Data Protection Policy

The objective of this Data Protection Policy is to safeguard the confidentiality, integrity and availability of all forms of information within GBS Corporate Training, hereafter known as GBS. Client information must be kept secure and it is **essential that we have adequate safeguards to ensure that it is not lost or compromised**. The Data Protection Policy covers the unauthorised disclosure of information.

The purpose of this Policy is to protect personal and corporate information from all threats, whether internal or external, deliberate or accidental. This Policy correctly applied and adhered to will achieve a comprehensive and consistent approach, ensure business continuity, and minimise both the likelihood of occurrence and the impact of any actual security incidents and breaches.

It is the policy of GBS to ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information required through regulatory and legislative requirements will be assured.
- Integrity of information will be maintained
- Information will be available to authorised personnel as and when required
- Regulatory and legislative requirements will be met
- Business Continuity Plans will be produced, maintained and tested
- All breaches of information security, actual or suspected, will be reported and investigated

A comprehensive framework is in place to support this policy. It will be upgraded regularly as required. All people involved in the handling of information in GBS have a legal duty of confidence towards clients, reinforced through their contract of employment (or equivalent formal relationships) with GBS. A breach of client confidentiality resulting from a breach of agreed procedures has always been, and will remain, a serious disciplinary matter.

Introduction

GBS has a legal duty to protect the data that are held on clients and staff. There is also a regulatory requirement to protect all GBS data. In order to meet this requirement, the policy document sets out the principles for handling information collected, processed and stored on and transferred between computers and related equipment in use in the company. It also covers the management control arrangements designed to assure that these principles work in practice.

The objective is to ensure the confidentiality, integrity and availability of information, and accountability for users, whilst minimising the risk of loss through the implementation of such standards, controls and procedures as underpinned in this policy.

Our policy covers all staff and associates. Whilst we are not generally party to any classified information from our clients, we operate a password-protected computer system in which sensitive issues are further protected with access by authorised staff only.

Scope

Information is defined as manually held records, electronic data, microfiche; information can be recorded or input; transported or transmitted; or stored as manual or computer data, on paper, magnetic media or as computer print-outs. Information can also held on video or audio tapes.

In addition, the secure storage and use of any person-identifiable records is included within the scope of this policy.

This policy applies to GBS employees and all others who directly or indirectly use or support GBS information or computing services.

The document is subject to change to ensure it includes policy statements to cover any new service offering and to ensure it remains compliant with any amendments to applicable laws and regulations as the exigencies of security requirements demand them.

Statement of data protection policy principles

GBS actively focuses on the following:

- developing a security culture through training and awareness events and by providing awareness education and training materials
- adhering to UK and European policy, standards and best practice guidelines for security and data protection in GBS

This framework addresses four fundamental security principles - authority, accountability, assurance and awareness.

- Authority - to act
- Accountability - for actions
- Assurance - that required actions are being taken
- Awareness - by individuals, of the actions required of them

Its objectives are to ensure that

- all Information Technology (IT) systems used in GBS are properly assessed to ensure that corporate procedures, responsibilities and IT security objectives, in particular the legal requirements, are fully met
- appropriate levels of security are in place to maintain the confidentiality, integrity and availability of information and information systems; and
- all employees are aware of the limits of their authority and the levels of their accountability for their actions

Authority – to act

- All actions by IT systems or individuals using IT systems must conform to this policy, to comply with legal requirements
- GBS, its separate bodies and agencies, must maintain an organised security infrastructure through which IT security matters can be discussed, approved and monitored
- Only correctly authorised people may access IT systems: Access will be restricted to information required for the authorised person's job function on a need-to-know basis
- Updating and other activities, which could affect the integrity of information, will be restricted to authorised and authenticated persons needing to do so as part of their job functions
- Controls and restrictions will be imposed to ensure that access to IT systems is restricted to such authorised and authenticated persons at designated terminals, workstation, laptops or any hand-held IT device (memory stick, smartphone, etc.)
- Access to GBS systems from external networks or via dial-up communication lines must be treated as extremely vulnerable and be subject to an additional layer or additional layers of security
- Access will be restricted to information required for the authorised person's job function, and to processes which enable the authorised person to perform that function optimally
- All IT equipment and media are protected from physical loss or damage, whether caused by accidental or malicious means
- All personnel are given appropriate and proportionate authority, defined within job descriptions, for their use of GBS systems

Accountability - for actions

- Staff who authorise the development, purchase or procurement of GBS IT systems will be responsible for ensuring that the specification conforms with the purpose or purposes for which the systems are required
- Developers of IT systems will be responsible for ensuring that systems produce results as specified, are fully compliant, and provide adequate means of security
- Operators of IT systems will be responsible for ensuring that they are suitably protected from security risks
- Where an IT system may be accessed by more than one user, each user of such shared IT systems will have a unique and verifiable identity
- Interaction with external shared systems will be recorded and monitored
- Compliance with the terms and conditions expressed in the GBS Information Security Policy will be enforced through GBS conduct and disciplinary procedures for staff, or through contractual arrangements for external contractors or service providers

Assurance - that required actions are being taken

- GBS will apply appropriate security in accordance with this policy to all its systems on the basis of perceived system risks, business criticality and management priority.

This will enable the development and maintenance of procedures and best practice guidelines for staff

- Contingency and recovery procedures ensuring an acceptable level of service and control will be considered for all IT systems and an appropriate contingency plan will be prepared where it is required. All contingency plans will be maintained and tested regularly as part of an ongoing IT Security management programme
- All breaches of IT Security and other security incidents will be recorded and investigated and reported initially to the Managing Director

Awareness - by individuals, of the actions required of them

- All GBS staff with access to IT systems will be kept aware of this Data Proection Policy and of relevant standards and procedures
- All staff required to use IT systems will be adequately trained in their security-related roles and responsibilities and in the correct use of those systems
- All staff must sign a copy of the GBS Confidentiality Statement
- All third-party contractors, agents or others who need access to GBS IT systems will be made aware of these requirements