

Connexion2

Data Protection, Handling and Security Policy

Document Issue:

Document title	Connexion2 Data Protection, Handling and Security Policy
Document reference	CP07A
Document retention location	C2\Policies\Security\ C2\ISO9001\Control Processes\
Document authors	Ann de Vere & Craig Swallow
Document owner	Managing Director (Craig Swallow)
Issued to	All Connexion2 staff (including temps) All Connexion2 Contractors All Connexion2 Subcontractors
Reason for issue	For information /action
Last reviewed	29/07/11
Review frequency	Annual (or earlier where changes to legislation and standards dictates)

Document Review and Revision:

Version	Date	Amended by	Approved by	Amendments
R2	29 th July 2011	CS	CS	

Contents

		Page
1	Introduction	4
2	Policy Statement	4
3	Scope	4
4	Policy	5
5	Responsibilities	5
6	Review and revision	7
Appendix A	Data Protection Act 1998 Data Protection Principles	8

1. Introduction

- 1.1. The data held by Connexion2 (the company), is fundamental to the continuing operation of the company's business. Furthermore, the company is obliged to comply with legislation and ensure protection of data in accordance with the Data Protection Act 1998 (the DPA).
- 1.2. The aim of this policy is to specify the way in which the company meets its legal obligations, based on the requirements of the DPA.

2. Policy Statement

- 2.1. This document defines the data protection, data handling and security policy for Connexion2 (the Company).
- 2.2. This policy applies to all data obtained, processed and stored by the Company, its employees and sub-contractors.
- 2.3. The objective of this policy is to ensure protection of data in accordance with the DPA; the key piece of legislation concerning security and confidentiality of personal data.
- 2.4. It is also the objective of this policy to support the Company's compliance to those relevant aspects of BS8484 relating to data security (specifically clauses 4.6 & 4.7).

3. Scope

- 3.1. This policy applies to all forms of data held by the company including (but not limited to):
 - All personal data processed and stored on both computer and manual records;
 - Staff and personnel data; and
 - Business, commercial and operational data.
- 3.2. This policy applies to all aspects of data handling including (but not limited to):
 - Databases and record systems (both paper based and electronic);
 - Data recording systems (paper, electronic and audio);
 - Data transmission systems (including portable media, email, fax, post and telephone);
and
 - Data storage and portability.
- 3.3. This policy covers all data/information systems developed, purchased and/or managed by or on behalf of the company.

3.4. This policy must be observed by any individual directly employed, or otherwise, handling data on behalf of the Company. All General Security Procedures that staff should abide by are detailed in BP13.2

4. Policy

4.1. It is necessary for the Company to obtain, handle, process, retain and delete data to conduct its day to day business in respect of (not an exhaustive list):

- Personnel;
- Connexion2 clients;
- SoloProtect solution users; and
- Contractors and sub-contractors.

4.2. Data may be retained in either computer or manual (paper based) record form. The Company will comply with the principles of the DPA with regard to such data. All Connexion2 client related data (i.e. user data) is to be held on servers hosted either by one of its Alarm Receiving Partners (ARC) or in an ISO27001 data centre. The Company will ensure that the data centre provider is audited annually against ISO27001 and a copy of its current certificate is kept on file. The Company will ensure that its ARC partners are audited annually against BS5979 Cat II and BS8484 and that copies of current certification is kept on file.

4.3. All staff (full time and part time) employed by Connexion2 will be subject to security checks as required by BS7858 and will be required to pass these with no material observations.

4.4. The Company will observe good practice and procedure with regard to security of portable data media and data transmission.

5. Responsibilities

The Executive Board

5.1. The Company's Executive Board members allow staff, contractors and sub-contractors to use computer and manual records only in connection with their work for the Company, and have legal responsibility for compliance with the DPA.

5.2. Data Protection compliance is the delegated responsibility of the Company's Managing Director, who will assume the role of the Data Protection Officer and retain responsibility for wider data and IT security.

The Data Protection Officer

5.3. The Data Protection Officer will (not an exhaustive list) ensure that:

- The Data Protection and Security policy is reviewed annually and kept up to date;
- Appropriate procedures and practices are developed and communicated to the Company and its personnel (be they directly employed or otherwise), in respect of Data Protection, and data security with regard to storage and transmission, and obtain their commitment to adopt such by signed agreement;
- Staff who regularly use and process data are aware of data security and protection principles;
- Staff receive appropriate training to use systems correctly and promote a pro-security culture throughout the Company;
- A wider IT security policy is developed, maintained and communicated to staff to minimise IT security risks, covering both external and internal threats;
- Act as a point of contact to escalate any Data Protection or security issues to and to provide advice and guidance concerning data protection and security; and
- Will ensure an incident reporting system is developed, maintained and adopted by the Company and its employees to make certain that any potential or actual data loss or security breaches are notified as soon as they are identified and that appropriate action plans are in place and followed to deal with such instances.

Managers

5.4. Company Managers will:

- Ensure their staff are aware of their Data Protection responsibilities;
- Ensure their staff have had appropriate Data Protection and systems training;
- Ensure staff are aware of how to securely store and transmit data to minimise risk of data loss; and
- Promote the Company's pro-security culture.

Company Staff

5.5. All Company staff (directly employed or otherwise) are responsible for:

- Complying with the DPA and this policy;
- Informing the Data Protection Officer of any new use of personal data as soon as possible following its identification;

- Reporting any suspected or known Data Protection or security breaches or loss of data to the Data Protection Officer as soon as this is identified;
- Ensuring they keep themselves abreast with and adhering to the Company's policies and procedures with respect to Data Protection and Security, data storage and transmission; and
- Adopting the Company's pro-security culture.

6. Review and Revision

- 6.1. This policy will be reviewed annually under the authority of the Company Executive Board members.
- 6.2. Associated Data Protection standards will be the subject of continuous development and review.

Appendix A

Data Protection Act 1998

The data protection principles

The Data Protection Act 1998 governs the use of personal information through the eight data protection principles.

These principles require that personal information is:

1. processed fairly and lawfully
2. processed for one or more specified and lawful purposes, and not further processed in any way that is incompatible with the original purpose
3. adequate, relevant and not excessive
4. accurate and, where necessary, kept up to date
5. kept for no longer than is necessary for the purpose for which it is being used
6. processed in line with the rights of individuals
7. kept secure with appropriate technical and organisational measures taken to protect the information
8. not transferred outside the European Economic Area (the European Union member states plus Norway, Iceland and Liechtenstein) unless there is adequate protection for the personal information being transferred