

นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ของกรมทรัพยากรทางทะเลและชายฝั่ง
Website Security Policy of Department of Marine and Coastal Resources
(www.dmcr.go.th)

๑. มาตรการ และวิธีการรักษาความมั่นคงปลอดภัยเว็บไซต์

กรมทรัพยากรทางทะเลและชายฝั่ง เป็นหน่วยงานราชการที่ให้ข้อมูล ข่าวสาร และองค์ความรู้ด้านทรัพยากรทางทะเลและชายฝั่ง มีความตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยเว็บไซต์ต่อการปกป้องข้อมูลของผู้ใช้บริการจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีความซื่อสัตย์ในการเข้าถึงข้อมูล จึงได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยเว็บไซต์ โดยใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลขั้นสูง ด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ ๑๒๘ bits (๑๒๘-bits Encryption) เพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้ง ที่มีการใช้บริการข้อมูลและระบบงานผ่านเครือข่ายอินเทอร์เน็ตของกรมทรัพยากรทางทะเลและชายฝั่ง ทำให้ผู้ที่ดักจับข้อมูลระหว่างทางไม่สามารถนำข้อมูลไปใช้ต่อได้ โดยจะใช้การเข้ารหัสเป็นหลักในการรักษาความปลอดภัยของข้อมูล โดยผู้ให้บริการสามารถสังเกตได้จากชื่อโปรโตคอลที่เป็น https://

๒. เทคโนโลยีเสริมที่นำมาใช้ในการรักษาความมั่นคงปลอดภัย

นอกจากมาตรการและวิธีการรักษาความมั่นคงปลอดภัยตามที่กล่าวมาข้างต้น กรมทรัพยากรทางทะเลและชายฝั่ง ยังใช้เทคโนโลยีระดับสูงในการปกป้องข้อมูลส่วนตัวของท่าน ดังต่อไปนี้

๒.๑ Firewall เป็นระบบฮาร์ดแวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่กรมทรัพยากรทางทะเลและชายฝั่ง อนุมัติเท่านั้นจึงจะผ่าน Firewall เพื่อเข้าถึงข้อมูลได้

๒.๒ Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการจะมีการติดตั้ง Software ป้องกัน Virus ที่มีประสิทธิภาพสูงและ Update อย่างสม่ำเสมอแล้ว กรมทรัพยากรทางทะเลและชายฝั่งยังได้ติดตั้ง Scan Virus Software บนเครื่อง Server โดยเฉพาะอีกด้วย

๒.๓ Cookies เป็นไฟล์คอมพิวเตอร์เล็กๆ ที่จะทำการเก็บข้อมูลชั่วคราวที่จำเป็นลงในเครื่องคอมพิวเตอร์ของผู้ขอใช้บริการ เพื่อความสะดวกและรวดเร็วในการติดต่อสื่อสาร อย่างไรก็ตาม กรมทรัพยากรทางทะเลและชายฝั่ง ตระหนักถึงความเป็นส่วนตัวของผู้ใช้บริการเป็นอย่างดี จึงหลีกเลี่ยงการใช้ Cookies แต่ในกรณีที่มีความจำเป็นต้องใช้ Cookies กรมทรัพยากรทางทะเลและชายฝั่งจะพิจารณาอย่างรอบคอบ และตระหนักถึงความปลอดภัย และความเป็นส่วนตัวของผู้รับบริการเป็นหลัก

๒.๔ Auto Log off ในการใช้บริการของกรมทรัพยากรทางทะเลและชายฝั่ง หลังจากเลิกการใช้งานควร Log off ทุกครั้ง กรณีที่ผู้ใช้บริการลืม Log off ระบบจะทำการ Log off ให้โดยอัตโนมัติภายในเวลาที่เหมาะสมของแต่ละบริการ ทั้งนี้เพื่อความปลอดภัยของผู้ใช้บริการเอง

๓. ข้อเสนอแนะเกี่ยวกับการรักษาความมั่นคงปลอดภัย

แม้ว่า กรมทรัพยากรทางทะเลและชายฝั่ง จะมีมาตรฐานเทคโนโลยีและวิธีการทางด้านการรักษาความปลอดภัยอย่างสูง เพื่อช่วยมิให้มีการเข้าสู่ข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับของท่านโดยปราศจากอำนาจตามที่กล่าวมาข้างต้นแล้วก็ตาม อย่างไรก็ตาม ด้วยเทคโนโลยีในปัจจุบันนี้ยังไม่มียาระบบรักษาความปลอดภัยใดๆ ที่จะสามารถปกป้องข้อมูลของท่านจากการทำลายหรือถูกเข้าถึงโดยบุคคลที่ปราศจากอำนาจได้อย่างเด็ดขาด ดังนั้น ท่านจึงควรปฏิบัติตามข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัย ดังต่อไปนี้

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

๓.๒ ไม่ควร Click Banner หรือ Link ที่พยายามบังคับให้เรา Download ไฟล์ต่าง อาจจะทำให้ติดไวรัสลงเครื่องได้

๓.๓ ไม่ควรเข้าเว็บไซต์ที่แจกจ่าย Serial Key ,Crack ต่างๆ อาจจะทำให้ติดไวรัสลงเครื่องได้

๓.๔ ควรติดตั้งระบบตรวจสอบไวรัสไว้ที่เครื่องและพยายามปรับปรุงให้โปรแกรม ตรวจสอบไวรัสในเครื่องของท่านให้มีความทันสมัยอยู่เสมอ

๓.๕ ติดตั้งโปรแกรมประเภท Personal Firewall , Antivirus , Anti malicious ต่างๆ เพื่อป้องกันเครื่องคอมพิวเตอร์ จากการจู่โจมของผู้ไม่ประสงค์ดี เช่น Cracker หรือ Hacker

นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ของกรมทรัพยากรทางทะเลและชายฝั่ง ได้ผ่านการพิจารณาจากคณะกรรมการบริหารจัดการด้านเทคโนโลยีสารสนเทศ กรมทรัพยากรทางทะเลและชายฝั่ง เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของกรมฯ ต่อไป

(นายศักดิ์ดา วิเชียรศิลป์)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง CIO
กรมทรัพยากรทางทะเลและชายฝั่ง