นโยบายการรักษามั่นคงปลอดภัยเว็บไซต์ของ (ชื่อหน่วยงาน/เว็บไซต์)

Website Security Policy of (Organization/ Website)

จัดทำเมื่อวันที่.....

มาตรการ และวิธีการรักษาความมั่นคงปลอดภัยเว็บไซต์

(หน่วยงาน/เว็บไซต์) ได้ตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยเว็บไซต์ เพื่อปกป้องข้อมูลของผู้ใช้บริการจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล จึงได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยเว็บไซต์ โดยใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลขั้น สูง ด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ 128 bits (128-bits Encryption) เพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้ง ที่มีการทำ ธุรกรรมทางการเงินผ่านเครือข่ายอินเทอร์เน็ตของ (หน่วยงาน/เว็บไซต์) ทาให้ผู้ที่ดักจับข้อมูลระหว่างทางไม่ สามารถนำข้อมูลไปใช้ต่อได้ โดยจะใช้การเข้ารหัสเป็นหลักในการรักษาความปลอดภัยของข้อมูล โดย ผู้ใช้บริการสามารถสังเกตได้จากชื่อโพรโทคอลที่เป็น https://

เทคโนโลยีเสริมที่นำมาใช้ในการรักษาความมั่นคงปลอดภัย

นอกจากมาตรการ และวิธีการรักษาความมั่นคงปลอดภัยโดยทั่วไปที่กล่าวข้างต้นแล้ว (หน่วยงาน/เว็บไซต์) ยังใช้เทคโนโลยีระดับสูงดังต่อไปนี้เพื่อปกป้องข้อมูลส่วนตัวของท่าน

1. Firewall เป็นระบบซอฟท์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่ (หน่วยงาน/เว็บไซต์) อนุมัติเท่านั้นจึงจะผ่าน Firewall เพื่อเข้าถึงข้อมูลได้
2. Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการจะมีการติดตั้ง Software ป้องกัน Virus ที่มีประสิทธิภาพสูงและ Update อย่างสม่ำเสมอแล้ว (หน่วยงาน/เว็บไซต์) ยัง ได้ติดตั้ง Scan Virus Software บนเครื่อง Server โดยเฉพาะอีกด้วย
3. Cookies เป็นไฟล์คอมพิวเตอร์เล็กๆ ที่จะทาการเก็บข้อมูลชั่วคราวที่จาเป็น ลงในเครื่อง คอมพิวเตอร์ของผู้ขอใช้บริการ เพื่อความสะดวกและรวดเร็วในการติดต่อสื่อสาร อย่างไร ก็ตาม (หน่วยงาน/เว็บไซต์) ตระหนักถึงความเป็นส่วนตัวของ ผู้ใช้บริการเป็นอย่างดี จึง หลีกเลี่ยงการใช้ Cookies แต่ถ้าหากมีความจาเป็น ต้องใช้ Cookies บริษัทจะพิจารณาอย่าง รอบคอบ และตระหนักถึงความปลอดภัย และความเป็นส่วนตัวของผู้ขอรับบริการเป็นหลัก
4. Auto Log off ในการใช้บริการของ (หน่วยงาน/เว็บไซต์) หลังจากเลิกการใช้งานควร Log off ทุกครั้ง กรณีที่ผู้ใช้บริการลืม Log off ระบบจะทาการ Log off ให้โดยอัตโนมัติภายในเวลาที่ เหมาะสมของแต่ละบริการ ทั้งนี้เพื่อความปลอดภัยของผู้ใช้บริการเอง

ข้อแนะนาเกี่ยวกับการรักษาความมั่นคงปลอดภัย

แม้ว่า (หน่วยงาน/เว็บไซต์) จะมีมาตรฐานเทคโนโลยีและวิธีการทางด้านการรักษาความปลอดภัยอย่างสูง เพื่อช่วยมิให้มีการเข้าสู่ข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับของท่านโดยปราศจากอำนาจตามที่กล่าวข้างต้นแล้วก็ตาม แต่ก็เป็นที่ทราบกันอยู่โดยทั่วไปว่า ปัจจุบันนี้ยังมิได้มีระบบ รักษาความปลอดภัยใดๆ ที่จะสามารถปกป้องข้อมูลของท่านได้อย่างเด็ดขาดจากการถูกทำลายหรือถูกเข้าถึงโดยบุคคลที่ปราศจากอำนาจได้ ดังนั้นท่านจึงควรปฏิบัติตามข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ด้วย คือ

1. ระมัดระวังในการ Download Program จาก Internet มาใช้งาน ควรตรวจสอบ Address ของเว็บไซต์ให้ถูกต้องก่อน Login เข้าใช้บริการเพื่อป้องกันกรณีที่มีการปลอมแปลงเว็บไซต์
2. ควรติดตั้งระบบตรวจสอบไวรัสไว้ที่เครื่องและพยายามปรับปรุงให้โปรแกรม ตรวจสอบไวรัสในเครื่องของท่านมีความทันสมัยอยู่เสมอ
3. ติดตั้งโปรแกรมประเภท Personal Firewall เพื่อป้องกันเครื่องคอมพิวเตอร์ จากการจู่โจมของผู้ไม่ประสงค์ดี เช่น Cracker หรือ Hacker