Document Management Information

Revision Details

Version No.	Revision Date	Particulars	Approved by

Document Contact Details

Role	Name	Email ID

Distribution List

Name	Designation

nformation Security Governance Policy

Contents

1. INTRODUCTION

Bindawood considers information as a critical asset for its success and is committed to preserving the confidentiality, integrity and availability of information used and maintained by the organization on behalf of its shareholder, customers, employees, and business partners.

This policy defines BinDawood's Information Security (IS) approach and the roles, and responsibilities of various stakeholders in relation to the implementation of such approach and the IS strategy. This policy is to complemented by domain-specific standards which are instrumental in ensuring clarity and consistency

2. PURPOSE

The purpose of this Policy is to

- Set expectations on the establishment of an enterprise-wide IS risk management framework, including defining and implementing the minimum requirements (controls and tools) for protecting information assets across BinDawood.
- Define an enterprise wide governance structure including establishing the roles, responsibilities and authorities for the development and implementation of Bindawood's IS strategy.
- Define the segregation of duties between IT operations, IS, and the business.
  Establish an overall direction and principles regarding IS.

3. SCOPE

This policy is applicable to BinDawood and all its subsidiaries BinDawood and Danube business units. All employees, contractors, part-time and temporary workers granted access to the organization's information or systems are covered by this Policy.

The Policy is intended to protect **INFORMATION** in whatever form, including, but not limited to paper documents and electronic records. **INFORMATION TECHNOLOGY** assets covered under this policy include all computer equipment, network or data communications equipment, computer programs, cloud platforms, and data storage devices and media.

4. INFORMATION SECURITY PRINCIPLES

- The IS program implemented across BINDAWOOD will ensure:
  - Effective mitigation of risks to the business
  - Compliance with applicable legal, regulatory and contractual requirements and
  - Adoption of generally accepted IS practices and standards.

  The information must be protected throughout its lifecycle according to its criticality based on the degree of damage that could result from its misuse, unavailability, destruction, unauthorized disclosure, use or modification.
- The IS program shall be subject to continuous and systematic review and improvement through periodic internal and external assessments.
  Information security education, training and awareness programs shall be implemented to ensure that users are aware of security threats and are equipped to apply organizational security policies and principles.
- A formal IS incident response program shall be implemented to ensure that incidents are comprehensively investigated and systematically managed throughout their lifecycle from detection to closure.
- A "secure by design" approach shall be adopted where systems must be designed from the foundation to be secure.
  This Policy shall be subject to review, and when required updated, at least on an annual basis.

5. INFORMATION SECURITY RISK MANAGEMENT

BinDawood shall continuously and proactively assess, monitor and manage the risks to information assets through a systematic risk management approach which is integrated and forms part of the enterprise risk management framework. The risk assessment shall be considered as the basis for setting out how the organization identifies and implements IS controls.

6. ROLES AND RESPONSIBILITIES

The overall enterprise IS governance and operating model is described in the following

Audit and Risk Committee

- Reviews and approves Information Security Strategy and Governance Policy.
- Provides oversight and direction in respect of our IS posture and approach to IS risk management.

Chief Executive Officer

- Set the roles, responsibilities and the authorities for the protection of the organization's information assets.
- Foster and promote Information Security culture with top down approach.
- Provide budget and support sufficient resource hiring to establish, implement, operate, monitor, review, maintain and improve the IS program.

Chief Transformation Officer

- Ensure the IS Strategy to ensure its alignment with business objectives and priorities.;
- Oversee and be accountable for the implementation of the IS strategy
- Approve the enterprise IS standards and handle escalations related to the approval or rejection of policy or standards exemption requests involving high risks;
- Identify and oversee the execution of enterprise-wide security initiatives;
- Sign-off on incident reports for any incident of high severity;
  Sign-off on BinDawood IS annual plans.
-

Head of Information Security

- Own the implementation of the IS program and strategy;
- Develops and is accountable for enterprise IS policies and frameworks;
- Leads independent IS reviews or self-assessments and ensures that actions are taken to rectify any identified gaps;
  Develops and implements a common framework for reporting IS status through KPIs;
- Leads IS incident response teams managing incidents of high severity;
- Is accountable for the development, performance and oversight of BinDawood Security Operations Center;
- Monitor compliance with the enterprise security policies and standards
- Accountable for the day-to-day IS operations

Heads of IT Operation and Digital Innovation

Ensure that information technology systems are implemented, configured and maintained in accordance with the security policies, standards, and procedures;

- Ensure all issues, vulnerabilities, weaknesses highlighted by the Security Lead are addressed;
- Report to the Head of Information Security on the status of information security KPI's
- Protect the organization's information assets by adhering to IS policies and procedures;
- Attend and promote IS awareness training;
- Timely report security incidents, suspicions, or violations.

7. EXCEPTION HANDLING

Exceptions to IS policies shall only be considered if submitted through a formal process that includes risk assessment. Exceptions shall be granted only if a business need justifies the additional risk exposu

8. DOMAIN-SPECIFIC INFORMATION SECURITY POLICIES

Additional policies and standards for specific security domains are to be developed as per business needs to meet the security objectives.

Acceptable Use

- BinDawood information, systems, services, and equipment are assets of the company and are provided for official and authorized business purposes. All information created, stored, used or processed on the corporate systems are the property of BinDawood.
- Information assets shall not be used in a manner that is illegal, harassing, offensive, harmful to the company or its employees, or in violation of other policies, standards, guidelines or regulatory requirements.
- Only pre-authorized systems, devices, platforms may be used to process BinDawood information.
- For security, compliance, and maintenance purposes, authorized individuals may monitor equipment, systems, files and network traffic at any time.

Information Access Control

- Access to information assets must be based on the specific role by providing only the level of access required to meet an approved business need or perform prescribed work responsibilities.
- Access shall be subject to formal authorization and periodic reviews by the information owners.

Human Resource Security

- Employees, contractors and third-party users shall receive the security training needed to support compliance with the security policies, standards, and procedures in the course of their ordinary work.
- All candidates considered for employment, contractors and third-party users should be adequately screened if they are required to access or handle sensitive information.
- Access rights of all employees, contractors and third-party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change and all company information assets must be returned.

IT Operations Security

- Detection and prevention measures for malicious code (e.g. viruses, worms, etc.) or other malicious system activities shall be implemented, maintained, and kept up to date.
- Information systems shall be subject to formal change control processes which provide a managed method by which changes are requested, tested, approved, communicated, and logged.
- All critical systems in the organization shall be patched and updated periodically against any security vulnerabilities.

- Critical audit trails and logs shall be activated to record security events within information systems. The logs shall be protected against manipulation and retained in accordance with regulatory requirements or at least for a period of not less than 90 days.

Physical and Environmental Security

Physical access must be restricted in areas containing information assets or where computer processing activities occur (e.g. data centers, computer rooms, offices). Physical access controls must be implemented adequate with the level required to protect the information assets and provide only the level of access needed to perform prescribed work assignments.

Vulnerability Management

- Vulnerability assessments through vulnerability scanning, configuration reviews, or penetration testing must be conducted periodically at a frequency adequate with their criticality.
- All publicly exposed (i.e. Internet facing) systems must undergo vulnerability assessment and penetration testing by a specialist third party on yearly basis.

Network and Communication Security

- Networks must be segmented into separate logical domains depending on security requirements, internal or external, business user groups and level of access.
- Remote access to information systems shall be provided only to meet an approved business need or perform prescribed work responsibilities.
- Only pre-approved methods, programs, or devices may be granted remote access.
- All connections to external networks shall be pre-authorized, protected using adequate perimeter devices (e.g. firewalls), and configured by default to deny network access unless specifically authorized on a granular level for a justified business need.

Supplier and Vendor Management

- Risks associated with suppliers and vendors having access to BinDawood information assets must be identified and security measures for mitigating any relevant IS risks must be deployed.
- Appropriate Confidentiality Agreement (CA) and Non-Disclosure Agreement (NDA) must be incorporated in relevant supplier and vendor agreements.

Threat Monitoring and Incident Response

- Security monitoring shall be performed to promptly detect threat and intrusion activities. The level of monitoring shall be based on the information classification and system criticality.
- Security incident response process and plans shall be developed and maintained in order to minimize impact and ensure orderly handling and

System Development, and Maintenance

- Security requirements shall be considered throughout the systems development lifecycle from the first stage of requirements gathering to ensure that security is an integral part of information systems being introduced.
- Separate development, testing, and production environments shall be established based on the on the system criticality.
- Principles for secure systems architecture and secure coding shall be established and applied to any information system implementation efforts.

Mobile and Bring Your Own Device (BYOD)

All mobile devices must be hardened with adequate security controls and management software before they are used to access the BinDawood organization's information.

- Personal mobile devices may be allowed to access the BinDawood organization's information and systems through an opt-in decision, where the employee explicitly agrees that a personal device maybe managed, reconfigured or remotely wiped by the organization as part of its data protection requirements.