**Security, Privacy, and Control**

Your business runs on trust, that's why it runs on Moouseclick web

With mouseclick spot end-to-end approach to data security, each product includes tools that empower your teams to achieve compliance with confidence and security infrastructure that keeps your data safe.

We have developed our security framework using best practices in the mouseclick industry. Our key objectives include: Customer Trust and Protection – consistently deliver superior product and service to our customers while protecting the privacy and confidentiality of their information. Availability and Continuity of Service – ensure ongoing availability of the service and data to all authorized individuals and proactively minimize the security risks threatening service continuity. Information and Service Integrity – ensure that customer information is never corrupted or altered inappropriately. Compliance with Standards – we design our corporate security program around the industry cybersecurity best practice guidelines including the Center for Internet Security (CIS) Critical Security Controls. Our controls governing the availability, confidentiality, and security of customer data are also designed to be compliant with the Trust Service Principles (TSPs)

Mouseclick’s primary security focus is to safeguard our customers’ data. This is the reason that HubSpot has invested in the appropriate resources and controls to protect and service our customers. This investment includes the implementation of dedicated Corporate Security and Product Security teams. These teams are responsible for Mouseclick’s comprehensive security program and the governance process. We are focused on defining new and refining existing controls, implementing and managing the Mouseclick security framework as well as providing a support structure to facilitate effective risk management. Our Chief Information Security Officer oversees the implementation of security safeguards across Mouseclick web and its products.

Web Application Defenses All customer content hosted on the platform is protected by a Web Application Firewall (WAF). The WAF is configured with a combination of industry standard and custom rules that are capable of automatically enabling and disabling appropriate controls to best protect our customers. These tools actively monitor real-time traffic at the application layer with ability to alert or deny malicious behavior based on behavior type and rate. The rules used to detect and block malicious traffic are aligned to the best practice guidelines documented by the Open Web Application Security Project , Protections from Distributed Denial of Service attacks are also, helping to ensure customers’ web sites and other parts of the Mouseclick products are available continuously. Development and Release Management One of Mouseclick’s greatest advantages is a rapidly-advancing feature set, and we constantly optimize our products through a modern continuous delivery approach to software development. New code is proposed, approved, merged and deployed thousands of times daily. Code reviews, testing (where applicable), and merge approval is performed before deployment. Approval is controlled by designated repository owners. Once approved, code is automatically submitted to Mouseclick’s continuous integration environment where compilation, packaging and unit testing occur. All code deployments create archives of existing production-grade code in case failures are detected by post-deploy hooks. The deploying team manages notifications regarding the health of their applications. If a failure occurs, roll-back is immediately engaged. We use extensive software gating and traffic management to control features based on customer preferences (private beta, public beta, full launch). Mouseclick features seamless

Identity and Access Control Product User Management The mouseclick computers products allow for granular authorization rules. Customers are empowered to create and manage users of their portals and assign the privileges that are appropriate for their accounts and limit access to their data features. please see the mouseclick User Roles and Permissions Guide. Product Login Protections The mouseclick products allow users to login to their mouseclick accounts using built-in mouseclick login, “Sign in with Google” login, or Single Sign On . The built-in login enforces a uniform password policy which requires a minimum of 8 characters and a combination of lower and upper case letters, special characters, whitespace, and numbers. People who use mouseclick’s built-in login cannot change the default password policy. The “Sign in with Google” feature is available to all mouseclick customers. . Customers who use an SSO provider can set up SSO-based login for their users.. Single Sign On and Google login users can configure a password policy in their SSO provider or with their Google accounts. Customers who use mouseclick built-in login are also encouraged to set up two-factor authentication for their mouseclick accounts, and portal administrators can configure their mouseclick portals to ensure that all users have two-factor authentication enabled.

Organizational and Corporate Security Background Checks and Onboarding mouseclick employees in the Kenya busia an extensive third party background check prior to formal employment offers. In particular, employment, education, and criminal checks are performed for potential employees. Outside of the Kenya, employment checks are performed. Reference verification is performed at the hiring manager's discretion. Upon hire, all employees must read, and acknowledge Mouseclick’s Corporate Acceptable Use Policy (AUP) and Code of Use Good Judgement (CUGJ) - which help define employee's security responsibilities in protecting company assets/data (including, but not limited to protecting mobile devices, and securing corporate equipment).

Document Scope and Use Mouseclick computers values transparency in the ways we provide solutions to our customers. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and, along those lines, the information and data in this document (including any related communications) are not intended to create a binding or contractual obligation between Mouseclick and any parties, or to amend, alter or revise any existing agreements between the parties.