นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์
สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
จัดทำขึ้นเมื่อ ปี พ.ศ. 2559

1. มาตรการ และวิธีการรักษาความมั่นคงปลอดภัยเว็บไซต์

สศช. ได้ตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยเว็บไซต์ เพื่อปกป้องข้อมูลของผู้ใช้บริการจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีสิทธิในการเข้าถึงข้อมูล โดยได้ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สศช.พ.ศ. 2558 เพื่อป้องกันปัญหาหรือภัยคุกคามต่างๆ ที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของ สศช.

2. เทคโนโลยีเสริมที่นำมาใช้ในการรักษาความมั่นคงปลอดภัย

สศช. ได้ใช้เทคโนโลยีต่าง ๆ สำหรับการรักษาความมั่นคงปลอดภัยเว็บไซต์ เพื่อปกป้องข้อมูลส่วนตัวของผู้ใช้บริการ ดังต่อไปนี้

- อุปกรณ์ Firewall ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่ สศช. อนุญาตเท่านั้นจึงจะผ่าน Firewall เพื่อเข้าถึงข้อมูลได้
- โปรแกรม Scan Virus เครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการของ สศช. มีการติดตั้งโปรแกรมป้องกัน Virus ที่มีประสิทธิภาพสูงและ Update อย่างสม่ำเสมอ
- Cookies เป็นไฟล์คอมพิวเตอร์เล็ก ๆ ที่จะทำการเก็บข้อมูลชั่วคราวที่จำเป็นลงในเครื่องคอมพิวเตอร์ของผู้ขอใช้บริการ เพื่อความสะดวกและรวดเร็วใน การติดต่อสื่อสารอย่างไรก็ตาม สศช. ตระหนักถึงความเป็นส่วนตัวของ ผู้ใช้บริการเป็นอย่างดี จึงหลีกเลี่ยงการใช้ Cookies แต่ถ้าหากมีความจำเป็นต้องใช้ Cookies สศช. จะพิจารณาอย่างรอบคอบ และตระหนักถึงความปลอดภัย และความเป็นส่วนตัวของผู้ขอรับบริการเป็นหลัก

3. ข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัย

แม้ว่า สศช. จะมีมาตรการทางเทคโนโลยี และวิธีการทางด้านการรักษาความปลอดภัยอย่างสูงสำหรับเว็บไซต์ เพื่อช่วยให้มีการเข้าใช้งานเว็บไซต์ที่มั่นคงปลอดภัยแล้วก็ตาม แต่ก็เป็นที่ทราบกันอยู่โดยทั่วไปว่า ปัจจุบันนี้ยังมิได้มีระบบรักษาความปลอดภัยใด ๆ ที่จะสามารถปกป้องข้อมูลของผู้ใช้บริการได้อย่างเด็ดขาดจากการถูกทำลายหรือถูกเข้าถึงโดยบุคคลที่ปราศจากสิทธิได้ ดังนั้นผู้ใช้บริการจึงควรปฏิบัติตามข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัย ดังต่อไปนี้

- ระมัดระวังในการ Download Program จาก Internet มาใช้งาน ควรตรวจสอบ Address ของเว็บไซต์ให้ถูกต้องก่อน Login เข้าใช้บริการเพื่อป้องกันกรณีที่มีการปลอมแปลงเว็บไซต์
- ควรติดตั้งโปรแกรมป้องกันไวรัสไว้ที่เครื่อง และพยายามปรับปรุงให้โปรแกรม ตรวจสอบไวรัสในเครื่องของผู้ใช้บริการมีความทันสมัยอยู่เสมอ
- ติดตั้งโปรแกรมประเภท Personal Firewall เพื่อป้องกันเครื่องคอมพิวเตอร์ จากการจู่โจมของผู้ไม่ประสงค์ดี เช่น Cracker หรือ Hacker เป็นต้น
