Policy on
Information Security and Data Privacy

Review date	11/06/2019
Revision number	10.0
Document reference	10-017

Document purpose and scope

This document sets out the Information Security and Data Privacy Policy of JBA Group Limited and its subsidiary operating companies, collectively known as 'JBA'. It covers activities undertaken by the Group throughout all office locations and operations worldwide.

This document will be reviewed for continued suitability, will be communicated within the JBA Group and, if appropriate, made available to interested parties. The review interval for this document is 2 years.

Policy statement

JBA is committed to ensuring compliance with the highest legal and ethical standards. This must be reflected in every aspect of the way we operate.

We are committed to maintaining and continually improving an Information Security Management System (ISMS) that satisfies applicable requirements and is certified to the international standard ISO 27001:2013.

We will conduct our operations in accordance with the demands of our ISMS and will comply with all legislation, standards, statutory and other obligations and best practices which are relevant to our activities and the jurisdictions in which we operate. We will seek to comply with client policies where required and reasonably possible to do so without conflicting with our own policies or other obligations.

Aim

This policy aims to prevent and minimise the impact of security incidents and business disruptions to help us provide a service that meets or exceeds the expectations of our clients, comply with our legal obligations, maintain our high ethical standards, and protect our reputation. We manage and control our information security risks to protect and preserve the confidentiality, integrity and availability of information. There are distinct commercial benefits to us acting with transparency and integrity, including in regard to how we protect personal data. These include improved chances of JBA being selected as a supplier, in both public and private sectors, and maintaining our valuable reputation.

We recognise that personal data belongs to the individual data subject, not to JBA, and that our misuse or failure to protect personal data which we collect, store, use or share may result in an adverse effect on the rights and freedoms of data subjects. It would also expose JBA (and its employees) to a series of operational and legal risks (including investigations by regulators and substantial fines), adverse publicity and serious reputational damage.

Responsibilities

The JBA Group Board is responsible for reviewing and approving the content and implementation of this policy and will assist each operating company by refreshing and reinforcing this policy via application, guidance and monitoring where appropriate.

Operating Company Directors are responsible for taking measures to help their staff act in compliance with this policy. Overall compliance with the requirements of this policy is the responsibility of each operating company within the Group. The Managing Director of each operating company will ensure their company's adherence to this policy.

Line managers are required to check that their staff are aware of this policy and any associated guidance.

All staff are required to comply with the policy requirements and share responsibility for our performance in implementing it. Employees are required to read and understand all aspects of this policy and the associated *Guide to Data Privacy*, and to adhere to them. Staff need to be sure they know how to raise a concern and how to seek further guidance.

JBA Group and Operating Company Board Directors, all staff members, clients, contractors and third parties are expected to take responsibility for the security of organisational information.

Implementation

We take care to look after personal data in a responsible manner and in accordance with legal and best practice guidance by following six principles:

- Top management commitment
- Privacy by design and default
- Proportionate processes and procedures
- Risk assessments (including, where relevant, data privacy impact assessments and legitimate interest assessments)
- Communication and training
- Monitoring and review.

We maintain our ISMS within a process based Integrated Management System (IMS) that also controls and documents our quality, environmental and health and safety management processes. Our IMS is a documented system that enables us to consistently meet client and other applicable statutory and regulatory requirements. All IMS policies, procedures and documents are accessible by all staff via our intranet.

We provide adequate and appropriate resources, including people, infrastructure and working environments, to establish, implement, maintain and improve the IMS. We assess the continuing suitability, adequacy and effectiveness of our IMS via regular management reviews, conduct internal audits of our IMS to ensure consistent conformity to requirements and disseminate lessons learned across the Group.

The JBA Group Board, in consultation with our Operating Company Boards, sets IMS objectives aligned to our business strategy. We monitor, measure and disseminate our performance against these objectives.

Strategic risks and opportunities associated with internal and external issues that may affect the ability of the IMS to achieve its intended outcomes are addressed in our Risks and Opportunities Register. We maintain an operational Risk Assessment and Risk Treatment Plan for our information assets.

Additional policies and procedures exist to support our Information Security Policy. These are documented and available in our IMS.

Approval

This document was adopted by the Board of JBA Group Limited on 11/06/2019.

Executive Chairman

JBA Group