

Security Addendum

EFFECTIVE DATE	LAST UPDATED
July 23, 2026	July 23, 2026

This Security Addendum describes the baseline safeguards CapConnect intends to maintain for CapConnect OS. It must be reviewed against the production architecture before publication.

1 1. Security Program

CapConnect will maintain a risk-based information security program appropriate to the size, maturity, nature, and scope of its operations and the sensitivity of data processed.

2 2. Access Control

CapConnect will use reasonable measures such as:

- unique user identities;
- role-based access control;
- least-privilege principles;
- multi-factor authentication for privileged or administrative access where supported;
- periodic review of access;
- prompt revocation following role change or separation; and
- logging of sensitive administrative activity where feasible.

3 3. Encryption

CapConnect will use industry-standard encryption for data in transit over public networks and encryption at rest where supported by the hosting platform and appropriate to the data.

4 4. Infrastructure and Hosting

CapConnect may use reputable cloud infrastructure and software providers. Production and non-production environments should be logically separated. CapConnect will maintain reasonable configuration, patching, monitoring, and vulnerability-management practices.

5 5. Secure Development

CapConnect will maintain reasonable development controls, which may include:

- source-control protections;
- code review;
- dependency and vulnerability scanning;
- separation of duties appropriate to team size;

- secrets management;
- change management;
- testing before production release; and
- remediation based on severity and risk.

6 6. Logging and Monitoring

CapConnect will maintain logs and monitoring appropriate for detecting operational failures, abuse, unauthorized access, and security events. Retention periods may vary by log type, provider, plan, and legal requirement.

7 7. Backups and Recovery

CapConnect will maintain backups or recovery mechanisms appropriate to the production service tier. Recovery point and recovery time objectives are targets, not guarantees, unless expressly stated in an Order Form or SLA.

Customer remains responsible for exports or backups it considers necessary for its own legal, operational, or archival obligations.

8 8. Incident Response

CapConnect will maintain procedures to identify, investigate, contain, remediate, document, and communicate material security incidents. CapConnect may engage forensic, legal, insurance, hosting, and security providers.

9 9. Personnel Security

Personnel with access to production systems or Customer Data will be subject to confidentiality obligations. CapConnect may conduct screening where lawful and appropriate to role and risk.

10 10. Vendor Management

CapConnect will evaluate material subprocessors based on risk and contractually require appropriate confidentiality and security obligations.

11 11. Data Segregation

CapConnect will use logical controls designed to prevent one customer from accessing another customer's data. No system can eliminate all risk.

12 12. Customer Security Responsibilities

Customer is responsible for:

- its users, devices, networks, and endpoints;
- secure identity and access settings;
- reviewing user permissions;
- protecting API keys and credentials;
- configuring integrations and communications lawfully;
- promptly removing former users;
- avoiding unnecessary sensitive data;
- monitoring exports and downstream copies; and

- notifying CapConnect of suspected compromise.

13 13. Security Testing

CapConnect may conduct internal or third-party security testing. Customer may not conduct penetration testing without prior written authorization specifying scope, timing, methods, and safeguards.

14 14. Compliance Roadmap

Any references to planned certifications, audits, or controls are forward-looking and not contractual commitments unless expressly included in an Order Form.

Questions about this document may be sent to legal@capconnectsolutions.com.