Cybersecurity Policy

HONASA Consumer Limited

DOCUMENT NAME	Cybersecurity Policy
DOCUMENT CLASSIFICATION	Public
VERSION	1.0

Contents

1. INTRODUCTION

This document contains a summary of the Information Security policies and data protection controls implemented in Honasa Consumer Limited (Henceforth referred to as “Honasa”) to ensure confidentiality, integrity and availability of systems and data belonging to the firm and its customers.

Honasa regards its information, including that of its customers, as valuable assets. These assets are fundamentally important to the Honasa’s business operations and are carefully guarded and preserved. Honasa understands the importance of guarding the information it holds from evolving threats and continually works to enhance the information protection programs already in place.

Honasa has a responsibility to keep customer and Honasa’s data safe and, to that end, has implemented policies and other security tools to safeguard information assets.

2. ORGANIZATION

Honasa has endorsed an Information security management system (ISMS) to enhance the existing information risk and security programs, demonstrating commitment to enhancing security against evolving threats and raising awareness. Honasa has defined following organization structure for implementing and sustaining Information ISMS. The Steering Committee of Honasa shall provide direction and necessary support for implementation and maintenance of management system to ensure information security and business continuity in line with the defined policy. Honasa’s ISMS is built on a comprehensive framework of policies, standards and guidelines aligned to the ISO 27000 series.

3. POLICIES

Honasa Information Security policies are aligned to the ISO 27001 and ISO 22301 series standard and are directed at those responsible for IT and security functions, and to establish the minimum policy and controls baseline for Honasa. Information security policies are published on the intranet and is intended to be read, understood and applied by those personnel who have responsibility for IT and information security in the firm. Honasa and its personnel are required to comply with policies. These policies are reviewed regularly and may be modified as needed.

Honasa personnel are made aware of the policies through a number of channels including the awareness mails and training sessions.

4. MOBILE DEVICE AND TELEWORKING POLICY

Mobile device and teleworking policy are designed both to protect the confidentiality of any data that may be stored on the mobile devices like Laptop, smartphones, tablets etc. Mobile computing equipment usage should be governed by appropriate controls such as physical protection, encryption, anti-virus protection and backups.

5.HUMAN RESOURCE SECURITY POLICY

The Human Resource Security Policy defines the areas affecting personnel security within an organization. The policy has controls defining information security in process prior to employment like screening, employment contract, information security during employment like trainings, awareness programs, disciplinary process and information security during termination of employment.

6. ASSET MANAGEMENT POLICY

The asset management policy defines the classification and security of information assets and systems (hardware and software assets), including data classification, acquisition, transfer, and disposal. This contains controls related to management of asset inventory, acceptable use and return of asset. The asset management policy also provides direction on information leakage and prevention.

7. ACCESS CONTROL POLICY

Honasa’s access control policy defines the controls that need to be implemented and maintained to protect information assets against unauthorized access. Access to Honasa’s information systems shall be controlled in accordance with the business requirement, with subject to the principles of least privilege, segregation of duty and information security considerations. The user access management shall include life cycle of user’s access, covering stages from access registration to de-registration, including allocation of privileged access rights.

8. CRYPTOGRAPHY POLICY

Cryptography policy defines acceptable business use as activities that directly or indirectly support business. It is intended to define the required protection level to maintain the confidentiality, integrity and authenticity of the confidential information assets and sensitive application systems of Honasa.

Honasa shall support the encryption algorithms suitable for its business needs. Use of a particular encryption algorithm shall be decided based on the Business Requirements and Regulation/ Law/ Standards and compliance requirement(s).

9. PHYSICAL & ENVIRONMENTAL SECURITY POLICY

Critical information system and assets of Honasa are hosted using cloud services provided by reputed cloud service providers. Hence, Honasa relies on the physical and environmental security measures deployed by cloud service provider. Further, to ensure physical security of the office premises, physical and environmental security policy is established.

10. OPERATION SECURITY POLICY

The operations security policy shall provide guidance on the controls that should be implemented to protect confidentiality, integrity and availability of Honasa information system. The policy provides guidance related to configuration management, change and patch management, capacity management, logging and monitoring controls, backup and protection against malware, vulnerability management and controls related to installation of software on operational systems.

11. COMMUNICATION SECURITY POLICY

Communication Security Policy is defined to ensure the protection of information in networks and its supporting information processing facilities. Honasa shall ensure adequate management and control of networks to protect information in Honasa systems and applications. The policy details out guidance related to security and segregation of network services, web filtering, information transfer and email security.

12. SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE POLICY

Honasa shall ensure that security considerations are embedded into all stages of the development life cycle, from the planning to the deployment stage. Secure Information system engineering principles shall be designed into all architecture layers i.e., business, data, applications, and technology. These shall balance the need for information security with the need for accessibility. For the customized (not off-the-shelf/ standard offerings) software developed by partners, arrangements pertaining to licensing, code ownership and intellectual property rights shall be agreed between Honasa and the partner.

13. SUPPLIER RELATIONSHIP POLICY

Honasa shall identify and mandate information security controls to specifically address third party's access to Honasa information. Honasa shall provide compliance requirements (where applicable) in the agreements with third parties involving accessing, processing, communicating, or managing Honasa information or information processing facilities which shall cover all relevant security requirements. Non-Disclosure Agreements or Confidentiality clauses within the agreement shall be defined to ensure information security.

While onboarding a cloud service it shall be ensured confidentiality, integrity, availability requirements for the subscribed services are mutually agreed with the cloud service provider.

14. INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

Management shall establish a process to ensure an effective, timely and orderly response to information security incidents. Roles and responsibilities for effective management of incidents shall be identified.

Honasa shall establish and implement a process for reporting, responding to, and escalating events leading to information security and business continuity impact. All employees, and Partner(s) shall be responsible for reporting all identified security events and incidents promptly. Honasa shall identify methods to collect, analyze and produce threat intelligence related to information security threats.

15. BUSINESS CONTINUITY MANAGEMENT POLICY

Honasa shall establish Business Continuity Management System at adequate level to meet the continuity and recovery objectives of the critical business process and/or associated information systems. Adequate continuity plans shall be developed to recover the process and associated information system. Honasa continuity plans which shall be exercised, tested and integrated into the organization's business processes. The respective departments shall identify business requirements for the availability of information systems and its processing facilities.

16. COMPLIANCE POLICY

All the copyrighted information of Honasa shall be used only for business purposes. Strict action shall be taken against those who misuse Honasa copyrighted material.

All Intellectual Property (means *including but not limited to patent, trademark, trade secret, design, know-how, copyright, etc. whether registered or unregistered*) of Honasa shall be used only for business purposes.

Honasa shall implement controls for collecting, processing, and disseminating personal information. Employee personal data maintained on information systems shall be secured through implementation of appropriate security controls.

Honasa top management may initiate information security reviews periodically to assess Honasa's conformity to applicable standards and regulation.