LANDBANK Retail Internet Banking (iAccess)

Online Security Policy

1. Introduction

At LANDBANK, we prioritize the security of our customers' personal and financial information. This Online Security Policy outlines the measures we implement to protect your data and offers guidance on how you can help safeguard your account, in compliance with Philippine regulations. By staying informed and adhering to the recommendations in this policy, you can help protect your personal information and preserve the integrity of your account.

2. Data Protection Measures

- Encryption: We employ advanced encryption technologies, including Secure Socket Layer (SSL), to protect your data during transmission over our website.
- Secure Access: All online transactions are conducted over secure protocols (HTTPS) to safeguard your financial information.

3. Account Security

- Strong Password Policy: Customers are encouraged to create strong passwords that include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information and change your password at least every 60 to 90 days.

4. Fraud Prevention

  - Website Verification: Always type the full website address into your browser rather than clicking on links, to avoid being redirected to fraudulent sites. The official URL of LANDBANK iAccess is https://www.lbpiaccess.com.
  - Look for 'https' and/or a padlock icon in the address bar, which indicates website security. You may also view the site's security certificate to confirm its authenticity and validity.
- Phishing Awareness:
  - We conduct awareness campaigns to help customers recognize phishing and scam attempts.
  - We will never request sensitive information via email or SMS. Always verify the authenticity of messages before providing personal information.

5. Customer Responsibilities

- Regularly update your information with the Bank to receive security alerts.
- Protect your credentials by not changing your passwords or personal information on shared or public devices. Avoid using browser features that save your login credentials.
- Always log out after every online banking session, especially when using shared or public devices.
- Secure your devices by installing and regularly updating antivirus software. Make sure your devices are free from malware.

- When conducting financial transactions in public areas, be cautious of shoulder surfers and ensure your screen is not visible to others.
- Monitor your accounts regularly. Review your activity and transaction history to promptly identify any unauthorized activity.

6. Incident Response and Reporting

- In the event of a security incident, we implement a comprehensive incident response plan aligned with Bangko Sentral ng Pilipinas (BSP guidelines). Affected customers will be promptly notified and provided with steps to secure their accounts.
- Our in-house Security Operations Center monitors, detects, and works to prevent cyberattacks targeting our digital platforms.
- If you notice suspicious activities or unauthorized transactions on your account, please contact our Customer Care Center immediately at 8-405-7000.

7. Regulatory Compliance

- We comply with all applicable BSP regulations, including those related to cybersecurity and data privacy. Our security policies are reviewed and updated regularly to remain compliant with evolving standards and requirements.

8. Continuous Improvement

- We are committed to continuous enhancement of our security measures and processes to address emerging threats and ensure protection of your information.

9. Contact Us

- For concerns regarding this policy or the security of your information, please reach out to the Customer Care hotline at 8-405-7000.