YAPSTER

Version 2.0 / Public / YAP-ISMS-PO-5.2

Information Security Policy

Purpose **3**

Scope **3**

Key Principles **3**

Information Security Policy **3**

Document Control **6**

- Change Record 6
- Reviewers 6
- Approvers 6
- Distribution 6

Purpose

The purpose of this document is to define the Information Security Policy for Yapster (Yapster).

Scope

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all the information and communication technology within the scope.

Users of this document are all employees and contractors of Yapster.

Key Principles

The key principles of adhering to the Information Security Policy are listed below:

- To create a culture of employee responsibility in relation to the handling and care of personal data and other confidential information;
- To promote assurance and confidence in our Customers;
- To reduce the risk of confidential or sensitive information / documentation being stolen or accessed by unauthorised individuals which could damage the integrity of Yapster;
- To help demonstrate compliance with Data Protection legislation

Information Security Policy

Yapster is a cloud based secure messaging business that provides a communication and collaboration tool for businesses. Security is a key aspect of all its activity and it is therefore vital that Yapster ensures that any information security risks to its ongoing business are mitigated.

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 the Organisation.

The Board and management of Yapster are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organisation, to preserve its competitive edge, cash-flow, profitability, legal, regulatory, contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Yapster objectives and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

The organisation’s current strategic business plan and information security strategy provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of the ISMS. Information-related risks are to be identified and controlled via routine reviews of business operations and individual risk assessments of all changes within the business. The Board, aided by the Compliance Officer is responsible for the management and maintenance of risk treatment.

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 being reviewed and implemented where necessary supported by specific, documented policies and procedures as detailed in the information security strategy.

All employees of Yapster and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy.

The ISMS is subject to continuous, systematic review and improvement as a living management framework.

Yapster has established an Information Security Working Group (3 Amigos board group with support from the Information Security Officer) including executives/technical specialist's/risk specialists to support the ISMS framework and to periodically review the security policy.

Yapster is committed to maintaining certification of its ISMS to ISO27001 standard.

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, will be made aware of, their responsibilities to preserve information security, to report security breaches (in line with the policy and procedures) and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in Yapster disciplinary policy. 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. Information resources must be resilient, and Yapster 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. Disaster recovery and business continuity plans are to be reviewed, implemented and documented to ensure appropriateness.

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 Yapster information and its systems including networks, websites, portals and extranet systems.

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 (for networks, web sites and extranets), data back-up plans, and security incident reporting. Yapster must comply with all relevant data-related legislation in those jurisdictions within which it operates.

Of the physical (assets)

The physical assets of the Yapster including but not limited to computer hardware, 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, web site(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.)

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, and which has been designed in accordance with the specification contained in ISO27001:2013

The **COO/CFO** is the **Owner** of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements of the standard.

A current version of this document is available to all employees in the company documents section of Yapster. It does not contain confidential information and can be released to relevant external parties.

This Information Security Policy was approved by the Yapster Board, on 01/02/2018

Document Control

Change Record

Author	Date	Version	Change Reference
Leigh Gordine	24/01/2018	V 0.1	First draft
Leigh Gordine	13/02/2019	V 0.2	Added Contents, DC and PSK sections
Leigh Gordine	25/03/2019	V 1.0	Versioned for publication
Leigh Gordine	29/10/2020	V 1.1	Small update to reflect cert status and reference 3 amigo group
Leigh Gordine	15/02/2021	V 2.0	Versioned for publication

Reviewers

Name	Date	Position
Jenna Gonzales	12/03/2019	Head of Customer Success
Nicci Setchell	13/03/2019	CFO/COO
Leigh Gordine	10/03/2020	Head of Information Security
Nicci Setchell	30/12/2020	CFO/COO

Approvers

Name	Date	Position
Nicci Setchell	25/03/2019	CFO/COO
Nicci Setchell	30/12/2020	CFO/COO

Distribution

Location	Date
G-Suite: Security Policy Documentation	25/03/2019
G-Suite: Security Policy Documentation	15/02/2021