Boomerang Information Security Policy

Boomerang, located at 11 St. Chad's Street, London, WC1H 8BG, operates primarily in the business of delivering digital messaging solutions. We are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information and assets, to meet the purpose and goals of the organisation.

The Operations Director is our designated Security Officer and is responsible for ensuring that Information and information security requirements will continue to be aligned with the organisation's business goals. This will take into account the internal and external issues affecting the organisation, and the needs and requirements of our interested parties. The objectives of our **Information Security Management System** (ISMS) are outlined and measured in accordance with the requirements of the ISO27001 standard.

Our ISMS is intended as a mechanism for managing information security related risks and improving the organisation to help deliver its overall purpose and goals. This includes a comprehensive approach to identifying, assessing, evaluating and controlling information related risks, through the establishment and maintenance of an ISMS.

The approach taken towards risk assessment and management, the Statement of Applicability and the wider requirements set out for meeting ISO 27001, identify how information security and related risks are addressed.

The ISMS Board is responsible for the overall management and maintenance of the risk treatment plan, with specific risk management activity tasked to the appropriate owner within the organisation. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks, for example during special projects that are completed within the context.

Control objectives for each of these areas are supported by specific documented policies and procedures, align with the comprehensive controls listed in Annex A of the ISO 27001 standard.

All employees and relevant Interested Parties associated to the ISMS have to comply with this policy. Appropriate training and materials to support it are available for those in scope of the ISMS and communication forums (such as our ISMS communications group), are available to ensure engagement on an ongoing basis.

The ISMS is subject to review and improvement by the ISMS Board. This Board is chaired by the Senior Information Risk Owner (SIRO) and has ongoing senior representation from appropriate parts of the organisation. Other executives / specialists needed to support the ISMS framework, and to periodically review the security policy and broader ISMS, are invited in the Board meetings and complete relevant work as required, all of which is documented in accordance with the standard.

We are committed to achieving and maintaining certification of its ISMS to ISO27001 along with other relevant accreditations that our organisation has sought certification against.

This policy will be reviewed regularly to respond to any changes in the business, its risk assessment or risk treatment plan, and at least annually. In this policy and the related set of policies that incorporate our ISMS, 'information security' is defined as:

Preserving

This means that all relevant Interested Parties have, and will be made aware of, their responsibilities which are defined in their job descriptions or contracts to act in accordance with the requirements of the ISMS. The consequences of not doing so are described in the Code of Conduct. All relevant Interested Parties will receive information security awareness training and more specialised resources will receive appropriately specialised information security training.

Availability

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The environment must be resilient and the organisation must be able to detect and respond rapidly to incidents or events that threaten the continued availability of assets, systems and information.

Confidentiality

This involves ensuring that information is only accessible to those authorised to access it and preventing both deliberate and accidental unauthorised access to the organisation's and relevant Interested Parties information, proprietary knowledge, assets and other systems in scope.

Integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data.

Of information and other relevant assets

The information can include digital information, printed or written on paper, transmitted by any means, or spoken in conversation, as well as information stored electronically. Assets include all information based processing devices owned by the organisation or those of relevant Interested Parties (including BYOD) in scope, that are processing organisation related information.

Of our organisation

The organisation and relevant Interested Parties that are part of our scope, have signed up to our security policy and accepted our ISMS.

The ISMS is the Information Security Management System, of which this policy, and other supporting and related policies which have been developed in accordance with the specification contained in ISO27001 and other relevant accreditation standards we have chosen to certify against.

A **security breach** is any weakness, event, or incident that causes, or may cause, a breakdown in the confidentiality, integrity or availability of the ISMS and the information or assets it seeks to protect and improve.

Signed: Peter Tanner - CEO

Date: 1st September 2019