นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ของกระทรวงยุติธรรม

Website Security Policy of Ministry of Justice

มาตรการ และวิธีการรักษาความมั่นคงปลอดภัยเว็บไซต์

กระทรวงยุติธรรม ได้ตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยเว็บไซต์ เพื่อปกป้องข้อมูลของผู้ใช้บริการจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล จึงได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยเว็บไซต์ โดยใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลขั้นสูงด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ ๑๒๘ bits (๑๒๘-bits Encryption) เพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้ง ที่มีการทำธุรกรรมทางการเงินผ่านเครือข่ายอินเทอร์เน็ตของกระทรวงยุติธรรม ทำให้ผู้ที่ดักจับข้อมูลระหว่างทางไม่สามารถนำข้อมูลไปใช้ต่อได้ โดยจะใช้การเข้ารหัสเป็นหลักในการรักษาความปลอดภัยของข้อมูล โดยผู้ใช้บริการสามารถสังเกตได้จากชื่อโปรโตคอลที่เป็น https://

เทคโนโลยีเสริมที่นำมาใช้ในการรักษาความมั่นคงปลอดภัย

นอกจากมาตรการ และวิธีการรักษาความมั่นคงปลอดภัยโดยทั่วไปที่กล่าวข้างต้นแล้ว กระทรวงยุติธรรมยังใช้เทคโนโลยีระดับสูงดังต่อไปนี้เพื่อปกป้องข้อมูลส่วนตัวของท่าน

– Firewall เป็นระบบซอฟท์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่กระทรวงยุติธรรมอนุมัติเท่านั้นจึงจะผ่าน Fire Wall เพื่อเข้าถึงข้อมูลได้

– Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการจะมีการติดตั้ง Software ป้องกัน Virus ที่มีประสิทธิภาพสูงและ Update อย่างสม่ำเสมอแล้ว กระทรวงยุติธรรมยังได้ติดตั้ง Scan Virus Software บนเครื่อง Server โดยเฉพาะอีกด้วย

– Auto Log off ในการใช้บริการของกระทรวงยุติธรรม หลังจากเลิกการใช้งานควร Log off ทุกครั้ง กรณีที่ผู้ใช้บริการลืม Log off ระบบจะทำการ Log off ให้โดยอัตโนมัติภายในเวลาที่เหมาะสมของแต่ละบริการ ทั้งนี้เพื่อความปลอดภัยของผู้ใช้บริการเอง

– IPS (Intrusion Prevention System) คือ Software หรือ hardware ที่ได้รับการออกแบบมาเพื่อให้ตรวจสอบการบุกรุกโดยจะทำงานคล้ายๆกับ IDS แต่จะมีคุณสมบัติพิเศษในการจู่โจมกลับหรือ หยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ไม่จำเป็นต้นอาศัยโปรแกรมหรือ hardware ตัวอื่นๆ

– Proxy Server คือเครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการต่างๆ แทนเครื่องเซิร์ฟเวอร์จริงๆ ที่ตั้งอยู่ในอินเตอร์เน็ต ซึ่งหน้าที่สำหรับเก็บข้อมูลที่ผู้ใช้บริการได้เรียกข้อมูลมาจากอินเตอร์เน็ต โดยผ่านทาง web browser ทำให้ผู้ใช้บริการรายต่อไปที่ต้องการค้นหาข้อมูลเดิมซ้ำกับที่มีผู้อื่นเรียกใช้บริการไว้ สามารถที่จะเรียกดูข้อมูลจากเครื่องแม่ข่าย Proxy Server ได้โดยตรง โดยไม่ต้องออกไปค้นหาข้อมูลจากข้างนอก

– WAF (Web Application Firewall) คือ อุปกรณ์สำหรับป้องกันเว็บแอพพลิเคชันที่ถูกติดตั้งด้านหน้า Web Servers เพื่อป้องกันการโจมตี, ติดตามการใช้งาน และเก็บ Log ทั้งเว็บที่ใช้งานภายใน และเปิดให้ผู้อื่น

เข้าถึงได้ นอกจากนี้ยังสามารถทำงานร่วมกับเทคโนโลยีด้านความปลอดภัยอื่นๆ เช่น โซลูชันสแกนช่องโหว่, ป้องกัน DDoS, ตรวจจับ Fraud และป้องกันระบบฐานข้อมูล ซึ่งบางทีอาจจะมีการเพิ่มฟังก์ชันเร่งประสิทธิภาพ เช่น การทำ Caching หรือพิสูจน์ตัวตน เป็นต้น

– Mail Gateway คือระบบที่ใช้กรอง Email ก่อนที่จะถูกส่งเข้ามายัง Mail Server หรือส่งออกจาก Mail Server ไปยังปลายทาง การทำงานของ Mail Gateway จะมีระบบในการตรวจสอบ Spam Mail, Virus และ Malware ที่แฝงมากับ Email ซึ่งถ้าตลอดเจอก็จะทำการ reject หรือ กักไว้ Quarantine ซึ่งช่วยทำให้เหลือแต่ Email ที่ใช้งานจริง ส่งต่อไปยัง Mail Server และยังช่วยลด Load การทำงาน รวมถึงพื้นที่จัดเก็บ Email ของ Mail Server ด้วย

ข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัย

แม้ว่า กระทรวงยุติธรรมจะมีมาตรฐานเทคโนโลยีและวิธีการทางด้านการรักษาความปลอดภัยอย่างสูง เพื่อช่วยมิให้มีการเข้าสู่ข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับของท่าน โดยปราศจากอำนาจตามที่กล่าวข้างต้นแล้วก็ตาม แต่ก็เป็นที่ทราบกันอยู่โดยทั่วไปว่า ปัจจุบันนี้ยังมิได้มีระบบ รักษาความปลอดภัยใด ๆ ที่จะสามารถปกป้องข้อมูลของท่านได้อย่างเด็ดขาดจากการถูกทำลายหรือถูกเข้าถึงโดยบุคคลที่ปราศจากอำนาจได้ ดังนั้นท่านจึงควรปฏิบัติตามข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ด้วยคือ

– ระมัดระวังในการ Download Program จาก Internet มาใช้งาน ควรตรวจสอบ Address ของเว็บไซต์ให้ถูกต้องก่อน Login เข้าใช้บริการเพื่อป้องกันกรณีที่มีการปลอมแปลงเว็บไซต์

– ควรติดตั้งระบบตรวจสอบไวรัสไว้ที่เครื่องและพยายามปรับปรุงให้โปรแกรม ตรวจสอบไวรัสในเครื่องของท่านมีความทันสมัยอยู่เสมอ

– ติดตั้งโปรแกรมประเภท Personal Firewall เพื่อป้องกันเครื่องคอมพิวเตอร์ จากการจู่โจมของผู้ไม่ประสงค์ดี เช่น Cracker หรือ Hacker