AxonIQ Cloud Security Addendum

AxonIQ's Cloud Security Addendum ("Security Addendum") outlines the technical and procedural measures that AxonIQ undertakes to protect customer data submitted via the event storage API ("Content") from unauthorized access or disclosure. AxonIQ may change this Security Addendum from time to time and such changes will be effective when posted. Capitalized terms used but not defined in this Security Addendum have the meanings as set forth in the AxonIQ Cloud Subscription Agreement or other written or electronic terms of a cloud service or cloud subscription agreement ("Agreement") entered into by the parties.

1. Customer Data Access and Management

1.1 Customer controls access to the Cloud Service via accounts at supported OAuth2 Identity Providers. Customer may manage organization membership and then delegate access to their data and services using the Cloud Console.

1.2 The Cloud Service encrypts data in-transit and uses storage that encrypts data at rest. For the purposes of data governance and data confidentiality, Customers should encrypt Content using an industry standard encryption methodology prior to sending it to AxonIQ.

1.3 AxonIQ uses Content only as appropriate to provide the Cloud Service to Customer, as specified in the Agreement.

1.4 Content is stored in the Cloud Service production environment, provisioned per the Agreement.

1.5 Depending on choices made by Customer during the setup of the environment in the Cloud Service, Content is replicated and retained by AxonIQ as described in the product. Customers are expected to consume the data they send to the Cloud Service regularly and store data in their data stores of choice beyond the retention policy specified.

2. Encryption and Logical Separation of Customer Data

2.1 The Cloud Service stores Content in storage products using encryption at rest. This is done using industry standard encryption methodologies employed on the storage backend.

2.2 The Cloud Service encrypts data in-transit with appropriate encryption standards for the networking technology used.

2.3 The Cloud Service includes logical separation of data between customers. Depending on the product purchased, the Cloud Service may provide physical separation using Customer-specific, dedicated cloud resources. In all cases, AxonIQ has implemented controls designed to prevent one customer from gaining unauthorized access to another customer's data.

3. AxonIQ Cloud Service Infrastructure Access Management

AxonIQ maintains policies regarding Access Management and Identification and Authentication. The most important elements from these policies are highlighted below.

3.1 Access to the systems and infrastructure that support the Cloud Service is based on the principle of least privilege allowing only authorized access for users which are necessary to accomplish assigned tasks.

3.2 Unique User IDs are assigned to employees, as part of their hiring and onboarding process. This way AxonIQ is able to ensure information systems can uniquely identify and authenticate users (or processes acting on behalf of users).

3.3 The server access policy for the Cloud Service adheres to AxonIQ standards, which includes 2-factor authentication.

3.4 Access privileges of terminated AxonIQ personnel are disabled promptly. Access privileges of persons transferring to jobs requiring reduced privileges are adjusted accordingly.

3.5 AxonIQ personnel access to the systems and infrastructure that support the Cloud Service is reviewed regularly.

3.6 Cloud provider firewall or firewall-equivalent controls have deny-all default policies and only enable appropriate network protocols for ingress network traffic.

3.7 Bastion hosts that utilize appropriate security measures are the only enabled remote administration point of access for AxonIQ employees on the Cloud Service production environment.

4. Risk Management

4.1 AxonIQ maintains a risk management program based on industry guidance as per the defined policy.

4.2 Based on the risk management policy AxonIQ conducts risk assessments of various kinds throughout the year, including self- and/or third-party assessments and tests, automated scans, and manual reviews.

4.3 Results of assessments, including formal reports as relevant, are reported to the CISO Office. Based on the assessments the CISO Office will identify control deficiencies and material changes in the threat environment, and to make recommendations for new or improved controls and threat mitigation strategies to executive management.

5. Vulnerability Management

AxonIQ maintains a policy regarding Vulnerability Management. The most important elements from the policy are highlighted below.

5.1 Vulnerability mitigation is a part of every AxonIQ engineer's responsibilities.

5.2 The potential impact of known vulnerabilities is evaluated and appropriate remediation actions are taken. .

5.3 Vulnerabilities that trigger alerts and have published exploits are reported to security leadership, which determines and supervises appropriate remediation action.

5.4 Security Operations monitors or subscribes to trusted sources of vulnerability reports and threat intelligence.

5.5 AxonIQ security events of interest are reviewed for malicious or inappropriate activity, and when appropriate reported to the CISO Office.

6. Remote Access & Wireless Network

AxonIQ maintains policies regarding (remote) Access Management and Identification. The most important elements from this policy are highlighted below.

6.1 All access to the Cloud Service networks requires authentication through an encrypted connection such as SSH, MFA, using regular-rotated SSH keys, and never solely passwords.

6.2 AxonIQ corporate offices, including LAN and Wi-Fi networks in those offices, require successful authentication in addition to authentication to public cloud provider accounts for access.

6.3 AxonIQ maintains a policy of not storing Content processed by the Cloud Service on local desktops, laptops, mobile devices, shared drives, removable media, as well as on public facing systems that do not fall under the administrative control or compliance monitoring processes of AxonIQ.

7. Cloud Service Location

7.1 Content is stored in the available Cloud Service region(s) identified in the Agreement, for the account requested by Customer. Customers can choose the region where Content is stored when creating a Context.

8. System Event Logging

8.1 Monitoring tools and services are used to monitor systems including network, server events, availability events, resource utilization, and other security events of interest.

8.2 AxonIQ infrastructure security event logs are collected in a central system and stored using appropriate security measures designed to prevent tampering. Logs are stored for 90 days.

9. System Administration and Patch Management

9.1 For systems that access Content, AxonIQ creates, implements, and maintains system administration procedures that meet or exceed industry standards, including without limitation, system hardening, system and device patching (operating system and applications).

9.2 AxonIQ's security team reviews relevant vulnerabilities announcements regularly, assesses their impact to AxonIQ based on AxonIQ-defined risk criteria, and reports to the CISO Office on applicability and severity.

9.3 Applicable security updates rated as "high" or "critical" are addressed and remediated as soon as reasonably possible but in either case within 14 days of the patch release.

9.4 The latest applicable patches and updates are applied promptly after becoming available and are tested in the Cloud Service's pre-production environments.

10. AxonIQ Awareness and Security Training

10.1 AxonIQ maintains a security awareness policy for AxonIQ personnel, which provides initial education, ongoing awareness, and an individual AxonIQ personnel acknowledgment of intent to comply with AxonIQ's corporate security policies. New hires complete initial training on security, sign a proprietary information agreement, and digitally sign the Policy Consent and Acknowledgement Form that covers key aspects of the AxonIQ information security program.

10.2 All AxonIQ personnel acknowledge they are responsible for reporting actual or suspected security incidents or concerns, thefts, breaches, losses, and unauthorized disclosures of or access to Content.

10.3 All AxonIQ personnel are required to satisfactorily complete mandatory parts of offered security training.

11. Physical Security Infrastructure

11.1 The Cloud Service is hosted in "public clouds", such as those provided by AWS, Azure, and GCP. Therefore, all physical security controls are managed by the applicable public cloud provider. Annually, AxonIQ reviews the applicable security and compliance reports of the public cloud providers it uses to ensure appropriate physical security controls.

12. Notification of Security Incident

12.1 AxonIQ will notify Customer in writing without undue delay after becoming aware of unauthorized access to Content.

12.2 Such notification will summarize the known details of the breach and the status of AxonIQ's investigation.

12.3 AxonIQ will take appropriate actions to contain, investigate, and mitigate any such breach. Containment and mitigation (in the event of a high likelihood of recurrence) may take precedence over detailed reporting.

13. Availability and Disaster Recovery

13.1 AxonIQ maintains a Disaster Recovery Policy (DPR). The DRP is tested annually.

13.2 AxonIQ's DRP covers Customer's account and user information. Recovery of data submitted via the event storage API is restricted by the Service Level chosen by the customer for the individual contexts configured in its account.

13.3 The Cloud Service is delivered to customers from different cloud providers such as AWS, Azure, and GCP.. Depending on the chosen provider the provisions for availability and disaster recovery may vary.

14. Additional Customer Responsibilities

14.1 Customer is responsible for managing and securing its Content and User Credential(s) within the Cloud Service and for protecting its own resources, including through the use of encryption. Customer will comply with the terms of the Agreement as well as all applicable laws.

14.2 Customer will immediately notify AxonIQ if a User Credential has been compromised or if Customer suspects possible suspicious activities that could negatively impact the security of the Cloud Service or Customer's account.

14.3 Customer may not perform any security penetration tests or security assessment activities without the express, prior written consent of AxonIQ's CISO.

14.4 AxonIQ has implemented reasonable security measures designed to prevent unauthorized access to and accidental loss of data uploaded to our service as described in this Security Addendum. AxonIQ does not, however, guarantee that unauthorized third parties will not obtain access to Content.

14.5 Customer shall not transmit cardholder or sensitive authentication data (as those terms are defined in the PCI DSS standards) unless such data is message-level encrypted by Customer.

14.6 Customer shall not transmit Protected Health Information (as defined under (HIPAA)) into the Cloud Service without first having entered into a BAA with AxonIQ.

14.7 Customer is responsible for ensuring a level of data protection commensurate with the sensitivity of the Content it uploads to the Cloud Service including, without limitation, an appropriate level of message-level encryption. Compliance with certain GDPR clauses may require Customer to use encryption on fields of data containing Personally Identifiable Information, in the context of an AxonIQ Cloud hosted Event Store.

14.8 Customer is responsible for managing a backup strategy regarding Content.