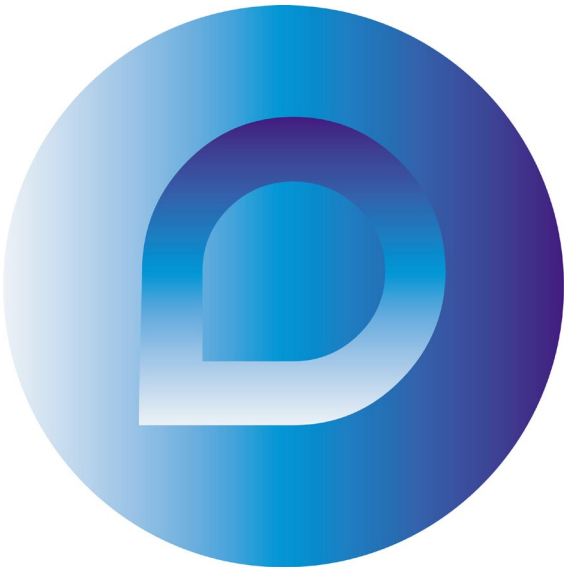
Baseline Data Compliance



Reviewed: April 2022

Reviewed:	07/04/2022
Expiry Date:	06/04/2023
Next Review:	April 2023
Appraised:	28/05/2019
Next Appraisal:	April 2023

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

Baseline Data Compliance

As a company By Design Group have adopted the following 6-point Baseline Data Compliance Standard.

1. Build and Maintain a Secure Data Network

a) Install and maintain suitable firewall and anti-virus configurations and systems to protect all By Design Group data.

b) Ensure passwords are not defaults and are change on a regular (6 monthly) basis

c) Employ IT professionals to advise, implement and manage all IT systems.

2. Protect Data

a) Protect all confidential physical and electronic data, examples of this would include personal information, personal bank details, employment records, employment contracts, company databases, etc

b) Encrypt the transfer of confidential / sensitive data across open public networks as required.

3. Implement and Maintain Security Programs

a) Use and regularly update anti-virus programs and software

b) Respond to security threats / viruses etc immediately

c) Monitor, develop, and maintain secure systems and applications

4. Implement Strong Access Control Measures

a) Restricted data (employment records, personal data etc) is limited to access on a strict 'need to know basis', authorized and recorded by the Office Manager or Managing Director.

b) Every person accessing the computer system has a unique ID and password which is monitored.

c) Electronic restricted data is stored on a secure partition of the company server with specific password access. This password is limited to the Office Manager and Managing Director and any additional access to specific data is recorded by the Office Manager.

d) Physical restricted data is locked in a secure location with keys held by the Office Manager and Managing Director. Access is again controlled and recorded by the Office Manager.

5. Regularly Monitor and Test Networks

a) Track and monitor all access to networks resources – this is undertaken on an on-going basis by our IT services provider.

b) Regularly test security systems and processes – this is undertaken on a routine monthly basis via our IT services provider

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

6. Maintain a Data Protection Policy

a) Please see the By Design Group Data Protection Policy.

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk