BUNKR Trust Center

Security architecture, SOC 2 Control Alignment, and Encryption Practices

BUNKR is designed for sensitive communications, documents, credentials, and regulated workflows. This public overview describes the security controls and technologies used to protect the platform and our customers' information.

SOC 2 Position

BUNKR's security program is mapped primarily to the AICPA SOC 2 Security Trust Services Criteria (Common Criteria CC1-CC9), with selected controls also supporting Availability and Confidentiality objectives. The mappings below describe BUNKR's implemented control environment and are provided as a technical control-alignment overview. Reference SOC 2 Common Control Criteria 6.6-6.7.

Communication & Addressing Model - Reachability is consent-based; identity is not broadcast

Reachability is consent-based by default; BUNKR does not broadcast identity

The application has no public directory, global search, or other mechanism for one customer to find or enumerate another customer's users.

In-app messaging is off until a connection exists. For standard users that connection is a **mutual invitation**. Knowing or guessing an identifier is not enough to open a channel.

Business customers may authorize administrators, under role-based least privilege, to **pre-connect users inside that customer's tenant** (for example a company address book or auto-connect group). That override applies only within the administrator's organization. It does not create a public or cross-customer directory. Those administrators may also change or revoke their users' access.

This reduces unsolicited contact and list harvesting. It does not block people from inviting someone via email, SMS, or other out-of-band means.

Summary

- No public or cross-tenant user discovery.
- No global platform directory.
- Default: mutual invitation before messaging.
- Optional tenant-only exception: customer admins may auto-connect or manage users in their own org.

Core Security Stack

Microsoft Azure

Cloud platform for application hosting, managed database and storage services, private networking, platform logging, and operational security controls.

Microsoft Azure VPN and Web Application Firewall

BUNKR uses Azure VPN and Web Application Firewall as part of its network defense. VPN-based controls restrict designated internal and administrative access, while Web Application Firewall protections inspect and filter HTTP/S traffic before it

Auth0

Identity provider for passwordless authentication, secure token issuance, MFA enforcement, and authentication-event logging.

reaches protected application services.

Azure Key Vault

Cryptographic key material and sensitive secrets are separated from application source code and customer data and protected through Azure Key Vault access controls. Access is restricted to authorized identities and operational processes, minimizing direct human access during routine operations.

Azure Application Insights

Application telemetry, error visibility, performance monitoring, and operational/security investigation support.

GitHub + Azure DevOps

Version control, peer-reviewed pull requests, branch protections, automated CI/CD, and controlled promotion across environments.

Internal Access & Patch Management

Devices used to build and support BUNKR are centrally managed under endpoint-security and patch-management controls, with administrative access restricted to authorized personnel and security updates/configuration centrally administered.

Core Principles and Overview of Encryption Technology

- Encryption in transit: BUNKR protects application traffic using HTTPS with TLS 1.2 or higher. Real-time communications management system uses secure sockets management over TLS, and mobile push delivery relies on the encrypted transport protections provided by Apple and Firebase/Google.
- Encryption at rest: Customer information stored in BUNKR's backend is protected by Microsoft Azure's managed encryption-at-rest controls. Azure built-in capabilities protect database storage, backups, and logs; Azure Blob Storage uses service-side AES-256 encryption.
- Additional encryption for sensitive credentials: Passwords that customers choose to store inside BUNKR's password manager receive an additional application-level AES encryption layer. Cryptographic private-key material is managed separately through Azure Key Vault under controlled access policies.
- Passwordless authentication: BUNKR does not maintain a traditional database of reusable customer login passwords. Authentication is handled through identify provider using passwordless authentication, multi-factor authentication, and supported device biometrics.
- Token-based API authorization: Following successful authentication, identity provider issues authorization tokens that BUNKR uses to validate access to protected API services. API traffic is transmitted over encrypted TLS connections and remains subject to BUNKR's authorization controls.
- Device-level credential protection: On supported mobile devices, sensitive authentication and biometric-related information uses secure platform storage backed by iOS Keychain and Android Keystore capabilities.
- Role-based and least-privilege access: BUNKR is designed around role-based permissions and least-privilege access. Users and administrators are granted only the application and administrative capabilities appropriate to their assigned role.
- Environment separation: Development, staging, and production environments are maintained separately, with production access restricted to authorized personnel and protected through appropriate authentication and access controls.
- Security logging and traceability: BUNKR maintains identity, application, and cloud-platform logging to support monitoring, troubleshooting, auditability, and security investigation.
- Secure development and operational security: BUNKR incorporates vulnerability management, controlled software deployment, security monitoring, incident response, and business continuity practices into its operating model.

SOC 2 Common Criteria: CC1-CC5, CC 6.6 – 6.7

These criteria establish the governance, risk, monitoring, and control foundation that supports the Security category.

Criterion	What It Addresses	BUNKR Control Implementation
CC1 - Control Environment	Security responsibilities, policy ownership, personnel expectations, accountability, and governance.	Formal Information Security Program; management support for security risk decisions; annual policy review; background checks; confidentiality agreements; Acceptable Use Policy; documented termination/access-revocation procedures.
CC2 - Information & Communication	Security-relevant information is identified, communicated, and made available to responsible parties.	Documented security policies and procedures; internal escalation of suspected security issues; responsible-disclosure channel; change logs and operational records; security documentation provided through controlled customer/vendor review.
CC3 - Risk Assessment	Identification and assessment of threats, vulnerabilities, misuse scenarios, and material changes.	Formal risk management, assessment, and treatment process; ongoing risk identification; severity/impact evaluation; documented treatment plans; architecture and feature-level threat modeling; consideration of unauthorized access, privilege escalation, token misuse, and data exposure.
CC4 - Monitoring Activities	Controls and system activity are monitored so deficiencies or anomalous behavior can be identified.	Authentication monitoring through Auth0; application telemetry through Azure Application Insights; Azure platform logging; monitoring of administrative and operational activity; periodic review of access rights; investigation of abnormal system behavior.
CC5 - Control Activities	Policies are translated into technical and operational safeguards.	Access-control, encryption, vulnerability-management, change-management, and incident-response policies; environment separation; controlled deployment workflows; peer approval requirements; standardized infrastructure configuration; documented administrative controls.
CC6.6–CC6.7	Boundary protection & secure information movement	Closed communication model: no in-platform user discovery or directory; message channels require mutual invitation and acceptance before communication is enabled.

Evidence-based readiness

The purpose of this mapping is to connect each criterion to specific BUNKR controls and evidence sources. A future SOC 2 examination would independently test control design and, for Type II, operating effectiveness over the examination period.

Technical Criteria: CC6-CC9

These criteria map most directly to BUNKR's identity, network, monitoring, incident-response, change-management, and risk controls.

Criteria	Focus	BUNKR Controls
CC6.1-CC6.3	Logical access, provisioning & revocation	Auth0 identity layer; passwordless authentication; MFA; standardized roles; least privilege; authorized provisioning; periodic access review; prompt role modification and deprovisioning.
CC6.6-CC6.7	Boundary protection & secure information movement	Controlled Azure networking; restricted internal service exposure; HTTPS-only public traffic; TLS 1.2+; secure WebSockets; restricted production-data export; explicit user-directed sharing.
CC7.1-CC7.2	Vulnerability awareness & anomaly monitoring	Azure platform/security advisories; GitHub dependency alerts; Auth0 authentication monitoring; Azure platform logs; Azure Application Insights telemetry; severity-based remediation.
CC7.3-CC7.5	Security-event evaluation, response & recovery	Formal incident-response lifecycle covering triage, containment, investigation, remediation, recovery, documentation, and notification where legally or contractually required.
CC8.1	Change management	GitHub pull requests, peer review, branch protection, GitHub/Azure DevOps CI/CD, development/staging/production separation, staging validation, controlled production promotion, logged changes.
CC9.1-CC9.2	Risk mitigation & vendor risk	Formal risk assessment/treatment; critical-vendor review; cloud/identity-provider due diligence; Business Continuity Plan; Disaster Recovery Plan; backups; dependency and threat monitoring.

Shared-responsibility controls

Physical datacenter controls relevant to SOC 2 are primarily inherited from Microsoft's cloud datacenter environment. BUNKR directly operates the application, identity, access, software-development, monitoring, incident-response, and customer-data controls described here.

Selected BUNKR controls also support Availability objectives (BCP, DRP, backups, service monitoring) and Confidentiality objectives (data classification, encryption, access restrictions, controlled sharing, and customer-data ownership). BUNKR does not currently represent a completed category-level attestation for those areas.

Authentication Architecture

BUNKR uses Auth0 as its identity provider and does not use traditional customer passwords as the standard login model. Authentication is token-based and designed around strong user verification rather than storing reusable customer passwords.

Passwordless authentication

End users authenticate through an Auth0-based identity flow rather than creating a traditional BUNKR password that must be stored by the platform.

MFA enforcement

Multi-factor authentication is part of the standard BUNKR authentication model rather than an optional add-on.

Biometric verification

Supported devices can use platform-native biometrics. Sensitive biometric-related credential material is handled through platform secure-storage capabilities.

Secure token authorization

After authentication, Auth0 issues access tokens used to authorize requests. Tokens are transmitted only over encrypted connections.

Authorization & Privileged Access

- Standardized roles include administrators, secondary administrators, and standard users/members.
- Permissions are assigned according to role and organizational responsibility to support least privilege.
- Administrative access to production and cloud-management systems is restricted to authorized personnel and protected by MFA.
- Access is provisioned through administrative controls, periodically reviewed, and revoked or modified as responsibilities change.
- Development and testing are separated from production to reduce routine engineering exposure to production customer data.
- Authentication and administrative activity is logged to support traceability and investigation.

Customer Data Access Model

Designed to minimize routine internal access

BUNKR's operating model is designed so normal development and support activities do not require personnel to browse customer vault contents. Administrative access is controlled, and customer-data access is limited to authorized operational or legal circumstances and user-directed platform functionality.

Layered Encryption

BUNKR uses transport, platform, application, and device-level protections. The public description below is intentionally specific enough for technical review while excluding key identifiers, secret locations, and exploit-sensitive configuration.

Layer	Technology / Standard	BUNKR Use
API transport	HTTPS over TLS 1.2 or higher	Standard application requests use HTTPS. TLS version and cipher suite are negotiated by the client/server stack; modern suites may include AES-GCM or ChaCha20-Poly1305 depending on endpoint support. Plaintext HTTP is not used for production customer traffic.
Real-time transport	Connections and Socket Management over TLS	Real-time connections management use secure socket management transport, providing the same TLS protection model used for HTTPS traffic.
Push delivery	APNs / Firebase Cloud Messaging transport security	Push delivery uses the encrypted transport protections provided by Apple and Firebase/Google for delivery to supported devices.
Azure PostgreSQL	Azure service-side encryption at rest	Database storage, backups, and logs are protected by Azure-managed encryption at rest without requiring application changes.
Azure Blob Storage	AES-256 service-side encryption	Stored blobs are protected automatically at the Azure Storage service layer using 256-bit AES encryption and Azure-managed key protection.
Application-level sensitive fields	AES encryption	Designated sensitive data such as vault password content receives an additional application-level AES encryption layer before or in addition to platform storage protection.
Key management	Azure Key Vault	Cryptographic private-key material is separated from source code and application data and managed through Azure Key Vault with controlled access policies.
Device secure storage	iOS Keychain / Android Keystore-backed secure storage	Sensitive authentication and biometric-related material uses platform secure-storage capabilities designed to leverage device security features.
Local application data	OS sandboxing + controlled app access	Offline and cached application data is isolated within the application's operating-system security boundary. Client-side storage controls are reviewed as part of ongoing security hardening.

Microsoft Azure Security Architecture

Cloud hosting

Production services use Microsoft Azure managed application, compute, database, storage, networking, and monitoring services.

Network protection

Internal service communication is restricted through controlled Azure networking; public-facing application traffic is HTTPS-only.

Managed encryption

Azure database and storage services provide service-level encryption at rest while application traffic is protected in transit.

Secrets & keys

Sensitive cryptographic material is separated from application source and protected through Azure Key Vault and cloud access controls.

Secure Software Development Lifecycle

- Source code is maintained in GitHub and changes are introduced through pull requests.
- Automated dependency review is incorporated into BUNKR's build process before release
- SAST is integrated into BUNKR's CI/CD process before production deployment. Confirm the tool, execution point, and whether findings gate releases.
- Peer review and branch protection are used to prevent unreviewed changes from being merged.
- GitHub and Azure DevOps CI/CD workflows provide repeatable, controlled builds and deployments.
- Development, staging, and production are separate environments; staging is used before production promotion.
- Production infrastructure access is restricted to authorized personnel.
- Design review considers authentication, authorization, token handling, customer-data isolation, trust boundaries, and misuse scenarios.

Vulnerability Management

- Third-party libraries and versions are tracked through version-controlled dependency manifests and lock files.
- GitHub dependency/security alerts identify known vulnerabilities in third-party components.
- Microsoft Azure advisories and managed-service security updates are monitored.
- Vulnerabilities are assessed by severity and potential impact and remediated through controlled development/deployment workflows.
- Critical issues receive expedited treatment with validation before production deployment when the risk scenario permits.

Monitoring & Auditability

Auth0 logs

Authentication attempts, outcomes, and identity-related events provide access visibility.

Azure Application Insights

Application telemetry, errors, performance information, and operational events support detection and investigation.

Azure platform logging

Administrative actions, service activity, and infrastructure changes provide system-level traceability.

Application audit records

Relevant user and administrative activity records support customer, operational, and security review.

Incident Response

BUNKR maintains a formal incident-response process covering:

- Identification - monitoring, alerts, and personnel reporting.
- Containment - isolation or restriction of affected accounts, systems, or traffic paths.
- Investigation - review of logs, configurations, and available evidence to establish scope and cause.
- Remediation & recovery - patches, configuration changes, additional controls, and restoration activities.
- Communication - internal documentation and external notification when required by law or contract.

Business Continuity & Availability

Business Continuity Plan

Documented planning for material operational disruption.

Disaster Recovery Plan

Documented recovery planning for critical technology and service operations.

Backups

Security policy requires customer-data backups to be maintained and stored securely.

Service monitoring

Cloud and application monitoring provide operational visibility used to identify service-impacting conditions.

Privacy & Confidentiality

BUNKR is designed to limit unnecessary exposure of customer information and keep access tied to legitimate business need, user authorization, and explicit sharing decisions. Privacy controls are integrated into BUNKR's access model, data-handling practices, and closed communication architecture to help protect customer information throughout its lifecycle.

- Customer information is classified and access controls are intended to follow sensitivity and business need.
- BUNKR does not sell customer information to advertisers, data brokers, or other third parties.
- BUNKR does not seek ownership of customer-derived data for its own purposes.
- Customer data is not made directly available to third parties as a general business practice.
- Customer information leaves production primarily through explicit, authorized user actions such as sharing or communication.
- BUNKR supports privacy controls intended to help customers meet applicable data-protection obligations, including GDPR where applicable. Regulatory or legal record-retention requirements may limit deletion or other data-subject actions in specific circumstances.
- Customer identifiers are not published in a platform directory; contact inside BUNKR follows explicit, bilateral invitation rather than open addressing.

Penetration Testing & External Exposure Monitoring

BUNKR's security-testing program is designed to combine recurring automated external vulnerability and exposure checks with deeper annual application penetration testing.

- Automated external testing focuses on identifying internet-facing vulnerabilities and exposure conditions. Periodic application testing combines automated assessment with human-led testing to identify application-layer weaknesses that automated checks may miss.
- Annual human-led penetration testing through independent third-party

Security Documentation for Qualified Reviews

- Completed vendor security questionnaire
- Information-security, access-control, encryption, and incident-response policies
- High-level architecture and data-flow documentation
- Business continuity and disaster recovery information
- Security testing or assessment summaries when available
- Additional technical documentation subject to appropriate confidentiality controls

For BUNKR's transparency regarding our business, security practices, and associated policies, visit:
https://bunkr.life/transparency-statements/

BUNKR Contact Information
Email: Contact@bunkr.life
Phone: +1 727-213-3400
Support: BUNKR Support in Direct Messages within the BUNKR app
Web: https://bunkr.life/contact-us/