

SASI Portal

A Day in the Life

State Administrative Systems Index
The Polity — Operational Simulation Guide

A hands-on walkthrough of daily operations across
16 user roles, 21 application modules, and the full
bureaucratic pipeline of The Polity.

Year 3, Quarter 4 — Operational Period
Generated: June 11, 2026

Table of Contents

Introduction	4
User Roster	4
Application Modules	5
0600 Hours — PL Keren, Disciplined Services	6
Asset Audit Review (MATS)	6
Sending the Discrepancy Report (SMP)	7
0800 Hours — Varen, J., First Ministry	7
Reviewing Overnight Messages (SMP)	7
Drafting a Directive (SDG)	8
Finalizing and Archiving (SDG + CARE)	8
Pushing to Gazette (SDG + GSP)	9
1000 Hours — Hald, T., Finance / Treasury	9
Reviewing the Fiscal Ledger (IFL)	9
Processing Payroll (PCS)	10
1200 Hours — Gorren, P., Public Works	10
Infrastructure Project Review (IMPT)	10
Budget Spreadsheet Update (TDP)	11
Preparing a Briefing (SPS)	11
1400 Hours — Mellen, C., BIT Archives	11
Archive Integrity Review (CARE)	12
Document Store Organization (Drive)	12
1600 Hours — Rogan, D., Interior	12
Case Management (CMDS)	12
Incident Cross-Reference (POIRS)	13

Employee Record Review (IERD)	13
1800 Hours — Kell, Workers World	14
Checking Stipend and Assignment (WWS)	14
Public Portal Services	14
Cross-System Workflow Map	15
Export Pipeline Reference	15
Quick Start: Running the SASI Portal	16

Introduction

The State Administrative Systems Index (SASI) is the unified digital backbone of The Polity, a fictional political-economic simulation state governed by a Sovereign, nine ministries, eighteen state-owned enterprises, and a 72-Title Code of Laws. SASI integrates 21 application modules ranging from document management and secure messaging to payroll, asset tracking, judicial case management, and public-facing citizen services. Every interaction within the system is governed by the Foundational Interagency Protocols (FIP), which enforce compliance, chain-of-custody, and audit-trail requirements across all modules.

This guide simulates a complete working day in The Polity, following 7 different users as they log in and out of the SASI portal, carry out their assigned duties, and move paperwork through the bureaucratic pipeline. From a First Ministry operator drafting directives at dawn to a Workers World citizen checking stipend balances at dusk, each scenario demonstrates the cross-system interconnections that make SASI more than the sum of its parts. By the end of this guide, you will understand not only how individual applications work, but how they interlock to enforce the FIP and keep the machinery of The Polity running.

User Roster

The following table lists all 16 registered SASI users. The seven users featured in this guide are marked with an asterisk. Each user has a unique role, ministry assignment, and clearance level that determines which applications and data they can access.

Username	Full Name	Role	Ministry	Clearance
varen.j *	Varen, J.	Operator	First Ministry	3
hald.t *	Hald, T.	Senior Examiner	Finance / Treasury	4
gorren.p *	Gorren, P.	Desk Chief	Public Works	3
keren *	PL Keren	DS Officer	Disciplined Services	2
mellen.c *	Mellen, C.	Archivist	BIT	2
rogan.d	Rogan, D.	Desk Chief	Interior	3
clerk.jud	Court Clerk	Clerk	Judiciary	2
ww.kell *	Kell	WW Operator	Workers World	1
admin	SASI Administrator	Admin	BIT	5
sovereign.liaison	Sovereign Liaison Velth	Sovereign Liaison	Sovereign's Office	5
dressen.m	Dressen, M.	Desk Chief	Commerce	3
foreman.l	Foreman, L.	Desk Chief	Agriculture	3

dr.seth	Dr. Seth	Examiner	Healthcare	3
ww.mira	Mira	WW Operator	Workers World	1
cas.dir	CAS Director	Director	Interior	4
mag.yuen	Magistrate Yuen	Magistrate	Judiciary	4

* Featured user in this guide. All passwords are "password" unless noted.

Application Modules

SASI comprises 21 application modules. Each module is a standalone Flask blueprint that integrates with the shared database, authentication system, and document store. The table below summarizes the core modules encountered in this guide, along with their primary functions and the FIP provisions that govern their use.

Module	Full Name	Primary Function	FIP Ref
SDG	State Document Gateway	Draft, finalize, and archive official documents	FIP-02
SMP	Secure Messaging Protocol	Internal and external correspondence with attachments	FIP-07
CARE	Central Archive & Records Entity	Long-term storage and retrieval of sealed records	FIP-02
GSP	Gazette Publication System	Draft, review, and publish official gazette notices	FIP-06
IFL	Interagency Fiscal Ledger	Chart of accounts and double-entry transaction ledger	Title VII
PCS	Payroll & Compensation System	Employee payroll processing and tax withholding	Title IX
MATS	Materiel & Asset Tracking System	Physical asset inventory, audit, and reconciliation	FIP-09
CMDS	Court Management & Docketing System	Case filing, scheduling, and judicial record management	Title VI
POIRS	Public Order & Incident Reporting	Incident reporting, escalation, and response tracking	FIP-05
IERD	Interagency Employee Registry Database	Employee records, evaluations, and organizational charts	Title IX
CHR	Clan House Registry	Clan registration, sponsorship, and conflict-of-interest tracking	Title III
IMPT	Infrastructure Maintenance & Project Tracking	Capital project budgeting, scheduling, and progress tracking	FIP-14
WWS	Worker Self-Service	Worker stipend balances, grievances, and pass requests	Title IX

CAL	Calendar	Shared governance calendar with cross-app event linking	N/A
GEO	Geospatial Information System	Interactive mapping of districts, compounds, and facilities	N/A
SPS	Slideshow Presentation System	Briefing slides with PPTX/PDF export	N/A
TDP	Tabular Data Processor	In-browser spreadsheets with XLSX/CSV export	N/A
Drive	Shared Document Store	Cross-system file storage supporting all filetypes	FIP-02
Workflow	Workflow Automation	Rule-based cross-system triggers and automated actions	Various
Public	Public WW Portal	Citizen-facing services: gazette, laws, service requests	Title IX

0600 Hours — PL Keren, Disciplined Services

The Western Garrison stirs before dawn. Platoon Leader Keren of the Disciplined Services is responsible for the FIP-09 quarterly asset reconciliation, a mandatory audit of all physical assets under DS custody. Two weapon serial numbers in Vault V-03 have already been flagged as discrepancies, and Keren must escalate them before the 0900 coordination meeting. He logs into SASI from the garrison terminal with username **keren** and password **password**.

Asset Audit Review (MATS)

PL Keren navigates to the MATS module from the portal sidebar. The asset inventory shows twelve items assigned to the Western Garrison and Armory. Two entries stand out immediately: MAT-0045 (Service Sidearm Mk. III, S/N 9901-112-A) with an audit status of "Mismatch" and MAT-0089 (Service Sidearm Mk. III, S/N 9901-113-A) with an audit status of "Missing." The FIP-09 reconciliation deadline is Day 315, and the discrepancies must be reported now to allow time for investigation before the quarterly close.

Step 1: From the SASI portal, click **MATS** in the left sidebar.

Step 2: Review the asset list. Note MAT-0045 (Mismatch) and MAT-0089 (Missing) in Vault V-03.

Step 3: Click **Escalate** on MAT-0045. This creates a POIRS incident (POIRS-2025-0007) automatically, logging the discrepancy as a formal incident report per FIP-09 Section 4.

Step 4: Click **Escalate** on MAT-0089. A second POIRS incident (POIRS-2025-0008) is created with elevated severity since the asset is unaccounted for.

Step 5: Confirm both incidents appear in POIRS with the source app listed as "MATS" and source references "MAT-0045" and "MAT-0089" respectively.

The MATS-to-POIRS escalation is a core cross-system workflow. When a FIP-09 audit discrepancy is detected, the system automatically generates an incident report in POIRS, creating a formal chain of custody record. This is not optional — it is a mandatory FIP compliance action. The workflow automation engine logs the escalation in the system events table, recording the actor (PL Keren), the source module

(MATS), the target module (POIRS), and the generated reference IDs.

Sending the Discrepancy Report (SMP)

After escalating the assets, Keren must notify his commanding officer, Captain Vassen, about the vault discrepancy. He composes a secure internal message via SMP, attaching the relevant asset records from his Drive.

Step 1: Click **SMP** in the portal sidebar.

Step 2: Click **Compose**. The recipient picker shows all registered users.

Step 3: Select **Capt. Vassen** as the recipient. (In the test system, use any available user such as "Varen, J." if Capt. Vassen is not a registered user.)

Step 4: Subject: "Armory Audit Discrepancy Report — Vault V-03." FIP Reference: "FIP-09 Section 4."

Step 5: Body: Describe the two serial mismatches and the escalation to POIRS. Reference incident IDs POIRS-2025-0007 and POIRS-2025-0008.

Step 6: Click the **Attach from Drive** dropdown and select the MAT-0045 and MAT-0089 asset files.

Step 7: Click **Send**. The message is delivered and logged with a seal hash for chain-of-custody verification.

SMP messages with attachments automatically create MessageAttachment records linking the SMP message to the DriveFile. The recipient can view the attachments inline, preview them if they are text or image files, or save copies to their own Drive. External-class messages are automatically archived to CARE per FIP routing rules.

0800 Hours — Varen, J., First Ministry

Varen is the operator at the First Ministry Coordination Desk, the central hub for inter-ministry communication. His morning begins with reviewing overnight messages, processing a new directive, and preparing it for gazette publication. He logs in with username **varen.j** and password **password**.

Reviewing Overnight Messages (SMP)

The SMP inbox displays messages from the Deputy Director (FIP-23 coordination draft), Treasury (Q4 disbursement confirmation), and Interior (Calden investigation status). Varen marks the Treasury message as read and notes the FIP-23 draft requires his markup by 0900.

Step 1: Click **SMP** in the portal sidebar. The inbox view shows unread messages with bold subject lines.

Step 2: Click on "Q4 Disbursement Schedule Confirmation" from Hald, T. to read the full message. The system marks it as read automatically.

Step 3: Note the FIP-23 coordination draft from the DD — this requires action before the 0900 deadline.

Drafting a Directive (SDG)

The Sovereign Liaison has requested a new operational directive formalizing the timber quota reduction. Varen navigates to SDG to create the document, ensuring all FIP-02 mandatory fields are populated before finalization.

Step 1: Click **SDG** in the portal sidebar. The document list shows existing documents with their status (Draft/Finalized).

Step 2: Click **Create Document**. Fill in the form:

Reference ID: **SDG-0309**

Title: **Operational Directive — Timber Yield Quota Enforcement**

Type: **Directive**

Classification: **Standard**

Origin Ministry: **Agriculture**

Origin Desk: **Forestry Division**

FIP Reference: **FIP-14 Section 2**

Subject: **Timber yield quota enforcement — 15% reduction**

Addressee: **All Clan Forestry Operations**

Body: **Pursuant to FIP-14 Section 2, all Clan forestry operations are hereby directed to reduce timber harvest yields by 15% effective Year 3 Day 315...**

Step 3: Click **Create**. The document is saved as Draft and automatically stored in the Drive as a SASI document file.

When a document is created in SDG, the system simultaneously creates a DriveFile in the Shared Document Store. This ensures every document has a persistent file representation that can be attached to messages, exported to multiple formats, or shared between users. The DriveFile is tagged with `source_app="SDG"` and `source_ref_id="SDG-0309"` for cross-referencing.

Finalizing and Archiving (SDG + CARE)

Once the Deputy Director approves the markup, Varen finalizes the document. Finalization triggers a cascade of cross-system actions that embody the FIP compliance philosophy of SASI.

Step 1: Return to the SDG module. Find SDG-0309 in the document list.

Step 2: Click **Finalize**. The system enforces FIP-02 validation: if any mandatory field (Subject, Addressee, FIP Reference, Body) is missing, the operation is rejected with a specific error message.

Step 3: Upon successful finalization, three automatic actions occur simultaneously:

a) The document status changes from "Draft" to "Finalized" and a finalization timestamp is recorded.

b) An ArchiveRecord is automatically created in CARE, generating a cross-reference ID such as CARE-0309-AG. The document is now sealed in the permanent archive.

c) A SystemEvent is logged documenting the finalization, the auto-archive action, and the actor (Varen, J.).

Step 4: Verify the archive record by navigating to **CARE** and searching for the new CARE reference ID.

Pushing to Gazette (SDG + GSP)

Timber quota directives must be published in the official gazette. Varen pushes the finalized document directly from SDG to GSP, creating a gazette submission that will be reviewed and published to the public portal.

Step 1: In the SDG module, find the finalized document SDG-0309.

Step 2: Click **Push to Gazette**. This creates a new GazetteSubmission in GSP with the document content, FIP reference, and ministry metadata pre-populated.

Step 3: Navigate to **GSP** to see the new submission in Draft status.

Step 4: Click **Submit for Review** to advance the submission to "Under Review" status.

Step 5: Once the GSP reviewer approves and clicks **Publish**, the notice is published to the Public WW Portal under the Gazette section, visible to all citizens.

The SDG-to-GSP pipeline demonstrates how a single document moves through multiple system boundaries: from draft creation (SDG) to archival (CARE) to gazette submission (GSP) to public publication (Public Portal). Each transition is logged as a SystemEvent, creating an unbroken audit trail from the moment of drafting to the moment of public disclosure.

1000 Hours — Hald, T., Finance / Treasury

Senior Examiner Hald is responsible for the quarterly payroll reconciliation and fiscal ledger integrity. The Q4 payroll run must be processed today, with disbursements recorded in the IFL ledger and linked to the PCS payroll records. He logs in with username **hald.t** and password **password**.

Reviewing the Fiscal Ledger (IFL)

Hald opens the IFL module to review the current account balances and recent transactions. The Sovereign Cash Reserves (ACT-1010) show 524,680 UE, while the Civilian Payroll account (ACT-3010) needs to be credited for the Q4 run. The most recent transaction, IFL-9816, records the Q4 payroll disbursement of 52,000 UE from the cash reserves to the payroll account, with source_module="PCS" indicating it was generated by the Payroll and Compensation System.

Step 1: Click **IFL** in the portal sidebar. The dashboard shows account balances, recent transactions, and fiscal year summary.

Step 2: Review ACT-3010 (Civilian Payroll) and verify the Q4 disbursement transaction IFL-9816 is present.

Step 3: Cross-reference the IFL transaction with the PCS payroll records to confirm that all employee payments are accounted for.

Processing Payroll (PCS)

The PCS module shows the current payroll period records. Each employee record includes base salary, tax withholding, net pay, and the linked IFL transaction ID. Hald notes that the record for Calden, T. (IERD-PW-04) shows a status of "Suspended" — a consequence of the ongoing FIP-19 investigation. His pay is being withheld pending the outcome of the Interior referral. This cross-system linkage between IERD employment status, PCS payroll processing, and CMDS case management is a critical FIP compliance mechanism.

Step 1: Click **PCS** in the portal sidebar. The payroll table lists all employees for the current period.

Step 2: Note the "Suspended" status for Calden, T. — this is linked to the FIP-19 investigation (CMDS-3005).

Step 3: Click **Run Payroll** to process the Q4 payments. The system generates IFL transactions for each employee and updates the fiscal ledger automatically.

Step 4: Export the payroll summary via **Export** button, selecting XLSX format for Treasury records.

The PCS-to-IFL linkage ensures that every payroll disbursement is automatically recorded as a fiscal transaction. The IFL transaction carries a `source_module="PCS"` tag, enabling auditors to trace any ledger entry back to its originating payroll run. This is a foundational principle of FIP financial compliance: no money moves without a corresponding ledger entry and an audit trail.

1200 Hours — Gorren, P., Public Works

Gorren assumed the interim Desk Chief position for Public Works Procurement after Calden was placed on administrative leave. His midday tasks involve reviewing infrastructure project progress, updating budget figures in TDP spreadsheets, and preparing a briefing for the First Ministry using the Slideshow Presentation System. He logs in with username **gorren.p** and password **password**.

Infrastructure Project Review (IMPT)

The IMPT module shows eight active projects. Gorren focuses on the Sector 7 Bridge Repair (IMPT-401), which has a budget of 45,000 UE with 28,000 UE already spent. The project is on schedule with a target completion date of Y3-D330. He also reviews the Compound 4-A Water Main Replacement (IMPT-402), which is 62.5% through its budget and proceeding on schedule.

Step 1: Click **IMPT** in the portal sidebar. The project dashboard shows all active, planning, and completed projects.

Step 2: Review IMPT-401 (Sector 7 Bridge Repair). Verify budget/spent figures and FIP-14 reference.

Step 3: Review IMPT-402 (Compound 4-A Water Main). Check progress against the target date.

Budget Spreadsheet Update (TDP)

Gorren needs to update the Q4 budget reconciliation spreadsheet. He opens the TDP module, locates the "Q4 Payroll Reconciliation" sheet, and adds the latest project expenditure figures. The TDP module provides an in-browser spreadsheet editor with cell-by-cell editing, formula support, and export to XLSX or CSV formats.

Step 1: Click **TDP** in the portal sidebar. The sheet list shows available spreadsheets.

Step 2: Click on "Q4 Payroll Reconciliation" to open the sheet editor.

Step 3: Update the relevant cells with the new project expenditure data from IMPT-401 and IMPT-402.

Step 4: Click **Save**. The changes are persisted to the database and the linked DriveFile is updated.

Step 5: Click **Export XLSX** to generate a downloadable Excel file for offline review.

Preparing a Briefing (SPS)

For the afternoon coordination meeting, Gorren creates a briefing presentation using the Slideshow Presentation System. He selects the "Ministry Report" template, which provides a professional layout with The Polity color scheme, and adds slides covering the bridge repair progress, water main replacement status, and budget reconciliation highlights.

Step 1: Click **SPS** in the portal sidebar. Click **New Presentation**.

Step 2: Title: "Public Works Q4 Progress Report." Template: **Ministry Report**.

Step 3: Add Slide 1 (Title/Body): "Infrastructure Progress" — summarize bridge and water main projects.

Step 4: Add Slide 2 (Two-Column): Left column: IMPT-401 budget/spent. Right column: IMPT-402 budget/spent.

Step 5: Add Slide 3 (Section Header): "Budget Reconciliation" — key figures from the TDP spreadsheet.

Step 6: Click **Present** to enter full-screen presentation mode, or **Export PPTX** to generate a PowerPoint file for distribution.

1400 Hours — Mellen, C., BIT Archives

Archivist Mellen is responsible for maintaining the integrity of the Central Archive and Records Entity. Her afternoon involves reviewing newly archived records, verifying seal hashes, and organizing the shared document store. She logs in with username **mellen.c** and password **password**.

Archive Integrity Review (CARE)

The CARE module displays all archived records with their source modules, classification levels, and seal hashes. Mellen reviews the most recent additions: CARE-3081-FM (the FIP-23 coordination protocol from SDG), CARE-3079-PW (the Calden administrative leave notice), and several older records from CMDS, IFL, and POIRS. She verifies that each record has a valid seal hash and that the source module and FIP reference fields are correctly populated.

Step 1: Click **CARE** in the portal sidebar. The archive list shows all records sorted by archival date.

Step 2: Review CARE-3081-FM. Verify the seal hash matches the source document in SDG.

Step 3: Review CARE-3079-PW. Confirm it is classified as "Internal" per the FIP-19 investigation hold.

Step 4: Export the full archive index as a PDF for the quarterly compliance report by clicking **Export** and selecting PDF format.

Document Store Organization (Drive)

The Shared Document Store (Drive) contains files from all source systems: SDG documents, TDP spreadsheets, SPS presentations, and user uploads. Mellen reviews the folder structure, checks for files that have been shared between users, and ensures that official documents are properly tagged with their source application and reference IDs.

Step 1: Click **Drive** in the portal sidebar. The file browser shows folders and files with type icons.

Step 2: Navigate to the /Documents folder. Review the SDG-origin files, checking that each has a source_app tag and source_ref_id.

Step 3: Navigate to the /Spreadsheets folder. Verify the TDP sheets are linked to their DriveFile records.

Step 4: Check shared files: Varen has shared two files with Hald (view permission), and Gorren has shared one file with Varen (edit permission). Verify these permissions in the share indicators.

Step 5: Use the **Export** function to download any file in its native format (DOCX, XLSX, PDF, etc.) for offline archival.

1600 Hours — Rogan, D., Interior

Rogan is the Desk Chief for Legal Compliance at the Interior Ministry. His primary responsibility this afternoon is advancing the FIP-19 investigation into Thoren Calden, the suspended Public Works procurement official. The investigation spans CMDS (court case), POIRS (incident tracking), and IERD (employee records), demonstrating how SASI enables cross-referential casework. He logs in with username **rogan.d** and password **password**.

Case Management (CMDS)

The CMDS module shows case CMDS-3005 (Interior Referral: T. Calden, FIP-19), currently in "Active" status before Magistrate Veln. The case has a linked incident (POIRS-3111) and references FIP-19 Section 8. Rogan reviews the case notes, which document the procurement irregularity investigation and the proto-Civil Service recommendation for escalation to a full FIP-19 investigation.

Step 1: Click **CMDS** in the portal sidebar. The case list shows all active, scheduled, and ruled-upon cases.

Step 2: Click on CMDS-3005 to view the full case details, including linked incidents and FIP references.

Step 3: Note the linked_incidents field references POIRS-3111. Click through to the incident record to verify cross-system linkage.

Step 4: Add a case note documenting the Interior referral progress and the proto-Civil Service assessment.

Incident Cross-Reference (POIRS)

Navigating to POIRS, Rogan reviews the incident linked to the Calden case. POIRS-3111 (Unauthorized Absence / Labor Violation) was the triggering event that brought Calden to the attention of Interior. He also reviews POIRS-3112 (Suspicious Activity at Harbor Pier 3), which is a separate but potentially related investigation involving NML-flagged cargo.

Step 1: Click **POIRS** in the portal sidebar. The incident dashboard shows open, under-investigation, and resolved incidents.

Step 2: Review POIRS-3111. Verify it is linked to CMDS-3005.

Step 3: Review POIRS-3112. Note the "Under Investigation" status and the DS Harbor Detail response unit assignment.

Step 4: Export the incident summary report as a PDF for the Interior Minister briefing.

Employee Record Review (IERD)

Rogan checks Calden's employee record in IERD to confirm the "Suspended" status and review the declining evaluation scores that preceded the investigation. The evaluation history shows scores of 82, 79, 65, and 40 — a clear downward trajectory that should have triggered earlier supervisory intervention.

Step 1: Click **IERD** in the portal sidebar. The employee directory lists all registered personnel.

Step 2: Search for or click on "Calden, Thoren" (IERD-PW-04). The employee profile shows classification, rank, cohort, clan affiliation, and evaluation history.

Step 3: Note the "Suspended" status and the clan affiliation: Clan Morren (Great Clan). This may represent a conflict of interest given Calden's procurement role and the Clan's commercial interests in shipping and real estate.

Step 4: Cross-reference with **CHR** (Clan House Registry) to check Clan Morren's conflict disclosures and sponsorship count.

1800 Hours — Kell, Workers World

Kell is a Tier 3 worker assigned to the Transport sector. After his shift, he accesses the Workers World Self-Service portal from a compound terminal. His SASI account has limited clearance (Level 1), restricting him to WWS, the Public Portal, and the Calendar. He logs in with username **ww.kell** and password **password**.

Checking Stipend and Assignment (WWS)

The WWS module provides Kell with a personal dashboard showing his stipend balance, current assignment, housing unit, and any open grievances or pending pass requests. Workers World citizens have the most restricted SASI access, reflecting their position in The Polity's hierarchical social structure.

Step 1: Click **WWS** in the portal sidebar. The personal dashboard displays the worker's current status at a glance.

Step 2: Review stipend balance. The amount reflects the base allowance for Tier 3 (10.0 UE) multiplied by the slab modifier and accumulated periods.

Step 3: Check housing unit assignment. Kell is assigned to a unit in Compound 4-A or 7-A depending on his registration record.

Step 4: Review any open grievances (typically 0-1) and pending pass requests (typically 0-1).

Public Portal Services

Kell can also access the public-facing portal, which provides gazette notices, the Code of Laws, ministry directory, compound maps, pay calculators, and a service request system. The public portal is the primary interface between The Polity's administrative apparatus and its Workers World citizens.

Step 1: Navigate to the **Public Portal** (accessible without login, or through the portal sidebar for authenticated users).

Step 2: Click **Gazette** to read the latest published notices, including the timber quota reduction and Q4 materiel reconciliation notice.

Step 3: Click **Services** to view available citizen services: Grievance filing, Pass requests, Housing applications, and Stipend inquiries.

Step 4: File a new service request: Type = "Pass Request," Description = "Requesting day pass for medical appointment at Sector 5 clinic." The request is routed to the Interior Ministry for processing.

Step 5: Use the **Pay Calculator** to verify stipend calculations based on tier and slab modifier.

Service requests submitted through the public portal create ServiceRequest records in the database, which are then routed to the appropriate ministry desk. The ministry operator can update the status from "Submitted" to "In Review" to "Resolved," and each transition is tracked. This provides transparency and accountability in the citizen-government interface — a core principle of The Polity's governance framework.

Cross-System Workflow Map

The power of SASI lies not in any single application but in the cross-system workflows that connect them. The following table summarizes the major cross-system actions demonstrated in this guide, showing how data flows between modules and what triggers each transition. Understanding these workflows is essential for any SASI operator, as they represent the mechanical enforcement of the Foundational Interagency Protocols.

Trigger	Source	Target	Action	FIP Ref
Document finalized	SDG	CARE	Auto-archive with seal hash	FIP-02
Document finalized	SDG	Drive	Save/update file in document store	FIP-02
Document pushed	SDG	GSP	Create gazette submission	FIP-06
Gazette published	GSP	Public	Publish to citizen portal	FIP-06
Asset discrepancy	MATS	POIRS	Create incident report	FIP-09
Payroll processed	PCS	IFL	Generate fiscal transaction	Title VII
External message	SMP	CARE	Auto-archive correspondence	FIP-07
Case linked	CMDS	POIRS	Link incident to case	FIP-05
Citizen request	Public	Ministry	Route service request	Title IX

Each cross-system action is logged in the SystemEvent table, creating a permanent audit trail. The Workflow Automation module (accessible from the portal sidebar) allows administrators to define additional rules that trigger actions based on conditions. For example, a workflow rule might automatically archive any document that has been in "Finalized" status for more than 30 days, or create a POIRS incident whenever a MATS asset audit status changes to "Missing." These rules are configurable by authorized users and their executions are logged for compliance review.

Export Pipeline Reference

Every major SASI module supports multi-format export, ensuring that data is never locked inside the system. The export pipeline generates files in industry-standard formats and automatically saves a copy to the Shared Document Store, maintaining the audit trail. The following table shows the available export formats by module. When an export is triggered, the system creates a DriveFile tagged with the source application and reference ID, ensuring that exported files remain traceable and retrievable.

Module	DOCX	PDF	ODT	XLSX	CSV	PPTX	TXT
SDG	Yes	Yes	Yes	--	--	--	Yes
SMP	Yes	Yes	--	--	--	--	Yes

TDP	--	--	--	Yes	Yes	--	--
SPS	--	Yes	--	--	--	Yes	--
CARE	Yes	Yes	--	--	--	--	--
IFL	--	Yes	--	Yes	Yes	--	--

Quick Start: Running the SASI Portal

To install and run the SASI portal for your own testing, follow these steps. The system requires Python 3.10+ and the packages listed in requirements.txt. The SQLite database is pre-seeded with realistic Polity data, including all 16 users, 8 documents, 7 messages, 10 archive records, 10 fiscal accounts, 10 payroll records, 7 court cases, 10 employees, 50 worker registrants, 8 incidents, 12 assets, 8 projects, 12 clans, 20 worker accounts, 3 spreadsheets, and a full set of system events and workflow rules.

Step 1: Extract the SASI portal zip file to a directory of your choice.

Step 2: Open a terminal and navigate to the **sasi/** directory.

Step 3: Install dependencies: **pip install -r requirements.txt**

Step 4: (Optional) Reseed the database: **python -c "from sasi import create_app; from sasi.seed import seed_all; app = create_app(); seed_all(app)"**

Step 5: Start the server: **python run.py**

Step 6: Open a browser and navigate to **http://localhost:5000**

Step 7: Log in with any of the credentials listed in the User Roster table above. All passwords are "password" except admin which is "admin".

Once logged in, the portal dashboard displays the full application catalog. Click any module in the left sidebar to begin exploring. The guide scenarios above provide specific step-by-step instructions for each featured user. Try logging in as different users to experience how the portal adapts to different roles, ministries, and clearance levels. The system is designed to be self-documenting: every action generates audit logs, and the cross-system workflows ensure that data flows correctly between modules in compliance with the FIP.