iRise
VISUALIZE. INNOVATE. DELIVER.

CLOUD FRAMEWORK & SECURITY OVERVIEW

From small businesses to the largest Fortune 500 Enterprises, customers trust the iRise cloud infrastructure when collaborating to define and design their applications.

This document explains why...

US: +1 800-556-0399
UK: +44 20 3574 4066
info@irise.com
www.iRise.com

iRise Los Angeles
2301 Rosecrans Ave
Suite 4100
El Segundo, CA 90245

iRise New York
545 Madison Avenue
9th Floor
New York, NY 10022

iRise London
7-8 Stratford Place
3rd Floor
London W1C1AY

PHYSICAL SECURITY

World-Class Data Centers

iRise uses Amazon EC2 to host most of its cloud infrastructure. In some cases, we can't use Amazon EC2. For example, a client may require that its data reside in the UK due to local privacy laws. (Amazon EC2 has no data center in the UK.) When a client's specific requirements disallow use of Amazon EC2, we host that client at Rackspace.

All data centers selected by iRise comply with SOC1 / ISAE 3402, SOC2, SOC3 and ISO 9001, among other key compliance standards/programs. This means that the facilities feature 24/7 manned security, physical and biometric access controls, extensive seismic bracing, the latest in early detection smoke and fire alarms, and digital surveillance systems.

Access to each system, network device, and application is limited to authorized personnel, and logged in detail. Event logs are reviewed on a regular basis. Details can be found here: Amazon Rackspace

Uptime of over 99%

In more than seven years of continuous service, iRise's uptime has consistently exceeded 99%. iRise offers options for clients who require a level of uptime greater than 99%.

Your Data is Separated from Other clients' data

On Amazon EC2, a client's data is stored on a dedicated EBS volume. On Rackspace, a client's data is stored on a dedicated CBS volume. Optionally, data may be stored on a physically distinct hard drive.

Your Data is Automatically Backed Up

Automatic data backup is included as part of your iRise cloud service. The backup data is physically separated from your data to ensure fault tolerance. Encrypted backup sets are optional.

NETWORK & SYSTEM SECURITY

Network Security

iRise uses industry-standard network protection procedures, including firewall and router technologies, network intrusion detection/prevention systems, and alert mechanisms that allow us to detect and immediately prevent malicious traffic and network attacks.

Regular internal network security audits and scanning give us an overview for quick identification of outdated systems and services.

Regular Updates and Patch Management

Operating systems, software, frameworks, and libraries used in iRise infrastructure are updated to the latest stable versions on a regular basis.

Whenever a vulnerability (e.g., a zero-day vulnerability) in a product used by iRise is publicly reported, immediate action is taken to mitigate any potential risks for our customers. We apply hot fixes and patches as soon as they become available.

System Integrity Protection

iRise uses cloud service provider built-in operating systems that are hardened according to NSA specification to minimize the threat vector and ensure the integrity of all system files.

APPLICATION SECURITY

Data Privacy and Sharing

Users can have one of three levels of access to an iRise project on the Definition Center. A role can be assigned directly to users who have been added individually to a project, or a role can be inherited from a user group that has been given access and to which the user belongs. In cases where a user has been assigned two separate roles (one as an individual user and one as a member of a group), the higher permission level will apply. The project activities in which users can engage are determined by their role on the project.

Authentication and Access Control

Each iRise user in a cloud instance has a unique account with a verified email address, protected with a password. Passwords must comply with password policy. iRise does not store passwords. Authentication data (secured per industry standards) is stored either on the cloud instance on the client's LDAP server. Your iRise administrator manages individual user rights by granting specific privileges (roles).

Data Encryption in Transit & At Rest

iRise uses 256-bit Transport Layer Security (TLS) with a preferred AES algorithm in CBC mode and 2048-bit server key length. When you access the iRise Definition Center, technology protects your information using both server authentication and data encryption. This is equivalent to network security methods used in banking and leading e-commerce sites. All users of iRise get the same in-transit encryption reliability so that passwords, cookies, and sensitive information are protected from eavesdropping.

iRise offers encryption at rest as an option for clients who require that their data be encrypted on disk. On EC2, Amazon typically manages the cryptographic keys. iRise provides an option that allows the client (or iRise) to manage the client's keys. On Rackspace, iRise manages the cryptographic keys.

Application Security Process

The robust application security process that has been fully integrated into iRise's software development life cycle (SDLC) includes:

- Defined in-house security requirements and policies, and well-known security best practices
- Security review of architectures, design of features, and solutions.
- Iterative manual source code review (and automated, using static code analyzers) for security weaknesses, vulnerabilities, and code quality.
- Regular manual assessment and dynamic scanning of pre-production environment.
- Security trainings conducted for IT teams according to their respective job roles.

ORGANIZATIONAL SECURITY

Operational Process

Designing and running a cloud infrastructure requires not just technology, but a disciplined approach to processes. This includes policies about escalation, management, knowledge sharing, risk, as well as the day-to-day operations. iRise's security team has years of experience in designing and operating cloud services, and we continually improve our processes over time.

iRise has developed best-in-class practices for managing security and data protection risk. All of these elements are essential pieces of iRise's security culture.

The Principle of Least Privilege

Only our highest clearance-level employees have access to our cloud infrastructure. There are strict security policies for employee access, all security events are logged and monitored. Our authentication methods are strictly regulated.

We limit access to customer data to employees with a job-related need, and require all those staff members to sign, and agree to be bound by, our Information Security Policy.

Data on an As-Needed Basis

Accessing data center information, as well as customer data, is only done on an as-needed basis, and only when approved by the customer (i.e. as part of a support incident), or by senior security management for the purposes of providing support, maintenance, and improving service quality.

ENTERPRISE GRADE SECURITY

Collaborate in a Secure Cloud Infrastructure

iRise is dedicated to providing enterprise grade security to all of it's customers, from small businesses to the largest Fortune 500 Enterprises. We realize it's an ongoing and ever-changing landscape. The job of securing our products and infrastructure is never done.

Need More Information?

If you have any security questions that are beyond the scope of this document, please contact our Sales team: 1-800-556-0399. Given you enter into an NDA with iRise, Sales can 1) arrange for a detailed security discussion, and/or 2) provide you with a copy of iRise's Information Security Policy.

If you have any questions about this document, please contact our Cloud Operations Security Team any time at security@irise.com.