Data Access Control Policy

Purpose

This policy establishes BELBIN's Access Control Policy, for managing risks to data security from user account management, access enforcement and monitoring, separation of duties, and remote access. This policy is designed to help BELBIN implement security best practices with regard to logical security, account management, and remote access.

Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by BELBIN. All users (BELBIN employees, contractors or others) of IT resources are responsible for adhering to this policy. For the purpose of this policy, "Data" refers to personal data (including, but not limited to: name, e-mail address, telephone number, address etc.) which is handled or otherwise processed by BELBIN's employees, agents and sub-contractors in the performance of their responsibilities.

Intent

The BELBIN Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish an access control capability throughout BELBIN to help the organization implement security best practices with regard to logical security, account management, and remote access.

Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk. Non-compliance with this policy could result in disciplinary action for employees, and contractual breaches in the case of third party suppliers, since it may have a significant effect on the efficient operation of the company and result in breach of data protection law, causing significant financial loss and an inability to provide necessary services to our customers**.**

Policy

BELBIN employees and contractors are permitted to access Data for the purposes of:

a) Providing information and services to customers when requested;
b) Providing customer support for technical or other issues;
c) Developing and maintaining BELBIN systems;
d) Conducting research on BELBIN-related topics and issues;
e) Sending marketing or other communications to customers, where explicit customer consent has been obtained.

Points (d) and (e) are subject to specific rules and permutations and may only be undertaken with the prior agreement of a Partner.

Data Access Control Policy

Access to data is restricted according to job function. BELBIN employees may not:

a) disclose Data to any third party unless requested by the customer or instructed by BELBIN;
b) access Data unnecessarily and without good reason;
c) transfer or disclose any Data outside the UK or European Economic Area without specific consent from the customer or BELBIN.

If an employee discovers any breach of data protection policy, or if data is corrupted, damaged or deleted, they must inform their line manager as a matter of urgency and in accordance with the Data Breach and Loss Policy.

Office computers

All computers must be protected with a secure password which meets pre-defined validation standards. Users will be prompted to change their password every 42 days.
Computers must be locked before being left unattended and will lock automatically after 15 minutes of inactivity.

Data may be saved to BELBIN's shared network drive, but must be deleted immediately after use.

Office computers are not to be removed from BELBIN's offices other than for specific, pre-approved business-related events.

Passwords

Passwords are the first line of defence for BELBIN's IT systems and, together with the user ID, help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

Weak and strong passwords

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.
A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

BELBIN employees and contractors must use strong passwords with a minimum standard of:

- At least seven characters;
- Contain a mix of alpha and numeric, with at least one digit;
- More complex than a single word (such passwords are easier for hackers to crack).

Data Access Control Policy

Handling payment
BELBIN employees may be required to receive and process credit card and/or bank account details for customers when processing invoice payments, credit notes or other transactions.

Data should be written on loose paper, processed and immediately destroyed after use (using secure confidential waste bins only), or redacted on documents which must be kept by BELBIN for accounting purposes. It may not be stored on computer or in any other form.

BELBIN employees are not permitted to solicit credit card details via e-mail or any other online method.

Mobile telephones
Data is not to be saved on personal mobile telephones. Exceptions are made for training courses and workshops, where explicit permission is obtained.

BELBIN e-mails may be accessed from personal mobile telephones on the following conditions:

- The phone is locked with a passcode/secure password;
- Mail may be accessed by the phone's browser but not via the mail app;
- The password for the mail website may not be saved in the phone's browser;
- The user signs out immediately after accessing mail.

Memory storage devices
USB keys must be signed in and out using the designated form.

Only password-protected USB keys may be used to store Data, if specific agreement has been obtained from the customer. Data must be removed from USB keys once it is no longer needed.

Remote access
Remote access is granted to certain authorized BELBIN employees.

Authorized employees must ensure that:

- Secure passwords and access codes are used;
- Non-BELBIN employees are not permitted to view data;
- They log off promptly from all systems after each session.

Attending events
BELBIN office computers and/or USB keys may be required for specific BELBIN-related events, such as conferences or training. The minimum number of computers required may be taken. Computers must be checked by a Data Protection officer prior to the event.

Use of third party software
No Data may be held on third-party software, such as Google Documents, Dropbox or similar.

Data Access Control Policy

Couriers

Data may be passed to our couriers to facilitate delivery of products and materials for training courses and other events. Data must be deleted from courier websites once the delivery has taken place.