## [**https://gemini.google.com/u/1/app/fd47ede3d905a3f2**](https://gemini.google.com/u/1/app/fd47ede3d905a3f2)

<https://gemini.google.com/u/1/app/440838222ac514d7>

Production-Ready Specification: public.user\_roles\_master Table

Version: 2.1 (Checklist V2-05-17-B Applied)

Date: 2025-05-17

1. Purpose & Primary Use-Cases

Mission Statement: To define and describe all available user roles within the pilgrimage platform, serving as the authoritative source for role codes, their default names/descriptions (in the primary reference language), permission summaries, UI icons, and audit trails for changes.

Key User-Story Touchpoints:

• Pilgrim, Host, Manager: Their assigned roles originate from this table. [cite: 428]

• Platform Administrator: Manages role definitions and assignments. [cite: 429]

• System: `handle\_new\_user` trigger queries for default role; `check\_profile\_roles` trigger validates against this table. [cite: 430]

2. Schema

| column | data\_type | constraints | description |

| :------------------------------ | :------------------------ | :----------------------------------------------------------------------------------------------------------------------------------- | :------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------- |

| role\_code | text | Primary Key, Not Null, CHECK (`role\_code` = lower(`role\_code`) AND `role\_code` ~ '^[a-z0-9\_]+$') | 🟠 Short, unique, machine-readable, lowercase role code (e.g., `pilgrim\_user`). Used in `profiles.roles`. [cite: 1371] |

| default\_display\_name | text | Not Null | Human-readable name in the primary reference language (e.g., "Pilgrim User"). (Translatable via `public.translations`) [cite: 1371] |

| default\_description | text | Nullable | Detailed description of the role in the primary reference language. (Translatable via `public.translations`) [cite: 1371] |

| icon\_identifier | text | Nullable | Optional identifier for a UI icon representing the role (e.g., a Material Design Icon name like 'person\_outline'). |

| permissions\_summary\_json | jsonb | Nullable | JSONB storing a human-readable summary of key permissions (e.g., `{"can\_edit\_own\_profile": true}`). For documentation/admin UI; enforcement via RLS/app logic. [cite: 1371] |

| role\_hierarchy\_level | integer | Nullable | Optional numerical level for role precedence (e.g., admin=100, pilgrim=10). Higher implies more privileges. [cite: 1371] |

| is\_system\_role | boolean | Not Null, Default false | If true, this is a core system role (e.g., `admin\_super`, `pilgrim\_user`) resistant to easy deletion/modification. [cite: 1371] |

| is\_role\_active | boolean | Not Null, Default true | If true, the role is active and assignable. Inactive roles might be deprecated or for future use. [cite: 1371] |

| default\_for\_new\_pilgrim\_users | boolean | Not Null, Default false, Unique Partial Index `uq\_one\_default\_for\_new\_pilgrim\_users` WHERE (`default\_for\_new\_pilgrim\_users` = TRUE) | 🟠 If true, this `role\_code` is auto-assigned to new standard pilgrim users. Only one role should have this true. [cite: 1371] |

| created\_at | timestamp with time zone | Not Null, Default `now()` | Timestamp of role definition creation. |

| updated\_at | timestamp with time zone | Not Null, Default `now()` | Timestamp of last role definition update (auto-updated by trigger). |

| created\_by\_profile\_id | uuid | Nullable, Foreign Key to `public.profiles(id)` ON DELETE SET NULL | Profile ID of the user who initially created this role entry. |

| updated\_by\_profile\_id | uuid | Nullable, Foreign Key to `public.profiles(id)` ON DELETE SET NULL | Profile ID of the user who last updated this role entry. |

| deleted\_at | timestamp with time zone | Nullable | Timestamp for soft deletion of a role definition. Prefer `is\_role\_active = false` for retiring roles in use. Checked by `check\_profile\_roles` trigger. [cite: 1371] |

3. PostgreSQL DDL

-- Table Definition

CREATE TABLE public.user\_roles\_master (

role\_code text NOT NULL PRIMARY KEY,

default\_display\_name text NOT NULL,

default\_description text NULL,

icon\_identifier text NULL,

permissions\_summary\_json jsonb NULL,

role\_hierarchy\_level integer NULL,

is\_system\_role boolean NOT NULL DEFAULT false,

is\_role\_active boolean NOT NULL DEFAULT true,

default\_for\_new\_pilgrim\_users boolean NOT NULL DEFAULT false,

created\_at timestamp with time zone NOT NULL DEFAULT now(),

updated\_at timestamp with time zone NOT NULL DEFAULT now(),

created\_by\_profile\_id uuid NULL REFERENCES public.profiles(id) ON DELETE SET NULL,

updated\_by\_profile\_id uuid NULL REFERENCES public.profiles(id) ON DELETE SET NULL,

deleted\_at timestamp with time zone NULL,

CONSTRAINT check\_role\_code\_format CHECK (role\_code = lower(role\_code) AND role\_code ~ '^[a-z0-9\_]+$')

);

-- Unique Partial Index to ensure only one role is default for new pilgrim users

CREATE UNIQUE INDEX uq\_one\_default\_for\_new\_pilgrim\_users

ON public.user\_roles\_master (default\_for\_new\_pilgrim\_users)

WHERE (default\_for\_new\_pilgrim\_users = TRUE); [cite: 1374]

-- Indexes

CREATE INDEX idx\_user\_roles\_master\_active\_default ON public.user\_roles\_master (is\_role\_active, default\_for\_new\_pilgrim\_users); [cite: 1375]

CREATE INDEX idx\_user\_roles\_master\_created\_by\_profile\_id ON public.user\_roles\_master (created\_by\_profile\_id) WHERE created\_by\_profile\_id IS NOT NULL;

CREATE INDEX idx\_user\_roles\_master\_updated\_by\_profile\_id ON public.user\_roles\_master (updated\_by\_profile\_id) WHERE updated\_by\_profile\_id IS NOT NULL;

-- Comments

COMMENT ON TABLE public.user\_roles\_master IS 'Defines all available user roles, their default names/descriptions (in primary reference language), permission summaries, UI icons, and audit trails for RBAC. Version 2.1.'; [cite: 1376]

COMMENT ON COLUMN public.user\_roles\_master.role\_code IS 'PK. Short, unique, machine-readable, lowercase role code (e.g., pilgrim\_user). Used in profiles.roles.'; [cite: 1377]

COMMENT ON COLUMN public.user\_roles\_master.default\_display\_name IS 'Human-readable name in the primary reference language. (Translatable via translations table).';

COMMENT ON COLUMN public.user\_roles\_master.default\_description IS 'Detailed description of the role in the primary reference language. (Translatable via translations table).';

COMMENT ON COLUMN public.user\_roles\_master.icon\_identifier IS 'Optional identifier for a UI icon representing the role (e.g., a Material Design Icon name like ''person\_outline'').';

COMMENT ON COLUMN public.user\_roles\_master.permissions\_summary\_json IS 'JSONB storing a human-readable summary of key permissions. For documentation/admin UI; enforcement via RLS/app logic.';

COMMENT ON COLUMN public.user\_roles\_master.is\_system\_role IS 'If true, this is a core system role resistant to easy deletion/modification.';

COMMENT ON COLUMN public.user\_roles\_master.default\_for\_new\_pilgrim\_users IS 'If true, role is auto-assigned to new pilgrims. Enforced unique true value by partial index.';

COMMENT ON COLUMN public.user\_roles\_master.created\_by\_profile\_id IS 'Profile ID of the user who initially created this role entry. FK to profiles.id. ON DELETE SET NULL.';

COMMENT ON COLUMN public.user\_roles\_master.updated\_by\_profile\_id IS 'Profile ID of the user who last updated this role entry. FK to profiles.id. ON DELETE SET NULL.';

COMMENT ON COLUMN public.user\_roles\_master.deleted\_at IS 'Timestamp for soft deletion. Prefer is\_role\_active = false for retiring roles in use. Used by profiles.check\_profile\_roles trigger.';

4. Triggers/Functions

-- Trigger for updated\_at timestamp

CREATE TRIGGER handle\_user\_roles\_master\_updated\_at

BEFORE UPDATE ON public.user\_roles\_master

FOR EACH ROW

EXECUTE FUNCTION extensions.moddatetime('updated\_at'); -- Using Supabase standard [cite: 1384]

-- Trigger function to clean up related translations on delete

CREATE OR REPLACE FUNCTION public.cleanup\_user\_roles\_master\_translations()

RETURNS TRIGGER AS $$

BEGIN

DELETE FROM public.translations

WHERE table\_identifier = 'user\_roles\_master'

AND row\_foreign\_key = OLD.role\_code;

RETURN OLD;

END;

$$ LANGUAGE plpgsql SECURITY DEFINER;

-- Apply the cleanup trigger for translations

CREATE TRIGGER trigger\_cleanup\_user\_roles\_master\_translations

AFTER DELETE ON public.user\_roles\_master

FOR EACH ROW

EXECUTE FUNCTION public.cleanup\_user\_roles\_master\_translations();

5. JSON Schema Mirror

{

"title": "user\_role\_master",

"description": "Defines user roles, their default display attributes (translatable), permission summaries, UI icons, and audit trails. Version 2.1.",

"type": "object",

"properties": {

"role\_code": { "type": "string", "description": "PK. Machine-readable role code.", "pattern": "^[a-z0-9\_]+$" },

"default\_display\_name": { "type": "string", "description": "Default human-readable name (primary lang). Translatable." },

"default\_description": { "type": ["string", "null"], "description": "Default detailed description (primary lang). Translatable." },

"icon\_identifier": { "type": ["string", "null"], "description": "Optional UI icon identifier." },

"permissions\_summary\_json": { "type": ["object", "null"], "description": "JSONB summary of permissions for UI/docs." },

"role\_hierarchy\_level": { "type": ["integer", "null"], "description": "Optional numerical hierarchy level." },

"is\_system\_role": { "type": "boolean", "default": false, "description": "True if a core system role." },

"is\_role\_active": { "type": "boolean", "default": true, "description": "True if role is active and assignable." },

"default\_for\_new\_pilgrim\_users": { "type": "boolean", "default": false, "description": "True if auto-assigned to new users (only one)." },

"created\_at": { "type": "string", "format": "date-time", "description": "Timestamp of creation.", "readOnly": true },

"updated\_at": { "type": "string", "format": "date-time", "description": "Timestamp of last update.", "readOnly": true },

"created\_by\_profile\_id": { "type": ["string", "null"], "format": "uuid", "description": "Profile ID of creator." },

"updated\_by\_profile\_id": { "type": ["string", "null"], "format": "uuid", "description": "Profile ID of last updater." },

"deleted\_at": { "type": ["string", "null"], "format": "date-time", "description": "Timestamp for soft deletion.", "readOnly": true }

},

"required": [ "role\_code", "default\_display\_name", "is\_system\_role", "is\_role\_active", "default\_for\_new\_pilgrim\_users" ],

"primary\_key": ["role\_code"],

"unique\_constraints": [

{"columns": ["default\_for\_new\_pilgrim\_users"], "name": "uq\_one\_default\_for\_new\_pilgrim\_users", "where\_clause": "default\_for\_new\_pilgrim\_users = TRUE"}

],

"foreign\_keys": [

{"columns": ["created\_by\_profile\_id"], "references\_table": "public.profiles", "references\_columns": ["id"], "on\_delete": "SET NULL"},

{"columns": ["updated\_by\_profile\_id"], "references\_table": "public.profiles", "references\_columns": ["id"], "on\_delete": "SET NULL"}

]

}

6. Relationships & Integrity

Primary Key: `role\_code` (text).

Foreign Keys:

• `created\_by\_profile\_id` references `public.profiles(id)`: ON DELETE SET NULL.

• `updated\_by\_profile\_id` references `public.profiles(id)`: ON DELETE SET NULL.

Referenced By: `profiles.roles` (validated by `check\_profile\_roles()` trigger). `translations` table for translatable fields.

Junction/Lookup Tables: This table \*is\* a lookup table.

Mermaid ER Snippet:

erDiagram

profiles { uuid id PK }

user\_roles\_master {

text role\_code PK

text default\_display\_name "Translatable"

text default\_description "Translatable"

text icon\_identifier

boolean default\_for\_new\_pilgrim\_users "Partial UK (TRUE)"

boolean is\_role\_active

uuid created\_by\_profile\_id FK

uuid updated\_by\_profile\_id FK

timestamptz deleted\_at

}

translations { text table\_identifier; text column\_identifier; text row\_foreign\_key }

profiles ..> user\_roles\_master : "roles array contains role\_code"

user\_roles\_master ..> translations : "default\_display\_name translated in"

user\_roles\_master ..> translations : "default\_description translated in"

user\_roles\_master }o--o| profiles : "created\_by (admin)"

user\_roles\_master }o--o| profiles : "updated\_by (admin)"

7. Multilingual Strategy

Translatable Fields: `default\_display\_name`, `default\_description` store primary reference language text. Translated versions are in `public.translations`. An `AFTER DELETE` trigger on this table ensures orphaned translations are cleaned up.

8. Role-Based Workflow & RLS Notes

Key Fields: `is\_system\_role`, `is\_role\_active`, `default\_for\_new\_pilgrim\_users`, `deleted\_at`.

RLS Policies:

• 🟢 Public read for active/system roles.

```sql

CREATE POLICY "select\_active\_or\_system\_roles" ON public.user\_roles\_master FOR SELECT USING (is\_role\_active = true OR is\_system\_role = true);

```

• 🟢 Admins manage all role definitions.

```sql

CREATE POLICY "admin\_manage\_all\_user\_roles" ON public.user\_roles\_master FOR ALL

USING (public.has\_role('admin\_platform') OR public.has\_role('admin\_super'))

WITH CHECK (public.has\_role('admin\_platform') OR public.has\_role('admin\_super'));

```

🟠 Caution on modifying/deleting `is\_system\_role` roles.

9. ENUM vs Lookup Discussion

🟢 This table \*is\* a lookup table, which is appropriate.

10. UI/UX Enablement

Columns powering UI: `default\_display\_name` (translated), `default\_description` (translated), `icon\_identifier`, `permissions\_summary\_json`, `is\_role\_active`, `is\_system\_role`.

Indexed Fields: PK, `idx\_user\_roles\_master\_active\_default`.

11. Auditing & Lifecycle Management

Audit Columns: `created\_at`, `updated\_at` (auto-managed). `created\_by\_profile\_id`, `updated\_by\_profile\_id` added for admin change tracking.

Lifecycle: `is\_role\_active` for retiring roles. `deleted\_at` for hard deletion (checked by `profiles` trigger).

12. Scalability & Future-Proofing

Scalability: Table will remain small and performant.

Future-Proofing: `role\_hierarchy\_level`, `permissions\_summary\_json`, `icon\_identifier` allow for evolution.

13. Seed Data (V1)

| role\_code | default\_display\_name | default\_description | icon\_identifier | is\_system\_role | is\_role\_active | default\_for\_new\_pilgrim\_users | created\_by\_profile\_id | updated\_by\_profile\_id |

| :------------------------ | :------------------------ | :--------------------------------------- | :-------------- | :------------- | :------------- | :---------------------------- | :-------------------- | :-------------------- |

| 'pilgrim\_user' | 'Pilgrim User' | 'Standard user planning or on a pilgrimage.' | 'person' | true | true | true | `[ADMIN\_UUID]` | `[ADMIN\_UUID]` |

| 'accommodation\_host' | 'Accommodation Host' | 'Manages accommodation listings.' | 'hotel' | false | true | false | `[ADMIN\_UUID]` | `[ADMIN\_UUID]` |

| 'regional\_content\_manager'| 'Regional Content Manager'| 'Manages content for specific regions.' | 'edit\_location' | false | true | false | `[ADMIN\_UUID]` | `[ADMIN\_UUID]` |

| 'content\_moderator' | 'Content Moderator' | 'Moderates user-generated content.' | 'gavel' | false | true | false | `[ADMIN\_UUID]` | `[ADMIN\_UUID]` |

| 'admin\_platform' | 'Platform Administrator' | 'Manages overall platform settings.' | 'admin\_panel\_settings' | true | true | false | `[ADMIN\_UUID]` | `[ADMIN\_UUID]` |

| 'admin\_super' | 'Super Administrator' | 'Full system access, manages core data.' | 'security' | true | true | false | `[ADMIN\_UUID]` | `[ADMIN\_UUID]` |

\*(Note: `[ADMIN\_UUID]` is a placeholder for an actual admin/system user profile ID used for seeding.)\*

14. Next-Action Checklist

• 🔴 Create Table: Execute DDL for `public.user\_roles\_master` including new audit columns and `icon\_identifier`.

• 🔴 Create Unique Partial Index `uq\_one\_default\_for\_new\_pilgrim\_users`.

• 🟢 Create Additional Indexes: `idx\_user\_roles\_master\_active\_default` and indexes for audit FKs.

• 🔴 Implement `updated\_at` Trigger using `extensions.moddatetime`.

• 🔴 Implement Translations Cleanup Trigger: Create and apply `trigger\_cleanup\_user\_roles\_master\_translations` (AFTER `public.translations` table is created).

• 🔴 Pre-populate Seed Data: Insert initial V1 roles as defined in Section 13.

• 🟢 Define `icon\_identifier` convention/source for roles.

• 🟠 Define how `created\_by\_profile\_id` and `updated\_by\_profile\_id` will be populated (application layer for admin actions, or manually for migrations).