Technical and Organizational Measures

Hereunder you will find a description of the technical and organizational measures implemented by us (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Infrastructure security

Server Network
The IXON Cloud is a complex network of over 150 servers, distributed globally among various hosting providers. All are situated in data centers maintaining the highest security standards.

High Availability
Most IXON servers are set up for high availability or have redundant deployments, ensuring that a single hardware or network failure won't compromise the IXON Cloud's availability.

Backups
Stateful servers are backed up weekly. Additionally, backups for essential customer and machine data are created every four hours. These backups are monitored in real-time for accuracy and undergo monthly validity tests.

Server Access
Only senior IXON personnel, including developers and administrators, can access servers. This is facilitated through unique usernames and private SSH keys. All server-related activities are logged and audited.

Real-time Monitoring
Servers are constantly monitored using an array of both standard and custom checks analyzing internal metrics. Any deviations or anomalies immediately alert relevant staff.

Server Configuration
A master node manages server configuration, guaranteeing uniformity across servers. This system also enables effortless deployment of new servers.

Server Hardening
Our servers undergo a hardening process, minimizing vulnerabilities by eliminating unused protocols, tightening file access permissions, and mandating robust passwords.

Patch Management
Critical patches are applied within a day. Weekly, non-critical software patches are assessed and those enhancing uptime, performance, or security are deployed.

Firewalls
Each server boasts a firewall, adopting a deny-all, permit-by-exception approach. Exceptions are rigorously evaluated to be as strict as possible, employing methods like source IP or protocol whitelisting.

Inter-server Exchange

IXON Cloud servers operate within an internal mesh network, ensuring that communications between servers never traverse the public Internet.

Data Privacy and confidentiality

Privacy by Design
Every change in data handling, from software updates to subcontractor shifts or internal process modifications, undergoes a privacy impact analysis to ensure data privacy.

GDPR Compliance
Personally identifiable information (PII) is processed and stored by EU-based third parties in line with GDPR legislation, as detailed in Part V. IXON has designated a privacy officer to ensure compliance.

Data Ownership
All personal and machine data stored or created in the IXON Cloud belongs to the user. IXON may not, in any shape or form, misuse, distribute or sell this information.

Data Retention
Data does not expire as long as you have an active user account. After deleting your account, data may be deleted after three months.

TLS Encryption
HTTPS and MQTT connections use TLS 1.2 or higher for encryption. We permit only "strong" encryption algorithms that support perfect forward secrecy, utilizing RSA keys of 4096 bytes.

VPN Encryption
VPN connections utilize single-use VPN certificates and are encrypted using AES-256-CBC with SHA512.

Password Hashing
IXON Cloud passwords are stored as hashes using Argon2id, configured with 3 iterations, 4 degrees of parallelism, 64 MiB memory, and a 16-byte salt.

Vulnerability management

Vulnerability scanning
IXON Cloud servers are tested for vulnerabilities every week using both internal and external scans.

Penetration Testing
Each year, the IXON Cloud and IXrouter undergo 2 to 3 third-party penetration tests. Tests range from black box evaluations of the entire IXON Cloud to white box analyses of significant architectural changes.

Log analysis
All server logs are gathered in a centralized log system and automatically analyzed according to community-maintained and custom security rules..

Incident handling

Security Breach Protocol
A protocol is in place to address security incidents effectively and efficiently. This protocol involves the following steps: 1) Incident verification, 2) Containment, 3) Evaluation, and 4) Lessons learned.

Incident Notification
Impacted parties and users are notified promptly about a security incident via email. We strive to be as transparent as possible in our communication.

Incident Training
Annually, using a tabletop setting or a simulated environment, we replicate a major security breach to ensure IXON personnel are familiar with their role in the security breach protocol.

Business Continuity Plan
A plan is in place to ensure business operations continue smoothly during various man-made or natural events.

Application Security

Authentication
The initial login to the IXON Cloud uses Basic Authentication. After successful login, users receive a Bearer token valid for their session duration.

Password strength
We don't enforce traditional complexity requirements for passwords. Instead, we mandate passwords be deemed "unguessable" (no. guesses > 10^8) by our strength estimator. This system also blocks commonly used passwords.

Brute force protection
Repeated failed login attempts (>10 tries) result in a temporary block. This time increases with subsequent failed attempts, up to a maximum of 1 hour.

Multi-factor authentication
Time-based one-time passwords (TOTPs) can be employed as an additional authentication factor. They can be activated for individual users or mandated for all users within your IXON Cloud environment.

Granular permission
Administrators can fine-tune permissions using user groups and roles, adjusting access for multiple users simultaneously. These permissions can provide access to all devices, target specific ones, or restrict certain device services, such as VNC, VPN, or HTTPS.

Logical separation of data
Although customer data resides in multi-tenant environments, we implement multiple layers to safeguard data confidentiality. Initially, requests validate your Bearer Token. Subsequently, data filtering occurs based on your domain, company ID, and permission role – returning only the information you're authorized to view.

Session control
Active IXON Cloud sessions are accessible within your account details. Implementing a security change, like updating your password, auto-revokes all ongoing sessions.

Audit trails
The IXON Cloud provides device-specific and company-wide audit trails, offering users a comprehensive record of historical events.

Software development

Security by design
Security requirements are created prior to development which must be met before changes may be deployed.

Peer reviews
Any code modifications undergo a review by at least one senior, independent developer. This ensures readability, clarity, and completeness. All identified issues must be resolved before approval.

Automated testing
Upon committing changes to our software versioning system, the code undergoes comprehensive automated tests. This encompasses unit tests, scenario tests, and security evaluations.

Staged deployment
We employ distinct environments to segregate (potentially) insecure code before it reaches production:

- Development: Runs locally on developers' systems, facilitating code modifications.
- Testing: Houses finished features and serves as a platform for manual tests.
- Staging: Contains code ready for production, and is utilized for integration and stress testing.

Organizational security

Vendor reviews
Suppliers and third parties undergo an initial security review and subsequent annual checks. Essential suppliers, like hosting providers, are mandated to possess an ISO27001 certificate or equivalent.

Training and awareness
All security personnel must meet a set training quota each quarter. New hires are trained on IXON's security policies during onboarding, and the entire staff regularly undergoes updates on pertinent security subjects.

Policy management
Our security policies are accessible via an internal webpage. Policy alterations are documented, requiring approval before being published. Policies undergo a biannual review.

Risk management
Quarterly risk assessments categorize threats by likelihood and impact. Risks exceeding acceptable thresholds are documented in a treatment plan, outlining specific corrective actions and their respective deadlines.

Endpoint protection
All company hardware features hard-disk encryption and endpoint protection software. In-depth antivirus scans run weekly, with any anomalies instantly reported to our security team.

Certification
IXON's management system holds certifications in:

- ISO9001 - Quality management
- ISO27001 - Information security management
- ISO27017 - Cloud System Information Security
- ISO27701 - Privacy management

Accredited third-party NCI conducts yearly external audits.

Internal audits
Every quarter, internal audits are undertaken by independent IXON employees.