Digital Islands
Growth Accelaration

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) POLICY

Purpose:

The purpose of this Information Security Management System (ISMS) Policy is to outline the security measures implemented by Digital Islands Business Services Limited (DIBSL) to ensure the confidentiality, integrity, and availability of its information assets. This policy applies to all employees, contractors, and third-party software applications used by DIBSL, including Google Workspace.

Scope:

This policy applies to all activities related to the management and handling of information by DIBSL, including but not limited to:

1. Collection, storage, processing, and transmission of information.
2. Access control and management of information assets.
3. Backup and recovery of information.
4. Incident management and response.

Information Security Objectives:

1. Protect the confidentiality of sensitive information by limiting access to authorised personnel only.
2. Ensure the integrity of information by regularly backing up and protecting against unauthorised changes.
3. Maintain the availability of information by implementing disaster recovery and business continuity plans.
4. Continuously improve the ISMS by regularly reviewing and updating the policy and procedures.

Responsibilities:

1. All employees, contractors, and third-party software applications are responsible for following the ISMS policy and reporting any suspected security incidents to the appropriate person.
2. The DIBSL management team is responsible for ensuring that the ISMS policy is implemented and maintained.

Password Management:

1. Employees must use strong passwords that are a minimum of 10 characters in length and include a combination of uppercase and lowercase letters, numbers, and symbols.
2. Passwords must be changed every 60 days.
3. Passwords must not be shared with anyone or written down.
4. Two-factor authentication must be used for all sensitive information.

Access Control:

1. Access to information assets is granted based on an employee's job function and level of responsibility.
2. Access to information assets must be revoked immediately upon termination of employment or the completion of a contractor's assignment.
3. All access to information assets must be logged and regularly reviewed.

Information Backup and Recovery:

1. All information must be backed up daily and stored in a secure location, with at least one backup kept off-site.

2. The DIBSL management team will regularly test the disaster recovery plan to ensure that information can be recovered in the event of a disaster.

Third-Party Software Applications:

1. All third-party software applications used by DIBSL must be approved by the management team and comply with the ISMS policy.
2. Regular security audits must be conducted on all third-party software applications to ensure they comply with the ISMS policy.

Incident Response:

1. Employees must report any suspected security incidents to the appropriate person as soon as possible.
2. The DIBSL management team will investigate all reported security incidents and take appropriate action to prevent future incidents, including reporting the incident to relevant authorities if necessary.
3. The DIBSL management team will regularly review the incident response procedures to ensure they remain effective.

Policy Review:

This ISMS policy will be reviewed annually by the DIBSL management team to ensure that it remains relevant and effective, and updated as necessary.

By following this ISMS policy, DIBSL is committed to protecting its information assets and maintaining the confidentiality, integrity, and availability of its information.

Last Updated: 2nd December 2022

Reviewed by: Gavin McWhirter, Managing Director, Digital Islands Business Services Ltd

Next Update: 1st December 2023