INFORMATION SECURITY POLICY STATEMENT

Lesha Bank LLC "Public" ("LB") is committed to serve its customers with securing the Confidentiality, Integrity, and availability of information for the day-to-day Business and Technical operations.

It is the policy of "LB" to protect its Information Assets in accordance with all applicable regulations, as well as with effective Information Security Practices and principles generally accepted as 'due diligence' followed by Information Risk Management Procedures, which ensure Confidentiality, Integrity and Availability of Customer's Information Assets.

LB specifically prohibits unauthorized access to, tampering with, deliberately introducing inaccuracies to, or causing loss of Information Assets. It also prohibits using Information Assets to violate any law, commit an intentional breach of confidentiality or privacy, compromise the performance of systems, damage software, physical devices or networks, or otherwise sabotage LB's Information Assets.

ISMS in LB is aligned to the requirements of ISO/IEC 27001:2013. The management of LB is committed to ensure that:

- Regulatory and legislative requirements related to LB are met;
- The confidentiality of information is protected and prevent disclosure of valuable or sensitive information;
- The integrity of information is maintained to ensure its accuracy and completeness;
- The availability of information is maintained to meet business needs and client's requirements;
- Business continuity plans are developed, maintained and tested;
- Information security awareness is provided to all LB employees;
- Incident management process is established and implemented to ensure that all breaches of information security, actual or suspected are reported and investigated;
- Risks are mitigated to an acceptable level through a risk management framework;
- The information security management system is continually improved;
- Appropriate resources are allocated in order to implement, operate and review an effective Information Security Management System;
- All stakeholders are responsible for implementation of respective security policies and procedures within their area of operation and oversee adherence by their team members.

LB management acknowledges the need of continual improvement and has introduced various methods to ensure that effectiveness and continual improvement of the processes are achieved.

LB shall follow a formal disciplinary process for employees who have allegedly violated the information security policies and procedures.

LB shall ensure that the review of the Information Security Policy and related documents is performed at least on an annual basis or when significant changes occur to ensure suitability, adequacy, and effectiveness of the ISMS framework.

Abdulrahman Totonji,
CEO

Document number: LB-ISMS-POL-01, Revision: 00, Issue date: 03.10.2022

بيان سياسة أمن المعلومات

يلتزم بنك لِشا ذ.م.م عامة ("بنك لِش") بخدمة عملائه من خلال تأمين سرية المعلومات وسلامتها وتوافرها للعمليات التجارية والتقنية اليومية.

وتتمثل سياسة بنك لِشا في حماية أصوله من المعلومات وفقاً لكافة الأنظمة المعمول بها، بالإضافة إلى ممارسات ومبادئ أمن المعلومات الفعالة المقبولة عموما كإجراءات "عناية واجبة" متبوعة بإجراءات إدارة مخاطر المعلومات، والتي تضمن سرية معلومات العملاء وسلامتها، وتوافرها.

ويحظر بنك لِشا على وجه التحديد الوصول غير المصرح به إلى أصول المعلومات أو التلاعب بها أو إدخال معلومات غير دقيقة عن عمد أو التسبب في فقدانها.

كما يحظر استخدام أصول المعلومات لانتهاك أي قانون، أو خرق السرية أو الخصوصية بشكل متعمد، أو الإضرار بأداء الأنظمة، أو إتلاف البرامج، أو الأجهزة أو الشبكات، أو تخريب أصول معلومات بنك لِشا بطريقة و أخرى.

ويتوافق نظام إدارة أمن المعلومات في بنك لِشا مع متطلبات ISO / IEC 27001: 2013.

وتلتزم إدارة البنك بضمان ما يلي:

- تلبية المتطلبات التنظيمية والتشريعية المتعلقة بالبنك،
- حماية سرية المعلومات ومنع الكشف عن المعلومات القيمة أو الحساسة،
- الحفاظ على سلامة المعلومات لضمان دقتها واكتمالها،
- الحفاظ على توافر المعلومات لتلبية إحتياجات العمل ومتطلبات العميل،
- تطوير خطط استمرارية الأعمال والحفاظ عليها واختبارها،
- زيادة وعي جميع موظفي بنك لِشا بأمن المعلومات،
- إعداد خطة لإدارة الحوادث وتطبيقها لضمان الإبلاغ عن كافة انتهاكات أمن المعلومات، الفعلية أو المشتبه بها، والتحقيق فيها،
- الحدّ من المخاطر إلى مستوى مقبول من خلال إطار إدارة المخاطر،
- تحسين نظام إدارة أمن المعلومات باستمرار،
- تخصيص الموارد المناسبة من أجل تطبيق نظام إدارة أمن معلومات فعال وتشغيله ومراجعته،

يتحمل جميع أصحاب المصلحة مسؤولية تنفيذ سياسات وإجراءات أمن المعلومات، كلّ وفق نطاق عمله، كما ويتحمل مسؤولية الإشراف على التزام أعضاء فريقهم بها.

تقر إدارة بنك لِشا بحاجتها إلى إجراء تحسينات مستمرة وقد بدأت اعتماد أساليب متنوعة لضمان تحقيق فعالية العمليات وتحسينها المستمر.

Date: 03.10.2022