ISMS DOC 5.1 – Information Security Policy

The Board of Directors and management of Taboola, located at Atrium Tower, 2 Jabotinsky St., 32nd fl., Ramat Gan 5250501, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Taboola's goals and the **I**nformation **S**ecurity **M**anagement **S**ystem (aka **ISMS**) is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

Taboola's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment and Risk Treatment Plan identify how information-related risks are controlled. The Information Security Manager is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Manual and are supported by specific documented policies and procedures.

All Employees of Taboola are expected to comply with this policy and with the ISMS that implements this policy. Employees, and certain external parties, will receive appropriate training. The consequences of breaching the information security policy are set out in Taboola's HR policy and, where applicable, in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

Taboola has established a top level management Information Security Committee, chaired by Chief Technology Officer (CTO) and including the VP IT and other executives to support the ISMS framework and to periodically review the security policy.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, ‘information security’ is defined as:

Preserving

This means that management, full time or part time Employees, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in Section 16 of the Manual) and to act in accordance with the requirements of the ISMS. Employees will receive information security awareness training and more specialised Employees will receive appropriately specialised information security training.

the availability,

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and Taboola must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

confidentiality

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to Taboola’s information and proprietary knowledge and its systems including its networks, website, SaaS services used by Taboola and management system.

and 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. There must be appropriate contingency including its networks, website, SaaS services used by Taboola and management system and data backup plans and security incident reporting. Taboola must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of Taboola including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and information assets

The information assets include information stored electronically on servers, websites, intranet, PCs, laptops, mobile phones and PDAs, as well as on USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the systems how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).
of Taboola***.***

The ISMS is the Information Security Management System, of which this policy, the Information Security Manual ('the Manual') and other supporting and related documentation is a part.

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of Taboola*.*

Document Owner and Approval

The Information Security Manager is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements in Clause 5.1.2 in the Manual.

A current version of this document is available to all members of staff on the corporate Brain web page. It does not contain confidential information and can be released to relevant external parties.

This information security policy was approved by the Company Management on date and is issued on a version controlled basis under the signature of the Chief Executive Officer (CEO).

Signature: Date:July 2 2017

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Kobi Afuta	April 3 2017
2	Minor text edits and management approval	Ariel Pisetzky	July 2 2017