นโยบายการรักษาความมั่นคงปลอดภัยของเว็บไซต์

ระบบ Labsafety ติดตั้งบน Virtual Machine (VM) ผ่านระบบคลาวด์กลางภาครัฐ Government Data Center and Cloud service (GDCC) มีความปลอดภัยและมีเสถียรภาพสูง ได้รับการรับรองมาตรฐาน ISO 27001, ISO 20000 และ CSA STAR รองรับการเชื่อมต่อเครือข่าย Public, Private และ GIN โดยมีทีมงานของ GDCC ดูแลระบบตลอด 24 ชั่วโมง

- **ระบบความปลอดภัยของ Labsafety ภายใต้นโยบาย GDCC**

1. Firewall Protection ระบบการป้องกันการบุกรุกเครือข่าย (Firewall) ให้กับระบบ Labsafety ซึ่งใช้งานอยู่บนระบบ GDCC การป้องกันนี้ ป้องกันการโจมตีหรือการ Hack เว็บไซต์ หรือ Web Application ของหน่วยงานในลักษณะของ customized rule Firewall และ WAF (Web Application Firewall)

2. Anti-Virus ระบบโปรแกรมการป้องกันไวรัสและมัลแวร์ (Anti-Virus) ให้กับระบบ Labsafety ซึ่งใช้งานอยู่บนระบบ GDCC โดยมีการอัพเดตฐานข้อมูล Virus/Malware อย่างสม่ำเสมอ และหากมีการ upload ไฟล์ที่มี Virus/Malware เข้าสู่ระบบ ระบบจะทำการบล็อกการอัปโหลดอัติโนมัติ

3. DDoS Protection ระบบป้องกันการโจมตีประเภท DDoS (DDoS Protection) ให้กับระบบ Labsafety ซึ่งใช้งานบนระบบ GDCC เพื่อป้องกันจากการถูกโจมตีในรูปแบบต่าง ๆ เช่น DNS Water Torture, Burst Attack, Zeros Day, Botnet หรือ Flood Attacks โดยเมื่อระบบตรวจพบว่ามีการโจมตีที่จะทำการ terminated การโจมตีทิ้ง ทำให้ระบบ Labsafety ปลอดภัย และสามารถใช้งานได้ต่อเนื่องได้

อ้างอิง : https://gdcc.onde.go.th/gdcc-service/

- **มาตรการ และวิธีการรักษาความมั่นคงปลอดภัยเว็บไซต์**

Labsafety ได้ตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยเว็บไซต์ เพื่อปกป้องข้อมูลของผู้ใช้บริการจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล จึงได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยเว็บไซต์ โดยใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลชั้นสูง ด้วยเทคโนโลยี Secured Socker Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ 128 bits (128-bits Encryption) เพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้งที่มีการทำธุรกรรมทางการเงินผ่านเครือข่ายอินเทอร์เน็ตของสำนักงานการวิจัยแห่งชาติ ทำให้ผู้ที่ถูกจับข้อมูลระหว่างทางไม่สามารถนำข้อมูลไปใช้ต่อได้ โดยจะใช้การเข้ารหัสเป็นหลักในการรักษาความปลอดภัยของข้อมูล โดยผู้ใช้บริการสามารถสังเกตได้จากชื่อโปรโตคอลที่เป็น https://

- **เทคโนโลยีเสริมที่นำมาใช้ในการรักษาความมั่นคงปลอดภัย **

นอกจากมาตรการ และวิธีการรักษาความมั่นคงปลอดภัยโดยทั่วไปที่กล่าวข้างต้นแล้ว สำนักงานการวิจัยแห่งชาติ ยังใช้เทคโนโลยีระดับสูงดังต่อไปนี้เพื่อปกป้องข้อมูลส่วนตัวของท่าน

1. Firewall เป็นระบบซอฟต์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่สำนักงานการวิจัยแห่งชาติอนุมัติเท่านั้น จึงจะผ่าน Fire Wall เพื่อเข้าถึงข้อมูลได้

2. Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการจะมีการติดตั้ง Software ป้องกัน Virus ที่มีประสิทธิภาพสูง และ Update อย่างสม่ำเสมอแล้ว สำนักงานการวิจัยแห่งชาติยังได้ติดตั้ง Scan Virus Software บนเครื่อง Server โดยเฉพาะอีกด้วย

3. Cookies เป็นไฟล์คอมพิวเตอร์เล็กๆที่จะทำการเก็บข้อมูลชั่วคราวที่จำเป็นลงในเครื่องคอมพิวเตอร์ของผู้ขอใช้บริการ เพื่อความสะดวกและรวดเร็วในการติดต่อสื่อสาร อย่างไรก็ตามสำนักงานการวิจัยแห่งชาติตระหนักถึงความเป็นส่วนตัวของผู้ใช้บริการเป็นอย่างดี จึงหลีกเลี่ยงการใช้ Cookies แต่ถ้าหากมีความจำเป็นต้องใช้ Cookies สำนักงานการวิจัยแห่งชาติจะพิจารณาอย่างรอบคอบ และตระหนักถึงความปลอดภัย และความเป็นส่วนตัวของผู้ขอรับบริการเป็นหลัก

4. Auto Log off ในการใช้บริการของสำนักงานการวิจัยแห่งชาติ หลังจากเลิกการใช้งานควร Log off ทุกครั้ง กรณีที่ผู้ใช้บริการลืม Log off ระบบจะทำการ Log off ให้โดยอัตโนมัติภายในเวลาที่เหมาะสมของแต่ละบริการ ทั้งนี้เพื่อความปลอดภัยของผู้ใช้บริการเอง

- **ข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัย **

แม้ว่าสำนักงานการวิจัยแห่งชาติจะมีมาตรฐานเทคโนโลยีและวิธีการทางด้านการรักษาความปลอดภัยอย่างสูง เพื่อช่วยมิให้มีการเข้าสู่ข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับของท่านโดยปราศจากอำนาจตามที่กล่าวข้างต้นแล้วก็ตาม แต่ก็เป็นที่ทราบกันโดยทั่วไปว่า ปัจจุบันยังมิได้มีระบบรักษาความปลอดภัยใดๆที่จะสามารถปกป้องข้อมูลของท่านได้อย่างเด็ดขาดจากการถูกทำลายหรือถูกเข้าถึงโดยบุคคลที่ปราศจากอำนาจได้ ดังนั้นท่านจึงควรปฏิบัติตามข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ด้วยคือ

1.ระมัดระวังในการ Download Program จาก Internet มาใช้งาน ควรตรวจสอบ Address ของเว็บไซต์ให้ถูกต้องก่อน Login เข้าใช้บริการเพื่อป้องกันกรณีที่มีการปลอมแปลงเว็บไซต์

2.ควรติดตั้งระบบตรวจสอบไวรัสไว้ที่เครื่องและพยายามปรับปรุงให้โปรแกรมตรวจสอบไวรัสในเครื่องของท่านมีความทันสมัยอยู่เสมอ

3.ติดตั้งโปรแกรมประเภท Personal Fire wall เพื่อป้องกันเครื่องคอมพิวเตอร์จากการจู่โจมของผู้ไม่ประสงค์ดี เช่น Cracker หรือ Hacker