

**นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ของ กรมคุ้มครองสิทธิและเสรีภาพ**  
**Website Security Policy of Rights and Liberties Protection Department**  
จัดทำเมื่อวันที่ 00 เมษายน 2559

**มาตรการ และวิธีการรักษาความมั่นคงปลอดภัยเว็บไซต์**

กรมคุ้มครองสิทธิและเสรีภาพ ได้ตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยเว็บไซต์ เพื่อปกป้อง ข้อมูลของผู้ใช้บริการจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีความซื่อสัตย์ในการเข้าถึง ข้อมูล จึงได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยเว็บไซต์ โดยใช้มาตรฐานการรักษาความปลอดภัยของ ข้อมูลขั้นสูงด้วยเทคโนโลยี Secured Socket Layer(SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ ระดับ 128 bits(128-bits Encryption) เพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้งที่มีการ ทำธุรกรรมทางการเงินผ่านเครือข่ายอินเทอร์เน็ตของ กรมคุ้มครองสิทธิและเสรีภาพ ทำให้ผู้ที่ดักจับข้อมูล ระหว่างทางไม่สามารถนำข้อมูลไปใช้ต่อได้ โดยจะใช้การเข้ารหัสเป็นหลักในการรักษาความปลอดภัยของ ข้อมูล โดยผู้ให้บริการสามารถสังเกตได้จากชื่อโปรโตคอลที่เป็น <https://www.rlpd.go.th/rlpdnew>

**เทคโนโลยีเสริมที่นำมาใช้ในการรักษาความมั่นคงปลอดภัย**

นอกจากมาตรการ และวิธีการรักษาความมั่นคงปลอดภัยโดยทั่วไปที่กล่าวข้างต้นแล้ว กรมคุ้มครอง สิทธิและเสรีภาพ ยังใช้เทคโนโลยีระดับสูงดังต่อไปนี้เพื่อปกป้องข้อมูลส่วนตัวของท่าน

– Firewall เป็นระบบซอฟต์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่ กรมคุ้มครองสิทธิ และเสรีภาพ อนุมัติเท่านั้นจึงจะผ่าน Firewall เพื่อเข้าถึงข้อมูลได้

– Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการจะมีการติดตั้ง Software ป้องกัน Virus ที่มีประสิทธิภาพสูงและ Update อย่างสม่ำเสมอแล้ว กรมคุ้มครองสิทธิและเสรีภาพ ยังได้ ติดตั้ง Scan Virus Software บนเครื่อง Server โดยเฉพาะอีกด้วย

– Cookies เป็นไฟล์คอมพิวเตอร์เล็กๆ ที่จะทำการเก็บข้อมูลชั่วคราวที่จำเป็น ลงในเครื่อง คอมพิวเตอร์ของผู้ใช้บริการ เพื่อความสะดวกและรวดเร็วในการติดต่อสื่อสาร อย่างไรก็ตาม กรมคุ้มครอง สิทธิและเสรีภาพ ตระหนักถึงความเป็นส่วนตัวของผู้ใช้บริการเป็นอย่างดี จึงหลีกเลี่ยงการใช้ Cookies แต่ถ้า หากมีความจำเป็นต้องใช้ Cookies กรมจะพิจารณาอย่างรอบคอบ และตระหนักถึงความปลอดภัย และความ เป็นส่วนตัวของผู้รับบริการเป็นหลัก

– Auto Log off ในการใช้บริการของ กรมคุ้มครองสิทธิและเสรีภาพ หลังจากเลิกการใช้งาน ควร Log off ทุกครั้ง กรณีที่ผู้ให้บริการลืม Log off ระบบจะทำการ Log off ให้โดยอัตโนมัติภายในเวลาที่ เหมาะสมของแต่ละบริการ ทั้งนี้เพื่อความปลอดภัยของผู้ใช้บริการเอง

**ข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัย**

แม้ว่า กรมคุ้มครองสิทธิและเสรีภาพ จะมีมาตรฐานเทคโนโลยีและวิธีการทางด้านการรักษาความ ปลอดภัยอย่างสูง เพื่อช่วยมิให้มีการเข้าสู่ข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับของท่านโดยปราศจากอำนาจ ตามที่กล่าวข้างต้นแล้วก็ตาม แต่ก็เป็นที่ทราบกันอยู่โดยทั่วไปว่า ปัจจุบันนี้ยังมิได้มีระบบรักษาความปลอดภัย ใดๆ ที่จะสามารถปกป้องข้อมูลของท่านได้อย่างเด็ดขาดจากการถูกทำลายหรือถูกเข้าถึงโดยบุคคลที่ปราศจาก อำนาจ ได้ ดังนั้นท่านจึงควรปฏิบัติตามข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ด้วยคือ

- ระวังระวังในการ Download Program จาก Internet มาใช้งาน ควรตรวจสอบ Address ของเว็บไซต์ให้ถูกต้องก่อน Login เข้าใช้บริการเพื่อป้องกันกรณีที่มีการปลอมแปลงเว็บไซต์
- ควรติดตั้งระบบตรวจสอบไวรัสไว้ที่เครื่องและพยายามปรับปรุงให้โปรแกรมตรวจสอบไวรัสในเครื่องของท่านมีความทันสมัยอยู่เสมอ
- ติดตั้งโปรแกรมประเภท Personal Fire wall เพื่อป้องกันเครื่องคอมพิวเตอร์จากการจู่โจมของผู้ไม่ประสงค์ดี เช่น Cracker หรือ Hacker