

# innius® Security Policy

## 1 Why this Policy?

- 1.1 We want you to know that we take security very seriously and our goal is to be as clear and open as we can about the way we handle security. We believe good security is based on three pillars: Confidentiality, Integrity and Availability. Confidentiality refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized users. Integrity refers to the trustworthiness of information resources, while availability refers to the availability of information resources.

## 2 What about Confidentiality?

- 2.1 Confidentiality is all about identification, authentication and authorization. At innius we use different types of identification, depending on which type fits the need the best. This also applies to authentication. The mechanism supports the key business capability of a collaborative, multi-tenant maintenance solution for industrial assets, used within a collaboration network of machine manufacturers, machine customers, technical service providers and other stakeholders involved in operation and maintenance of industrial assets over its entire life cycle. Access to data must pass authorization checks and the user authentication subsystem uses internet standards for authentication, such as OAuth. We also chose a flexible architecture that allows stronger authentication mechanisms to be applied in the future if that becomes necessary.
- 2.2 By default, access to the data is not allowed. Only if you assign an authorization policy for the customer (or another role, such as an employee) that allows them to view that data will they be able to see it. The authorization part of innius provides insight into the different authorization groups and their authorization policies, as well as their members (persons). One machine can be part of multiple groups, and in that case you yourself must define who has access to a particular machine. All authorization requests are implicitly limited to the resources owned by the customer.

## 3 What about Integrity?

- 3.1 It's important that you can trust our solution and your data. It requires a high level of data protection and insight in and traceability of the processes that are performed. The environment that hosts innius maintains multiple certifications for its datacentres, including ISO 27001 compliance, PCI Certification, and SOC reports. Interactions with the innius cloud or the AWS services which involve confidential information are performed over the internet by means of SSL/TLS connections. For some data types an additional checksum is performed to ensure request integrity. The apps use https connections as well. Only a very limited amount of data is stored on the phone, such as your favorites list and missed conversations. If you lose your phone, you have the option to block a user. This prevents any device from accessing innius with that user's credentials.

## 4 What about availability?

- 4.1 The innius solution has been designed with reliability and scalability in mind. The micro services we use are capable of dynamically configuring themselves to changing circumstances, because they use a fault-tolerant distributed registry and key value store for service registration and configuration information. In innius, the complete configuration of a run-time environment and of all services involved, is stored as code in the versioned source repositories. In that way it is possible to recreate a full environment for more than 95% automatically. Many of the AWS services that are used by the innius solution are highly scalable and fault-tolerant. For instance, the DynamoDB database service offers configurable scalability for read and write operations, in addition to a three-way redundant storage of data in an AWS region. Offloading a complete data set for backup and recovery is facilitated.

## 5 Where is my data stored?

- 5.1 We believe the best place to store data is within the jurisdiction of the EU's Data Protection Directive. Therefore we store your data in Ireland. The EU's Directive provides strong protection for personal data.

## 6 If I have additional questions?

- 6.1 Feel free to reach us via our website, we are happy to answer your questions.

© 2022 Innius B.V. Last updated: March 11, 2022.