

Information Security Management Programmes

This document outlines BTS Group and Bangkok Smartcard System Company Limited (BSS)'s Information Security Management Programmes. The Company is committed to safeguarding sensitive data, ensuring business continuity and complying with relevant regulations. In this way, the Company can maintain the trust of stakeholders and uphold the Company's reputation for data integrity and privacy.

1. Business Continuity Plan

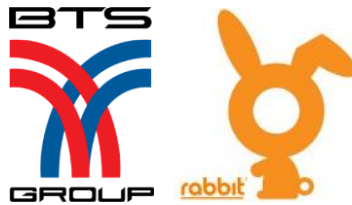
BSS has developed a business continuity strategy and plans to ensure the availability of information and services at the required level and within the required timeframes following an interruption to critical business processes. The plans include identifying critical business functions, defining and agreeing upon recovery time objectives with management, and identifying events that could cause interruptions to business processes—along with their probability and impact—through risk assessment and business impact analysis.

2. Vulnerability Analysis

BSS understands that business-critical systems and those at high risk must be regularly monitored for abnormal activities and assessed for technical vulnerabilities. To achieve this, BSS conducts an annual vulnerability analysis. This analysis identifies potential technical vulnerabilities, evaluates exposure to them, and pinpoints associated risks and impacts. Appropriate measures are then taken to address these risks.

3. Information Security Management Systems - Internal Audit

BSS conducts an internal audit of its information security management systems on an annual basis. The primary purpose is to ensure the integrity, security, and proper functioning of software, data, and production systems while minimising disruption to business operations and protecting sensitive information. BSS ensures that audit checks are strictly read-only for software and data, audit scope and access must be explicitly identified and agreed upon with relevant management before the audit commences, checks on production systems are tightly controlled and restricted to authorised personnel only to prevent business disruptions and safeguard sensitive information from disclosure.



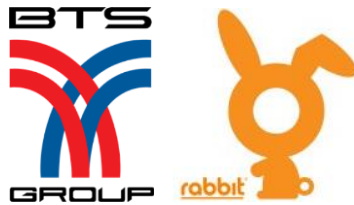
4. Information Security Management Systems – Independent External Audit

BTS Group and BSS's Information Security Management System has been certified under ISO 27001.






5. Escalation Process for Incidents, Vulnerabilities or Suspicious Activities

In case of any information security events, incidents, vulnerabilities or suspicious activities, employees shall report to their manager or IT Support as quickly as possible. Incidents shall be handled through an information security incident management procedure. The reporting channels must be established to ensure a quick, effective and orderly response to information security incidents based on the severity and urgency of each incident or activity. The knowledge gained from information security incidents shall be used to identify problems, needs of improvement, strengthen and improve information security controls. If required by regulations, any incidents causing significant impacts on the Company shall be reported to relevant authorities.



6. Information Security Awareness Training

Information security awareness training is mandatory for all BTS Group employees. The course, aptly titled "ตระหนก 6 ฉาก," features 6 short skits that explain various information security topics. These videos are also accessible on BTS Group's intranet.

IT SECURITY AWARENESS	
	<p>ตระหนก 6 ฉาก</p> <p>EP 1 : Post it เป็นเหตุ</p> <p>รหัสผ่านคือความลับ ควรเก็บรหัสผ่านไว้ในที่ปลอดภัย ไม่ควรจกรหัสผ่านลงกระดาษหรือบันทึกไฟล์เอกสารที่ไม่มีการป้องกันการเข้าถึงและไม่ควรจกรหัสผ่านให้ผู้อื่นรับทราบ เพราะอาจเป็นสาเหตุทำให้ข้อมูลสำคัญรั่วไหลหรืออาจจะโดนผู้อื่นนำบัญชีไปใช้ในทางที่ผิดได้</p>
	<p>ตระหนก 6 ฉาก</p> <p>EP 2 : อย่าเผลอก็กี่แล้วกัน !!</p> <p>ไม่ควรส่งรหัสผ่านที่คาดเดาได้ง่าย ไม่ควรใช้ข้อมูลระบุตัวตนส่วนตัวลงรหัสผ่าน เช่น ชื่อ นามสกุล วันเกิด หรือ เบอร์โทรศัพท์ และไม่ควรรหัสผ่านซ้ำเหมือนกันทุกเว็บไซต์ เพราะอาจจะทำให้โดนโจรกรรมข้อมูลจากผู้ใช้ไม่หวังดีได้</p>
	<p>ตระหนก 6 ฉาก</p> <p>EP 3 : หวังร้ายแต่ช่วย X2</p> <p>หากได้รับอีเมลหรือข้อความที่มีลิงก์หรือไฟล์แนบ ควรตรวจสอบให้แน่ใจก่อนที่จะเปิดไฟล์หรือกดเปิดลิงก์ เพราะอาจเป็นข้อความหลอกลวงที่ส่งมาเพื่อขโมยข้อมูลส่วนตัวหรือข้อมูลสำคัญขององค์กรได้</p>