Policy on
Information Security

Review date	29/05/2018
Revision number	9.0
Document reference	10-017

Document purpose and scope

This document sets out the Information Security 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 1 year.

Policy statement

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, client policies and best practice, where required, reasonably possible and relevant to our activities and the jurisdictions in which we operate.

Aim

This policy aims to prevent and minimise the impact of security incidents and business disruptions in order to ensure we provide a service that meets or exceeds the expectations of our clients. We manage and control our information security risks to protect and preserve the confidentiality, integrity and availability of information.

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 and the Heads of Group Support Team 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.

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 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 with defined processes and procedures that enable us to provide services that consistently meet client and other applicable statutory and regulatory requirements. All IMS policies, procedures and documents are accessible by all staff via our intranet.

The JBA Group Board, in consultation with the Operating Company Boards, sets IMS objectives aligned to our business strategy. We monitor and measure our performance throughout the year and cascade the results throughout the Group and, where appropriate, make available to interested parties.

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.

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. Our operational risk assessment process is documented in *16-020 Risk Assessment and Risk Treatment Plan*.

We conduct internal audits of our IMS in accordance with our planned audit schedule to ensure consistent conformity to requirements. Lessons learned are disseminated across the Group.

We take care to look after personal data in a responsible manner and in accordance with our Data Privacy Policy and General Data Protection Regulation (GDPR) guidance.

Use of employees' own devices

Employees are allowed to use their own devices to connect to the JBA network, but all staff are expected to

- comply with *10-016 JBA Policy on Communications*;
- have suitable anti-virus software installed, up-to-date and running;
- keep the operating system of their devices up-to-date;
- not store any JBA information locally on their device (other than emails stored in the email app);
- restrict access to JBA information from non-JBA employees (e.g. family members); and
- report any loss of equipment used to connect to JBA IT services to the IT Team.

Failure to comply with the above may result in disciplinary action in line with the Employee Handbook.

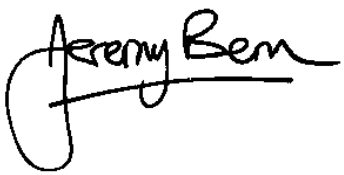
Further details

Policies relating to specific areas of our ISMS are recorded in the following documents:

- *06-045 Guide to Mobile Devices and Teleworking*
- *19-023 Statement on System and Application Access Control*
- *19-028 Statement on Cryptographic Controls and Key Management*
- *19-010 Statement on Equipment*
- *19-015 Statement on Backup*
- *19-013 Statement on Development and Support Processes*
- *19-043 Statement on Information Security in Supplier Relationships*

Approval

This document was adopted by the Board of JBA Group Limited on 29/05/2018.



Executive Chairman

JBA Group