INFORMATION SECURITY STATEMENT OF IOTSPOT B.V.

1 General

iotspot B.V. (“we” or “iotspot”) agrees to comply without restriction with all security stipulations set forth below, for provisioning of our Services.

2 Information security organization

iotspot B.V. has an information security management (ISM) officer that raises employee awareness of ISM topics, releases ISM guidelines and controls ISM implementation. The security officer directly reports to iotspot's management.

3 Employee confidentiality obligation

3.1 All employees engaged to provide our Services have a written commitment to comply with data confidentiality.

3.2 In addition to that every member of the iotspot support team will be in the possession of a security clearance provided by the Dutch Information and Security Agency (AIVD). This is the result of an extensive background security check. This security clearance is an official document which provides the person concerned with a ‘statement of no objection’ (‘verklaring van geen bezwaar’/security screening Dutch department of Justice).

3.3 In the event, iotspot engages Third Party staff and/or external contractors, both these parties as well as the designated employee(s)/contractor(s) have committed in writing to comply with our data confidentiality.

4 Data protection

4.1 Encryption of data in transit and data at rest. The goal of data encryption is confidentiality, i.e. to conceal the meaning of the content of any records to unauthorized access to the data processing systems. To that end, iotspot encrypts all transactional, privacy sensitive and personal data both in transit and at rest.

4.2 Physical Access Control. The goal of access control is to deny unauthorized persons access to those data processing systems that process or use transactional, privacy sensitive and personal data.
The iotspot datacenter site(s) is secured against unauthorized access through automated access control systems. In addition, the datacenter is equipped with permanent video surveillance and access is monitored by security personnel and/or entry gates. The security service performs regular patrols at night.

A clearly defined system for authorized access is also in place outside of the company’s data center(s). Employee access is controlled by scanners at office entrances (electronic access control). Reception personnel is also present. Visitors and third parties are recorded in visitor lists and are only permitted access to iotspot premises while accompanied.

Access to data center rooms is additionally secured through single-person entry systems. Automated access control is supplemented by other established methods of access authorization, such as pinpads, DES dongles, and permanent security personnel. Access to the inner security areas is only permitted for a small, selected number of support personnel. Individual entry and presence is recorded by video in certain security areas.

4.3 User Access Control. The goal of User Access Control is to prevent unauthorized persons from using data processing systems that process and use personal data.

Data terminals (PC, servers, and network components) are accessed by means of authorization and authentication in all systems. Access control regulations include the following measures:

a) Passwords (lower- and upper-case letters, special characters, numbers, minimum 8 characters, changed regularly, password history).

b) Passwords are stored encrypted with Blowfish one-way hash with random salt in the database. No reverse engineering possible.

c) Role-based rights are tied to access ID (classified according to administrator, user, etc.).

d) Screen lock with password activation in user’s absence.

e) Encryption of data storage devices while in transit (including notebook hard drives).

f) Use of firewalls and antivirus software including regular security updates and patches.

4.4 Data Access Control. Data Access Control measures prevent unauthorized activities (e.g. unauthorized reading, copying, modification or removal) in data processing systems by persons without the appropriate authorization.

iotspot ensures the system-wide authentication of all users and data terminals including access regulations and user authorizations.

Data access control incorporates the following measures:

a) A written authorization concept is in place.

b) An individual Customer based authorization concept is implemented with role definitions according to ITIL have been made.

c) Shared systems have Customer separation.

d) A clean desk policy is in place.

e) Data storage devices in all mobile systems are encrypted while in transit (including notebook hard drives).

f) Use of firewalls and antivirus software including regular security updates and patches.

4.5 Transmission Control. The purpose of transmission control is to enforce that transactional, privacy sensitive and personal data cannot be read, copied, modified or removed while being transmitted, transported or saved to a data storage medium, and that it is possible to verify and establish to which bodies personal data may be transmitted using data transmission equipment.

Data can be transmitted from the Customer to iotspot in a number of ways and must be agreed between the parties. iotspot supports standard secure transmission types, such as network-based encryption through SSL 3.3 /TLS 1.2 (server-server or server-client), encrypted connection tunnelling or secure transmission, such as sFTP (secure File Transfer Protocol).

Additional measures are:

a) Policy for mobile devices.

b) Disposal of data storage device in a manner compatible with data protection regulations (The medium shall be physically destroyed in compliance with DIN 32757 minimum security level 3).

c) Clean desk policy is in place.

d) Encryption of data storage media while in transit (including notebook hard drives).

e) Secure file exchange.

4.6 Input Control. The goal of input control is to ensure by means of appropriate measures that the circumstances surrounding data input can be established and verified.

iotspot has implemented access regulations and user authorizations that enable the identification of all users and data terminals in the system. The activities of users are traceable through extensive logging functions. Modifications are logged on servers or programs.

Within the iotspot software, strict authentication methods only grant access to users that have been identified and validated. In this way, iotspot safeguards the integrity of the available (database) information by preventing unauthorized users to view or modify data which they should not have access to. In this reference a wide variety of authorization levels can be implemented, as the presentation and accessibility of the available information strongly depends on business confidentiality and relevance. Depending on the required functionality and the applicable security legislation and requirements, a user can be either granted access to a subset of the data or this access can be revoked.

4.7 Order Control. The goal of order control is to ensure that transactional, privacy sensitive and personal data, which is processed on behalf of the Customer, is processed only in accordance with the Customer's directives.

a) Processing of privacy sensitive or personal data is always based on a Customer order. At a minimum, there is an existing contract in effect.

b) Standard changes in which personal data is processed can only be requested by an authorized Customer representative. A workflow procedure at the order entry position ensures compliance.

c) The procedure described in ITIL is implemented for change requests. As above, only an authorized Customer representative is permitted to release a change request.

4.8 Availability Control. The goal of Availability Control is to ensure that transactional, privacy sensitive and personal data is protected from accidental destruction or loss. Privacy sensitive and personal data and data saved for later processing is stored at a RAID-1/10 system that protects against hardware-related data loss. If the need for protection increases, data is stored in redundant systems up to a spatially separate area, in order to guarantee short recovery time and high overall availability protection in catastrophic scenarios.

In addition, there is an emergency plan/crisis plan/disaster recovery plan for the data center in place and

documented in backup and emergency plans. The functionality of these plans is verified on a regular basis (usually annually). Emergency plans are subjected to a regular verification and improvement process.

Data is backed up on a regular basis according to the service agreement.

4.9 Separation Control. The goal of separation control is to ensure that data collected for different purposes can be processed separately.

The following measures are implemented:

a) To the extent that there are no dedicated systems in use for exactly one Customer, the employed systems are multi-client capable.

b) Development, Software and Platform quality assurance systems are completely separated from operational systems in order to ensure productive operation. The only exchange that takes place is in the form of files that are needed for processing data (program files, parameter files, etc.).

c) Customer systems are only accessed through a secured network by authorized persons. Direct administrative transitions between Client servers are excluded, as is the ability to reach another Customer's environment from one Customer's network client.

5 Data location, servers and back-ups

5.1 The data and back-ups of these data that iotspot B.V. stores in relation to our Services is located on the servers that our service provider Amazon Web Services provides. Amazon Web Services' service fully complies with the General Data Protection Regulation.

Furthermore, all the Amazon Web Services adopted by iotspot are certified for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015. Please view the following link https://aws.amazon.com/compliance/iso-certified/ to view more about these certifications.

5.2 For our EU-based customers the servers of Amazon are located physically in Frankfurt and Dublin.

5.3 Data back-ups are made continuously - and redundantly retained on the same servers - to be able to restore any potential data-error of our Services. We retain these back-ups for a maximum period of 168 hours or so much shorter as we deem necessary.

6 Termination and data retention

6.1 Upon termination of the iotspot Services as confirmed in writing by iotspot B.V., iotspot will delete all data associated with privacy sensitive, personal data of Customer and User(s). Effectively, data records as defined in article 3 and 4 of our Privacy Statement are deleted from our databases 168 hours after the date of the confirmation of termination.

6.2 Usage or transactional data, such as but not limited to, number of reservations, occupation time slot, reservation time slot, Desk & Room scans, type of smart device, App versions, are retained by iotspot B.V. to improve our service, offer appropriate maintenance & support, research of workspace management and providing information about our Services to customers and prospective parties.

7 Amendment of this Information Security Statement

We reserve the right to modify or amend this Information Security Statement in accordance with applicable laws and regulations.

8 Information security

iotspot B.V. provides its Services based on information security management (ISM). This is based on statutory regulations as well as internally established regulations. The implemented security procedures are continuously reviewed. These guidelines are also binding for subcontractors.

May 1st, 2021