



Purpose

This policy summarises Senso.cloud backup and restore arrangements for customer assurance purposes.

Area	Current source-based position
Backup types	Full, differential and transaction backups are used for point-in-time restore (PITR).
Transaction log backups	Generally occur every 5-10 minutes according to the BCP/DR document.
Other backup intervals	Other transactions run every 2 hours; database routines vary from 5 minutes to 2 hours depending on compute size and activity.
Differential backups	Generally occur every 12 hours according to the BCP/DR document.
Backup location	Backups are stored in containers replicated to a paired data centre in the same geolocation as the hosted data.
Australia	For Australian tenancies, backups and disaster recovery replicas are retained within Australia according to the Australia Addendum.
Restore capability	Restore database to a point in time within retention period; restore deleted database to deletion time or within retention period; restore from paired datacentre in geographic disaster.
Supplier assessment summary	Backup frequency from 10 minutes to 2 hours depending on the area of the platform.
User Accounts Database	52 weeks LTR and 35-day PITR according to the supplier assessment.
Audit Database	12 weeks LTR and 7-day PITR according to the supplier assessment.
Logging Database	7 days LTR according to the supplier assessment.

Restore request process

1. Customer raises a support request through the support portal or agreed escalation channel.
2. Senso assesses the affected data, available restore points, business impact and scope.
3. Senso restores from the latest appropriate backup or point-in-time restore within the applicable retention period.

4. Where restore is not possible, Senso will explain known limitations, including retention window or catastrophic failure limitations.

Limitations

- Customer data restore is subject to the available backup and retention window.
- Customer-caused or third-party-caused loss may be subject to limitations in the Terms.
- Complete catastrophic failure scenarios may have different restoration characteristics, as described in the BCP/DR document.

Source basis

- Business Continuity & Disaster Recovery, revised 17 May 2019
- Senso.cloud Privacy Notice Australia Addendum for Schools, effective 1 October 2025
- Supplier Data Security Assessment Questionnaire, completed 10 May 2023