Rules of behavior for external personnel

1. General Provisions

The following conditions contain rules of behavior (duties and responsibilities) for persons who are not in an employment relationship to SIX; however, who within the scope of their job spend time in on the premises of SIX, and in particular who handle business information and data as well as computer equipment and documentation (referred to herein as "external personnel").

2. Rules of Behavior

External personnel are obligated to follow the SIX Directives and data sheets that have been brought to their attention as well as the guidelines of the individual business units. The following rules must be adhered to:

- The connecting of workstations, notebooks or other technical devices from third parties (customers, partners, suppliers, etc.) to network of SIX is prohibited. Exemptions are to be approved in advance by Corporate Security.
- The means of identification, authentication and working tools like userid, password, token, notebook etc. needed for accessing SIX systems and data are personal and may not be transferred to third parties or be made accessible to them or used for private purposes.
- External personnel are required to complete all mandatory trainings assigned by SIX within the defined timelines. These trainings help ensure a consistent understanding of key security, compliance, and risk requirements and contribute to the protection of SIX, its clients, and its employees. If mandatory trainings are not completed as required, SIX reserves the right to restrict or withdraw access, escalate the matter to the contracting company, or end the assignment.
- Each external person is responsible for the activities conducted on his/her account.
- All information and data are to be classified.
- Passwords (encryption key) are to be stored and sent separately from the encrypted data.
- Business data stored or transferred locally on computer equipment or mobile data carriers must be encrypted (except for internal data or data that has been classified as public).
- All information received and created within the scope of the assignment are to be regularly saved on the SIX systems (backup).
- Data carriers and data and programs imported from non-SIX sources must be inspected on an up to date virus scanner for viruses and trojans before being saved or transmitted to third parties.
- The information and information medium as well as data and data carriers for sound, text and images (e.g. notices on paper, sound recordings, film or print output) are to be returned once they are no longer needed or at the end of the assignment at the latest, or are to be destroyed or otherwise appropriately disposed of.
- The traceability of all activities (such as the processing of data and programs or the changing of configurations) must be ensured at all times.
- In case of the potential misuse, loss or theft of systems, components or SIX data, the assigned SIX contact person must be informed immediately
- Additional details on operating guidelines can be found in the following documents of internal law:
    - Compliance Directive 5: Secrecy within the Group
    - CRO Regulation C4: Handling and Protection of Information
    - Compliance Directive 1: Data Protection
    - CRO Regulation S2: Information Security
    - CRO Regulation S2 Annex 4: Information Management
    - CFO Regulation 13: Identity and Access Management
    - IT Standard: Password-Based Authentication

3. Certification by the External Person

The external person confirms with his/her signature that he/she has read, acknowledged and accepted these rules of behavior.

Place / Date: _____

Company: _____

Signature: _____

Name in block letters: _____

Contact for questions regarding the content: corporate-security@six-group.com