

# Backup and Recovery

# Backup and Recovery

| Field              | Value                                                            |
|--------------------|------------------------------------------------------------------|
| Distribution       | WCT English — OpenC5ISR                                          |
| Product            | OpenC5ISR                                                        |
| Release            | 0.15.1                                                           |
| Deployment         | openc5isr-en.wallacecorptech.com                                 |
| Source             | /srv/wct/releases/OpenC5ISR-v0.15.0                              |
| Evidence           | Continuity standard                                              |
| Source fingerprint | 63d2b1097707e25d666401cdc6362e395968600a40a08690210cd8c0b75fbf50 |
| Status             | Generated baseline — human review required                       |

“ **Verification boundary:** This page combines platform design guidance with static evidence from the release. It does not prove that every detected interface is enabled, reachable, secure, or operational in the deployed environment.

## Backup scope

| Asset             | Backup requirement                                                                           | Restore verification                                              |
|-------------------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Release artifacts | Retain exact immutable packages/checksums; normally do not back up regenerated dependencies. | Checksum and extraction test.                                     |
| Configuration     | Versioned protected copy excluding or separately encrypting secrets.                         | Syntax test and controlled comparison.                            |
| Databases         | Consistent database-native dump/snapshot with schema/version metadata.                       | Restore into isolated environment and run integrity/query checks. |

| Asset              | Backup requirement                                                                 | Restore verification                              |
|--------------------|------------------------------------------------------------------------------------|---------------------------------------------------|
| Files/evidence     | Content plus metadata, ownership, access policy, checksums and provenance.         | Sample restore, checksum and access-control test. |
| Knowledge/ontology | Graph data, ontology versions, shapes, indexes and configuration.                  | SPARQL/constraint tests against restored graph.   |
| Audit/history      | Protected retention according to policy; preserve ordering and integrity evidence. | Query selected events and verify integrity chain. |

# Recovery order

1. Infrastructure, DNS/TLS and time.
2. Protected configuration and secrets.
3. Databases, knowledge and artifact stores.
4. OpenBus/shared backends.
5. Edition-specific applications and reverse proxy.
6. Sensors/edge agents and external integrations.
7. End-to-end acceptance tests and user access.

# Recovery objective

Define and test RPO/RTO by data class. A backup that has never been restored is an optimistic file collection, not a recovery capability.

# Maintainer Notes

Add human-reviewed deployment notes, corrections, decisions, screenshots, and links here. Content outside the generated block is preserved on future runs.

Revision #1  
Created 2026-08-28 15:05:02 UTC by Nexus Ops Administrator  
Updated 2026-08-28 15:05:02 UTC by Nexus Ops Administrator