นโยบายการรักษาความปลอดภัยของข้อมูล

บริษัท เพอร์เพิล เวนเจอร์ส จำกัด ("บริษัท") เป็นบริษัทจดทะเบียนในประเทศไทย มีสำนักงานใหญ่ตั้งอยู่ที่ เลขที่ 19 อาคาร 3 ชั้น 22 ไทยพาณิชย์ ปาร์ค พลาซ่า ถนนรัชดาภิเษก แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 ซึ่งมีวัตถุประสงค์ในการประกอบธุรกิจเทคโนโลยีทางการเงิน

การเคารพสิทธิในความเป็นส่วนตัวของท่าน

บริษัทเคารพสิทธิในความเป็นส่วนตัวของข้อมูลของท่าน และบริษัทเข้าใจดีว่าท่านมีความประสงค์ที่จะได้รับความปลอดภัยสูงสุดในการทำธุรกรรมผ่านเว็บไซต์ แอปพลิเคชัน และ/หรือช่องทางอื่นใดของบริษัท ดังนั้น บริษัทจะนำข้อมูลของท่านที่บริษัทได้รับไปใช้ตามวัตถุประสงค์ที่ได้รับอนุญาตจากท่านเท่านั้น และบริษัทจะดำเนินมาตรการที่เข้มงวดในการรักษาความปลอดภัย ตลอดจนจะป้องกันมิให้มีการนำข้อมูลของท่านไปใช้โดยมิได้รับอนุญาต

ข้อมูลที่บริษัทรวบรวมและเก็บรักษาไว้

บริษัทจะเก็บรวบรวมข้อมูลของท่าน ซึ่งรวมถึงข้อมูลส่วนบุคคล ข้อมูลชีวภาพ (เช่น ลายนิ้วมือ ใบหน้า เป็นต้น) ข้อมูลการทำธุรกรรม และ/หรือข้อมูลอื่นใด ไม่ว่าเป็นข้อมูลที่ท่านให้แก่บริษัทโดยตรง หรือข้อมูลที่บริษัทเก็บรวบรวมจากการที่ท่านทำธุรกรรมและ/หรือใช้บริการของบริษัทผ่านช่องทางเว็บไซต์ แอปพลิเคชัน Call Center และ/หรือช่องทางให้บริการอื่นใด หรือข้อมูลที่บริษัทเก็บรวบรวมจากแหล่งอื่นใดที่น่าเชื่อถือ เช่น หน่วยงานราชการ บริษัทในเครือ และ/หรือบริษัทพันธมิตรของบริษัท เป็นต้น ทั้งนี้ เพื่อประโยชน์ของท่านในการทำธุรกรรมและ/หรือใช้บริการกับบริษัท เพื่อประโยชน์ในการให้บริการแก่ท่าน เพื่อปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง และ/หรือเพื่อประโยชน์อื่นใดที่ท่านได้ให้ความยินยอมไว้แก่บริษัท โดยบริษัทจะเก็บรักษาข้อมูลของท่านตามมาตรการรักษาความปลอดภัยของบริษัท

การใช้ข้อมูลของท่าน

บริษัทจะใช้ข้อมูลของท่านเพื่อประกอบการทำธุรกรรมและ/หรือการใช้บริการของท่าน เพื่อประโยชน์ในการให้บริการแก่ท่าน และ/หรือเพื่อประโยชน์อื่นใดที่ท่านได้ให้ความยินยอมไว้แก่บริษัท ซึ่งรวมถึงเพื่อการวิเคราะห์ข้อมูล เสนอ ให้ ใช้ และ/หรือปรับปรุงผลิตภัณฑ์และ/หรือบริการใดๆ นอกจากนี้ บริษัทอาจใช้ข้อมูลของท่านเพื่อการปฏิบัติหน้าที่ตามสัญญาระหว่างบริษัทและท่าน และปฏิบัติตามกฎหมายหรือกฎระเบียบของหน่วยงานของรัฐหรือหน่วยงานกำกับดูแล

การเปิดเผยข้อมูลแก่บุคคลภายนอก

ท่านมีสิทธิในความเป็นส่วนตัวในข้อมูลของท่าน และบริษัทจะเปิดเผยข้อมูลของท่านให้แก่บุคคลภายนอก ในกรณีดังต่อไปนี้

- การเปิดเผยข้อมูลให้แก่พนักงานผู้ที่ได้รับอนุญาตของบริษัทและบริษัทในเครือ รวมถึงผู้สอบบัญชีหรือผู้ตรวจสอบภายนอกของบริษัท สถาบันการเงิน และ/หรือบุคคลภายนอกที่บริษัทเป็นคู่สัญญาหรือมีความสัมพันธ์ด้วย และ/หรือผู้ให้บริการ Cloud Computing ทั้งในประเทศไทยและต่างประเทศ

- การเปิดเผยข้อมูลดังกล่าวเป็นไปเพื่อให้ท่านสามารถทำธุรกรรม และ/หรือใช้บริการที่ท่านประสงค์ได้
- การเปิดเผยข้อมูลดังกล่าวเป็นไปเพื่อปฏิบัติตามกฎหมาย เพื่อการสอบสวนหรือการดำเนินการทางกฎหมาย
- การเปิดเผยข้อมูลดังกล่าวเป็นไปตามกฎหมายหรือตามคำสั่งของหน่วยงานของรัฐ หรือหน่วยงานกำกับดูแล
- การเปิดเผยข้อมูลให้แก่บุคคลภายนอกที่บริษัทได้รับความยินยอมจากท่านให้เปิดเผยข้อมูลของท่านให้แก่บุคคลดังกล่าวได้

มาตรการและวิธีการรักษาความปลอดภัยโดยทั่วไป

บริษัทมีระบบรักษาความปลอดภัยที่เข้มงวด เพื่อป้องกันการเข้าถึงข้อมูลของท่านโดยมิได้รับอนุญาต นอกเหนือจากกระบวนการปกติที่ใช้ในการเข้าถึงระบบอินเทอร์เน็ตของบริษัทแล้ว บริษัทไม่มีนโยบายที่จะติดต่อท่านเพื่อสอบถาม User ID, Password หรือข้อมูลส่วนตัวใดๆ ของท่าน ดังนั้น หากท่านพบการกระทำดังกล่าว โปรดแจ้งบริษัทที่ Call Center หมายเลขโทรศัพท์ 02-777-7564 หรือ ติดต่อหน่วยงานของบริษัทที่ท่านใช้บริการอยู่

ท่านควรเก็บ User ID และ Password ไว้เป็นความลับอย่างดีที่สุด อย่าเขียนหรือบันทึกข้อมูลดังกล่าวบนสื่อใดๆ หรือเปิดเผยข้อมูลดังกล่าวต่อบุคคลใดๆ เพื่อความมั่นใจว่าท่านจะทราบข้อมูลเหล่านี้เพียงผู้เดียวเท่านั้น บริษัทไม่มีและจะไม่มีนโยบายใดๆ ที่จะสอบถาม User ID และ Password ของท่าน หากท่านสงสัยว่า User ID และ/หรือ Password ของท่านอาจถูกเปิดเผยแก่บุคคลภายนอก หรือสูญหาย หรือถูกขโมย และได้มีการทำรายการโดยมิได้รับอนุญาต กรุณาแจ้งบริษัททันที

บริษัทจะทราบ User ID แต่ท่านจะทราบ Password ของท่านเพียงผู้เดียว บริษัทได้ให้ความสำคัญกับระบบรักษาความปลอดภัยที่เข้มงวดเพื่อให้มั่นใจได้ว่า Password ของท่านจะได้รับการป้องกันให้ปลอดภัยอย่างแท้จริง อย่างไรก็ตาม ท่านควรตระหนักถึงและปฏิบัติตามแนวทางและมาตรการดังต่อไปนี้เพื่อป้องกันและรักษาสิทธิในความเป็นส่วนตัวของท่านในการใช้บริการอิเล็กทรอนิกส์ของบริษัท

- ไม่อนุญาตให้บุคคลใดๆ เห็น Password ของท่าน ขณะที่ท่านล็อกอินเข้าเว็บไซต์ และ/หรือแอปพลิเคชันของบริษัท
- พยายามจำ Password ของท่าน และไม่บันทึก Password ของท่านไว้ในที่ใดๆ
- เปลี่ยน Password ของท่านเป็นประจำ และไม่นำ Password เดิมของท่านกลับมาใช้ใหม่
- ไม่ใช้ข้อมูลส่วนตัวเป็น Password ของท่าน ซึ่งอาจทำให้สามารถคาดเดาได้ง่าย เช่น นามสกุล หมายเลขโทรศัพท์ หรือวันเกิด เป็นต้น
- Password ต้องมีความยาวไม่ต่ำกว่า 6 ตัวอักษร โดยอาจประกอบด้วยตัวเลข หรือตัวอักษรก็ได้ และไม่ควรเป็นคำที่อยู่ในพจนานุกรม
- เปลี่ยน Password ของท่านทันทีที่ท่านสงสัยว่ามีบุคคลอื่นทราบ Password ของท่าน
- ไม่อนุญาตให้บุคคลใดๆ เข้าระบบโดยใช้ User ID และ Password ของท่าน มิฉะนั้น ท่านจะต้องรับผิดชอบต่อธุรกรรมใดๆ ก็ตามที่เกิดขึ้นจากการใช้ User ID และ Password ดังกล่าว

- ควรใช้ User ID และ Password ในเครื่องคอมพิวเตอร์ที่ส่วนตัวที่ท่านสามารถมั่นใจได้ว่าไม่มีการติดตั้งเครื่องมือหรือซอฟต์แวร์ ที่จะสามารถเรียกคืนข้อมูลหรือเปิดเผย User ID และ Password ดังกล่าว ให้แก่บุคคลอื่นได้
- ไม่ควรใช้เครื่องคอมพิวเตอร์สาธารณะ เช่น อินเทอร์เน็ตคาเฟ่ เนื่องจากอาจมีโปรแกรมบางอย่างที่ติดตั้งบนเครื่องคอมพิวเตอร์ดังกล่าว ซึ่งสามารถดักจับและเรียกคืนข้อมูลที่สำคัญของท่านได้

เทคโนโลยีเสริมสำหรับการรักษาความปลอดภัย

นอกจากมาตรการและวิธีการรักษาความปลอดภัยโดยทั่วไปที่กล่าวข้างต้นแล้ว บริษัทยังใช้เทคโนโลยีระดับสูงดังต่อไปนี้เพื่อปกป้องข้อมูลส่วนตัวของท่าน

- Intrusion Detection เป็นระบบซอฟท์แวร์ที่ใช้ตรวจสอบและดักจับการลักลอบเข้าระบบโดยไม่ได้รับอนุญาต ซึ่งบริษัทใช้ระบบที่มีประสิทธิภาพสูงสุดและมีการ Update อย่างสม่ำเสมอ
- Firewall เป็นระบบซอฟท์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่ได้รับสิทธิจากบริษัทเท่านั้นในการเข้าถึงข้อมูล โดยบริษัทใช้ระบบ Double Firewall Protection
- Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องของบริษัทที่ให้บริการจะมีการติดตั้งซอฟท์แวร์ป้องกัน Virus ที่มีประสิทธิภาพสูง ซึ่งมีการ Update อย่างสม่ำเสมอแล้ว บริษัทยังได้ติดตั้ง Scan Virus Software บนเครื่อง Server โดยเฉพาะอีกด้วย
- Secured Socket Layer (SSL.) เป็นเทคโนโลยีการเข้ารหัสสำหรับการเข้าถึงข้อมูล เพื่อป้องกันการแอบดักจับข้อมูลขณะที่มีการส่งผ่านเครือข่ายอินเทอร์เน็ต โดยเทคโนโลยีนี้จะทำให้ผู้ที่ต้องการดักจับข้อมูลไม่สามารถเข้าใจความหมายของข้อมูลที่ดักจับไปได้ นอกจากนี้ เทคโนโลยีนี้ยังใช้สำหรับการยืนยันความมีอยู่จริงของเว็บไซต์ของบริษัทได้อีกด้วย บริษัทใช้ 128 Bits SSL (SSL.128) สำหรับการส่งข้อมูล
- Data Encryption ใช้สำหรับข้อมูลที่มีความสำคัญมากๆ เช่น Password ซึ่งบริษัทมีมาตรการรักษาความปลอดภัยอย่างเข้มงวด โดยก่อนนำข้อมูลเข้าสู่ฐานข้อมูลเครื่องคอมพิวเตอร์ของบริษัท จะมีการเข้ารหัสโดยใช้ Algorithm ที่ซับซ้อน ทำให้ไม่มีผู้ใดสามารถรู้ข้อมูลสำคัญดังกล่าวได้ แม้แต่พนักงานของบริษัท
- Cookies เป็นไฟล์คอมพิวเตอร์เล็กๆ ที่จะเก็บข้อมูลที่จำเป็นในเครื่องคอมพิวเตอร์ของท่านไว้ชั่วคราวเพื่ออำนวยความสะดวกในการติดต่อสื่อสาร บริษัทตระหนักถึงความเป็นส่วนตัวของท่านเป็นอย่างดี จึงหลีกเลี่ยงการใช้ Cookies อย่างไรก็ตาม หากมีความจำเป็นต้องใช้ Cookies บริษัทจะพิจารณาอย่างรอบคอบ และตระหนักถึงความปลอดภัยและความเป็นส่วนตัวของท่านเป็นลำดับแรก
- Auto Log off ท่านควรออกจากระบบ (Log off) ทุกครั้ง หลังจากท่านได้ทำธุรกรรมผ่านบริการของบริษัทเสร็จสิ้นแล้ว กรณีที่ท่านลืมออกจากระบบ (Log off) ระบบจะทำการ Log off ให้โดยอัตโนมัติภายในเวลาที่เหมาะสมสำหรับการใช้บริการ ทั้งนี้เพื่อความปลอดภัยของท่านเอง

คำแนะนำเรื่องความปลอดภัย

แม้ว่าบริษัทจะมีมาตรฐานเทคโนโลยีและวิธีการทางด้านการรักษาความปลอดภัยอย่างสูง เพื่อป้องกันมิให้มีการเข้าถึงข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับของท่านโดยไม่ได้รับอนุญาตตามที่กล่าวข้างต้นแล้วก็ตาม แต่ก็เป็นที่ทราบกันอยู่โดยทั่วไปว่า ปัจจุบันนี้ยังไม่มีระบบรักษาความปลอดภัยใดๆ ที่จะสามารถปกป้องข้อมูลของท่านได้อย่างเด็ดขาดจากการ

ถูกจู่โจมโดยไวรัสคอมพิวเตอร์ หรือถูกเข้าถึงโดยบุคคลที่ปราศจากอำนาจได้ ดังนั้น ท่านจึงควรปฏิบัติตามมาตรการและวิธีการดังต่อไปนี้

- ระมัดระวังในการดาวน์โหลดซอฟท์แวร์ที่ให้ใช้งานได้ฟรี (freeware) ผ่านอินเทอร์เน็ต และควรตรวจสอบที่อยู่ของเว็บไซต์ให้ถูกต้องก่อนล็อกอินเข้าใช้บริการเพื่อป้องกันการเข้าเว็บไซต์ที่ถูกปลอมแปลง
- ควรติดตั้งซอฟท์แวร์ตรวจสอบไวรัสบนเครื่องคอมพิวเตอร์ส่วนตัวของท่านและควร update อย่างสม่ำเสมอ
- ติดตั้งซอฟท์แวร์ประเภท personal firewall เพื่อป้องกันเครื่องคอมพิวเตอร์จากการจู่โจมของผู้ไม่ประสงค์ดี เช่น Cracker หรือ Hacker
- ควรติดตามข่าวสารเกี่ยวกับคอมพิวเตอร์ให้ทันสมัยอยู่เสมอ
- ควรตรวจสอบสถานะทางการเงินอย่างสม่ำเสมอเพื่อความปลอดภัย เช่น ยอดเงินคงเหลือ วันที่ทำรายการ เป็นต้น
- ควรลงชื่อออกจากระบบ (sign off) หลังจากทำธุรกรรมเสร็จสิ้นแล้ว และไม่ควรละทิ้งเครื่องคอมพิวเตอร์ไว้ขณะกำลังทำธุรกรรม
- เก็บรักษาข้อมูลส่วนบุคคล ข้อมูลทางการเงิน หรือหมายเลขบัตรเครดิตไว้เป็นความลับ ข้อมูลส่วนบุคคลไม่ควรถูกเปิดเผยบนเว็บไซต์ที่ไม่ได้รับรองโดยผู้ให้บริการทางด้านความปลอดภัยอินเตอร์เน็ตที่ไว้ใจได้ (a trusted Internet security solution provider) และ
- หลีกเลี่ยงการเปิดอีเมลขยะ (junk mail)

การแก้ไขเปลี่ยนแปลงนโยบายการรักษาความปลอดภัยของข้อมูล

ท่านสามารถตรวจสอบนโยบายการรักษาความปลอดภัยของข้อมูลของบริษัทฉบับล่าสุดได้ในหน้าเว็บไซต์นี้ ทั้งนี้ บริษัทขอสงวนสิทธิในการแก้ไขเปลี่ยนแปลงนโยบายการรักษาความปลอดภัยของข้อมูลของบริษัทได้ทุกเมื่อ และบริษัทจะแจ้งให้ท่านทราบโดยเร็วหากบริษัทมีการแก้ไขเปลี่ยนแปลงนโยบายการรักษาความปลอดภัยของข้อมูลในสาระสำคัญที่กระทบสิทธิในความเป็นส่วนตัวของท่าน

การติดต่อสื่อสารกับบริษัท

กรณีท่านต้องการความช่วยเหลือจากบริษัท ไม่ว่าในกรณีเกี่ยวกับข้อมูลเพิ่มเติม ความผิดพลาด ข้อสงสัยของการเคลื่อนไหวบัญชีหรือธุรกรรมใดๆ ที่เกิดขึ้นโดยไม่ได้รับอนุญาตจากท่าน ท่านจะต้องแจ้งบริษัทโดยการติดต่อ Call Center หมายเลขโทรศัพท์ 02-777-7564 หรือส่งหนังสือมายังแผนกที่เกี่ยวข้องกับการให้บริการโดยไม่ชักช้า ทั้งนี้ ท่านจะต้องแจ้งรายละเอียดดังต่อไปนี้ให้แก่บริษัท

- ชื่อและหมายเลขบัญชีของท่าน
- จำนวนที่ผิดพลาดโดยประมาณ
- ประเภทของธุรกรรมหรือกิจกรรม รวมทั้งวันและเวลาของเหตุการณ์ดังกล่าว
- รายละเอียดของความผิดพลาดและหมายเลขอ้างอิง (reference code) (ถ้ามี) และ
- ชื่อและที่อยู่ที่สามารถติดต่อได้ รวมทั้ง Email Address (ถ้ามี)

หลังจากบริษัทได้รับข้อมูลความผิดพลาดหรือกิจกรรมที่ผิดปกติใดๆ ที่เกิดขึ้นตามที่กล่าวไว้ข้างต้น บริษัทจะดำเนินการตรวจสอบความผิดพลาดหรือความผิดปกติดังกล่าวโดยทันที และแจ้งท่านให้ทราบผลการตรวจสอบดังกล่าวโดยเร็ว

Privacy Policy

PURPLE VENTURES CO., LTD. (the “Company”), is registered in Thailand with its headquarter located at SCB Park Plaza, 22 Floor, Building 3, 19 Rutchadapisek Road, Chatuchak, Chatuchak, Bangkok 10900, and with the purpose for conducting the business of financial technology.

Respectfulness on Your Privacy Right

The Company respects your privacy right and recognizes that your expectation is to obtain the highest standard of security in entering into any transactions with the Company via the Company’s website, application and/or other channels. Therefore, your information received by the Company will principally be used pursuant to the purpose permitted by you only and the Company will proceed with rigorous measures and procedures for security purpose and prevent such information from any unauthorized use without obtaining your prior permission.

Information Collected or Retained by the Company

The Company will collect your information, which includes personal information, biometric data (such as fingerprints, face, etc.), transaction data and/or other information, whether provided by you to the Company or collected by the Company from your execution of transactions and/or from your use of services via websites, applications, call center and/or other channels, or collected by the Company from reliable sources, such as governmental authorities, group companies and/or business partners of the Company, for your benefit in executing transactions and/or using services with the Company, for providing services to you, for the purpose of the compliance with relevant laws and regulations and/or for any other purposes specified in your consent provided to the Company. The Company will keep your information secure under the Company’s security measures.

Use of Your Information

The Company will use your information in connection with your execution of transactions and/or your use of services, for providing services to you, and for any other purposes specified in your consent provided to the Company, which includes for the purpose of data analysis, offering, giving, using and/or improving any products and/or services of the Company. In addition, the Company may use your information to perform any contractual obligations between the Company and you and to comply with the relevant laws and regulations of governmental authorities or regulatory body.

Disclosure of Information to Third Party

You have privacy right over your information. The Company will disclose your information to third parties under the following circumstances:

- the disclosure of information is made to the Company's authorized officers and group companies, including the Company's auditors or external auditors, financial institution and/or any third persons which are the Company's partner of contract or having the relationship with the Company, and/or Cloud Computing service providers, in Thailand or overseas.
- the disclosure of such information is for the purpose of executing the transaction and/or using services required by you;
- the Company is legally compelled or required to disclose such information for any investigation or legal proceeding;
- the disclosure of such information is made in compliance with any laws, orders or instructions of any governmental authorities or regulatory body; or
- the Company has obtained consent or permission from you to disclose such information to such person.

General Security Measures and Procedures

Rigid security system is applied by the Company in order to protect your information from being accessed without your permission. Further to normal process required for internet access of the Company's system, the Company does not have policy to contact you directly for inquiry of your User ID, Password, account number or your personal information. Hence, if you detect or spot any of such actions other than normal process needed to be rendered for your access to the Company's system via Internet, please inform the Company at Call Center at +662-777-7564 or at the Company's division in charge of such service provision.

You should keep your User ID and Password at utmost confidential. Please do not write them down or record them in or on any media or disclose them to any person(s) in order to ensure you that you are the only person knowing your User ID and Password. The Company does not and will not have any policy to query you for them. If you are in doubt that your User ID and/or Password may have been disclosed to any third person or lost or stolen and that there were any transactions executed without your authorization, please notify the Company promptly.

The Company knows your User ID but only you know your Password. Strict security system is focused on by the Company to ensure that your Password is truly and well protected. You, however, should be aware of the following guidelines and comply with these recommended measures in order to protect and maintain your privacy rights in connection with your using of the Company's electronic services:

- do not allow any person to see your Password when you are logging in the Company's website or applications;
- memorize your Password and do not record it on any place;
- change your Password regularly and do not re-use your recent Password;
- do not use any of your personal information as Password which may be guessed easily; such as, family name, telephone number, date of birth, etc.;
- at least 6 characters are required to identify your Password, each of which could either be a number or a letter, and any words contained in the dictionaries should not be used as your Password;
- do change your Password immediately upon your uncertainty as to whether your Password is known by any other person(s) or not;
- do not allow or authorize anyone to access the system by using your User ID and Password as you will have to be responsible for all actions and transactions executed by using those User ID and Password;
- use your User ID and Password with your private computer on which you may rely and be able to ensure that there is no equipment or software installed on it that could retrieve or disclose such User ID and Password to other person(s); and
- public computers are not recommended for use; such as, computers in any Internet Cafes, since there might be some computer program installed on those computers that could detect and retrieve your material information.

Additional Technology Used for Security

In addition to general security measures and procedures stated above, the Company also employs the following leading edge technologies to protect your private information:

- Intrusion Detection: Intrusion Detection is a system software used for checking up and detecting any intrusion into the system without authorization. The most efficient intrusion detection system is employed by the Company and such system is regularly updated.
- Firewall: Firewall is a software system that will allow only the person authorized by the Company to access the information. In this regard, Double Firewall Protection is employed by the Company.
- Scan Virus: In addition to high efficient scan virus software installed onto all computers of the Company which has been regularly updated), Scan Virus Software for the server is also specifically installed.
- Secured Socket Layer ("SSL"): SSL is an encryption technology for information access. This encryption technology is applied in order to prevent any information from being detected while transmitted via Internet. By using this technology, any person wishing to detect or grasp information will not be able to understand the information detected or grasped. Moreover, this technology is used for confirmation as to the existing of the Company's website. The Company uses 128 Bits Secured Socket Layer for transferring data.

- Data Encryption: Data Encryption is employed in respect of vital information; such as, Password which is the information on where stringent security is concentrated by the Company. Complex algorithm is always used prior to transferring those data into the Company's databases. In this way, there will be no person knowing such vital information, including the Company's officers.
- Cookies: Cookies are small computer files that temporarily collect necessary information in your personal computer in order to facilitate and expedite your communication. The Company recognizes your privacy right; therefore, the Company tries to avoid using Cookies. If the Company deems that using Cookies is necessary in some certain aspects, due care in using Cookies will be rendered, and your security and privacy right are first priority of the Company.
- Auto Log Off: You should log off every time when you have completed your transactions via the Company's services. Should you forget to log off, the system will, for your security, be automatically logged off within an appropriate period of time for each use of the services.

Security Tips

Although high security standards, technologies and procedures are employed by the Company to help unauthorized access to your private or confidential information as discussed above, it is envisaged by everyone that there is currently no security measure that could absolutely prevent your information from being attacked by computer virus or worm or being accessed by unauthorized persons. Therefore, the Company recommends that the following procedures should also be observed and followed:

- be careful when download freeware via the Internet. Always check the address of the website that you enter before login to prevent accessing to false website;
- anti-virus software should always be installed on your personal computer and be updated regularly;
- personal firewall software should be installed for protection against any crackers or hackers;
- keep yourselves updated in respect of computer news;
- check your financial status regularly for security purpose; such as, account balance, transaction date, etc.;
- always sign off the system after completing your transaction. Do not leave your computer unattended during the transaction;
- keep your personal information, financial status or credit card number confidential. Personal information should not be disclosed on websites that are not certified by a trusted Internet security solution provider; and
- avoid opening Junk mail.

Changes to this Privacy Policy

You can access to the latest Privacy Policy of the Company via this website. The Company reserves its rights to make any changes to this Privacy Policy at any time. The Company shall inform you as soon as possible, in case the Company has made any substantial change that may affect to your privacy right.

Communication with the Company

If you want any assistance from the Company regardless of whether such assistance is required in respect of any additional information, any errors, any doubts of your account movement, or any transactions previously executed without your permission, you yourselves shall have to inform the Company by contacting call center at +662-777-7564 or by writing a letter to the Company's department by which the relevant service is being or was previously provided without any delay. In connection with this, you shall have to provide the Company with the following details:

- your name and account number;
- estimated amount of errors;
- type of transaction or activity, including the date and time of occurrence thereof;
- details of errors and reference code (if any); and
- your reachable contact name and address, including your e-mail address (if any).

After the Company receives information of any errors or irregular activity incurred as stated above, the Company will investigate such error or irregularity promptly and inform you the result of such investigation as soon as possible.