INTERSYSTEMS PLATFORM
PRIVACY AND SECURITY SPECIFICATION

This InterSystems Platform Privacy and Security Specification is incorporated into and made a part of the written agreement between InterSystems and Customer that references this document (the “Agreement”) and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this InterSystems Platform Privacy and Security Specification, this InterSystems Platform Privacy and Security Specification shall govern.

InterSystems delivers InterSystems Platform Service either through (1) infrastructure-as-a-service cloud providers as further described in the Agreement and/or Documentation (each, a "Cloud Provider") or (2) InterSystems Managed Services private cloud as further described in the Agreement and/or Documentation (“InterSystems Managed Services”) and provides the InterSystems Platform Service to Customer using a VPC/VNET and storage hosted by either the applicable Cloud Provider or InterSystems Managed Services (as selected by the Customer, the “Cloud Environment").

InterSystems maintains a comprehensive documented security program based on ISO 27001 (and incorporating NIST SP 800-53 and any industry recognized successor frameworks), under which InterSystems implements and maintains technical and organizational measures designed to protect the confidentiality, integrity, availability, and security of the InterSystems Platform Service and Customer Data (the “Security Program”), including, but not limited to, as set forth below. InterSystems regularly tests and evaluates its Security Program, and may review and update its Security Program as well as this InterSystems Platform Privacy and Security Specification, provided, however, that such updates shall be designed to enhance and not materially diminish the Security Program.

1. Certifications & Standards

1.1. Hosting.

1.1.1. If a Cloud Provider is selected by the Customer for the Hosting Location, the information security management system used by the Cloud Provider used to provide the InterSystems Platform Service shall be assessed by independent third-party auditors as described in the following audits and certifications ("Cloud Provider Audits"), on at least an annual basis: (i) SOC 2 Type 2 and/or (ii) HITRUST CSF Certification (where AWS or Microsoft is the Cloud Provider).

1.1.2. If an InterSystems Managed Service is selected by the Customer for the Hosting Location, the information security management system to provide the InterSystems Platform Service shall be based upon ISO 27001 with U.S.-based services including HITRUST CST requirements. The security of the InterSystems Platform will be assessed by an independent third party on at least an annual basis with: (i) the Managed Services US operations audited for SOC 2 Type 2 and HITRUST CSF Certification; and (ii) the Managed Services UK operations audited for ISO 27001, ISO 22301, and ISO 20000-1.

1.1.3. Upon written request and at no additional cost to Customer, InterSystems shall provide Customer, or its appropriately qualified third-party representative (collectively, the "Auditor"), access to reasonably requested documentation evidencing InterSystems's compliance with its obligations under this InterSystems Platform Privacy and Security Specification in the form of (i) InterSystems’s ISO 27001 or HITRUST CSF third party certifications or (ii) InterSystems's SOC 2 Type 2 audit report (“InterSystems Audit Reports”). Cloud Providers Audits can be accessed directly from the Cloud Provider.

2. Hosting Location; Encryption

2.1. Hosting Location. The hosting location of Customer Data is the production Cloud Environment in the Region offered by InterSystems and selected by Customer on an Order Form or as Customer otherwise configures via the services.

2.2. Encryption of Customer Data. InterSystems encrypts Customer Data at-rest using AES 256-bit (or better) encryption. InterSystems uses Transport Layer Security (TLS) 1.2 (or better) for Customer Data in-transit over untrusted networks.

3. System & Network Security

3.1. Access Controls. All InterSystems personnel access to the Cloud Environment is via a unique user ID and consistent with the principle of least privilege. All such access requires a VPN, with multi-factor authentication and passwords meeting or exceeding NIST SP 800-63-3 length and complexity requirements.

3.2. Endpoint Controls. For access to the Cloud Environment, InterSystems personnel use InterSystems-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Malicious Code (as defined below), and (iii) vulnerability management in accordance with Section 4.7.3 (Vulnerability Management).

3.3. Separation of Environments. InterSystems logically separates production environments from development and testing environments. The Cloud Environment is both logically and physically separate from InterSystems's corporate offices and networks.

3.4. Firewalls / Security Groups. InterSystems shall protect the Cloud Environment using industry standard firewall or security groups technology with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business-required.

3.5. Hardening. The Cloud Environment shall be hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this InterSystems Platform Privacy and Security Specification.

3.6. Monitoring & Logging.

3.6.1. Infrastructure Logs. Monitoring tools or services, such as host-based intrusion detection tools, are utilized to log certain activities and changes within the Cloud Environment. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering for at least one year.

3.6.2. User Logs. As further described in the Documentation, InterSystems also captures logs of certain activities and changes within the Account and makes those logs available to Customer for Customer's preservation and analysis.

3.7. Vulnerability Detection & Management.

3.7.1. Anti-Virus & Vulnerability Detection. The Cloud Environment leverages advanced threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code (collectively, “Malicious Code”). InterSystems does not monitor Customer Data for Malicious Code.

3.7.2. Penetration Testing & Vulnerability Detection. InterSystems regularly conducts penetration tests throughout the year and engages one or more independent third parties to conduct penetration tests of the InterSystems Platform Service at least annually. InterSystems also runs weekly vulnerability scans for the Cloud Environment using updated vulnerability databases.

3.7.3. Vulnerability Management. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the InterSystems Platform Service. Upon becoming aware of such vulnerabilities, InterSystems will use commercially reasonable efforts to address private and public (e.g., U.S.-Cert announced) critical and high vulnerabilities within 30 days, and medium vulnerabilities within ninety (90) calendar days. To assess whether a vulnerability is ‘critical’, ‘high’, or ‘medium’, InterSystems leverages the National Vulnerability Database’s (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

4. Administrative Controls

4.1. Personnel Security. InterSystems requires criminal background screening on its personnel as part of its hiring process, to the extent permitted by applicable law.

4.2. Personnel Training. InterSystems maintains a documented security awareness and training program for its personnel, including, but not limited to, onboarding and on-going training.

4.3. Personnel Agreements. InterSystems personnel are required to sign confidentiality agreements. InterSystems personnel are also required to sign InterSystems's information security policy, which includes acknowledging responsibility for reporting security incidents involving Customer Data.

4.4. Personnel Access Reviews & Separation. InterSystems reviews the access privileges of its personnel to the Cloud Environment at least quarterly, and removes access on a timely basis for all separated personnel.

4.5. InterSystems Risk Management & Threat Assessment. InterSystems’s risk management process is modeled on ISO 27001 (Appendix 2 of Annex SL of the ISO/IEC Directives, Part 1). InterSystems's management review committee meets regularly to review reports and material changes in the risk environment, and to identify potential control deficiencies in order to make recommendations for new or improved controls and threat mitigation strategies.

4.6. External Threat Intelligence Monitoring. InterSystems reviews external threat intelligence, including US-Cert vulnerability announcements and other trusted sources of vulnerability reports. U.S.-Cert announced vulnerabilities rated as critical or high are prioritized for remediation in accordance with Section 4.7.3 (Vulnerability Management).

4.7. Change Management. InterSystems maintains a documented change management program for the InterSystems Platform Service.

4.8. Vendor Risk Management. InterSystems maintains a vendor risk management program for vendors that process Customer Data designed to ensure each vendor maintains security measures consistent with InterSystems's obligations in this InterSystems

Platform Privacy and Security Specification.

5. Physical & Environmental Controls

5.1. Cloud Environment Data Centers. To ensure appropriate physical and environmental controls for data centers hosting the Cloud Environment, InterSystems regularly reviews those controls as audited under either the Cloud Provider Audits or InterSystems Audit Reports. Such controls, shall include, but are not limited to, the following:

5.1.1. Physical access to the facilities are controlled at building ingress points;

5.1.2. Visitors are required to present ID and are signed in;

5.1.3. Physical access to servers is managed by access control devices;

5.1.4. Physical access privileges are reviewed regularly;

5.1.5. Facilities utilize monitor and alarm response procedures;

5.1.6. Use of CCTV;

5.1.7. Fire detection and protection systems;

5.1.8. Power back-up and redundancy systems; and

5.1.9. Climate control systems.

5.2. InterSystems Corporate Offices. While Customer Data is not hosted at InterSystems's corporate offices, InterSystems's technical, administrative, and physical controls for its corporate offices shall include, but are not limited to, the following:

5.2.1. Physical access to the corporate office is controlled at office ingress points;

5.2.2. Badge access is required for all personnel and badge privileges are reviewed regularly;

5.2.3. Visitors are required to sign in;

5.2.4. Use of CCTV at building ingress points;

5.2.5. Tagging and inventory of InterSystems-issued laptops and network assets;

5.2.6. Fire detection and sprinkler systems; and

5.2.7. Climate control systems.

6. Incident Detection & Response

6.1. Security Incident Reporting. If InterSystems becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "Security Incident"), InterSystems shall notify Customer without undue delay, and in any case, where feasible, notify Customer within seventy-two (72) hours after becoming aware.

6.2. Investigation. In the event of a Security Incident as described above, InterSystems shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Any logs determined to be relevant to a Security Incident, shall be preserved for at least one year.

6.3. Communication and Cooperation. InterSystems shall provide Customer timely information about the Security Incident to the extent known to InterSystems, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by InterSystems to mitigate or contain the Security Incident, the status of InterSystems's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because InterSystems personnel do not have visibility to the content of Customer Data, it will be unlikely that InterSystems can provide information as to the particular nature of the Customer Data, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of InterSystems with Customer in connection with a Security Incident shall not be construed as an acknowledgment by InterSystems of any fault or liability with respect to the Security Incident.

7. Deletion of Customer Data.

7.1. By Customer. To the extent that InterSystems Platform Service stores Customer Data for the Customer, the InterSystems Platform Services provides Customer controls for the deletion of Customer Data, as further described in the Documentation.

7.2. By InterSystems. Subject to applicable provisions of the Agreement, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "retrieval period" set forth in the Agreement, InterSystems shall promptly delete any remaining Customer Data.

8. Customer Shared Privacy and Security Responsibilities

8.1. Sensitive Customer Data. Customer must implement all appropriate Customer-configurable security controls, including IP allow-listing and MFA for all User interactive logins (e.g., individuals authenticating to the InterSystems Platform Service) to protect Customer Data for which HIPAA or similar heightened requirements apply.

8.2. Shared Security Responsibilities. Without diminishing InterSystems's commitments in this InterSystems Platform Privacy and Security Specification, Customer agrees:

8.2.1. InterSystems has no obligation to assess the content of Customer Data to identify information subject to any specific legal, regulatory or other requirement and Customer is responsible for making appropriate use of the InterSystems Platform Service to ensure a level of security appropriate to the particular content of Customer Data, including, where appropriate, implementation of encryption functionality, pseudonymization of Customer Data, and configurations to back-up Customer Data;

8.2.2. to be responsible for managing and protecting its User roles and credentials, including but not limited to (i) requiring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) reporting to InterSystems any suspicious activities in the Account or if a user credential has been compromised, (iii) appropriately configuring User and role-based access controls, including scope and duration of User access, taking into account the nature of its Customer Data, and (iv) maintaining appropriate password uniqueness, length, complexity, and expiration; and

8.2.3. to appropriately manage and protect any Customer-managed encryption keys to ensure the integrity, availability, and confidentiality of the key and Customer Data encrypted with such key;