

Information Security Management System

The Viewpoint Organisation (TVO) maintains an information security management system (ISMS), a set of policies and procedures for systematically managing data. The goal is to minimize risk and ensure business continuity for TVO and customers by pro-actively limiting the impact of any security breach. This system is endorsed by TVO executive.

The Information Security Management System is summarised below.

The TVO Executive recognises that Information Security:

- supports the overall the aims and values of the organisation
- is an integral component of sound management of the organisation
- requires a comprehensive and integrated approach
- requires that responsibility and accountability are made explicit
- should be reassessed periodically

The priorities when establishing a good security system are always the Confidentiality, Integrity and Availability of the data. Non-Repudiation, not denying the validity of data, is also a key factor, assuring the integrity and origin of the data. TVO Security Policy is geared around the risk management of the asset the company is responsible for, that is the data held for the customer, which can have varying levels of sensitivity. Risk in this case is defined as the size of a threat multiplied by the vulnerability the Viewpoint System has to that threat,

Security needs are summarised in three separate sections:

- Personnel Security: human safeguards – people and procedures
- Information Security: data safeguards
- Physical Security: technical safeguards – hardware and software

and the Information Security Management System for TVO is drafted using this framework

Personnel Security

- All staff employed by TVO must be appropriately vetted (Working with Children Checks, Disclosure and Barring Service UK clearance)
- TVO maintains:
 - recruitment and selection procedures which must be followed when staff are recruited.
 - An Employee Handbook setting out employee responsibilities including responsibilities for the security of company assets and property, use of internet, email (including secure email use) and non-company software,

use of anti-virus software and regularity of scanning. The Handbook also states procedure to be followed when an employee leaves.

- TVO holds customer data of a sensitive nature and it is important to recognise personal responsibilities related to confidentiality
 - TVO employees will be made aware that confidential information will not at any time for any reason whatsoever be disclosed or permitted to be disclosed to any third party.
 - TVO will ensure that all its employees having access to any confidential information, documents or such matters enter into a suitable confidentiality agreement
 - TVO will ensure that all staff are aware of password management protocols and follow these.
 - TVO ensures that all staff understand that TVO maintains a role-based access method to customer databases and understand their own roles and customer responsibilities for role allocation.
 - TVO Helpdesk staff to follow policies and procedures for verifying contacts to the Helpdesk

Information Security

The TVO Executive recognises that TVO is storing and processing confidential information on behalf of customers,

- In entering into contracts with TVO, customer organisations consent to the storage and processing of confidential information by TVO, and that TVO employees shall have access to confidential information, documents and all other matters arising out of the service that belong to the Customer.

The TVO Executive affirm that:

- such confidential information will not at any time or for any reason whatsoever be disclosed or permitted to be disclosed to any third party except as permitted by the customer.
- information inputted on to Viewpoint Information System software by customer 'users' remains the property of the customer.
- copyright in questionnaires or other documents remains with the original copyright holder.
- TVO undertakes to comply with the provisions of Data Protection and Privacy legislation in so far as they are data processors or data controllers.
- TVO employees understand their responsibilities in respect of data security and confidentiality

- These obligations are incorporated in contracts with customers and survive the expiry or the termination of the contract for whatever reason.

In entering into a Contract the Customer agrees to establish and document a formal procedure for the use of the Viewpoint Information System, setting out the roles and responsibilities of staff in relation to the use of the Viewpoint Information System and level of authorisation (permissions) they have to access data stored by the Viewpoint Organisation in compliance with the Data Protection and Privacy legislation

The TVO Executive agrees that all access to the Viewpoint Information System is password protected:

- all passwords are encrypted
- the TVO Information System can provide complex passwords and customers decide on the level of complexity
- TVO employees only use complex passwords which are changed periodically
- Separate logging capabilities are provided for specified individuals to access the physical server, application and database.

The TVO supports the encryption of personally identifying information stored in customer databases.

The TVO Executive ensures that all data is backed up/replicated to a different physical location. The backup/replication is provided the same logical security as the production data. Systems are monitored for any sign of weakness or recurrence.

TVO provides 2 web interfaces: the first is Audio Computer Assisted Self-Interviewing and is provided over HTTPS; the second is the Management Centre for managing user access and for running reports, which is also provided of HTTPS.

- TVO internal procedures for the use of the web interfaces and for developments to the software are documented and stored securely
- All software is stored in a secure repository
- Development follows a documented procedure involving use of separate secure development environments and formal testing on test servers before release is planned

Physical Security

All data is stored securely online using Microsoft SQL Server, a relational database management system. In the UK, Europe and Canada the Microsoft Azure platform is used, and in Australia and New Zealand the Servers Australia platform is used. All

systems are fully managed and maintained environments, 24 x7 x 365 with fully managed firewalls for Internet Protocol Security. Data is stored on live servers and replicated to a spare or data recovery server. A Recovery Time Objective of up to 1 hour and a Recovery Point Objective of up to 15 minutes. All data centres are ISO 270001 certified. Data Processing Agreements are available to all customers ensuring that local data processing standards and requirements are complied with.

Access by designated Viewpoint staff to the Viewpoint software and database is obtained via a RDP session from a fixed IP address and VPN.

Physical security is reviewed regularly and enhancement as required is supported. Any security incidents are analysed, how it was handled, and steps for preventing a recurrence identified.