



ClickSoftware® Information Security Program

LAST UPDATED: May 14, 2019

This Information Security Program forms part of the ClickSoftware Cloud Service Agreement and any other ClickSoftware ordering document that incorporates this Information Security Program (the “**Agreement**”). Any capitalized but undefined term herein shall have the meaning given to it in the Agreement.

1. **General.** ClickSoftware, either itself or through a third party provider, uses at least industry standards to provide for the security and confidentiality of Client Data contained within the Service, to protect against any anticipated threats or hazards to the security or integrity of the same, and to protect against unauthorized access to the Service or Client Data that could result in harm to Client. Notwithstanding the foregoing, Client acknowledges and agrees that, use of or connection to the Internet provides the potential opportunity for illegal access to the Service and Client Data by unauthorized third parties.
2. **Requirements.** ClickSoftware:
 - i. stores Client Data in a secure format that:
 - a. is separate from data of other customers of ClickSoftware, and
 - b. is accessible only by Client’s authorized personnel and by ClickSoftware personnel who need to access the Client Data to enable ClickSoftware to provide the Service to Client in accordance with the Agreement, and who are bound by obligations of confidentiality sufficient to protect Client Data in accordance with the terms of the Agreement (each, an “Authorized Personnel”);
 - ii. trains ClickSoftware’s Authorized Personnel regarding their confidentiality obligations hereunder; and
 - iii. ensures that the transmission of all Client Data provided or made accessible to ClickSoftware under this Agreement uses industry-standard encryption,
 - iv. employs or facilitates adequate physical security for all premises in which Client Data will be processed and/or stored;
 - v. implements a network security program which provides for
 - a. appropriate access controls and data integrity controls;
 - b. testing of all controls; and
 - c. appropriate corrective action and incident response plans.
3. **Confidentiality.** ClickSoftware shall use the same efforts to enforce the confidentiality obligations of Authorized Personnel as ClickSoftware uses to enforce such obligations with respect to its own Confidential Information, provided that ClickSoftware shall not use less than reasonable efforts in such enforcement.
4. **Security Breach.** In order to (i) facilitate that both ClickSoftware and Client have the ability to address, contain and mitigate risks stemming from any actual, alleged or potential unauthorized use, disclosure, compromise or theft of Client Data, and (ii) provide a consistent process for identifying, reporting, investigating and closing information security incidents, ClickSoftware maintains an information security incident reporting process (hereinafter a “SIRP”). At a minimum, the SIRP must (a) mandate that relevant ClickSoftware personnel notify their management in the event that any ClickSoftware personnel become aware of any action which indicates that there has been or may be



an information security incident, and (b) mandate that an officer of Client must be contacted as soon as reasonably practicable in the event of any actual or imminent disclosure of Client Data, in accordance with the aforementioned escalation procedure.

5. **Disaster Recovery.** ClickSoftware maintains a disaster recovery plan that reasonably ensures that all Client Data in ClickSoftware's possession or control at a given time is capable of being recovered, and that the integrity of all such recovered Client Data is retained, in the event of a Security Breach or of any significant interruption or impairment of operation of ClickSoftware equipment or any material loss, deletion, corruption or alteration of data ("**Disaster Recovery Plan**").
6. **Assessments.** Company performs periodic code inspections for applicable components of the Service. Company shall address any issues noted in the inspections with corrective actions. The Parties agree that, if applicable and subject to confidentiality obligations, Company will provide information regarding its subcontractors as reasonably requested by Client.
7. **Vulnerability Assessments.** ClickSoftware will perform periodic vulnerability assessments of its Service and network and will provide executive reports to Client upon request. In addition, Client reserves the right to have a mutually agreed upon third party periodically audit the Service to ensure compliance with the requirements of this Information Security Program. Any third party audit of the Service shall not include penetration testing, unless mutually agreed to in writing by the parties.