inRiver

Service Security

inRiver PIM Service

inRiver AB - info@inRiver.com - www.inriver.com Last updated March 4, 2021

Table of Contents

1. Definition and scope

inRiver PIM Service is a service hosted on Microsoft Azure platform and not dependent on inRiver sites for continuous delivery. Only parts directly influenced by inRiver will be described below, such as, but not limited to secure SaaS (multi-tenant) operations, backup policies, authorization and protection.

inRiver uses Microsoft AzureCloud Computing Services (subservice organization) and Microsoft provides their own set of compliance certifications, assessments, and reports. All which can be found on their website https://www.microsoft.com/en-us/trustcenter/compliance/default.aspx.

Additionally, inRiver submits to undertake yearly audits by independent service auditors for compliancy with SOC2/Type 2; an assessment to evaluate the suitability of the design of inRiver security controls to provide customers reasonable assurance that inRiver's service commitments and system fulfill the requirements of the relevant trust services criteria for security and availability, as set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

2. Data Centers

- All data centers used by inRiver are operated by Microsoft Azure.
- The inRiver PIM Service is hosted in multiple data centers/regions in the world.
- Customers can decide which of the available data centers/regions their customer data is stored.
- inRiver ensures that customer's data is stored in the customer requested data center/region.
- Authentication of inRiver PIM Service is available in all data centers/regions that the service is available in.

3. Access Control and Security

i. Authorization

Only authorized operations personnel have access to inRiver PIM Service. The authorized personnel are kept to a minimum. If authorized operations personnel leave the employment of inRiver or inRiver's authorized subcontractor or for any other reason no longer need access rights to the inRiver PIM Service, inRiver will remove all access within 24 hours.

ii. Password Control

Passwords must be at least eight characters long; include at least one uppercase letter and must also include at least one number. A user will be allowed up to 10 login attempts, after which the user's account will be locked. The lockout continues for 30 min. Operations personnel accounts are secured with multi factor authentication.

iii. Encryption and Communication Security

All data is encrypted in transit and at rest in the inRiver PIM Service. Communication with inRiver PIM Service is encrypted with the industry standard Transport Security Layer (TLS) 1.2.

iv. Physical Security

Physical access to datacenters and physical servers is controlled by Microsoft Azure.

The inRiver (Microsoft Azure) data centers are protected by layers of in-depth security that include perimeter fencing, video cameras, security personnel, secure entrances, and real-time communication networks. This multi-layered security model is in use throughout every area of the facility including each physical server unit. inRiver relies on the extensive certification of the Microsoft Azure platform.

v. Office Facilities

inRiver offices have electronic locks. Each employee receives a personal entrance key (and a personal code) which can be electronically revoked.

All guests must register before entering the office, must wear a name-tag identifying the guest.

inRiver's internal and guest Wi-Fi networks are password-protected and fully encrypted. No secure systems are available over the guest network. inRiver uses multiple internal networks to ensure access to particularly sensitive systems which can be restricted to a specific internal network.

4. inRiver SSO (client service)

inRiver PIM Service is Single Sign-On (SSO) as centralized login system that enables a single access point to inRiver PIM Service. A single ID is used to validate user credentials and establish the identity of the user, sharing user information with all subsystems that require the data once the identity of the user is established.

The inRiver SSO utilizes SAML 2.0. Security Assertion Markup Language (SAML) is an XML-based framework for authentication and authorization between two entities, the service provider and an Identity provider. SAML is a standard SSO format.

5. Backups

- SQL Database backups are done daily (with point-in-time restore) and are stored in geo-redundant storage for 30 days. Backups of customers data and logs are included in the service.
- The physical isolation between datacenters in the geo-redundant storage is more than 300 miles (approx. 480 km).
- Media backups are done daily and are saved for 30 days.
- Specific inRiver intervals for recovery have proved enough to provide minimal to no data loss (i.e., RTO/RPO);
  - Recovery Time Objective (RTO) - addressed within 8 hours
  - Recovery Point Objective (RPO) - addressed within 15 minutes

- inRiver performs regular data recovery tests in respect of the data which has been backed up. Recovery tests are done twice per year.
- All backed up data are encrypted.

6. Malware Protection and updates

- Malware protection is installed on all servers and services used by the inRiver PIM Service and authorized operation personals computers.
- inRiver keeps inRiver PIM Service up-to-date with the latest security patches and continues releases of software ensures customers are running the latest and greatest software.

- inRiver monitors and mitigates vulnerabilities and threats with Azure Security Sentinel (an SIEM solution) and other monitoring solutions.
- Microsoft ensures that the platform Microsoft Azure is protected and up-to-date. Read more here: https://www.microsoft.com/en-us/trustcenter/security.

7. Vulnerability Management & Penetration Testing

inRiver performs regular vulnerability management and penetration testing of inRiver PIM Service to ensure that the services are sufficiently protected from Malware and other external security threats. Microsoft performs such similar tests on Microsoft Azure on a regular basis likewise.

To ensure that inRiver PIM Service is secure, inRiver performs automated tests on every new release to verify that OWASP TOP 10 protection on the Web Application works as expected. The OWASP Top 10 list is regularly revised as threats emerge, along with the techniques and best practices for avoiding and remediating the vulnerabilities. Below is the current list of test categories performed by OWASP.

1) SQL Injection Attacks
2) Broken Authentication & Session Management
3) Cross-Site Scripting (XSS) Attacks
4) Insecure Direct Object References
5) Security Misconfiguration
6) Sensitive Data Exposure
7) Missing Function Level Access Control
8) Cross-Site Request Forgery Attacks (CSRF)
9) Using Components with Known Vulnerabilities
10) Invalidated Redirects and Forwards

inRiver does not share their testing results externally for these or other tests as a security assurance measure.

8. SaaS-Based Cloud Monitoring

i. Microsoft Azure Security Center

inRiver uses all the available processes and assets afforded by Microsoft Azure Security Center, i.e., event monitoring and reporting, host-based intrusion detection systems (IDS), and event management (network activity, logs, and alerts).

ii. Azure SIEM Sentinel

inRiver has implemented Azure Sentinel with advanced AI-based real-time security, event monitoring, and analytics. Microsoft Azure Sentinel is a scalable, security information event management (SIEM) tool with security orchestration automated response (SOAR) to more effectively monitor across all users, devices, applications, and infrastructure.

9. Code Security

iii. Securing Source Code

All developer activities and operations personnel activities are tracked through the version control system or support tickets, and both document all changes. inRiver utilizes a continuous integration and verification process involving multiple environments with gated code check-ins that enforce peer review of all code changes along with automated tests to verify proper functioning.

inRiver uses Microsoft Team Foundation Server (TFS) with Git version control and Visual Studio Team Services (VSTS) to secure the source code. Tracking of work, issues and versioning of code is an important part to deliver high quality code with DevOps workflow and secure change control policy.

Any source code used by inRiver in the provision of the inRiver PIM Service will is securely handled and subject to appropriate access control procedures.

iv. Security Vulnerabilities in Code and Coding Hygiene

inRiver takes the appropriate measures to ensure that there are no security vulnerabilities in the system, or the software required to provide the inRiver PIM Service.

All inRiver developers attend an OSCP education to hold an understanding of the importance of security https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/.

10. inRiver Employees and Contractors

inRiver's recruitment process for employees and engagement of contractors involves education for security awareness. The closer the role is to the service and customer data, the more rigorous education. Security awareness is also assessed in the selection of contractors.

inRiver's IT policy mandates secure IT practices for all employees and contractors, including but not limited to:

- Locking laptops automatically when not used.
- Using data encryption on all devices.
- Using up to date centrally managed anti-virus.

There are processes and automated mechanisms in place to ensure that accounts are decommissioned immediately on employee termination.

System credentials that must be shared are stored only in encrypted form through password management software, and access is limited to the minimal set of technical staff who need it.

All inRiver's employees and contractors sign a non-disclosure agreement or confidentiality undertaking upon employment or engagement.

InRiver employees and contractors are granted access to systems in accordance with the principle of least privilege.