UID/GID Standards

UID/GID Standards

The Flora Family homelab uses a standardized UID/GID mapping system to ensure security, prevent ID collisions, and simplify file permission management across the container infrastructure.

□□ Infrastructure Core (System IDs)

These IDs are reserved for the underlying data layers and databases.

- **70:70 (Postgres):** Standard ID for all Postgres and pgvector instances.
- **970:970 (Redis/Valkey):** Standard ID for all Redis and Valkey caching/session instances.

□□ Family & Admin (50,000 Block)

Reserved for human users and administrative bots.

- **50002:60002:** Christopher
- **50003:60003:** Erin
- **50001:60001:** Media (Service account for shared media access)
- **50004:60004:** Flobot (The Robot)

□□ Automated Services (51,000 Block)

Reserved for containerized services and application logic.

UID	GID	Service	Category

51004	61004	Caddy	Core Proxy
51010	61010	Paperless	Organizational
51020	61020	BookStack	Organizational
51052	61052	Immich	Media/Photos
51054	61054	n8n	Automation
51055	61055	OpenWebUI	AI Interface
51100	61100	Minecraft	Gaming
51101	61101	Foundry	Gaming

□□ Security Principles

1. **Non-Root Execution:** No containers (except Watchtower & beszel-agent) run as root.
2. **Config Isolation:** All docker-compose files in `/srv` are owned by `root:root` with 755/644 permissions.
3. **Data Ownership:** All volume mounts in `/main/appdata` are owned by their respective service account.
4. **Least Privilege:** env files are restricted to `600` permissions.

Revision #2
Created 2026-02-09 14:35:33 UTC by Chris
Updated 2026-02-09 14:37:08 UTC by Chris