INFORMATION SECURITY POLICY OF STANDUPLY

Document Control

Reference: ISMS DOC 5.2
Issue No:
Issue Date:11/06/2020

The Board of Directors and management of Standuply, Inc, located at 340 S. Lemon Ave. #1448, Walnut, CA 91789, which operates in the IT sector and provides Standuply software for automation of software development processes and internal company Q&A services, 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, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with [Organisation Name]'s goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

Standuply, Inc. 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, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. Artem Borodin as a Head of Risk 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.

All staff of Standuply, Inc. are expected to comply with this policy and with the ISMS that implements this policy. All staff, and certain external parties, will receive appropriate training(s). The consequences of breaching the information security policy are set out in Standuply, Inc. disciplinary policy and in contracts and agreements with third parties.

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

Standuply, Inc. has established a top level management steering group named as Information Security Committee, chaired by Artem Borodin - Chief Product Officer (CPO) / Oleg Krasavin - Chief Information Security Officer (CISO) and including the Alexandt Druzhinin - Information Security Manager and other executives/specialists/risk specialists to support the ISMS framework and to periodically review the security policy.

Standuply, Inc. takes ISO27001:2013. as its guideline standard for company ISMS.

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, all full time or part time staff, 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

INFORMATION SECURITY POLICY OF STANDUPLY

Document Control

Reference: ISMS DOC 5.2
Issue No:
Issue Date:11/06/2020

Manual) and to act in accordance with the requirements of the ISMS. All staff will receive information security awareness training and more specialised staff 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 Standuply, Inc. 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 should be appropriate business continuity and incidents respond 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 Standuply, Inc. information and proprietary knowledge and its systems including its network(s), website(s), extranet(s), and other systems.

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 for network(s), payment system(s), website(s), extranet(s)] and data backup plans and security incident reporting. Standuply, Inc. must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of Standuply, Inc. 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 printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, 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 system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

Of Standuply, Inc.

Standuply, Inc. and such partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS.

The ISMS is the Information Security Management System, of which this policy and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2013.

Standuply, Inc.

INFORMATION SECURITY POLICY OF STANDUPLY

Document Control

Reference: ISMS DOC 5.2
Issue No:
Issue Date:11/06/2020

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 Standuply, inc.

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.

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

This information security policy was approved by the Board of Directors on 11/06/2020 and is issued on a version controlled basis under the signature of the Chief Executive Officer (CEO).

Signature: 

Date: 06/11/2020

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Alexander Druzhinin	11/06/2020