open the physical file profile.
2. Click the Electronic Documents action tab or upload section.
3. Enter a clear Document Title.
4. Select the Document Type.
5. Select the file from your computer.
6. Enter Document Date if known.
7. Enter Version No. Use 1.0 for a first upload if your office has no version rule.
8. Select Confidentiality if the scanned copy contains sensitive information.
9. Enter Notes explaining why the document is attached.
10. Click Upload / Save.
11. Confirm that the document now appears in the Electronic Documents list.

> **Good practice**
>
> Do not upload duplicate scans with unclear names such as scan001.pdf. Use a meaningful title so another user can identify the document without opening every attachment.

Registrar control note

Administrators and registrars should periodically review uploaded documents for poor naming, duplicates, incorrect confidentiality and files attached to the wrong physical folder. Removal should be used carefully because it is recorded in the custody/audit timeline.

Bulk Operations

Bulk operations are for registrars handling many records at once. They save time but must be used carefully because a mistake can affect many files.

Available bulk operations

Operation	Purpose
Bulk Register / Import	Create many file records from CSV/Excel template.
Bulk Assign Location	Move many files to the same storage location.
Bulk Send to User	Send many files to one receiver.
Bulk Receive	Receive multiple files in one operation.
Bulk Archive	Mark selected files archived.
Bulk Print Labels	Print labels for multiple files.
Bulk Update Category/Classification	Correct or standardize many file records.

Step-by-step: import/register files in bulk

1. Prepare the import template with File No, Description, Category, Classification, Location, Barcode, Owner Department and Confidentiality.
2. Check for duplicate file numbers before import.
3. Open Bulk Operations.
4. Choose Bulk Register / Import.
5. Upload CSV or XLSX file. CSV is safest if the server does not support Excel import.
6. Review the preview grid.
7. Correct errors before applying.
8. Run the import.
9. Review imported file count and rejected row messages.
10. Print labels and scan sample records to confirm quality.

> **Bulk control warning**
>
> Never bulk update category, location or archive status without first filtering and reviewing the selected records. Export a list before large changes if the client requires audit evidence.

Security and Confidential File Control

Confidentiality controls protect files containing sensitive information such as HR, payroll, legal, disciplinary or executive documents. The system can mask file details, restrict access and record view audit information.

Step-by-step: classify a file as confidential

1. Open the file profile.
2. Review the contents/type of physical file.
3. Edit the confidentiality level.
4. Choose the correct level such as HR Confidential, Payroll Confidential, Legal or Executive.
5. Save the profile.
6. Test with a normal user if needed to confirm restricted visibility.
7. Record access exceptions through the security/access setup if a specific user needs full access.

Step-by-step: review confidential access audit

1. Open Admin or Security panel.
2. Open confidential file access/view audit section.
3. Filter by file, user or date if available.
4. Review FULL, LIMITED or DENIED view results.
5. Investigate unusual access attempts.
6. Export the access log if needed for audit.

View result	Meaning
FULL	User was allowed to view complete details.
LIMITED	User saw masked/limited details only.
DENIED	User was not allowed to view the file.

Notifications, Escalation and Daily Digest

Notifications turn the register into an active control system. They remind users and registrars about waiting receipt, overdue files, issues and files not scanned recently.

Step-by-step: run alert check

1. Open the Notifications or Admin/Analytics area.
2. Click Run Alert Check if available.
3. Wait for completion message.
4. Review unread alerts count.
5. Open pending notifications.
6. Follow up 1-day, 3-day or 7-day overdue items according to registry policy.

Escalation logic

Trigger	Typical recipient	Purpose
1 day overdue	Receiver/current custodian	Gentle reminder.
3 days overdue	Receiver and sender	Escalation to both parties.
7 days overdue	Registry/admin fallback or sender/receiver	Registry follow-up.
30 days not scanned	Current custodian	Confirm file still exists and is under control.

File Lifecycle Management

Lifecycle controls help registry officers mark files as active, returned to registry, archived, missing, inactive or destroyed. Advanced records governance features such as legal holds and record series are not part of the current implementation scope.

Step-by-step: archive a file

1. Open the file profile.
2. Confirm the file is no longer needed for active daily work.
3. Open Lifecycle.
4. Choose Archive.
5. Select retention policy if required.
6. Enter archive note.
7. Confirm action.
8. Place the physical file in the archive location.
9. Update storage location if it moved.

Step-by-step: request destruction approval

1. Open the file profile.
2. Confirm the file is eligible for destruction according to client policy.
3. Open Lifecycle.
4. Click Request Destruction Approval.
5. Enter reason/note.
6. Submit for approval.
7. Do not destroy the physical file until approval is recorded.

Step-by-step: mark as destroyed and print certificate

1. Open the approved file profile.
2. Open Lifecycle.
3. Choose Mark Destroyed.
4. Enter certificate number or allow system to generate one.
5. Enter destruction note.
6. Save.
7. Open/print the destruction certificate.
8. File the certificate according to client policy.

Reports, Exports and Analytics

Reports and analytics help management monitor whether file custody is under control. They should be used during daily registry work, monthly audits and management review.

Report / Dashboard	Use it for
Current Custody Report	Who currently holds each file.
Files With Each Employee	Identify heavy custodians and follow-up needs.
Files In Transit	Find handovers not yet received.
Overdue Files	Escalation and compliance follow-up.
Audit Exceptions	Missing/unexpected files from physical audits.
Confidential File Access Log	Security review.
Analytics Dashboard	Overdue files, movement volume, requested files and management trends.

Step-by-step: run a report

1. Click Reports / Exports.
2. Choose the report type.
3. Enter filters such as date range, employee, category or location.
4. Click Run / Preview.
5. Review results on screen.
6. Export to CSV/Excel or print/PDF if needed.
7. Save the output to the official audit folder if required by policy.

Step-by-step: use analytics dashboard

1. Click Analytics.
2. Review key cards such as overdue files, waiting receipt and open issues.
3. Open top lists such as top custodians or most requested files.
4. Use the results to plan follow-up, audit or user training.
5. Do not treat analytics as a replacement for detailed reports when audit evidence is required.

Admin and Configuration Center

The Admin center provides setup lists used throughout the platform. Good setup data makes the system easier to use; poor setup data makes searching and reporting unreliable.

Step-by-step: add or edit setup value

1. Click Admin.
2. Select the setup area such as Categories, Classifications, Locations, Move Reasons, Statuses, Confidentiality Levels, Retention Rules or Notification Rules.
3. Click Add New or open an existing row.
4. Enter a short clear code/name and description.
5. Set Active to Yes if the value should be available.
6. Save.
7. Test by opening Register/Edit file form and confirming the value appears.

Setup naming rules

Good setup value	Avoid
HR Registry	HRREG1 without description
Employee File	Emp, employeefile, EmpFile duplicates
Payroll Confidential	Payroll secret / Pay conf duplicates
Annual Leave Request	ALR unless all users understand it

Recommended Registry Routines

A file tracking system works best when registry staff follow a routine. The routine below can be adapted for each client.

Daily routine

- [ ] Open dashboard and check files waiting for registry.
- [ ] Receive returned files by scanning.
- [ ] Check Files I Sent Out / In Transit.
- [ ] Review overdue files and contact custodians.
- [ ] Process new requests.
- [ ] Register and label new physical files.
- [ ] Upload scanned copies received that day.
- [ ] Investigate open issues.
- [ ] Close the day with no unprocessed physical files on the desk.

Weekly routine

- [ ] Run overdue report.
- [ ] Review files not scanned recently.
- [ ] Audit one cabinet/shelf/box sample.
- [ ] Review duplicate/unclear file descriptions.
- [ ] Check confidential access log.
- [ ] Confirm backup/export process if applicable.

Monthly routine

- [ ] Run custody report by employee/department.
- [ ] Review analytics trends.
- [ ] Review open issues older than 7 days.
- [ ] Review archive/lifecycle candidates.
- [ ] Conduct a formal storage audit sample.
- [ ] Report exceptions to management.

Training New Users

New users should not be trained only by describing features. They should physically scan sample files and perform the daily procedures.

Suggested 45-minute training plan

Time	Activity
0-5 min	Explain custody principle and why scanning matters.
5-10 min	Show cockpit layout and dashboard.
10-20 min	User searches and opens sample files.
20-30 min	User receives, sends and requests sample files.
30-35 min	User reports a sample issue.
35-40 min	User views/uploads an electronic document.
40-45 min	Questions and quick checklist review.

Minimum user competency checklist

User must be able to

- [ ] Search by file number.
- [ ] Scan barcode/QR/RFID.
- [ ] Receive a file.
- [ ] Send a file using outbox.
- [ ] Request a file.
- [ ] Report an issue.
- [ ] Open file profile and read custody history.
- [ ] View electronic documents.

Troubleshooting and Frequently Asked Questions

Problem	Likely Cause	What to do
Scanner types nothing	Cursor is not inside the scan box or USB reader is not connected.	Click the scan field, reconnect reader, test in Notepad, then try again.
Scanner types value but no action occurs	Reader may not send Enter automatically.	Press Enter manually after scan or configure scanner suffix to Enter.
RFID tag not found	Tag is not assigned to any file or wrong scan mode.	Search manually, open file, assign RFID if authorised.
File shows In Transit	Sender checked it out but receiver has not confirmed.	Receiver should scan/click Receive. Registrar may follow up.
Cannot see confidential file details	Your access does not allow full view.	Request access through registry or administrator.
Uploaded document will not open	File path, browser permission or access issue.	Check document link, server documents folder and user permission.
Camera scan does not start	Browser camera permission denied or unsupported.	Allow camera permission or use USB/manual scan.
Register area too narrow	Panel layout is not suitable for current work.	Use More Register Space or Register Full Screen.
SQL column error after upgrade	Schema script not applied or wrong database version.	Run the matching schema upgrade script before deploying the PHP page.
Users cannot upload documents	Upload folder permission missing.	Check documents/asset_documents folder permissions.

When to contact support

• A file record is missing from the register after confirming it exists in the old system.
• A movement was recorded to the wrong employee and cannot be corrected by normal workflow.
• A confidential file is visible to users who should not see it.
• Schema upgrade was applied but the page still reports missing database columns.
• Document uploads fail for all users.

Appendix: Registry Best Practice Checklist

Best practice checklist

- [ ] No file should circulate before registration and labelling.
- [ ] No file should be physically handed over without system check-out.
- [ ] Every receiver should confirm receipt promptly.
- [ ] Confidential files must be classified correctly.
- [ ] RFID tags must be tested after assignment.
- [ ] Electronic documents must have meaningful titles.
- [ ] Physical storage path should be precise enough for another person to locate the file.
- [ ] Audit exceptions must be resolved, not ignored.
- [ ] Bulk changes should be previewed before applying.
- [ ] Reports should be reviewed regularly by registry management.