InterSystems Corporation
One Memorial Drive
Cambridge, MA 02142-1356

Main: +1 617 621 0600
Support: +1 617 621 0700
InterSystems.com

WHITE PAPER- Managed Services Security Practices

The information security practices outlined below provide standards expected of each staff member, consultant, or customer staff member granted access to the InterSystems Managed Services environments. These practices also detail the standards applied for the overall security of the systems within the Managed Services environments. This document and any underlying policies and standards must be reviewed by all InterSystems Personnel, including employees and contractors, acting as Managed Services staff upon initial hire or contracting and then annually. All InterSystems Personnel must review and agree to comply with the policies and standards prior to administrative access being granted.

Communication about Managed Services is documented through InterSystems Worldwide Response Center ("WRC"), which may be accessed to create support application tickets is via telephone, fax, email, or via the web and is available 24/7/365. WRC staff is always available to initiate inquiries related to Managed Services and standard business hours are Monday – Friday, 8:00 a.m. to 6:00 p.m. Central time, but qualified oncall staff are always available.

All members of our development team are asked to confirm understanding of key policies on an annual basis. This includes our Secure Development policy.

This white paper highlights more specifics of our security practices as they pertain to the InterSystems Managed Services environment.

User Access

- Users, which includes InterSystems Personnel and customer staff, are granted access to the Managed Services systems on an as-needed basis solely for delivery of the Managed Services.
- Users are authorized access only to the systems and data directly related to their job responsibilities during delivery of the Managed Services.
- Administrative access is allowed to only a single customer environment at a time for any consultants that may be engaged by multiple customers.
- Consultants with multiple customers using Managed Services must have a unique username for each customer environment identifying both them and the associated customer.
- Users and their management are required to report any change in role that would require reduced access to be applied.
- When job requirements change such that access is no longer required, access is removed.

- Administrative access for customer staff and their representatives will only be granted upon request via a service request with WRC, submitted by an authorized customer staff member.
- Administrative access to any Managed Services systemis gained via approved IPsec VPN client and requires two factor authentication.
- Distribution of passwords to administrative users must be done securely and cannot be emailed nor given to another user or manager. Passwords are to be delivered only to the specific user.
- Strong password standards are applied for access to both the HealthShare customer solution and to administrative access for the hosted solution components of Managed Services.
- In any customer environment, all user and administrative accounts are to be unique, named accounts. Sharing of usernames and/or passwords is prohibited.
- No access to the production environment may be granted to customer staff or customer consultants outside the access granted via the application administration tools, unless reviewed and approved by InterSystems.
- Any access to the production environment for customer staff or customer consultants will be temporary and only to address work documented and approved through WRC.
- All InterSystems contracted consultant access can be granted only after the consultant has been formally enrolled as an InterSystems consultant via standard Human Resources processes. They must exist in the staff database of record before any accounts can be created or access granted.
- Ongoing access to the production environment for Managed Services is granted only to active InterSystems employees assigned to support Managed Services.
- Temporary access to the production environment is granted to approved InterSystems Personnel and/or customer staff or customer consultants while an active incident or problem exists in WRC for the Managed Services and only if such support requires access. All regular work by customer staff and customer consultants takes place in non-production environments.
- Administrative access to a customer's multiple environments can be controlled on a per environment basis.
- The customer is responsible for auditing and keeping current the access granted to the Managed Services systems for customer staff and customer consultants. Any additions, changes, or deletions to administrative level accounts should be submitted via WRC.
- Access to the solution and its associated account maintenance is controlled solely by the customer. Managed Services does not manage solution user account creation – only administrative accounts. Administrative accounts can typically be identified by the need for VPN client access to the Managed Services environment.
- Managed Services will provide an account summary report to the customer at least monthly detailing accounts granted access to any customer environments.

- Physical access to the Managed Services hosting datacenters is controlled by the vendor, Latisys/Zayo, using stringent controls expected of a professional datacenter and confirmed via SOC 2 Type II and SOC 3 report completions

Data Management

- All customer data stored or passing through the Managed Services customer environment is owned by the originating source. No customer data is owned by InterSystems.
- All customer data must be stored and accessed to comply with requirements of HIPAA and other regulations and standards applicable to the customer.
- All customer data is stored within the continental United States.
- All customer data access is granted on an as-required basis resulting from job requirements related to delivery of the Managed Services customer environment.
- No access to customer data is ever granted to InterSystems Personnel to provide reporting, development, testing, or other activities unrelated to the delivery of the services to the client, unless explicit permission by the client is granted and documented in WRC.
- Only changes documented and approved using the Managed Services change process can be applied to the production environment.
- No data is to be removed from the Managed Services hosting datacenters, except as directed by the customer. Security and encryption for any transfer of data outside the hosting datacenters must be reviewed and agreed by both InterSystems and the customer prior to removal to ensure data protection and future access capabilities.
- All Managed Services customer environments and data will be securely isolated from other customers.
- Managed Services customer environments may be deployed on either shared or dedicated servers and storage according to customer contract, but underlying infrastructure is shared. This includes storage controllers, networking components, server chassis, and any other components not including servers or specific storage.
- All data in production environments will be restored from backup and checked for database integrity at least once per week.
- All customer data will be encrypted both at rest and in flight using a minimum of 256 bit encryption.
- All backups of data will be located in either the primary or secondary datacenter used for Managed Services.
- Backups will be encrypted and an inventory of those backups maintained.

- Disaster recovery services are typically provided only for the production environment. Exceptions must be specified in the hosting contract.
- Environments with disaster recovery services will have data updates replicated from the primary datacenter to a secondary datacenter.
- Disaster recovery services are delivered with 15 minute RPO and 2 hour RTO.
- The Disaster Recovery Environment, located in the secondary datacenter, is an operational environment with ongoing access by InterSystems Personnel only. It is not accessible by customer staff or customer consultants except during a disaster recovery event. It cannot be used by the customer for any other purpose.
- Upon termination of Managed Services, InterSystems will provide a backup of the data to the customer. All ATNA log data and tools for accessing that data will also be provided, typically via a virtual machine on encrypted media. Once the above listed data is returned to the client, InterSystems will destroy all hosted data not required for hosted operation compliance audits.

Monitoring and Auditing

- All security-related logs will be audited either manually or automatically on at least a monthly basis.
- Intrusion detection services are active in all Managed Services customer environments.
- Continuous monitoring and alerting services will be active for all Managed Services customer environments, including servers, storage, connectivity, and related infrastructure supporting the Managed Services solution at all times.
- Monitoring alerts reporting risk to delivery of the production environment and/or related hosting infrastructure will generate an incident ticket in WRC and result in response by InterSystems staff within 30 minutes, both during and outside business hours.
- Monitoring alerts related to non-production environments will generate an alert email to the appropriate InterSystems team and result in review by InterSystems within 24 hours during standard business hours.
- All accounts providing administrator access of any level will be reported weekly and audited by InterSystems.
- Internal vulnerability scans will be performed weekly.
- Virus scanning will be regularly performed on all systems.
- Third party penetration testing will be engaged against all externally facing IP addresses of the hosting data centers at least annually.
- SOC 2 Type 2 audits of data center operations and security will be conducted annually.

Training

- Security training will be provided to each new InterSystems Personnel supporting Managed Services in the form of confirmed review of policies and procedures.
- All InterSystems Personnel supporting Managed Services must review security policies annually.
- All InterSystems Personnel supporting Managed Services will receive ITIL training.
- All InterSystems Personnel supporting Managed Services will receive training in the location and access methods for standard policies and procedures.

Security Incident Response

A security incident is any identified breach of access, data handling, or security policy. When identified, a security incident will be addressed with the highest level of response and will receive continuous effort 24/7 until any data risk is removed.

- All security incidents will be reported to InterSystems Legal Department immediately upon detection. The Legal Department will coordinate communication with the customer.
- The Vice President of Client Services will be informed and will be responsible for InterSystems senior management communication.
- Security incidents will NOT be documented in WRC. This is to ensure that no additional data risk is introduced.
- Disclosure of security incidents related to Managed Services customers will not be made public without specific written authorization from the customer
- Any incident that results in a data breach will follow InterSystems standard data breach procedure.
- For any security incident, the response will prioritize data protection. Managed Services will evaluate the risk and may prioritize data security over system availability.