DATA QUALITY & SECURITY POLICY

OVERVIEW

blu-3 Holdings and all subsidiary companies (blu-3) holds information on its staff, commercially confidential information about Its business, and Information entrusted to it by clients and suppliers. blu-3 understands the Importance of holding accurate Information and protecting It from misuse and malicious access.

It is therefore blu-3's policy to apply the eight principles of data protection to all Information that Is of Importance to the business.

PURPOSE

1. Processing data fairly and lawfully

blu-3 will not allow information it holds to be used to cause damage to individuals or organisations, nor to be used to further illegal or criminal acts. Particular care is taken with information that is held legitimately but could be damaging if publicised (e.g., accident reports, non-conformance reports).

2. Processing data for specified purposes

Data that is suitable for the purpose for which it was collected may be damagingly misleading for a different use. The origin and method of collection of data will be checked to make sure it is valid for any new purposes proposed.

3. Data shall be adequate, relevant and not excessive

Storing unnecessary or irrelevant data costs the company both in storage and processing. Information is only collected for clearly defined needs.

4. Data shall be accurate and kept up to date

Inaccurate data can result in bad decisions that damage individuals, clients and the business. All blu-3 information is subject to periodic review and update.

5. Data shall not be kept longer than is necessary

Keeping information that is no longer needed costs the company in storage and processing and can cause confusion with more recent information. All data is culled or archived as soon as possible.

6. Data Is not sent to anywhere that will not provide protection.

blu-3 uses a cloud provider with data centres in known UK locations. blu-3 does not store information outside the EU.

7. Adequate security to prevent unlawful access or loss

7.1 Sensitive personal data is either stored within blu-3's document management system (SharePoint) using file encryption and granular user access permissions or paper records are stored in secure, lockable filing cabinets.

7.2 For personal data, blu-3 computer security offers high quality protection against viruses and malware, hard drives are encrypted, and computer and mobile devices are enrolled to Mobile Device Management (MDM) allowing remote wipe if necessary.

7.3 Access to databases and folders is controlled and recorded by the blu-3 IT Support Dept. Subject to the company Authorisation Matrix.

7.4 Loss or corruption of information could damage the company and our clients, but unauthorised access is not a high risk.

Bring Your Own Device (BYOD): blu-3 is positive about staff trialling improved methods of data collection from sites and a number of personal tablets, phones and specialist sub-contractor notebooks are used. However, private devices do not have access to personal data and may not be used to collect it.

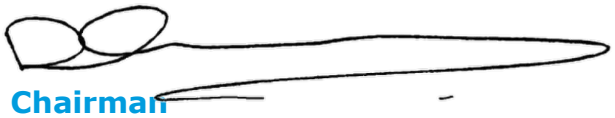
DEFINITIONS

Not applicable

PROCEDURE/PROCESSES

Supporting procedures/processes are available on SharePoint; contained within the Procedure & Process section of the IMS.

Danny Chaney



Chairman