



IR Cloud Security Statement

Updated: July 2025

Overview

Protecting customer data is of paramount importance to IR. It is for this very reason IR has an ongoing strategic investment to keep maturing our resources, capabilities, and controls in information security and data privacy. Our information security is architected on the principles of secure by design and defence in depth. IR security policies, controls, technology, and governance follow industry standard practices adopted through globally recognised frameworks including SOC2, ISO27001, ISO31000, OWASP, and PCI-DSS. Data privacy obligations are assessed across our products and enterprise using pertinent standards and regulations as applicable, such as GDPR.

This Cloud Security Statement applies only to current production Prognosis Cloud platform services offered by IR, hosted in Amazon Web Services (AWS). AWS is audited and certified by independent assessors against industry standards and regulations, a full list of which is available on the [AWS Compliance page](#). AWS provides a shared security model under which security and compliance is a shared responsibility between AWS and IR. AWS is responsible for the security of its data centres and the infrastructure that run the services in the AWS cloud, while IR is responsible for security of the services we offer, the applications we operate, and the data generated and collected. Further information about security provided by AWS is available from the [AWS Security website](#), including [AWS's overview of security processes](#).

Access Controls

The principle of least privilege is followed, and role-based security is used to manage access privileges and permissions within the production environment. Appropriate levels of segregation of duties are implemented to avoid access related conflicts. Unique user accounts are provisioned to ensure accountable actions are performed in the production environment. Access granted to critical components and services is periodically reviewed. Access is altered for employees moving within business functions and/or roles. Also, access is immediately revoked upon employee termination. Access to administrative accounts and to customer data is restricted through role-based security to only a limited number of employees within IR, solely for the purpose of maintenance and troubleshooting. Employee access is continuously logged and audited. Unauthorised access identified within IR's production environment either for malicious purposes or through erroneous actions is considered as a security incident and follows the Security Incident Management Process.

Customers are granted administrative privileges to manage access and role-based security for their respective data and application settings.

Data Segregation

Applications are developed on AWS multi-tenancy architecture, designed to segregate customer data by using unique authentication session keys. This limits customers to operate within their respective data and application cloud tenancy settings, without hampering the data integrity and confidentiality of other customers.

Data Encryption

Industry best standard encryption technologies in compliance with FIPS140-2 validated cryptographic algorithms are leveraged to encrypt customer data at rest and in-transit.

The Prognosis Cloud platform services use AWS server-side encryption with Amazon S3 managed keys (SSE-S3). Each object is encrypted with a unique key and as an additional safeguard encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt customer data. More information can be found [here](#).



Application Security Test

Depending on the classification of data and the associated risk, bespoke application security test procedures in-line with OWASP recommendations are designed and executed during static & dynamic application security tests and application penetration testing as part of the Secure Product Lifecycle process.

Change Management

All changes made to the production environment, within IR's application code, infrastructure, or data, are periodically reviewed and approved. Unit, system, and security tests are performed to assess the operational readiness of the product before any change gets deployed into the production environment. After the deployment of every change, the applications are closely monitored to ensure the change is as intended and has caused no issues to the application.

Security Operations Monitoring and Management

Security events are continuously monitored and risk assessed against current attack surfaces and tactics, techniques and practices (TTPs) by our managed security service provider. Internal systems provide 24/7 monitoring and alerting of operations, performance, security logging and status of the underlying AWS infrastructure and services, to detect critical outages. Service infrastructure-related risks are validated with compliance standards such as AWS Well Architected Framework and CIS AWS Foundations.

Incident Management

Security incidents are managed in-line with our documented policy and process, which details incident categories, escalation matrix, SLA, RACI and procedures that must be followed during an incident. Based on the category or severity of a security incident, relevant teams are engaged to respond, contain and resolve the issue. Affected customers will be notified promptly after a security event has been identified and classified as an incident. IR will provide continuous communications about the status of the security incident through relevant channels as we work through the resolution process.

Privacy

IR understands the importance of data privacy and is committed to ensuring the privacy of your personally identifiable information and complying with applicable privacy regulations. We aim to be clear and transparent about how we process such information. For further details, please see our [Privacy Policy](#).

Security and Privacy Training

At IR, security awareness training is a mandatory on-going process that aims at increasing the security and privacy knowledge across the organisation. Cyber threats and attack vectors keep changing, so must the guidance, information and the training we provide to our employees. Security education and training is conducted for all internal employees and contractors that outlines the importance of industry best practices.

External Audit & Certifications

IR holds both ISO/IEC 27001:2022 and SOC2 certifications and conducts audits annually to maintain such certifications and attestations. Upon a client's request, IR will provide the most recent SOC2 report and ISO/IEC 27001:2022 certificate.

Questions?

IR is committed to provide continual improvement in our security and privacy risk posture. Despite relevant policies, processes, controls, technology and governance in place, we cannot guarantee absolute security. If you have any questions about IR Information Security, please contact us at <https://www.ir.com/contact-support>.