

IT Asset Repository (ITAR)

Business Requirements Document (BRD)

Version: 3.0
Date: Nov 20, 2026
Status: Final Review

Document control

Version	Date	Author	Changes
3.0	Nov 2026	Cross-Functional Team	Final Review

Table of Content

1. Introduction....4
1.1 Purpose....4
1.2 Scope....4
1.2.1 In-scope....4
1.2.2 Out of scope....5
1.3 Users....5
1.4 Business value....6
1.5 Success metrics and KPIs....6
2. Process flows....7
2.1 Browse the products....7
2.2 Request a stack....7
2.3 Admin decision....8
2.4 Product maintenance....8
3. Usage scenarios....9
3.1 A developer explores Identity stacks....9
3.2 An agency requests SSO and APIG....9
3.3 Stack admins approve one stack and decline another....9
3.4 Super admin registers a future stack....10
3.5 Admin searches stack usage....10
4. Capabilities....10
5. Functional requirements....10
5.1 FR-1: Product browsing requirements....11
5.2 FR-2: Stack detail requirements....11
5.3 FR-3: Authentication requirements....12
5.4 FR-4: Stack request requirements....13
5.5 FR-5: Admin review and decision requirements....13
5.6 FR-6: Usage register and admin search requirements....14
5.7 FR-7: Product administration requirements....15
5.8 FR-8: Dynamic Fields requirements....16
6. Non-functional requirements....18
7. Logical architecture....18
7.1 Components (indicative)....18
8. Data, security and retention....19
8.1 Data model (indicative)....19
8.2 Retention....20
8.3 Security controls....20
9. Glossary....20

1. Introduction

1.1 Purpose

ITAR is a single product portal for GovStack building blocks. It will register the current GovStack products: Feedback Block (FDBKB), Unified Client Support (UCS), Identity Conversion Block (IDCB), Single Sign-On (SSO), Master Data Management (MDMB), and Public Service Registry (PSR). It must also be flexible enough to add future products without restriction. These include the National Data Exchange (NDE), Document Management System (DMS), Notification Block (NTFB), Journaling Block (JLB), and Observability. For each building block, the portal will give clear information, including an overview, APIs, and documentation, with every item tracked by version. All products will be reachable from this one portal. The portal will also run a request-and-approval process whenever a Government Agency (GA) system wants to use a GovStack product, with the GA's details pulled from PSR.

So, this ITAR aims to:

- Give a single access point for all GovStack building blocks, from which every product can be reached.
- Give clear information on each building block, including its overview, APIs, and documentation, all tracked by version.
- Provide a secure, NDI/SSO-authenticated request and approval process for systems to use building blocks, linked to the public services they support (sourced from PSR).
- Make administrator decisions transparent and accountable: every decline carries a recorded reason, and every requester is notified of the outcome.
- Keep an authoritative record of which systems and public services use which building blocks.
- Allow new building blocks to be added without changing the system, so the number of products is not limited.

1.2 Scope

1.2.1 In-scope

- Public product portal landing page: categories, stack cards, search, filters
- Category view listing all stacks in that category
- Stack detail page: overview, features, current version and version history, APIs and documentation by version, access link, owner/contact, status
- NDI/SSO sign-in to request a stack
- Stack usage request: GA details and service from PSR, one or more stacks, system name, purpose, supporting documents

- Stack admin notification and review (with attachments); each stack approved, or declined with a mandatory reason
- Requester notification of decision; “My requests” view with status and history
- Usage register: which systems and services are approved to use which stacks
- Product administration: register current and future stacks with no limit on number; categories, versions, APIs, documents, status and the visibility of API and documentation details. All configurable with no code change
- Documents held in DMS; ITAR keeps references only
- Audit events to JLB
- Role administration: a super admin creates, reads, updates and deletes stack admins and stacks; each stack has its own stack admin(s)

1.2.2 Out of scope

- System registration stages (DST → DSD → DSOM) and division asset records (v2.0 scope)
- Physical hardware asset management, CMDB, licence compliance, vulnerability management
- Hosting, running or operating the stacks themselves
- Issuing credentials or API keys. On approval, access is provisioned by the stack team and NDE; ITAR records and notifies only
- Authentication and identity logic. NDI/SSO issues identity and role claims; ITAR enforces them
- Storing document files inside ITAR
- Billing, metering or chargeback of stack usage
- Vendor log-in. Vendors act only through the requesting agency’s user

1.3 Users

ID	User	What the role can do
IT1	Visitor	Browse categories and stacks, search, view stack overviews and any API or documentation details marked Public. No log-in
IT2	Requester	Any authenticated GA user (NDI/SSO). Sees API and documentation details released to signed-in users, or to approved systems once approved. Raises stack requests for a GA system, attaches documents, tracks own requests, receives notifications
IT3	Stack admin	Assigned to one or more stacks by the super admin. For own stacks: creates, reads, updates and deletes stack content (overview, versions, APIs, documentation) and sets who can see API and documentation details; receives requests with

ID	User	What the role can do
		attachments; approves each, or declines with a reason; revokes approvals; searches the usage register for own stacks
IT4	Super admin	Full privileges. Creates, reads, updates and deletes stack admins and stacks; manages categories, master data and dynamic fields; can act on any stack and decide any request; searches the full usage register; sees configuration history
IT5	PSR (system actor)	Supplies GA details and the list of public services for the request form
IT6	NDE / stack team (system actor)	Receives approval notice and provisions access; ITAR takes no part in provisioning

1.4 Business value

- One place for agencies and vendors to find out what GovStack offers, before they build anything.
- Less duplicate build: teams reuse approved stacks instead of building identity, gateway or document functions again.
- Consistent, documented approval of stack use, with a reason recorded for every decline.
- GovTech can answer “which systems use which stack, and for which service” from one register.
- A tamper-evident trail of every request and decision.

1.5 Success metrics and KPIs

KPI	Target	Measurement
Product coverage	100% of current GovStack products registered with current version, APIs and documentation	Product portal vs GovStack product list
Request turnaround	90% of requests decided within 5 working days	Submission vs decision timestamps
Decline quality	100% of declines carry a reason	Decline records with empty reason = 0
Usage register accuracy	100% of NDE consumers of a stack have an approved ITAR request	NDE consumer list vs usage register

KPI	Target	Measurement
Unapproved use	Zero stack calls from systems without approval	NDE logs vs register
Page performance	Product listing and detail pages load < 2 seconds (95%)	APM (Application Performance Monitoring)
Availability	99.9% monthly	Monitoring

2. Process flows

2.1 Browse the products

Step	Actor	Action	Result
1	Visitor	Opens ITAR	Landing page: category card with stack name and cards for all registered stack
2	Visitor	Clicks a category (e.g. Identity)	Category view lists its stacks (SSO, IDCB) as cards
3	Visitor	Filters by status or searches by keyword	List narrows; result count shown
4	Visitor	Clicks a stack card	Detail page: overview, version selector, APIs and documentation for that version as far as their visibility allows, access link, owner, “Request to use”

2.2 Request a stack

Step	Actor	Action	Result
1	Visitor	Clicks “Request to use” on a stack	Redirected to NDI/SSO if not signed in
2	NDI/SSO	Authenticates user	Returns identity, agency and role claims
3	ITAR	Opens request form; pre-selects the stack; pulls GA details and services from PSR	Form ready
4	Requester	Confirms GA details, selects service (PSR), adds or removes stacks, enters	Draft saved; request ID assigned

Step	Actor	Action	Result
		system name and purpose, attaches supporting documents	
5	Requester	Submits	ITAR checks mandatory fields. Fail: stays in draft with missing-field list. Pass: status "Submitted"
6	ITAR	Stores attachments in DMS; NTFB notifies the stack admin of each requested stack	Each stack appears in its stack admin's queue
All	JLB	Receives an event for every action	Audit trail

2.3 Admin decision

Step	Actor	Action	Result
1	Stack admin	Opens request from notification or queue	Sees requester, GA details, service, system name, stacks, purpose and all attachments
2	Stack admin	Approves own stack, or declines it with a reason	A decline needs a reason, or it cannot be saved
3	ITAR	Records the decision for each stack: Approved or declined	NTFB notifies requester of each stack's decision and any decline reason
4	ITAR	On approval, writes usage-register entry; notifies NDE/ stack team	Access provisioned outside ITAR (O4)
5	Stack admin	May later revoke an approval with reason	Status "Revoked"; requester and stack team notified; register updated

2.4 Product maintenance

Step	Actor	Action	Result
1	Super admin	Creates a category or stack (current or future) and assigns its stack admins	Live on next page load; stack admins notified

Step	Actor	Action	Result
2	Stack admin	Updates own stack details and publishes a new version with release notes, APIs and documentation, setting each item's visibility	Version selectable on the stack page; each item shown only to its set audience
3	Administrator	Moves a stack to Retired	Request button disabled; existing approvals retained
All	JLB	Receives configuration change events	Versioned history

3. Usage scenarios

3.1 A developer explores Identity stacks

Deki, a vendor developer, opens ITAR without signing in. She clicks Identity and sees two cards: SSO and IDCB. She opens SSO and reads the overview and the current version, v2.1, with its release notes. The OpenAPI spec and integration guide are marked Signed-in users, so she signs in with NDI/SSO to download them, then switches the version selector to v2.0 to compare the API changes. She shares the page link with her agency focal person.

3.2 An agency requests SSO and APIG

Karma (MoAL IT) clicks "Request to use" on SSO and signs in with NDI/SSO. On the form, SSO is pre-selected and MoAL's GA details are pulled from PSR. He picks the service "Livestock Vaccination Registration" from the PSR list, adds MDMB, and names the system "Livestock Vaccination Tracking System". He then enters the purpose and attaches the approval letter and architecture diagram. When he submits, ITAR refuses: the purpose is empty. He fills it in and submits again, and the status becomes "Submitted".

3.3 Stack admins approve one stack and decline another

Yeshi (SSO stack admin) gets an NTFB alert, opens the request with both attachments and approves SSO. Sonam (MDMB stack admin) gets his own alert and declines MDMB with the reason "The livestock master data the system needs is not yet published in MDMB; request again after the next MDMB release". SSO shows "Approved" and MDMB shows "Declined" with the reason. Karma is notified of both decisions, and NDE is notified to provision SSO. The usage register now shows the Livestock Vaccination Tracking System using SSO for the Livestock Vaccination Registration service.

3.4 Super admin registers a future stack

GovTech plans to release the National Data Exchange (NDE). Tashi (super admin) registers NDE under the Integration category with status Upcoming and assigns Dorji as its stack admin. Dorji uploads the overview (Public), the draft API specification (Admins only) and the documentation (Signed-in users) as version 0.9. NDE appears in the product portal the same minute, without a deployment. Because it is Upcoming, the request button is hidden. At release Dorji publishes version 1.0, changes the API specification to Signed-in users, adds the access link and sets the status to Available, and the button appears.

3.5 Admin searches stack usage

Tashi (super admin) types “MDMB” in the admin search. The results list every system using MDMB, with its service, GA, version, approval date and status, including one revoked entry with its reason. She then searches “Livestock Vaccination Tracking System” and sees the stacks that system uses: SSO, approved on the request in 4.3. Finally she filters by Category = Identity and GA = MoAL to see every Identity stack MoAL systems use, and exports the list to CSV. Sonam, the MDMB stack admin, running the same searches sees only MDMB results.

4. Capabilities

- Single public portal for all GovStack products, browsable by category, with search and status filters
- Stack pages with overview, APIs and documentation tracked by version, and an access link to each stack
- NDI/SSO-gated stack requests with GA details and services pulled from PSR, and supporting documents
- Per-stack decisions by each stack’s stack admin, with a mandatory decline reason
- Notifications to stack admins and requesters through NTFB
- Usage register with admin filter search: by stack (which systems use it) or by system (which stacks it uses)
- No-code registration of current and future stacks, with no limit on number
- Stack-admin-set visibility for API and documentation details
- Super admin control: create, read, update and delete stack admins and stacks
- JLB audit of every request, decision and configuration change

5. Functional requirements

MoSCoW priority. Acceptance criteria are verifiable conditions.

5.1 FR-1: Product browsing requirements

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-1.1	Landing page shows category tiles and stack cards for all registered stacks	MUST	Each tile shows the name and stack name.
ITAR-FR-1.2	Selecting a category lists only its stacks	MUST	Identity shows SSO and IDCB only; result count displayed
ITAR-FR-1.3	Stack card shows name, one-line description, category and status lifecycle	MUST	All five elements on every card
ITAR-FR-1.4	Filter by status (Available, Upcoming, Retired) combinable with category	MUST	Combined filter returns the intersection
ITAR-FR-1.5	Keyword search over stack name, description, category and features	MUST	Results within 2 s; “Identity” returns SSO and IDCB
ITAR-FR-1.6	Product listing and detail pages viewable without log-in	MUST	No NDI/SSO prompt until “Request to use”
ITAR-FR-1.7	Each stack has a stable shareable URL	SHOULD	URL opens the same stack after updates

5.2 FR-2: Stack detail requirements

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-2.1	Detail page shows overview, key features, status	MUST	All sections render; empty sections hidden
ITAR-FR-2.2	Shows current version with release date and release notes	MUST	Version and date always visible at top
ITAR-FR-2.3	Version selector lists every version with its release notes	MUST	Ordered newest first; selecting a version shows its APIs and documentation

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-2.4	API section lists API name, description and spec (OpenAPI file or link) for the selected version, each shown only to the audience its stack admin sets	MUST	Items hidden from audiences not allowed, in the UI and the API
ITAR-FR-2.5	Documentation section lists user and integration guides for the selected version, served from DMS, each shown only to the audience its stack admin sets	MUST	Public items open without log-in; other items require NDI/SSO and the set audience; DMS checks access on every open
ITAR-FR-2.6	“Request to use” button shown for Available stacks only	MUST	Hidden for Upcoming and Retired
ITAR-FR-2.7	Shows the number of systems using the stack	SHOULD	Count only to visitors; list to the stack admin and super admin
ITAR-FR-2.8	Visibility levels for each API and document: Public, Signed-in users, Approved systems, Admins only	MUST	New items default to Admins only until the stack admin sets a level; a change applies on next page load

5.3 FR-3: Authentication requirements

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-3.1	Requesting requires NDI/SSO sign-in	MUST	Unauthenticated request API calls return 401
ITAR-FR-3.2	Requester identity and role taken from token claims; GA details pulled from PSR	MUST	Pre-filled and read-only on the form
ITAR-FR-3.3	Stack admin and super admin functions restricted to role claims, enforced server-side; a stack admin acts only on stacks assigned to them	MUST	Calls outside the role or assignment return 403 and are logged to JLB

5.4 FR-4: Stack request requirements

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-4.1	Request form pre-selects the stack from which it was opened	MUST	Selected stack shown on load
ITAR-FR-4.2	GA details and service list pulled from PSR; requester selects one service	MUST	Values match PSR; cached copy used if PSR unavailable
ITAR-FR-4.3	Requester may add or remove stacks (requestable stacks only)	MUST	Multi-select; only Available stacks offered
ITAR-FR-4.4	System name is mandatory	MUST	Submit refused while empty
ITAR-FR-4.5	Purpose is mandatory	MUST	Submit refused while empty
ITAR-FR-4.6	At least one supporting document is mandatory; files stored in DMS	MUST	ITAR stores reference, name, type, uploader, time; allowed types and size limit configurable
ITAR-FR-4.7	Drafts can be saved before submission	MUST	Unique immutable request ID on first save
ITAR-FR-4.8	Warn on an existing open or approved request for the same system and stack	SHOULD	Warning lists matches; requester may continue or cancel
ITAR-FR-4.9	Requester can withdraw before decision	SHOULD	Status “Withdrawn”; stack admins notified
ITAR-FR-4.10	“My requests” lists own requests with status, decision, reasons and history	MUST	Sortable by date and status

5.5 FR-5: Admin review and decision requirements

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-5.1	On submission, the stack admin of each requested stack is notified through NTFB	MUST	Notification names requester, GA, system, service and stack

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-5.2	Each stack admin's queue lists pending requests for own stacks, with age; the super admin sees all	MUST	Filter by stack, GA, status; oldest first by default
ITAR-FR-5.3	Stack admin sees the full request and opens all attachments	MUST	Attachments open via DMS with stack admin access
ITAR-FR-5.4	Stack admin approves, or declines with a reason, each requested stack they administer; the super admin can decide any	MUST	Each stack carries its own status, Approved or Declined; no partial-approval status exists
ITAR-FR-5.5	Decline requires a reason	MUST	Save refused with empty reason
ITAR-FR-5.6	Requester notified of decision with reasons through NTFB	MUST	Notification sent within 1 minute of decision
ITAR-FR-5.7	On approval, NDE and stack owner notified to provision access	MUST	Notice contains system, service, stack and requester
ITAR-FR-5.8	Stack admin can revoke an approval with reason	SHOULD	Status "Revoked"; requester and stack owner notified; register updated
ITAR-FR-5.9	Decision stores approver, time, decision, reason	MUST	Immutable once saved; visible in history

5.6 FR-6: Usage register and admin search requirements

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-6.1	Each approved stack line creates a register entry: system, service, GA, stack, version, approver, date	MUST	Entry present immediately after approval

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-6.2	Admin search by stack: entering a stack name returns every system using that stack	MUST	Searching “MDMB” lists each system using MDMB, with service, agency, version, approval date, and status
ITAR-FR-6.3	Admin search by system: entering a system name returns every stack that system uses	MUST	Searching “Livestock Vaccination Tracking System” lists each stack it uses, with version, approval date, and status
ITAR-FR-6.4	Admin filters, combinable with search: category, stack, system, service, GA, status (Approved, Revoked), approval date range	MUST	Filters return the intersection; result count shown; results within 2 s
ITAR-FR-6.5	Search suggests matching stacks and systems as the admin types	SHOULD	Each suggestion labelled Stack or System
ITAR-FR-6.6	Each result opens its originating request with attachments and decision history	MUST	Opens from the result row
ITAR-FR-6.7	Revoked entries remain with status and reason	MUST	Not deleted; shown when the status filter includes Revoked
ITAR-FR-6.8	Usage register and admin search available to stack admins (own stacks only) and the super admin (all stacks)	MUST	Stack admin results limited to own stacks; other calls return 403 and are logged to JLB

5.7 FR-7: Product administration requirements

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-7.1	Super admin creates, edits, reorders and deactivates categories without code change	MUST	Live on next page load

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-7.2	Super admin registers current and future stacks and can edit every stack like stack admin; stack admins edit own stacks: name, category, description, owner, status	MUST	Live on next page load; no limit on the number of stacks or categories
ITAR-FR-7.3	Stack admin publishes versions with release notes, APIs and documentation	MUST	New version becomes current; earlier versions stay selectable
ITAR-FR-7.4	Stack admin uploads or links API specs and documents and sets each item's visibility	MUST	Visibility enforced per FR-2.8
ITAR-FR-7.5	Stacks or categories holding requests can be deactivated, not deleted	MUST	Delete blocked; history retained
ITAR-FR-7.6	Every configuration change versioned with user and time	MUST	History visible to administrators and sent to JLB
ITAR-FR-7.7	Super admin creates, updates and deletes stack admin accounts and have the same privileges as stack admin to manage the content of each and every stack	MUST	Changes effective on next sign-in; deleting a stack admin removes their assignments; history kept
ITAR-FR-7.8	Super admin assigns and removes stack admins per stack; a stack can have more than one	MUST	Removing the last stack admin of an Available stack is refused
ITAR-FR-7.9	Stack admin creates, reads, updates and deletes the content of own stacks only	MUST	Changes to other stacks return 403 and are logged to JLB

5.8 FR-8: Dynamic Fields requirements

ID	Requirement	Priority	Acceptance criteria
ITAR-FR-8.1	Super admin adds a field to any form or page, at any time: category, stack detail page,	MUST	Field appears in the chosen place on the next page load;

ID	Requirement	Priority	Acceptance criteria
	request form, decision form, usage register entry		no code change or redeployment
ITAR-FR-8.2	Field types: text, long text, number, date, dropdown, multi-select, checkbox, URL, email, phone, document (stored in DMS)	MUST	Each type validates its input
ITAR-FR-8.3	Field properties: label, mandatory flag, default value, validation rule, section and display order	MUST	Each property takes effect on next page load
ITAR-FR-8.4	Visibility set per field; public, requester or admin only	MUST	Field hidden from roles not allowed, in the UI and the API
ITAR-FR-8.5	Super admin creates and edits dropdown value lists without code change	MUST	New values selectable immediately; deactivated values stay on existing records but cannot be chosen
ITAR-FR-8.6	Mandatory dynamic fields enforced on submit and save	MUST	Submit refused with a missing field list
ITAR-FR-8.7	A field holding data can be deactivated, not deleted	MUST	Deleted blocked; field hidden from forms; values kept in history
ITAR-FR-8.8	Dynamic fields searchable and filterable in admin search	MUST	Field usable as search term and filter once it holds data
ITAR-FR-8.9	Super admin previews a form before publishing a field change	SHOULD	Preview shows the layout without changing the live form
ITAR-FR-8.10	Every field change versioned with user and time	MUST	History visible to the super admin and sent to JLB

6. Non-functional requirements

The common NFR Annexure applies; where it and the targets below differ, the stricter one prevails.

ID	Area	Target
ITAR-NFR-1	Availability	99.9% monthly excluding approved maintenance
ITAR-NFR-2	Performance	Product, category, detail and search < 2 s (95%)
ITAR-NFR-3	Configurability	Categories, stacks, versions, master data and dynamic fields changed without code change or redeployment
ITAR-NFR-4	Security	OWASP Top 10
ITAR-NFR-5	Public exposure	Public pages read-only; WAF and rate limiting; no request or register data, and no API or documentation item above Public, on public pages
ITAR-NFR-6	Auditability	Every request, decision and configuration change produces a JLB event
ITAR-NFR-7	Retention	Requests, decisions and register kept 10 years after stack sunset
ITAR-NFR-8	Accessibility	WCAG 2.1 AA
ITAR-NFR-9	Concurrency	500 concurrent visitors; 100 concurrent authenticated users
ITAR-NFR-10	Responsive	Usable on desktop, tablet and mobile

7. Logical architecture

7.1 Components (indicative)

Component	Responsibility	Technology
Product Service	Categories, stacks, versions, API and document references	Node.js or Spring Boot; PostgreSQL
Request Service	Request lifecycle, per-stack decisions, register	Same stack

Component	Responsibility	Technology
Search Service	Product and register search	Elasticsearch or PostgreSQL full-text
Portal UI	Public stack pages, request form, My requests, admin console	React; UDS components
PSR Adapter	GA details and service list with cache	REST client via NDE
Document Adapter	DMS upload and access delegation	DOCS REST client
Notification Dispatcher	Stack admin, requester, NDE/stack-owner notices	NTFB client
JLB Publisher	At-least-once audit delivery with local buffer	Kafka producer

8. Data, security and retention

8.1 Data model (indicative)

Entity	Attributes
CATEGORY	category_id, name (dz/en), icon, description, order, active
STACK	stack_id, code, name, category_id, logo, short_desc, overview, features, owner_team, contact, access_url, status, active
STACK_VERSION	version_id, stack_id, version_no, release_date, release_notes, is_current
API_REF	api_id, stack_id, version_id, name, description, spec_ref, visibility
DOC_REF	doc_id, stack_id or request_id, version_id, dms_ref, name, type, visibility, uploaded_by, uploaded_at
REQUEST	request_id, requester_id, ga_id (PSR), service_id (PSR), system_name, purpose, status, submitted_at
REQUEST_LINE	line_id, request_id, stack_id, version_id, decision, reason, decided_by, decided_at
USAGE_REGISTER	entry_id, line_id, ga_id, system_name, service_id, stack_id, status, approved_at, revoked_at, revoke_reason

Entity	Attributes
ADMIN_ASSIGNMENT	assignment_id, user_id, role (stack admin / super admin), stack_id, assigned_by, assigned_at, active
CHANGE_LOG	entity, entity_id, old, new, user, changed_at, jlb_ref
FIELD_DEFINITION	Field_id, placement (category, stack, request, decision, register), selection, label (dz/en), type, value_list_id, mandatory, default, validation, visibility, display_order, help_text, active, version
VALUE_LIST/VALUE	List_id, name, active/value_id, list_id, label(dz/en), display_order, active
FIELD_VALUE	Entity, entity_id, field_id, value, updated_by, updated_at

8.2 Retention

Category	Hot	Archive
Product and version history	Indefinite	—
Requests, decisions, register	10 years after stack retirement	JSON export to GTA archive
Audit events	1 year	10 years via JLB WORM

8.3 Security controls

- TLS 1.3 in transit; AES-256 at rest.
- NDI/SSO token claims are authoritative for identity, agency and admin role. They are enforced at NDE and in the services, not only in the UI.
- Attachments are never exposed on public pages; DOCS enforces access on every open.
- Admin decisions and revocations require two-factor confirmation.
- Inputs validated against OpenAPI 3.0 schemas; attachments malware-scanned before storage.

9. Glossary

Term	Definition
Stack	GovStack building block offered to GA systems as a shared service
Category	Grouping of stacks in the product (e.g. Identity, NDE, DOCS)
APIM / APIG	API Manager / API Gateway (NDE stacks)

Term	Definition
DOCS	Document Store
GA system	GovTech Agency-owned or -managed system
JLB	Journaling block (audit)
NDE	National Data Exchange / API gateway
NDI	National Digital Identity
NTFB	Notification block
PSR	Public Service Registry
SSO	Single Sign-On
Usage register	Record of which systems and services are approved to use which stacks