Annex 2 – Technical and Organisational Measures

1. Access control to premises and facilities

Technical and organisational measures to control access to premises and facilities, particularly to check authorization:

a) Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities
b) For the purposes of secure disposal or re-use, equipment containing storage media that may possibly contain personal data are treated as though it does
c) Mobile equipment has appropriate protections (password or pin protection, full storage encryption recommended)
d) Equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access

2. Access control to systems

Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:

a) An access control policy is established, documented and reviewed based on business and information security requirements
b) Users are provided with access to the network and network services that they have been specifically authorized to use
c) The allocation and use of privileged access rights is restricted and controlled
d) A formal user access provisioning process is implemented to assign or revoke access rights for all user types to all systems and services
e) The allocation of secret authentication information is controlled through a formal management process
f) Temporary passwords are given to users in a secure manner. The use of third parties or unprotected (clear text) electronic mail messages must be avoided
g) Password policy is known and implemented by every employee of Fix The Status Quo
h) Password management system ensures quality passwords (14 alpha-numeric characters)

i) The Local Administrator and other privileged accounts passwords never appear unscrambled on the network
j) Inactive session are shut down after a defined period of inactivity
k) Access to Information and application system functions by users and support personnel are restricted in accordance with the defined access control policy

3. Access control to data

Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:

a) An access control policy to customer's data is established, documented and reviewed based on business and information security requirements
b) Fix The Status Quo implemented a comprehensive encryption solution for data in transit (incl. Network)
c) Personal Data in Database has opt-in encryption
d) Operating Systems are hardened to enforce required security controls
e) Fix The Status Quo ensures that procedures are established which guarantee correctness, integrity and availability of Fix The Status Quo data throughout all stages of data processing
f) Media are disposed securely when no longer required, using formal procedures

4. Disclosure control

Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

a) Access to systems that keep or process customer's data is allowed via secured network connections
b) Logging facilities and log information is protected against tampering and unauthorized access

5. Input control

Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

a) Security related application events are logged on application level
b) The log policy regulates that the log entries shall not contain any sensitive information

6. Job control

Measures (technical/organizational) to segregate the responsibilities between Fix The Status Quo (as processor) and Customer (as data controller):

a) Unambiguous wording of the Data Processing Agreement between Fix The Status Quo and the Customer with clear specifications of Fix The Status Quo' and the Customer's obligations
b) Careful selection of Fix The Status Quo as processor by the Customer
c) Monitoring of the performance of the Data Processing Agreement on a regular basis by Fix The Status Quo and the Customer

7. Availability control

Measures to assure data security (physical/logical):

a) Fix The Status Quo developed a disaster recovery plan, which contains all the procedures and support Information required for business resumption
b) Fix The Status Quo' procedures are established which guarantee correctness, integrity and availability of Fix The Status Quo data throughout all stages of data processing
c) Access to backups is restricted to authorized personnel only
d) Backups are encrypted

8. Segregation control

Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

a) Usage of production un-anonymized data on development environment is not allowed.