INX Business Hosting

OVERVIEW

Available for INX InControl, INX InFlight, INX InForm, INX InHealth and INX InTuition

Date: 18 September 2023

v 1.0

Contents

Introduction

Thank you for choosing INX Software as your trusted partner for hosting solutions.

This overview provides a concise and high-level understanding of the key components and characteristics regarding the security posture, service levels, and disaster recovery of the INX Business Hosting solution.

Our commitment

We take pride in our dedicated and skilled multidisciplinary team of engineers. They work tirelessly to maintain and support the hosting environment, ensuring that it operates at its peak potential. Our team's commitment to excellence allows us to set a high uptime target of 99.9%, depending on the subscription plan selected by our valued clients.

Our hosting environment is continuously monitored and optimised against potential threats, guaranteeing a seamless and secure experience for all our users. We remain committed to delivering exceptional service and consistently improving our hosting infrastructure to meet and exceed your expectations.

Our products

A range of our intelligent solutions are supported on INX Business Hosting:

- INX InControl
- INX InFlight
- INX InForm
- INX InTuition
- INX InViron
- INX InHealth

Overview

We have partnered with Amazon Web Services (AWS) to host and deploy its application. One of their cloud-computing platforms, Amazon Elastic Compute Cloud (Amazon EC2), provides scalable computing capacity in the AWS cloud.

Amazon EC2 enables us to launch as many or as few virtual servers as required, configure security and networking, manage storage, and scale up or down to handle changes in forecast traffic. Read more about Amazon’s compliance.

Our hosting infrastructure

Regions and availability zones

Amazon EC2 is hosted in multiple areas world-wide, known as regions. Our platform is deployed to the AWS Sydney region and all data collected and processed from our application is retained in Australia.

If you require hosting outside of Australia, please contact your Account Manager.

Each Amazon EC2 region is completely isolated from the other Amazon EC2 regions. Within each Amazon region, there are multiple isolated locations known as Availability Zones.

Amazon EC2 provides us with the ability to place resources, such as instances (servers), and data in multiple locations within that region to ensure the highest level of fail over and redundancy in the situation of a disaster.

The Availability Zones in each region are connected through low-latency links. We use both the separation of regions and Availability Zones within AWS to maintain data protection and implement both disaster recovery and backup.

EC2 instances

Amazon enables us to deploy multiple instances (servers) to meet our business requirements and platform needs. Amazon EC2 scales to meet our platform needs and enable us to implement solutions to support performance, disaster recovery and backup requirements.

Vertical scaling

Vertical scaling means to add more resources to a single node within a system, such as increasing the CPU or memory requirements for a single server. It is used to increase performance to align with forecast user traffic and manage performance of its application when under load.

Vertical scaling is the process of increasing the instance type (hardware performance) for each instance on Amazon. We use a variety of instance types, depending on the purpose and requirements for the application or software that is run on the instance.

Time zones

Our products outlined in this document inherit the time zone from the server Operating System. We currently have time zones that cater for Australian Western Standard Time (AWST) and Australian Eastern Standard Time (AEST).

The choice of time zone should be considered during the implementation phase for your INX Software products.

Security posture

We take the protection of your data extremely seriously. This security overview describes the organisational and technical measures we have implemented in our platform, processes and systems designed to prevent unauthorised access, use, alteration or disclosure of user data.

Our services operate on AWS, with this policy describing our activities within our instance on AWS, unless otherwise specified.

Our compliance

Our business' processes, procedures and application undergo regular reviews (or every 12 months) to ensure everything we do meets stringent international quality and security standards.

AWS is compliant with a range of standards as outlined on their website, including SOC 2.

Our infrastructure

- All our services run in the cloud and are hosted using AWS. We do not run our own routers, load balancers, DNS servers, or physical servers.
- All our services and data are hosted in AWS facilities in Australia and are protected by AWS and our internal security, as described on the AWS website.
- AWS does not disclose the location of its data centres. As such, we build on the physical security and environmental controls provided by AWS. Find more details of AWS security infrastructure here.
- All our servers are within our own virtual private cloud (VPC), with network access control lists (ACLs) that prevent unauthorised requests reaching our internal network.

Data

- All your data (including user data) is stored in Australia.
- Your data in dedicated instances is stored in single tenant datastores.
- Your data in shared instanced is stored in multi-tenant datastores.
  - Strict privacy controls exist in our application code that are designed to ensure data privacy and to prevent one client from accessing another client's data (i.e., logical separation).
- Encryption at Rest is available in both dedicated and shared hosting options.

Data transfer

- Our API and application endpoints are TLS/SSL only (TLS1.2).
- All data sent to and from INX Software is encrypted in transit using TLS/SSL (TLS1.2).

Authentication

- We are 100% served over https.
- We have two-factor authentication (2FA) and strong password policies on all cloud services used in the hosting and development of our products.

Endpoint security

We employ a cutting-edge, security solution that is globally renowned for its excellence and innovation. The solution monitors and protects endpoints in real-time against cyber threats, leveraging AI and behavioural analysis for threat detection and response.

Maintenance windows

Maintenance windows exist for environments to enable us to identify, test, and apply patches or updates to software or operating systems, applications, and other IT infrastructure components. This allows us to address security vulnerabilities, improve functionality, and enhance performance.

It is a crucial aspect of cybersecurity and overall IT management.

The maintenance windows are scheduled as follows:

- Test/UAT – the second Friday of the month, from 6pm AWST – 9pm AWST
- Production – the fourth Friday of the month, from 6pm AWST – 9pm AWST

Security audits and penetration testing

- We annually engage with third party auditors to audit our application, and work with them to resolve potential issues.
- We use a technology that provides an audit trail over our infrastructure and our application. Auditing allows us to do security analysis, track changes made and audit access to the application.
- We engage with external consultants for annual application penetration tests. These assessments test our applications across a broad range of industry standards and testing methodologies. This ensures rigorous testing of our application's authentication mechanisms, application design, data validation, session management and more.
- For security and confidential reasons, we will only provide the executive summary from penetration testing reports.
- You are prohibited from penetration testing our applications and application infrastructure.

Security awareness training

All employees undertake security awareness training each year, as part of our security calendar. Our team also sign a non-disclosure agreement outlining their responsibility in protecting your data.

Security calendar and governance structure

Our Security Operations team meet on a regular basis to review cyber security events, incidents, risks, projects and processes.

Cyber incident response

In the case of a cyber incident, an incident response plan is followed, which provides guidance and the associated steps to follow in response to a cyber incident.

This plan is ensuring we contain, assess and manage cyber incidents in a timely fashion and in compliance with relevant legislative requirements to mitigate any potential harm to affected individuals.

The plan includes an assessment report that contains key tasks, roles and responsibilities, checks and procedure for notification in the event of a cyber incident.

Your responsibilities

As our valued client, there is a small list of things you need to do to help us keep your data secure:

- Manage your own user accounts and roles from within our products.
- Comply with the terms of your services agreement with us, including with respect to compliance with laws.
- Promptly notify us if a user credential has been compromised or if you suspect possible suspicious activities that could negatively impact security of our service or your account.
- Do not perform any security penetration tests or security assessment activities without our written consent in advance.

Service levels

The platform service levels (PSL) outline the hosting and delivery measures and requirements for the delivery and use of our products. The PSL defined remains valid until superseded by a new version.

Goals and objectives

The purpose and goal of this PSL is to ensure the proper elements and commitments are in place to provide consistent delivery and availability of our products to you organisation and your users.

The objectives of the PSL are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present your organisation a clear, concise and measurable description of service provision .
- Match perceptions of expected service provision with actual service support and delivery.

Periodic review

The PSL is valid from the effective date and is valid until further notice. This will be reviewed at a minimum once per fiscal year; however, in lieu of a review during any period specified, the current PSL will remain in effect. Contents of this PSL may be amended as required, and communication will occur to all affected parties 30 days prior.

Availability

The hosted production environment will be available online 24/7, 365 days a year with a targeted 99.9% uptime (excluding planned maintenance).

Monitoring

We use numerous tools to assist with infrastructure, application and performance monitoring, and log analytics and on call alerting.

Disaster recovery and backups

We are committed to delivering undisrupted service that allows you and your users to maintain the continuity of your operations.

Backup

Backup scheme

- AWS managed backup for EC2 instances
- SQL based backups for more granular recoverability

Disaster recovery

Our application is designed to be resilient in the face of an outage of one or more servers. This provides a real time fail over solution in the case of a disaster within one of AWS' availability zones .

In the event of failure of one or more web servers, our application can automatically provision additional redundant instances to handle end-user traffic.

- The target recovery point objective (RPO) is 4 hours.
- The target recovery time objective (RTO) is 24 hours.

More stringent targets may be implemented, depending on your requirements.

When there is a change to the circumstances, we will provide an update to the client contacts detailing the change. Where domain re-delegation is required, there may be a 12 to 24-hour delay between restoration of system functionality and the system becoming available via the internet, due to the delay in DNS propagation.

Disaster recovery response process

In the event of a significant disruption to production services or disaster affecting the availability of our hosting providers and your environment. Our team will follow steps outlined in the Disaster Recovery policy to ultimately remediate affected services.

Security incident response process

In the event of a security incident affecting the confidentiality, integrity or availability of our client data and environments. Our team will follow steps outlined in the Incident Response policy to secure affected assets.

INX Software

GET IN TOUCH
sales@inxsoftware.com
6373 2900

INXsoftware.com

Protecting people & planet