

VoxGuard: Secure team communication and emergency response platform, data security

VoxGuard is a cutting-edge mobile communication platform for teams that need immediate, secure, and reliable coordination in challenging environments. Whether it is emergency response, a large event, or corporate communication.



Why VoxGuard?

When your team's communication is critical—whether it's on-call duty, operational management, or the transmission of sensitive information—VoxGuard is a partner that won't let you down. We combine data security with a seamless user experience.

Our mission is simple: your data is your data. Always.



Multi-layered protection

Independent security layers ensure that the failure of a single layer does not compromise the whole system.



Principle of least privilege

Users and services receive only what they need for their tasks—nothing more.



Privacy first

We collect only the information necessary for the operation of the service.



Full transparency

Your administrator has comprehensive management tools and audit visibility.

Communication is secured, in transit and at rest

Encryption in all data transmission

Every bit is protected with modern TLS encryption (version 1.2+), utilizing the industry's strongest AES-256 algorithm. Prevents eavesdropping, data tampering, and man-in-the-middle attacks.

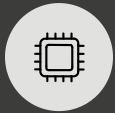
- Certificate pinning supported on managed devices
- All API requests are authenticated with short-lived tokens
- Revoked tokens are invalidated immediately

Data kept safe

All databases and object storage are protected.

- Row-Level Security (RLS) — users only see their own data
- Encrypted backups with strict retention policies
- Every recovery action is documented and traceable

Real-time Audio



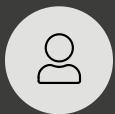
Professional media stream protection

Your push-to-talk calls are protected by AES-based encryption. Your audio is heard only by the group for which it is intended—no intermediaries, no eavesdroppers.



End-to-end encryption available

For organizations with higher security requirements, we offer configurations where audio streams are encrypted end-to-end.



Strict access control

Only authenticated users with correct group permissions can join channels. Access control is implemented at both the application and server level.



Identity and Access Management

Only the right people in the right place



Strong authentication

Standard-based email/password authentication with strict policies. Password policies can be defined according to your organization's needs.



SSO and multi-factor authentication

Single Sign-On (SSO) and multi-factor authentication (MFA) supported depending on your identity provider. Single sign-on, multiple layers of protection.



Fine-grained authorization

Role-based and group-based access management. Every action is authorized—no shortcuts.



Token hygiene

Short-lived session tokens and secure refresh flows minimize the impact of a leaked token. Redeemed tokens are invalidated immediately.

Application and device security from the ground up

Secure defaults

VoxGuard stores a minimal amount of data on the device. Sensitive session tokens are kept in the operating system's secure storage.

- iOS Keychain / Android Keystore — not in plain text files
- Least privilege: microphone for voice, location for map features
- No mysterious permission requests

Runtime protections

All user input is validated and the most common mobile and web threats are mitigated.

- XSS, CSRF, and SQL injection prevented
- Deserialization secured
- Parameterization and framework protections in use

Infrastructure, hardened cloud-native



Robust foundation

Network segmentation, firewalls, and least-privilege IAM roles. Every component is isolated and secured.



Continuous monitoring

All security-related events are logged, and anomalies trigger automatic alerts.



Secure development

Code reviews, dependency security scans, and automated checks in the CI/CD pipeline. Security is part of every sprint.



Secrets management

API keys and encryption keys are stored in managed secrets vaults. Every access is audit-ready.

Compliance and Privacy

Data Residency

Your data is stored in cloud services located within the EU. Regional hosting options can be discussed based on your specific requirements.

Our Privacy Commitment

- We do not sell or share data with third parties
- We do not track users across websites
- We do not build profiles for sales purposes
- Your data is your data. Always.

Regulatory Compliance

VoxGuard is designed to adhere to general security and privacy expectations, including the principles of GDPR.

Formal certifications and specific requirements can be discussed on a case-by-case basis.

Shared responsibility, a partnership that works

Security is a team effort. VoxGuard handles its part, and you handle your organization's part.

VoxGuard's responsibility

Component	Area of responsibility
Application	Code, architecture, security mechanisms
Backend systems	Servers, databases, infrastructure
Encryption	Automatic in transit
Configuration	Service settings and updates
Monitoring	Operational logging and alerts

Your responsibility

Component	Area of responsibility
Devices	Mobile device management and updates
Identity	SSO/MFA configuration
Network	Organizational network policies
Access rights	Internal access management and roles

Frequently Asked Questions

Is communication end-to-end encrypted?

Voice streams are encrypted in transit by default (using AES-based encryption). End-to-end encryption is available for organizations with specific security requirements. Please contact us to learn more.

Can you integrate with SSO and MFA?

Yes. Single Sign-On (SSO) and Multi-Factor Authentication (MFA) are supported via standard-based identity providers.

Where is our data stored?

Data is stored in encrypted cloud databases within the EU. Regional hosting options can be agreed upon separately.

Do administrators have audit visibility?

Yes. All logins, permission grants, and data changes are logged. We can customize dashboards and export reports according to your needs.

What happens if my device is lost or stolen?

The session token can be revoked via remote management. The application stores minimal sensitive data in the operating system's secure storage.

Can third parties access my data?

No. We do not sell, rent, or share your data with third parties. The only exception is a legal data request.

VoxGuard, security is the foundation

Your organization is protected with layered security.



Encrypted communication — everywhere



AES-256 encryption in transit



Strong identity: authentication, authorization, auditing



Granular access control



Hardened cloud base, monitoring and recovery

Would you like to discuss further? Get in touch, and we will design a solution that fits your needs together.