CLIENT DATA MANAGEMENT POLICY

Purpose

This Policy is designed to provide an overview for retrieval, archiving and destruction of client records held by Cognisco and to ensure that they are held in line with the relevant legislation and codes of practice. A separate policy is in place for non-client records.

Principles

Personal data for client's employees should be held in SharePoint in the client 'J Drive' location prior to being loaded into the client MyKNOW system.

Developers using local copies of data should ensure that the data has been processed and is anonymous.

Data Archiving

Clients may purchase data archiving services from Cognisco.

Data is retained within the boundaries of the United Kingdom.

Archived data is retained within a single archiving system.

Copies of data may be retained on other authorised Cognisco systems for the purpose of future operational use. All copies will be destroyed upon termination of the data archiving agreement.

Process for Archiving

To archive data the following steps are to be followed:

1. Mark data as ready for archiving and add to the change control notice.
2. Circulate the change control notice for review and sign-off.
3. Dump to archive medium. Verify the data as it is transferred, updating the disk record.
4. Read archived data and list it.
5. Place one copy in a fireproof safe or off site.
6. Remove the archived data from the disk.
7. Update the archive index.
8. Update the data retention schedule on the 'Data' calendar.

Data Destruction

Process for Destruction

It is the responsibility of the client Lead Consultant to issue a notice to destroy data. The notice will be created as an internal support request case on the corporate CRM

system. A copy of the notice will be sent to the manager of each department and the nominated sales person.

To destroy data the following steps are to be followed:

1. Draw up a list of data items for deletion.
2. Create an anonymous copy of the data for retention and used by Cognisco.
3. Mark data for destruction and add to the change control notice.
4. Circulate the change control notice for review and sign-off.
5. Execute data destruction technique (as per the Cognisco policy).
6. Attempt recovery by technical inspection and documented recovery techniques.
7. Verify destruction of data.
8. Record destruction event on the 'Data' calendar.
9. Issue data destruction notification to client. *(Letter templates below)*

Disposal of Equipment

The following table is not an exhaustive list of all possible media types, but instead offers a representative sample of the most common forms of media currently in use. These media types also demonstrate the characteristics that determine the appropriate deletion or destruction methods required to assure data is non-retrievable.

Media Type	**Data Storage Mechanism**	**Suggested Removal Methods**
Hard Disk Drives	Non-volatile magnetic	Pattern wiping, Incineration
CDROM/DVD-R	Write once optical	Abrasion, Incineration
CD-RW/DVD-RW	Write many optical	Abrasion, Incineration
Magnetic Tape	Non-volatile magnetic	Degaussing, Incineration
Flash Disk Drives	Solid state	Pattern wiping, Physical destruction
Paper Based	Locked cabinet	Shredding, Incineration

Removal of Data from Site and Remote Access

Client data will not be removed from site except in exceptional circumstances and only with the written permission of the Data Protection Officer and the client.
The Domain Administrators, as agreed by the Data Protection Officer, will be allowed remote access. The list of Domain Administrators will be reviewed every 3 months by the Data Protection Officer.
Remote working may be permitted in exceptional circumstances for other employees, but only after consultation with the client and written authorisation from the Data Protection Officer.
Please also see section 4.4 of the Sub-contractor Policy.

Anonymous Data

On occasions Cognisco may be permitted to retain a version of a client's assessment results which have been made anonymous. This means that no data can be identified as belonging to any specific individual/employee.

It must not be possible to identify the organisation or any individual by combining separate pieces of information held by Cognisco.

All references to identifiable data must be replaced with a ‘type’ or randomised name. For example, the client name should be changed to ‘UK International Bank 2’. A Job Title must be changed to remove specific references e.g. “Head of Retail Banking (HBSC)” would change to just “Director” or “Head of Department”.

The following information data should be subject to this process if the client has agreed in writing to the process:

- Organisation Name
- Project Name
- Programme Name
- Module Name
- Topic Name
- Question Stem/Response
- User Login Name, Password, First Name, Surname, Job Title
- Group Names
- Database Name
- Network Folder Name

Following the process to ensure all retained data is anonymous, and the destruction of all other data is completed an audit will be undertaken by a suitably trained member of staff.