Data Protection Policy

In order to safeguard TrustOn Security's physical and information assets, its staff members have to comply with the law. High standards must be maintained and enforced.

Responsibilities & Organisations

- Responsibility for ensuring compliance with the Code of Practice rests with the Managing Director of TrustOn Security
- All staff members must comply with the Code of Practice
- All other users must be instructed about the Code of Practice and the correct use of IT facilities
- All users leaving TrustOn Security must have their access to TrustOn Security's premises and information systems withdrawn immediately

Passwords

- TrustOn Security's computers shall have a password which must be unique, known only to authorised users and not written down except for safekeeping as described below
- Password(s) should be kept in sealed envelopes in a safe or locked draw. When someone leaves, all passwords should be revised
- The communication of a password to an unauthorised person is an act of misconduct. The unauthorised use of a password is an act of gross misconduct

System Access

- Under no condition may a departing authorised user delete or remove any files or discs from TrustOn Security
- System access and use shall be reviewed regularly to ensure compliance with the Code of Practice and to detect unauthorised use.

Security of Personnel & Physical Assets

- In order to ensure the security of TrustOn Security personnel and assets, access to TrustOn Security must be controlled at all times
- All major physical assets must be accounted for. All data must be controlled by the Managing Director of TrustOn Security
- Equipment may not be removed from the premises of TrustOn Security without permission from the Managing Director obtained in advance. Equipment belonging to TrustOn Security must not normally be used for any unofficial or private business

Safeguarding Files

- All documents containing sensitive personal or commercial details will be assumed to be "confidential" and must be registered, stored and used according to the principles set out in the Code of Practice

Disaster Recovery

- TrustOn Security must maintain a Disaster Recovery Plan to ensure that critical business processes can continue to function in the event of a disaster

Software Controls

- No-one is permitted to load unauthorised or "external" software or data onto a computer without the permission of the Managing Director

Misuse of IT Facilities

- TrustOn Security facilities may not usually be used for any purposes other than TrustOn Security business without the permission of the Managing Director
- Personal use should not be allowed, except under special circumstances. Any costs incurred to TrustOn Security should be reimbursed

Exchanges of Data

- Exchanges of data in any format between TrustOn Security and other organisations must be carried out on the basis of formal agreements

Reporting of Suspected Incidents

- All suspected violations or malfunctions of security must be reported to the Managing Director. The Managing Director must investigate these, consulting with any person or body, whom s/he feels is appropriate
- The Managing Director must then report the results of the investigation to the next management
- All cases of actual or suspected fraud, theft or corruption must be notified immediately to the Managing of TrustOn Security
- Everyone within TrustOn Security is encouraged to report suspected weaknesses

Compliance with the Code of Practice

- A member of staff who breaches the Code of Practice may be subject to disciplinary action under TrustOn Security's Disciplinary Procedure
- Authorised users who breach the Code of Practice will have their authority removed and may be subject to other action by TrustOn Security
- The adequacy and adherence to the Code of Practice must be reviewed yearly by the Management Committee of TrustOn Security

The Data Protection Act 1998

- All data must comply with the Data Protection Act 1998 and any other data protection legislation and principles
- TrustOn Security must register as a data user with the Data Protection Registrar

Review

- The first review should be within 12 months of the policy's implementation. Thereafter, TrustOn Security should assess whether staff members and others are in compliance with the policy on an annual basis