INTRODUCTION

This policy provides management direction and support for information technology security in accordance with the KBA Group's operational requirements, relevant laws and regulations.

KBA Group aims to maintain an information security profile consistent with industry requirements and best practices in compliance with applicable laws and regulations. This policy defines the framework by which information security will be managed and supported across the KBA Group. KBA Group has established objectives and targets to support and maintain the effectiveness of the Information Security Management System (ISMS) and will monitor and review the objectives during Management Review to ensure continual improvement of the ISMS.

Risk management is at the core of the KBA Group's Information Security Management System (ISMS). Information security risks must be identified, assessed, mitigated and monitored to help protect the confidentiality, integrity and availability of the KBA Group's information and information systems.

Information security controls are established, implemented, monitored, reviewed and improved, where necessary, to help ensure that the specific security and strategic objectives of the KBA Group are met.

SCOPE

This policy applies to the KBA Group in its entirety, including its controlled entities.

GENERAL PRINCIPLES

KBA Group selects appropriate controls to protect KBA Group Information and Communications Technology (ICT) resources. Where an explicit procedure, manual, guideline or control is not cited in this Policy, the following security principles are to be applied by each user to guide their decision making regarding the use and protection of the KBA Group's ICT resources:

- All users are responsible for following the KBA Group's policies and procedures for managing information in a secure manner;
- A risk-based approach to information security should be adopted by all users to help ensure that all information related risks are managed in a consistent and effective manner;
- All users are to assist with the protection of KBA Group data and information to prevent disclosure to unauthorised individuals;
- All users must comply with relevant legal and regulatory requirements; and
- Users are to use or apply approved information security solutions and services to avoid creation of disparate IT security controls.

INFORMATION SECURITY CONTROLS

Human Resources Security

All applicable users are subject to appropriate security processes before, during and after the cessation of their employment with the KBA Group in accordance with the Information Security Management System and F023 – New Employee Checklist.

Exit procedures should be followed as far as practicable where a staff member is transferring to a new role or work location within the KBA Group. The staff member's direct manager (from the area that the staff member is transferring from) is responsible for 2inimize2g the exit procedures.

Security awareness training must be provided to all KBA Group employees and should be provided to contractors and third-party users of the KBA Group's ICT resources and connected systems to 2inimize possible security risks.

Asset Management

Inventory of Assets

A register will be maintained by the Head of Optimisation and Innovation of all the KBA Group's major information assets and the information owner of each asset is to be clearly stated.

Information and Data Classification

Information Owners must classify their assigned information assets upon creation according to the classifications outlined in the Information Classification Policy (P018). The classification of an information asset is based on the asset's importance and risk, relative to the goals and objectives of KBA Group.

Information Owners must review the data classifications of their information assets upon any significant change to the asset, or changes in regulatory requirements, to ensure that appropriate controls remain in place for the asset as it evolves over time.

Information Handling

Based on the data classification, System Owners and System Administrators must comply with the applicable controls to help maintain the confidentiality, integrity and availability of information assets under their control.

All users must ensure that information is handled in accordance with its classification as set out in the Information Classification Policy.

Access Control

Access to KBA Group information assets, and KBA Group ICT resources that store or process those assets, should only be granted following a controlled and auditable process on the basis of operational and security requirements defined by the nominated information owner. Access is managed and monitored by the Head of Optimisation and Innovation through the external IT Provider.

All users must protect passwords and other types of credentials in accordance with the requirements of the KBA Group's Information Security Management System.

Physical and Environmental Security

The Head of Optimisation and Innovation is responsible for defining the standards, processes and procedures related to the management and access of physical ICT facilities, such as data centres, network rooms, servers and networking hardware.

The physical protection of ICT resources must be managed to ensure protection against malicious or accidental damage, or loss.

Operations Management

Information Security Operations Management Manual

The minimum requirements for each of the items in this section of the policy, "Operations Management", are set out in the Information Security Management System Manual.

Operations Security

System Owners and System Administrators are responsible for the documenting and maintaining Standard Operating Procedures (SOP) for the ICT resources and information assets that they manage. These must be made available to all users who need them, to ensure the correct and secure operation of the KBA Group's ICT resources and information assets. SOPs are to be approved by the Systems Manager and Chief Executive Officer for inclusion in the ISMS prior to distribution.

Users involved in the administration, development, testing and commissioning of the KBA Group's ICT resources must follow appropriate change management procedures, defined in the KBA Group's Information Security Management System Manual.

Controls Against Malicious Code

System Owners and System Administrators are responsible for:

a. implementing detection, prevention, and recovery controls to protect against malicious code; and
b. appropriate user awareness procedures for the ICT resources they manage.

These controls must also be implemented in accordance with the Information Security Management System Manual.

Backup

Data backups are an essential control and safeguard to ensure the availability of KBA Group information.

The Head of Optimisation and Innovation must ensure the backup of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements (Please see Information Security Management System Manual).

Backup procedures must be tested to confirm that recovery can be completed in a timely manner to help ensure the continuity of KBA Group operations.

Log Management
All System Owners and System Administrators are responsible for ensuring that event logs to record user relevant information security events (such as user activity, exceptions and failures) are produced for the ICT resources that they manage and kept for an appropriate period of time. Event logs may be used to identify potentially unauthorised activity, assist in investigations, and to facilitate appropriate follow up action.

Vulnerability Management
The Head of Optimisation and Innovation is responsible for ensuring that security patch and vulnerability management processes are defined to identify, prioritise and remediate security vulnerabilities for ICT resources. This will help to minimise the risk of malicious attacks compromising the confidentiality, integrity or availability of KBA Group information assets and ICT resources.

Security patching and vulnerability management of the KBA Group's ICT resources must be carried out in accordance with the Information Security Management System Manual.

Network Communications Security
The System Owner and System Administrator must manage, control and segregate those parts of the network for which they are responsible to protect information in systems and applications in accordance with the Information Security Management System Manual.

System acquisition, development and maintenance
The Head of Optimisation and Innovation shall ensure that information security is an integral part of information system and application architecture and design across the entire lifecycle of the KBA Group's ICT resources.

System Owners and System Administrators must ensure that all of the applications and services for which they are responsible for within the KBA Group's ICT environment, are security reviewed and benchmarked against industry best-practice prior to acquisition or upgrade, in consultation with the Head of Optimisation and Innovation .

Users must only use applications or services approved by the Head of Optimisation and Innovation to store or process KBA Group information assets.

Supplier Relationships
To ensure protection of the KBA Group's ICT resources and information assets, any access provided to external providers must be correctly risk-managed and covered by a formal agreement. Any agreement to be entered into on behalf of the KBA Group must be approved by the Head of Optimisation and Innovation .

The KBA Group will work with those third parties who access, support and service the KBA Group's ICT resources to ensure, as far as reasonably practicable, that they comply with this policy and information security requirements. These requirements must, where applicable, be outlined in the formal agreement with the relevant external provider.

Information Security Incident Management

To ensure a consistent and effective approach to identifying and managing information security incidents that could impact the KBA Group's ICT resources, defined guidelines have been developed and implemented. See Information Security Incident Response Policy and Procedure.

All users of the KBA Group's ICT resources must report any suspected event or weakness that might have an impact on the security of KBA Group information assets and ICT resources to the Head of Optimisation and Innovation.

ENFORCEMENT

All Users of the KBA Group's ICT resources should be aware of this policy, their responsibilities and obligations.

Non-compliance with the provisions of this policy may result in disciplinary action.

The Head of Optimisation and Innovation (or their nominee) is responsible for monitoring the use of the KBA Group's ICT resources to measure compliance with this policy.

Where a user has been found to fail to comply with this policy or any other of the KBA Group's IT policies, procedures, manuals, or guidelines, access to KBA Group's ICT resources may be disconnected or restricted.

ROLES AND RESPONSIBILITIES

Head of Optimisation and Innovation

The Head of Optimisation and Innovation is responsible for managing the implementation and operation of the KBA Group's information security capabilities to ensure that the requirements of this policy are appropriately applied.

The Head of Optimisation and Innovation is responsible for:

a. defining the KBA Group's IT application and technology standards;
b. maintaining a repository of the KBA Group's approved applications and services;
c. monitoring use of the KBA Group's ICT resources, and disconnecting or restricting a user's access if the user has failed to comply with this policy or any of the KBA Group's other IT policies, procedures, manuals and guidelines; and

Systems Manager

The Systems Manager is responsible for information security policy development, and for ensuring compliance with and maintaining certification for ISO27001.

The Systems Manager is responsible for:

a. ensuring that users are aware of this policy;

b. reviewing and updating this policy to ensure that the policy continues to be suitable, adequate and effective.

Learning and Development Team Leader

a. ensuring that users are aware of the ISMS policy;
b. Training
c. completing regular role-based training to ensure the effective management of the ICT resource;
d. Onboarding and Offboarding

Information Owner

The Information Owner's responsibilities include the following in relation to applicable information:

a. determining the value of the information;
b. determining the statutory requirements regarding privacy and retention;
c. assigning an appropriate security classification according to the Information Classification Policy;
d. developing guidelines for, and authorising and reviewing access to, the information;
e. ensuring that risk assessments for their information assets are performed; and
f. ensuring that appropriate controls are specified and communicated to the system owner who has technical control of the information.

System Owner

The System Owner's responsibilities include the following:

a. managing system risk;
b. developing and updating Standard Operating Procedures to protect the system in a manner commensurate with risk;
c. maintaining compliance with requirements specified by information owners for the handling of data processed by the system; and
d. designating a System Administrator for the system.

System Administrator

The System Administrator's responsibilities include the following:

a. the day-to-day administration of the ICT resource;
b. developing, maintaining and documenting SOPs that include data integrity controls, authentication, recovery, and continuity of operations;
c. ensuring that access to information and the ICT resource is secured as defined by the System Owner and Information Owner;
d. implementing security controls and other requirements of this policy on ICT Resources for which the System Administrator has been assigned responsibility;
e. completing regular role-based training to ensure the effective management of the ICT resource;
f. taking corrective action in respect of audit findings, system vulnerabilities and any reported security breaches; and
g. developing and testing disaster recovery plans.

Information Security Team

The Information Security Team reports to the Head of Optimisation and Innovation. The Information Security Team is responsible for:

a. performing compliance and audit functions in accordance with the Information Security Audit Considerations section of the Information Security Management System Manual; and
b. investigating and reporting on suspected breaches of this policy.

Richard McKinnon
Chief Executive Officer

Date: 11 November 2023