inriver Service Security

1. DEFINITION AND SCOPE

1.1. Data. In the context of this document, "data", refers to all customer supplied data to inriver PIM.

1.2. inriver PIM. inriver PIM is a multi-tenant SaaS (Software-as-a-Service) solution hosted on Microsoft Azure. Hence, there is no dependency on any inriver on-premises resources for continuous service delivery.

1.3. Scope. Only parts directly influenced by inriver will be described below, such as, but not limited to secure SaaS (multi-tenant) operations, backup policies, authorization, security, and vulnerability management.

1.4. SOC2. This is the Service Organization Control 2 Report (SOC 2). It is an auditor report assessing controls for security and compliance.

1.5. SOC2 Type II. SOC2 Type II audits examine the effectiveness of controls in place to protect and secure the system or services over a specific period (usually a year). This also includes the assessment of any possible risks, and the suitability of any plans to mitigate such risks appropriately.

2. SECURITY AUDIT

2.1. Security audit (SOC2 Type II). inriver submits to undertake yearly audits by independent service auditors for compliancy with SOC2 Type II. This is an assessment to evaluate the suitability of the design of inriver security controls in inriver PIM to provide reasonable assurance and commitment that the system fulfills the requirements of the relevant *Trust Services Criteria* for security, availability, processing integrity, confidentiality, and privacy set forth for SOC2 by *AICPA* (American Institute of Certified Public Accountants):

- *security* – inriver PIM is protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.
- *availability* – inriver PIM is available for operation and use to meet inriver's objectives.
- *process integrity* – refers to the completeness, validity, accuracy, timeliness, and authorization of inriver PIM processing.
- *confidentiality* – information designated as confidential is protected to meet inriver's objectives.
- *Privacy* – personal information is collected, used, retained, disclosed, and disposed of to meet inriver's objectives.

2.2. SOC2 attestation report. inriver will provide a copy of the Security Audit report upon request.

3. DATA CENTER

The inriver PIM Service is hosted in multiple data centers/regions in the world. All the data centers are operated by Microsoft Azure. Authentication of inriver PIM Service is available in all data centers/regions that the service is available in.

3.1. Data storage. Customers can decide which of the available data centers/regions (in EU or US) their data is stored. inriver ensures that customer's data is stored in the customer requested data center/region.

4. DISASTER AND RECOVERY

4.1. Redundancy. There are two regions in use for inriver PIM, the US-East and EU-West. Where possible, backups are stored in at least zone-redundant storage. This helps protect against outages that affect backup storage in one datacenter. It allows the possibility of restoring databases from another datacenter if there is an outage in a particular datacenter.

4.2. Business continuity. All backups are created and stored to ensure a retention of no less than 30 days. Backup and retention for SQL Databases is based on Microsoft's business continuity features in Azure. Azure SQL server audit logs have a retention policy of 30 days. *Recovery Time Objective (RTO)* and *Recovery Point Objective (RPO)* are based on Microsoft Azure service support for business continuity. Currently the RTO is 12hrs and RPO is 1hr. Microsoft may update the above Azure features. Please visit Microsoft Azure website for the most up-to-date information on Microsoft's SQL Database business continuity features. Media backups are done daily.

4.3. Disaster recovery. Specific inriver intervals for recovery have proved enough to provide minimal to no data loss. inriver PIM disaster recovery is based on extensive business continuity program and data retention plan that is according to Microsoft Azure Storage Redundancy and Replication procedure.

4.4. Testing and Formal internal policy. inriver has a business continuity and disaster recovery (BC/DR) policy and procedure for the production environment based on inriver's SOC2 policy. inriver performs business continuity and disaster recovery (BC/DR) tests annually.

5. ACCESS CONTROL AND SECURITY

5.1. Inriver SSO. inriver PIM users have the option of enabling single sign-on (SSO). If SSO is not enabled, you will sign in using forms authentication. The login procedure and the login page are the same. The basic difference is that forms users are asked to enter their password when signing in.
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.

5.2. Authorization for inriver personnel. 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.

5.3. Password Control. Passwords must be at least eight characters long. Each password must include at least one uppercase letter, at least one lowercase letter, at least one number, and at least one non-alphanumeric character.

5.4. Encryption and Communication Security. All customer supplied data to inriver PIM service is encrypted in transit and at rest in the inriver PIM Service. Communication with inriver PIM Service is encrypted with at least Transport Security Layer (TLS) 1.2, configured to use secure cipher suites. Transparent data encryption (TDE) in Azure encrypts the databases, backups, and logs using AES 256 encryption algorithm.

5.5. Access Control. inriver implements access control policies and procedures that address onboarding, offboarding, transition between roles, regular access reviews, limitations and usage control of administrator

privileges, and inactivity timeouts. inriver enforces principles of “least privilege” and “need to know”, as well as review user access rights on a regular basis to identify excessive privileges.

5.6. Physical Security. Physical access to datacenters and physical servers for inriver PIM is controlled by Microsoft Azure.

5.7. 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 and 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.

5.8. Security Measures. inriver implements and maintains administrative, technical, and physical safeguards with appropriate level of security measures. inriver maintains commercially reasonable administrative and technical safeguards designed to secure data against accidental or unlawful destruction, access, loss, alteration, or disclosure. inriver may update the security measures in this document or stated elsewhere by inriver from time to time, so long as the updated measures do not materially decrease the overall protection of customer data.

5.9. Security Incident or Data Breach Notification: inriver complies with GDPR with regards to data breach notification requirements. In the unlikely event of a security incident or data breach, inriver will notify the affected customers and authorities without undue delay of any security incident and take commercially viable and appropriate actions to mitigate the impact and prevent recurrence. In the notification inriver will include steps taken to mitigate the potential risks and steps inriver recommends the customer take to address the security incident or data breach. inriver is committed to ensuring the security and privacy of its customers’ data. inriver’s notification of or response to an security incident or data breach will not be construed as inriver’s acknowledgement of any fault or liability with respect to such security incident or data breach.

6. MALWARE PROTECTION

Malware protection is installed on all servers and services used by inriver PIM and authorized operation personal computers. inriver monitors and mitigates vulnerabilities and threats with the support of Microsoft Azure inbuilt anti-malware and security monitoring tools.

7. VULNERABILITY MANAGEMENT

7.1. Penetration Testing. inriver engages an independent third-party company to perform penetration testing on an annual basis based on inriver’s SOC2 policy. In addition, inriver performs regular internal penetration tests.

7.2. Vulnerability scans. inriver engages an independent third-party company to perform network vulnerability scans on a weekly basis. The scans can also be triggered on demand by inriver. Microsoft Azure in-built tools provide additional 24/7 security infrastructure scanning.

7.3. Code security. Code scanning tools are used to check for secure coding practices, and security evaluation of third-party or open-source libraries. Any source code used by inriver in the provision of the inriver PIM Service is securely handled and subject to appropriate access control procedures. All inriver developers take mandatory security training for general security awareness and secure coding best practices.

7.4. Secure CI/CD pipeline. To facilitate the deployment of consistent and quality code, inriver utilizes a version control system, and continuous integration and continuous deployment (CI/CD) and release pipelines. A verification process is also in place with gated code check-ins that enforce peer review of all code changes along with automated tests.

7.5. Documentation and remediation. Documentation and remediation commitments of vulnerabilities are based on inriver's SOC2 policy. Results from the penetration tests and vulnerability scans are analyzed by our inhouse cybersecurity experts together with our external consultants.

8. SECURITY MONITORING

8.1. SOC Monitoring 24/7. inriver uses a third-party Managed Security Services Provider (MSSP) / Managed Detection and Response (MDR) company. The company provides 24/7 SOC (Security Operation Center) continuous security monitoring, threat remediation, and management of inriver's internal and Microsoft Azure environment and assets. The provider uses its own proprietary tools as well as Microsoft Azure built-in tools (for example, Defender for Cloud and Microsoft Sentinel SIEM) to support the security monitoring and remediation activities.

8.2. Azure Monitoring. inriver uses Azure built-in tools to compliment 24/7 SOC monitoring activities by the MSSP/MDR provider.

- *Microsoft Defender for Cloud* is used for Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) solution.
- *Microsoft Sentinel* is the Security Information and Event Management (SIEM) used to support monitoring of security threats across all users, devices, applications, and infrastructure more effectively. The SIEM is used as part of the 24/7 SOC monitoring activities.
- *Azure Monitor* is a comprehensive monitoring solution for collecting, analyzing, and responding to telemetry for inriver's applications and services that are hosted in Azure.

9. INRIVER EMPLOYEES AND CONTRACTORS

inriver employees and contractors are granted access to systems in accordance with the principle of least privilege. inriver's recruitment process for employees and engagement of contractors involves education for security awareness.

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 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.

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