AGENOR
delivering change, managing risk

# ICEFLO Security and Risk Management Overview

AGENOR
delivering change, managing risk

# Table of Contents

# 1 Our Company and Product

Agenor Technology are a consulting services company and cloud software solution provider based in Scotland. Formed in 2006 we have seen rapid growth, opening offices in London, Amsterdam and Dubai, while being recognised by Deloitte and Sunday Times Tech Track as being among the fastest growing technology companies in the UK. We are also a recognised Gartner Cool Vendor. We provide consulting services covering:

- Digital Change and Transformation across delivery, testing and business analysis
- Digital delivery covering Hybrid Cloud, Analytics and Platforms
- Cyber Security

We provide a unique cloud SaaS solution, ICEFLO, with three main capabilities:

- Enables clients to deliver complex technology implementation cutovers
- Delivers a sophisticated real-time deployment management solution
- Cloud based collaboration across dispersed teams enhancing client service delivery.

## 1.1 ICEFLO Security and Risk Governance

ICEFLO's primary security focus is to safeguard our customers' data. This is the reason that we have invested in the appropriate resources and controls to protect and service our customers. This investment includes the implementation of a dedicated team. The Infrastructure and Security Team is responsible for ICEFLO's comprehensive security and risk management program and the governance process. In n ever changing world of risks and threats he team is focused on defining new and refining existing controls, implementing and managing the ICEFLO security framework as well as providing a support structure to facilitate effective risk management.

## 1.2 Our Security and Risk Management Objectives

We have developed our security framework using best practices in the SaaS industry. Our key objectives include:

- **Customer Trust and Protection:** consistently deliver superior product and service to our customers while protecting the privacy and confidentiality of their information.
- **Availability and Continuity of Service:** ensure ongoing availability of the service and data to all authorized individuals and proactively minimize the security risks threatening service continuity
- **Information and Service Integrity:** ensure customer information is never corrupted or altered inappropriately.

To meet the objectives listed above we have processes and controls aligned with current regulatory and industry best practice guidance. We have designed our security program around best practice guidelines for cloud security.

## 1.3 Document Scope and Use

Agenor values transparency in the ways we provide solutions to our customers. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and the information and data in this document are not intended to create a binding or contractual obligation between Agenor and any parties, or to amend, alter or revise any existing agreements between the parties.

# 2 ICEFLO Security Controls

To allow us to ensure we protect data entrusted to us we implemented an array of security controls. ICEFLO's security controls are designed to minimize risk while allowing for a high level of employee efficiency. The following sections describe a subset of controls.

## 2.1 ICEFLO Security Overview

| | Description |
|---|---|
| **About** | The ICEFLO platform is our industry leading command and control solution for implementation and cutover activities. It provides easy to use, effective tools to manage our client's implementation events. |
| **Product Infrastructure** | The ICEFLO platform uses IBM Cloud, enabling redundancy, flexibility and responsiveness, ensuring world class infrastructure, network security and availability. All locations are SOC (1/2) and ISO27001 certified and maintain facilities secured against electronic and physical intrusion |
| **Application Protection** | The ICEFLO platform is protected by network level firewalls and further infrastructure connectivity controls. We also perform regular penetration testing both internally and externally. |
| **Customer Data Protection** | The ICEFLO platform is not used to process, store, collect or capture sensitive or personal data such as credit card numbers, financial information, passport information or similar identifiers.<br>Client data is segregated with industry standard fine grained access control.<br>All sensitive interactions with ICEFLO (e.g. API, logs, authenticated sessions) are encrypted in-transit with TLS 1.2 and 2,048 bit keys. Certain information is encrypted at rest. |
| **Privacy Protection** | We work hard to maintain the privacy of customer data. Data stored is yours and we use it only to provide the service to you. We never share your data or sell it. |
| **Business Continuity** | We have a comprehensive business continuity process covering system resiliency, recovery and backup. |
| **Corporate Security** | Our corporate security ensures standards around employee checks, internal processes, access control and security awareness of our employees. |

## 2.2 ICEFLO Product Infrastructure

### 2.2.1 Data Centre Security

ICEFLO outsources hosting of its product infrastructure to leading data centre providers. The ICEFLO product infrastructure is housed in IBM Cloud, providing high levels of physical and network security. IBM Cloud maintains an audited security program, including SOC-1, SOC-2 and ISO 27001 compliance. We do not host any production systems within corporate offices. IBM's world class data centres leverage the most advanced facilities infrastructure such as power, networking, and security. Facilities uptime is guaranteed between 99.95% and 100%, and the facilities ensure a minimum of N+1 redundancy to all power, network and HVAC services. Access to these data centres is highly restricted to both physical access as well as electronic access through public (internet) and private (intranet) networks to eliminate any unwanted interruptions in our service to our customers. These data centres' security protections, including continuity and recovery plans, have been independently validated as part of certifications. Information about data centre security, is available at the IBM Cloud compliance site.

### 2.2.2 Network Security and Perimeter Protection

The ICEFLO product infrastructure is built with internet scale security protections in mind. Network security protections are designed to prevent unauthorized network access to and within the internal product infrastructure. These security controls include enterprise-grade routing and network access control lists (firewalling). This allows for finely grained control for network traffic from a public network as well as between server instances on the interior of the infrastructure. Within the service infrastructure environment, internal network restrictions allow a multi-tiered approach to ensuring only approved "white listed" inter-component IP level connections are permitted.

### 2.2.3 Configuration Management

The ICEFLO product infrastructure is commissioned and managed in a highly controlled environment. Server instance builds are semi-automated, meaning that any server's configuration is tightly controlled from birth through decommissioning. All server type configurations are embedded in images and configuration files – server commissioned is based on a proven functional server clone. Server-level configuration management is handled using these images and configuration scripts when the server is built. Changes to the configuration and standard images are managed through a controlled change management process. Each instance type includes its own hardened configuration, depending on the instance. Rigorous configuration management is baked into our infrastructure processing.

### 2.2.4 Infrastructure Access

Timely anomaly response cannot happen without a stringent, consistent, and well-designed access control model. That is, it is impossible to quickly and automatically address the unexpected without first strictly controlling and defining expected patterns. Along those lines, internal access to Agenor systems is strictly controlled. Direct network connections to infrastructure devices is prohibited, and engineers are required to authenticate first through an intermediary before accessing pre - production or production environments. Server level authentication uses user-unique SSH keys and token-based two factor authentication.

### 2.2.5 Alerting and Monitoring

Agenor invest heavily in automated monitoring, alerting and response technologies to continuously identify potential issues. The ICEFLO product infrastructure is instrumented to alert when key anomalies or errors are identified. As unexpected or malicious activities occur, we bring in the right people to ensure that the issue is rapidly addressed. Agenor adopt industry standard automated tooling to protect the ICEFLO platform against a wide variety of undesirable situations. The power behind ICEFLO's ability to detect anomalies is our 24x7x365 monitoring program and extensive logging. We capture and store logs that include all the technologies that comprise our platform. At the application layer, all logins, page views, modifications, and other access to ICEFLO are also logged. In the infrastructure back-end, we log authentication attempts, horizontal and vertical permission changes, infrastructure health, and requests performed. Logs and events are monitored in real time on a 24x7 basis and key events are escalated immediately to developers and engineers to take appropriate action. Our alerting and monitoring toolset includes Nagios, Splunk, IBM, EM Express and New Relic.

## 2.3 Application Protection

### 2.3.1 Development and Release Management

ICEFLO has a rapidly advanced feature set, and we provide constant improvements through a modern continuous delivery approach to software development. New code is proposed, approved, merged, tested and deployed. Application code security and quality assurance reviews are performed by specialised teams of development engineers with intimate knowledge of ICEFLO as it is developed. Approval is controlled by designated repository owners. Once approved, code submitted to a continuous integration environment where compilation, packaging and unit testing are carried out. Completion of Unit testing is a precursor to a comprehensive cycle of Functional, Use-acceptance and Performance testing. If all passes, the new code is deployed across the application tier during clearly defined and agreed service windows. Major feature changes, while the code might have been released incrementally, are communicated directly to customers and via subscription to our status pages.

### 2.3.2 Vulnerability Scanning, Penetration Testing and Scanning

The ICEFLO Infrastructure and Security team manages a multi-layered approach to vulnerability scanning, using a variety of industry recognized tools to ensure comprehensive coverage of our technology stack. We perform a variety of vulnerability scanning and penetration testing activities against ourselves on a continuous basis. We perform vulnerability scanning against our networks, applications, and corporate infrastructure. External security scans are performed on a regular basis by independent 3rd party security testers. Continually running scans, adaptive scanning inclusion lists, and continuously updating vulnerability signatures help ICEFLO stay ahead of many security threats. To get a second opinion about our ability to identify and respond to security risks, we bring in industry-recognized third parties to perform penetration testing. The goal of these programs is to iteratively identify flaws that present security risk and rapidly address any issues.

## 2.4 Customer Data Protection

### 2.4.1 Confidential Information in ICEFLO

The ICEFLO platform is a command and control implementation platform. The information stored therein is client data relevant to implementation activities. As per the ICEFLO Terms of Service and Acceptable Use Policy, our customers ensure that they capture only appropriate information to support their implementation activities. The ICEFLO platform is not used to store, collect or capture sensitive data such as credit or debit card numbers, personal financial account information, social security numbers, passport numbers, driver's license numbers or similar identifiers, or employment, financial or health information. There is no PCI-DSS data stored in ICEFLO and no customers pay for the service by credit card. ICEFLO does not store, process or collect credit card information.

### 2.4.2 Encryption IN-TRANSIT and AT-REST

All sensitive interactions with the ICEFLO product (e.g. API calls, login, authenticated sessions etc.) are encrypted in-transit with TLS 1.2 and 2048-bit keys. Certain information is encrypted or hashed at rest, based on the sensitivity of the information. For instance, user passwords are hashed and certain email features work by encrypting message data at rest. Other data is stored in our database and is only accessible via authenticated login and is not encrypted at rest. Database fields are a mixture of text and some raw large object blocks (LOBs). No documents are stored in free standing storage or data directories. No data can be read as free text without either authenticated access or via authenticated SQL queries. ICEFLO does not permit collecting or storing of sensitive information like financial or health data through its service, as outlined in our Terms of Service.

### 2.4.3 User Authentication and Authorisation

The ICEFLO platform enforces a uniform password policy. The password policy requires a minimum of 8 characters that include a combination of lower and upper-case letters, special characters, whitespace, and numbers.

### 2.4.4 Employee Access

Agenor controls individual access to data within its production and corporate environment. A subset of Agenor's employees are granted access to production data based on their role in the company through role-based access controls (RBAC) or on an as required basis in the case of a production incident. Members of the Infrastructure team may be granted access to various production systems, as a function of their role. Common access needs include alert responses and troubleshooting, as well as to analyse information for product decisions as well as product support. Access to the production infrastructure is limited by network access and user authentication and authorization controls. Customer Support, Services, and other customer engagement staff with a need-to-know may request access on a time limited basis. Requests for access are limited to their work responsibilities associated with supporting and servicing our customers. All access requests, logins, queries, page views and similar information are logged.

All Agenor employees are security screened prior to their engagement.

### 2.4.5 Client Access Management

Clients have full control over their own data and who can access it. Access management for Client user access is delegated to the Client System Administrators who control and manage user access through ICEFLO roll based access control.

## 2.5 Privacy

The privacy of our customers' data is one of ICEFLO's primary considerations. As described in our Privacy Policy, we never sell your data to any third parties. The protections described in this document and other protections that we have been implemented are designed to ensure that your data stays private and unaltered.

### 2.5.1 Data Retention Policy

Customer data is retained for as long as you remain an active user of the ICEFLO service. Former customers' core data is removed from live databases upon a customer's written request or after an established period following the termination of the customer agreement. In the case where there is no formal written request to remove a former customers' data it is purged 90 days after all customer relationships are terminated. Information stored in replicas, snapshots, and backups is not actively purged but instead naturally ages itself from the repositories as the data lifecycle occurs. Agenor reserves the right to alter the data pruning period and process at its discretion to address technical, compliance, or statutory needs.

### 2.5.2 Privacy Program Management

Agenor's legal, security, and other teams collaborate to ensure an effective and consistently implemented privacy program. Information about our commitment to the privacy of your data is described in greater detail in our Privacy Policy and Data Processing Agreement.

## 2.6 Business Continuity and Disaster Recovery

Agenor maintains a constantly improving disaster recovery plan focusing both on preventing outage through redundancy of telecommunications, systems and business operations, and on rapid recovery strategies in the event of an availability or performance issue. Whenever customer-impacting situations occur, Agenor's goal is to quickly and transparently isolate and address the issue. Identified issues are published on our ICEFLO status site and are subsequently updated until the issue is resolved.

### 2.6.1 System Resiliency and Recovery

Business continuity testing is part of ICEFLO normal processing. ICEFLO recovery processes are validated continuously through normal maintenance and support processes. We follow continuous deployment principles as part of our regular maintenance and growth. We also use those procedures to recover from failures, allowing us to practice our recovery process. ICEFLO primarily relies on infrastructure redundancy, real time replication and backups.

### 2.6.2 Backup Strategy

ICEFLO ensures data is replicated and backed up across multiple datastores. The retention period of backups depends on the nature of the data. Seven days of backups are kept for any database in a way that ensures restoration can occur easily. By default, all backups will be protected through access control restrictions on ICEFLO product infrastructure networks, access control lists on the file systems storing the backup files and/or through database security protections.

## 2.7 ICEFLO Corporate Security

### 2.7.1 Employee Authentication and Authorisation

Agenor enforces an industry standard corporate password policy. That policy requires changing passwords at least every 90 days. It also requires a minimum password length of 8 characters and complexity requirements including special characters, upper and lowercase characters and numbers. We prohibit account and password sharing by multiple employees. Employees generally authenticate to ICEFLO product infrastructure using passwords and SSH keys. Additionally, many of the capabilities we use to build the ICEFLO products leverage multi-factor authentication or are protected by SSO solutions.

### 2.7.2 Access Management

Agenor has regimented and automated authentication and authorization procedures for employee access and all access is logged. Most frequently, access is granted based on a role-based access control model. We deploy a process to streamline and automate our security management and compliance activities. We constantly review to ensure that permission grants are appropriate, to manage employee events, to revoke accounts and access where needed, to compile logs of access requests and to capture compliance evidence.

### 2.7.3 Background Checks

All Agenor employees undergo an extensive 3rd party background check prior to formal employment offers including employment, education and criminal checks for all potential employees. Reference verification is performed at the hiring manager's discretion. All employees receive security training within the first month of employment as part of the security program along with role specific follow up training. All employees must comply with Non-Disclosure Agreements and Acceptable Use Policy as part of access to corporate and production networks.

### 2.7.4 Vendor Management

We leverage a small number of 3rd party service providers who augment the ICEFLO products' ability to meet our client's needs. We maintain a vendor management program to ensure that appropriate security and privacy controls are in place. The program includes inventorying, tracking, and reviewing the security programs of the vendors who support ICEFLO. Appropriate safeguards are assessed relative to the service being provided and the type of data being exchanged. Ongoing compliance with expected protections is managed as part of our contractual relationship with them. Our Infrastructure and Security team, senior management, and the business unit who owns each contract coordinate unique considerations for our providers as part of contract management.

### 2.7.5 Security Awareness and Security Policies

To help all our engineering, support, and other employees with regards to protecting client data, Agenor developed and maintains an Information Security Policy. The policy covers data handling requirements, privacy considerations, and responses to violations, among many other topics. With this policy and the myriad protections and standards in place, we also ensure staff are well-trained for their roles. General security awareness training is offered to all new employees and covers ICEFLO security requirements. After initial training, different training tracks are available based on an employee's role. Recurring training is provided through regular updates, notices, and internal publications.

## 2.8 Security Incident Management

ICEFLO support team is setup to respond quickly to all security and privacy events. ICEFLO's rapid incident response program is responsive and repeatable. Many automated processes feed into the incident response process, including malicious activity or anomaly alerts, vendor alerts, customer requests, privacy events, and others. In the event of an incident, we first determine the exposure of the information and determine the source of the security problem, if possible. We communicate back to the customer (and any other affected customers) via email or phone (if email is not sufficient). We provide periodic updates as needed to ensure appropriate resolution of the incident.