1 Technical and organisational measures

1. The technical and organisational measures set out in the appendix are binding.
2. The contractor shall contribute to preparing codes of procedure, and must supply the principal with the required details.
3. The contractor shall respect the principles of correct data handling. It shall ensure that the data protection measures agreed in the contract and prescribed by law are carried out.
4. The technical and organisational measures may be adjusted during the contract relationship to correspond with further technical and organisational developments. Important changes must be agreed in writing.
5. Insofar as the security measures agreed with the contractor are not sufficient for the principal's requirements, then the contractor must inform the principal of this without delay. The same applies for faults, for violations of data protection regulations or of the specifications agreed in assignment by the contractor or persons working for it and for suspected data breaches or irregularities in processing personal data.

2 Hornetsecurity GmbH's general technical and organisational measures

2.1 Physical entry control

Any unauthorised (physical) entry to the computer centre will be prevented. The technical and organisational measures for entry control, and in particular for identifying authorised individuals, are:

- Identity check using an official ID card; this is to be carried out by the personnel of the relevant computer centre in the control room before entry into the centre.
- Monitoring of the computer centre rooms via a video system (visual and infrared cameras).
- Entry is gained to the computer centre via two access controls:
    - Door intercoms to the control room with electronic door openers
    - Door locking system using a magnetic card.
- In addition, Hornetsecurity's rack/tower servers are furnished with their own lock system.
- Entry is logged by noting the access time, name and company, as well as the time that access was concluded.

2.2 Virtual entry control

Unauthorised persons shall be prevented from entering the data processing systems by Hornetsecurity.

- Password policy: minimum 8 characters, must meet at least 3 of 4 criteria (capital letter, lowercase, number, special character), password changed every six months
- One user master record per employee
- User rights restricted to areas of activity
- All systems are protected from unauthorised access with appropriate firewall systems, access to systems is restricted to precisely defined IP address ranges
- Hard disks in computer systems are always encrypted.

2.3 Access control

Unauthorised activities in data processing systems not included in access granted will not be allowed. The authorisation concept, access rights and their monitoring and reporting are all designed to be needs-based:

- Access privileges only granted for areas required for specific activities (role-based authorisation)
- Checks regarding unauthorised access attempts (IDS/IPS)
- Transaction logging for system changes of any kind
- 'Four-eye principle' applies for all software changes.

2.4 Data transmission control

The transmission of personal data (electronic communication, data transport, communication control) shall be regulated. The following measures apply for transport, transmission and forwarding or storage on data storage media (manually or electronically), as well as for subsequent inspections:

- External access to data shall be carried out using VPN only
- Offline work files (laptops, etc.) must be kept on encrypted disks.

2.5 Input control

Traceability and documentation shall be guaranteed for data management and maintenance. Any data modifications are logged by transaction. It is not possible to alter the log. This ensures that it can subsequently be established at any time if and by whom data was entered, altered or removed (deleted).

2.6. Assignment control

The task of processing data of the principal will be carried out by Hornetsecurity only and will not be passed on to third parties. Third parties will only be assigned basic services (computing centre services, internet connection, transport and installation of systems and data storage media).

2.7 Avaiability control

Data shall be protected against accidental deletion or loss. Data protection measures (physical & logical) are:

- Hornetsecurity shall employ at least two independent and geographically distant computer centres for data processing. Each of these computer centres shall have their own:
  - Redundant power supply
  - Redundant network service
  - Redundant climate control
  - Redundant extinguisher systems
- Data processing shall be guaranteed in full even using one single computer centre. The second and further computer centres are employed to increase redundancy.
- Data are always saved on mirrored storage media using appropriate RAID procedures.
- In addition, central data systems are duplicated via automated repetition and also equipped with hot failover functionality.
- Data are also regularly saved to a tape system so that past data can be restored.

2.8 Separation control

All data will be stored in dedicated databases, separated according to the brief. For internal purposes (e.g. development, testing and backup) separate systems with their own data structures will be used.