Security Policy

1. Preamble

The subject matter, scope, nature, and purpose of data processing shall result from the business relationship based on the sales & service agreement concluded between the parties and shall replace all previous agreements regarding this matter. These Security Measures shall supplement the sales-contract concluded between the Customer and Axess insofar as it relates to the processing of customer data and shall be deemed an integral part thereof. Axess guarantees the following IT security measures within the framework of the customer relationship between Axess and the Customer.

2. General technical and organizational measures

Axess will always take all measures necessary in accordance with the GDPR for the processing of the transferred data in the data processing systems. It ensures that the internal organization is designed to meet the requirements of data protection. The following terms apply regardless of where the server is hosted.

2.1 Intended use control:

It is guaranteed by the following measures that data collected for different purposes are processed separately:

> Software- based (e.g. Customer segregation)
> Segregation through access regulation (database principle)
> Segregation of test and current data
> Segregation of test and current systems (technology, programs)

2.2 Pseudonymization

Insofar as possible for the respective data processing the primary identification features of the personal data will be removed in the respective data application and stored separately.

2.3 Input control:

It is guaranteed that it can be subsequently checked and determined whether and by whom personal data are entered in, changed, or removed from data processing systems. Axess will document or record inputs/logfiles for this purpose.

2.4 Privacy by Design & Privacy by Default

Appropriate default settings as part of the technical and organizational measures ensure that, as a matter of principle, only personal data whose processing is necessary for the specified processing purpose is processed.

> Personal data will only be collected if they are necessary for the processing of the sales-contract (e.g. season tickets, etc.)
> The setting of cookies in Axess web-shops is only possible with the consent of the user
> The use of the personal data for marketing purposes is only permitted by the active consent of the user

3 Technical and organizational measures in case of server hosting by Axess

If the customer uses Axess DATA CENTER SERVICE, it is ensured that security areas and the circle of authorized persons or access authorizations are defined, access routes are secured appropriately, and data carriers are controlled and stored securely. The following measures apply only if the server is hosted by Axess.

3.1 Admission control:

Unauthorized persons are prohibited from gaining admission to data processing systems, with which data are processed or used. The computer rooms are located in an office building that is classified as earthquake-proof. Only IT, Facility and Management employees have access to the premises. Access control is ensured by the following measures:

> Authorization-/Chipcard

The presence in the security zone is recorded. Non-authorized personnel and persons who do not belong to the company (service technicians, consultants, cleaning staff, etc.) may only enter the rooms when accompanied by authorized persons. The admission control is supported by the following further organizational/technical measures:

> Alarm system
> Building surveillance
> Video technology

3.2 Entry control:

A use of the data processing systems by unauthorized persons is prevented by the following measures:

> Password

Each authorized person has an own password that is only known to him/her, which must be changed at regular intervals. Automatic protocols (Log files) are created regarding all activities on the data processing and telecommunication system. The use of data processing systems with the help of equipment for data transmission by unauthorized persons is prevented by the following measures:

> VPN (Virtual Private Network)

3.3 Access control:

It is guaranteed that the persons authorized to use a data processing system can exclusively access their data that are subject to access authorization and that data cannot be read, copied, changed, or removed without authorization during the processing, use as well as storage. The restriction to the access possibility of the authorized person exclusively to the data subject to his access authorization is guaranteed by the following measures:

> Automatic examination of the access authorization (in the system)

3.4 Transfer control:

It is guaranteed that personal data with the electronic transmission or during their transport or their storage on data carriers cannot be read, copied, changed, or removed without authorization and that it can be checked and determined, at which point a transfer of personal data is foreseen by data transfer devices. The shipment of data carriers is documented and controlled by registration and accompanying documents. It is not permitted to bring and use private data carriers into the rooms. Data carriers are destroyed in the following manner:

> Magnetic data carriers by write-over and physical destruction (external service provider)

Insofar as the internet is used to forward personal data the following security measures will be used:

> Firewall
> Virtual Private Network (VPN)

3.5 Availability control:

It is guaranteed by the following measures that personal data are protected against accidental destruction or loss:

> Daily/weekly/monthly/annual data backup
> Storage Area Network (SAN)
> Disk mirroring (RAID among others)
> Uninterruptible power supply (UPS)
> Overvoltage filter
> Emergency generator
> Outsourcing of data
> Fire prevention devices

3.6 Data protection management

It is ensured that a data protection management is set up and implemented. The data protection management is broken down into the following points:

> List of processing activities
> Contract data processing
> Data protection impact assessment
> Incident response management
> Report of breaches of data protection
> Training
> PDCA (Plan, Do, Check, Act): regular checks

3.7 Incident response management

Measures were taken concerning how the responsible persons should react to potential scenarios. These include data security breaches, DoS (Denial of Service), DDoS (Distributed Denial of Service), gaps in the firewall, outbreaks of viruses or malware and threats by insiders.
The incident response management is divided into six important phases:

> Preparation: Both the users as well as the IT employees are trained or informed that potential incidents happen, and which steps have to be initiated.
> Identification: Determination whether an event concerns a data protection incident.
> Containment: To limit the damages caused by the incident and isolate the affected systems to avoid further damages.
> Eradication: To find the cause or what triggered the incident off and to remove the affected systems from the productive environment.
> Recovery: To integrate affected systems into the productive environment again, after it has been ensured that no further threats exist.
> Gained knowledge: Completion of the incident documentation and analysis what the team or the company can learn from the incident. This way future responses can be improved under certain circumstances.

4 Access to Customer Data

In order to provide adequate support in case of problems, Axess, as data-processor, reserves the right to access the Customer system or data, provided that such access is covered by the sales-contract between the Axess and the Customer or the Customer has consented to such access, or the reseller has passed on the desired request of service to Axess on behalf of the customer. Axess guarantees that:

> any physical access to the hardware of the data center takes place only if the customer obtains the Data Center Service from Axess;
> Access to the Customer's data via the remote maintenance tool only in the case described above and with the consent of or on behalf of the Reseller and/or Customer;
> Access to the local devices is only granted in case of support upon request of the customer or the reseller.

5 Order processing:

Supplementary to the present business relationship, these provisions on commissioned processing ensure that all mutual obligations under the General Data Protection Regulation ("GDPR") are fulfilled.
Axess processes personal data on behalf of the Customer, whereby the subject, scope, type, categories of data processed, the purpose of the processing,

Security Policy

as well as the categories of data subjects (Customer Data) result from the respective sales contract concluded between the contracting parties. These provisions on commissioned processing therefore supplement all agreements concluded between the Customer and Axess insofar as they relate to the processing of personal data.

The data processing by Axess shall be carried out exclusively in a Member State of the European Union, whereby cross-border data processing pursuant to Article 4 line 23 GDPR (within the Union) must be notified to the Customer, as the responsible party, in due time prior to the commencement of the processing, so that the Customer can object. Silence to this notification means consent to the processing.

5.1 Obligations of the Processor:
By signing the purchase contract, the customer agrees to the technical and organizational measures set forth in this policy. By implementing this policy and complying with the customer's general and individual instructions regarding personal data (e.g. deletion of customer data, anonymization of data), Axess ensures a state-of-the-art level of protection of the contractual data applications, so that claims of any kind can only be made in the event of a breach.

Changes to the technical and organizational measures that ensure a consistent level of protection for the personal data processed or increase such level shall be deemed approved and shall be disclosed to the Customer upon request but need not be disclosed to the Customer by Axess.

Axess shall take the technical and organizational measures described above to enable the Customer to comply with the rights of data subjects under Chapter III of the GDPR (information, access, rectification, erasure, restriction, data portability, objection as well as automated decision-making in individual cases) within the statutory time limits.

5.2 Data processing
Axess undertakes to process personal data only within the framework of existing contracts and in accordance with the individual instructions of the customer. If Axess is obliged to hand over the data to third parties by law, Axess will inform the customer about the legal obligation to disclose the data. Any other transfer of data for purposes outside of the contractual relationship shall only take place on the instruction of the customer based on a written order.

Axess shall ensure that all persons entrusted with data processing are bound to confidentiality prior to commencement of their activities - with confidentiality remaining in force even after termination of their activities - or that they are subject to an appropriate legal obligation of confidentiality.

5.3 Duty to inform
Axess shall assist the Customer in complying with the obligations set out in Art 32 to 36 GDPR (security of processing, notifications of personal data breaches to the supervisory authority, notification of the person affected by a personal data breach, data protection impact assessment, prior consultation)

Upon request, Axess shall provide the Customer with all necessary information (e.g. existing certifications, technical and organizational measures, etc.) to demonstrate compliance with the obligations set forth in Article 28 of the GDPR (obligations of the Processor). Furthermore, Axess shall enable and contribute to audits - including inspections - carried out by Customer or another auditor appointed by Customer.

Axess shall inform Customer without undue delay in the event of a breach of the GDPR or if Axess believes that an instruction of Customer violates data protection provisions of the Union or the Member States.

5.4 Order control
It is ensured that personal data processed on behalf of the client are only processed in accordance with the client's instructions. Axess maintains contracts with external parties for the following types of commissioned data processing:
> Data processing by external parties
> Data media destruction / disposal by external parties
> Maintenance and remote maintenance by external parties
> Administration / remote administration by external parties

The processing of personal data on behalf of the client - only in accordance with the client's instructions - is guaranteed by the following measures.
> Written instructions
> Offer and order confirmation
> Pseudonymization

5.5 Sub-processors
Axess is authorized to use sub-processors for the processing of personal data. Intended changes with regard to the sub-processor shall be notified to the Customer in writing in sufficient time to enable the Customer to object to the change. Excluded from this rule are situations in which notification is not possible or feasible (especially in case of imminent danger). Axess concludes a written contract with the sub-processors and agrees with them, mutatis mutandis, the same obligations under data protection law as those presented in this chapter.
The following sub-processors are contracted by Axess:
> Designa Axess Industries Holding with its affiliated companies
> Axess AG with all affiliated companies
> Designa Verkehrsleittechnik GmbH with all affiliated companies
> Designa Digital Solutions GmbH
> Microsoft Corporation
> HubSpot, Inc.

In case of a purchase contract with an official reseller of Axess, Axess will only deliver data to the respective contractor (partner or reseller).

6 Handling of the contractual data at the end of the agreement
Upon termination of the underlying business relationships, Axess shall return all Personal Data to the Customer in a format customary for data processing or delete it, unless there is an obligation to store the Personal Data under Union or Member State law.

7 Final provisions
The Security Policy shall have the same duration as the duration of the business relationship between Axess and the Customer. The final provisions of the same shall apply correspondingly to the order processing agreement.