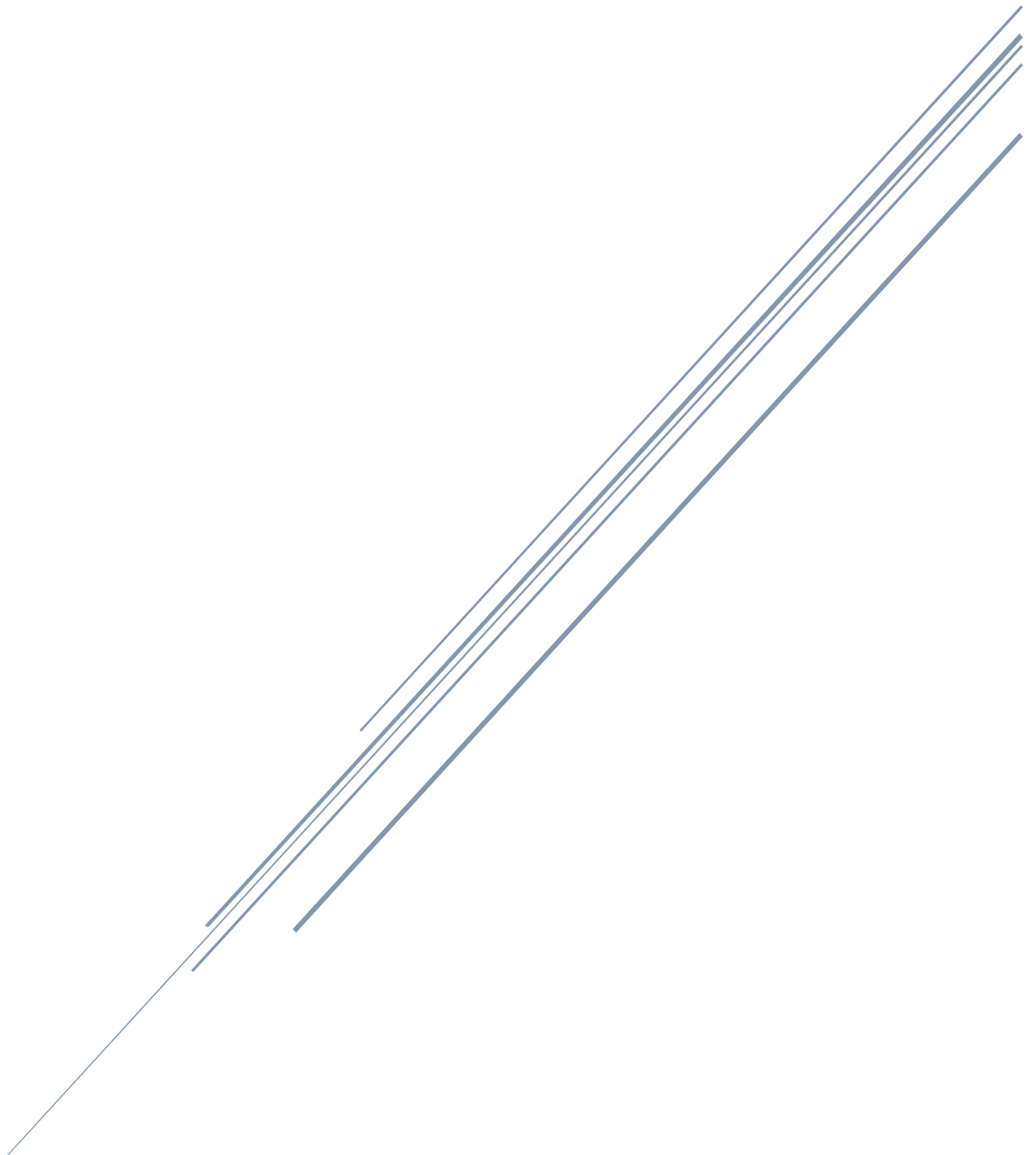# Information Security Policy

INF / PLY - 002

Document Control:

This document is valid for a period of 12 months from the date of issue and will be subject to an annual revalidation review by Hazard 360 Ltd.

Amendments will only be made with the approval Alan Smith Director. All amendments will be recorded in the tables below.

Document Status:

Document Reference	Hazard Legal Policies - Statements
Document Title	Information Security Policy
Reference Number	INF / PLY 002
Status	Live
Section No / Pages	6/6
Date	01 / 01 / 2018
Author	Alan Smith
Approved By	Alan Smith
Owned by	© Hazard 360 Ltd

Revision History

Reference	Date	Revision Author	Summary Changes
INF / PLY 002	01/01/2018	Alan Smith	New Information Security Policy
INF / PLY 002	01/01/2019	Alan Smith	No Change Required
INF / PLY 002	01/01/2020	Alan Smith	No Change Required

Contents

1: Introduction

This document defines the information security policy of Hazard 360 Ltd.

As a modern, forward-looking business, Hazard 360 Ltd recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, Hazard 360 Ltd has implemented a set of information security controls to address its perceived risks.

Information security has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

This policy applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Hazard 360 Ltd systems.

The following supporting documents are relevant to this information security policy and provide additional information about how it is applied:

- Cloud Computing Policy
- Mobile Device Policy
- Access Control Policy
- Cryptographic Policy
- Physical Security Policy
- Anti-Malware Policy
- Network Security Policy
- Electronic Messaging Policy
- Data Protection Policy

2: Information Security Policy

2.1 Information Security Requirements

A clear definition of the requirements for information security within Hazard 360 ltd will be agreed and maintained with the internal business and cloud service customers so that all information security activity is focussed on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements with regard to the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the Hazard 360 Ltd information security programme that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

2.2 Framework for Setting Objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

Information security controls will be adopted where appropriate by Hazard 360 Ltd. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans.

In addition, enhanced and additional controls from relevant codes of practice will be adopted and implemented where appropriate. The adoption of these codes of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

2.3 Continual Improvement of Information Security

Hazard 360 Ltd policy with regard to continual improvement is to:

- Continually improve the effectiveness of information security controls

- Enhance current processes to bring them into line with good practice as defined within relevant standards

- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security

- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions

- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data

- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties, including cloud service customers

- Review ideas for improvement at regular management meetings in order to prioritise and assess timescales and benefits

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews

2.4 Information Security Policy Areas

Hazard 360 Ltd defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, the organization.

The table below shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties.

Associated Policy Documents:

Policy Title	Areas addressed	Target audience
Cloud Computing Policy	Due diligence, signup, setup, management and removal of cloud computing services.	Employees involved in the procurement and management of cloud services
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by the organization or the individual for business use.	Users of company-provided and BYOD (Bring Your Own Device) mobile devices
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.	Employees involved in setting up and managing access control
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management.	Employees responsible for protecting the organization's infrastructure from malware
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks and remote access; network security management, including roles and responsibilities, logging and monitoring and changes.	Employees responsible for designing, implementing and managing networks
Electronic Messaging Policy	Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.	Users of electronic messaging facilities
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.	Employees responsible for creation and management of records
Data Protection Policy	Applicable data protection legislation, definitions and requirements.	Employees responsible for designing and managing systems using personal data

2.5 Application of Information Security Policy

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the top management of Hazard 360 Ltd and must be complied with. Failure by an employee to comply with these policies may result in disciplinary action being taken in accordance with the organization's employee disciplinary process.