มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ของสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม : งานบริการข้อมูลข่าวสาร

ขั้นตอน	ทรัพย์สินสารสนเทศ (information asset)	ความเสี่ยงที่สำคัญ	ระดับความเสี่ยง	มาตรการที่จำเป็น[๑]		
				เชิงองค์กร	เชิงเทคนิค	ทางกายภาพ
๑. เก็บรวบรวม	เครื่องแม่ข่ายของระบบ e-Request (https://esc.mnre.go.th/info)	เก็บข้อมูลส่วนบุคคลมากเกินความจำเป็นหรือไม่ครบถ้วน	สูง	🔒 ป้องกันโดยเก็บข้อมูลเท่าที่จำเป็นเพื่อการยืนยัน พิสูจน์ตัวตนและการติดต่อ ไม่มีการเรียกเก็บสำเนาบัตรประจำตัวประชาชนของผู้ขอข้อมูลข่าวสาร	🔒 ป้องกันโดยจัดทำ e-Form ให้มี input เท่าที่จำเป็นและต้องกรอก (required)	🔒 ป้องกันโดยจัดให้มี QR Code ของระบบ e-Request แสดง ณ จุดบริการ
		มีการเข้าถึงข้อมูลในเครื่องแม่ข่ายโดยผู้ไม่มีหน้าที่เกี่ยวข้องหรือโดยมิชอบ	สูง	🔒 ป้องกันโดยกำหนดสิทธิ Admin ๑ คน มีหน้าที่ดูแลระบบ e-Request / เก็บ username และรหัสผ่านเป็นความลับ ใช้รหัสที่คาดเดายาก / มีการพิสูจน์และยืนยันตัวตนในการเข้าใช้งาน / มีระบบตรวจสอบย้อนหลังเกี่ยวกับการเข้าใช้งาน	🔒 ป้องกันโดยใช้ระบบคลาวด์กลางภาครัฐที่มีระบบรักษาความปลอดภัยตามมาตรฐาน	🔒 ป้องกันโดยไม่อนุญาตให้บุคคลอื่นมองดูหน้าจอคอมพิวเตอร์ขณะเข้าใช้งานเครื่องแม่ข่าย
		ผู้ขอข้อมูลข่าวสารกรอกข้อมูลคลาดเคลื่อน	ปานกลาง	📝 ป้องกันโดยจัดทำและเผยแพร่คู่มือการใช้งาน / ตรวจสอบยืนยันกับข้อมูลในระบบ GDX	📝 ป้องกันโดยจัดทำคู่มือออนไลน์พร้อมคลิปวิดีโอสาธิตการใช้งาน และแสดง placeholder ใน input / ให้ผู้ขอตรวจสอบข้อมูลก่อนส่งคำขอ	-
		ระบบล่ม จากการถูกโจมตีหรือสาเหตุอื่น ๆ	สูง	⚙ เฝ้าระวังโดยตรวจสอบการทำงานและช่องโหว่ของระบบทุกวัน ⚙ รีบประสานกู้ระบบกรณีเกิดเหตุ	⚙ ป้องกันการโจมตีทางไซเบอร์ด้วย Firewall/Antivirus/Web Application Firewal/DDoS Attack	⚙ เผชิญเหตุโดยให้บริการผ่าน Backup site บนเครื่องแม่ข่ายสำรอง (http://lib.mnre.go.th/info)
	กล่องอีเมลของหน่วยงาน	อีเมลถูกเข้าถึงโดยผู้ไม่มีสิทธิ์	สูง	🔒 ป้องกันโดยกำหนดสิทธิ์ พิสูจน์ตัวตนเจ้าหน้าที่ และเปลี่ยนรหัสผ่านทุก ๙๐ วัน	🔒 ป้องกันโดยกำหนดรหัสผ่านให้คาดเดายาก	🔒 ป้องกันโดยเก็บรักษารหัสผ่านเป็นความลับ ไม่จดไว้บนกระดาษที่วางไว้บริเวณเครื่องคอมพิวเตอร์
		อีเมลล่ม หรือข้อมูลสูญหาย	สูง	⚙ ป้องกันรักษาระบบอีเมลให้ใช้งานได้ตลอดเวลา	⚙ ป้องกันการโจมตีระบบอีเมล	⚙ เผชิญเหตุโดยใช้คำขอกระดาษ ที่พิมพ์จากระบบไว้ก่อนแล้ว
		ถูกเข้าถึงโดยผู้ไม่มีหน้าที่เกี่ยวข้อง	สูง	🔒 กำหนดชั้นความลับ และปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ. ๒๕๔๔ อย่างเคร่งครัด	-	🔒 เก็บคำขอในตู้เหล็กมีกุญแจล็อค และให้นายทะเบียนข้อมูลข่าวสารลับเป็นผู้ควบคุมกุญแจ
	เอกสารคำขอ	แก้ไขคำขอ	สูง	🔒 เอกสารคำขอห้ามมีรอยลบ ขีดฆ่า ฯ หากมี ต้องมีลายมือชื่อของผู้ขอข้อมูลข่าวสารกำกับไว้ทุกแห่ง	-	🔒 จัดทำสำเนาคู่ฉบับ เก็บไว้ตรวจสอบ
		สูญหาย	สูง	⚙ จัดทำทะเบียนคุมเรื่อง	⚙ 🔒 จัดทำไฟล์ PDF ของคำขอที่มีรหัสป้องกันการเปิดไฟล์โดยมิชอบ	🔒 จัดทำสำเนาคู่ฉบับ เก็บไว้ใช้แทนกรณีต้นฉบับสูญหาย

[๑] คำนึงถึงความสามารถในการธำรงไว้ซึ่งการธำรงไว้ซึ่งความลับ (confidentiality : 🔒) ความถูกต้องครบถ้วน (integrity : 📝) และสภาพพร้อมใช้งาน (availability : ⚙)

ขั้นตอน	ทรัพย์สินสารสนเทศ (information asset)	ความเสี่ยงที่สำคัญ	ระดับความเสี่ยง	ประเภท : มาตรการ		
				เชิงองค์กร	เชิงเทคนิค	ทางกายภาพ
๒. ใช้	ระบบอีเมล	การส่งต่ออีเมลไปยังบุคคลอื่น	สูง	🔒 ชักซ้อมแนวปฏิบัติในการรับคำขอทางอีเมล ห้ามส่งต่อคำขอนั้นไปยังบุคคลหรือหน่วยงานหนึ่งหน่วยงานใด	🔒 ตรวจสอบกล่อง Forward ต้องไม่มีการส่งต่อ	-
		ถูกโจมตีโดย Hacker	สูง	⚙ ใช้ระบบอีเมลของ DGA	⚙ ใช้มาตรการของ DGA	🔒 เก็บรักษารหัสผ่านให้มิดชิด
	ระบบ e-Tracking	ใช้หมายเลขประจำตัวประชาชนของผู้ขอในการติดตามสถานะคำขอ อาจรั่วไหลไปยังบุคคลอื่น	สูง	🔒 กำหนดให้ข้อมูลหมายเลขประจำตัวประชาชนของผู้ขอเป็นข้อมูลข่าวสารลับ	🔒 เข้ารหัสหมายเลขประจำตัวประชาชนก่อนเก็บข้อมูลในเครื่องแม่ข่ายด้วย algorithm ที่ไม่มีประวัติการถูกโจมตีสำเร็จ / ปกปิดรหัสด้วยวิธี toggle	🔒 ดูแลรักษาความปลอดภัยของบริเวณห้องจัดเก็บเครื่องแม่ข่าย
		มีการแก้ไข source code ของระบบ ทำให้ข้อมูลคลาดเคลื่อน	สูง	📋 กำหนดสิทธิ์ Admin ให้มีจำนวนเพียง ๑ คน	📋 พัฒนาโปรแกรมหลังบ้านสำหรับจัดการฐานข้อมูลแทนคน (ระบบ e-Tracking Backend)	📋 เก็บสำรองข้อมูล source code ไว้ในที่ปลอดภัย
	เอกสารประกอบการประชุมคณะกรรมการข้อมูลข่าวสารของ สป.ทส.	มีการถ่ายภาพหรือแอบจัดทำสำเนาโดยกรรมการหรือเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้อง	สูง	🔒 กำหนดชั้นความลับ / ชักซ้อมแนวปฏิบัติ ห้ามกรรมการหรือเจ้าหน้าที่ถ่ายรูปหรือจัดทำสำเนาเอกสารประกอบการประชุม / จัดทำข้อความเตือนไว้ที่เอกสารทุกแผ่นทุกหน้า ห้ามเปิดเผย และใช้ในการประชุมเท่านั้น	🔒 ไม่แชร์ไฟล์เอกสารวาระการประชุมทางไลน์กลุ่มหรือไลน์ส่วนตัว	🔒 เก็บเอกสารประกอบการประชุมในที่ปลอดภัย เข้าถึงไม่ได้โดยผู้ไม่มีหน้าที่เกี่ยวข้อง
	ไฟล์นำเสนอในที่ประชุมคณะกรรมการข้อมูลข่าวสารของ สป.ทส.	ไฟล์นำเสนอในที่ประชุม รั่วไหล ภายหลังการประชุม	สูง	🔒 ชักซ้อมแนวปฏิบัติให้ลบไฟล์ใน Notebook ทันทีหลังเลิกประชุม	🔒 ไม่ upload ไฟล์เข้าสู่ระบบ internet	🔒 เก็บไฟล์ต้นฉบับในเครื่องคอมพิวเตอร์ที่ไม่เป็นสาธารณะ
	หนังสือแจ้งผลการพิจารณา	ข้อมูลส่วนบุคคลรั่วไหลในขั้นตอนการเสนอเรื่องต่อผู้บริหาร	สูง	🔒 กำหนดชั้นความลับ และปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ. ๒๕๔๔ อย่างเคร่งครัด	🔒 ไม่นำข้อมูลเข้าสู่ระบบ internet	🔒 เก็บคำขอในตู้เหล็กมีกุญแจล็อค และให้นายทะเบียนข้อมูลข่าวสารลับเป็นผู้ควบคุมกุญแจ
	ไฟล์หนังสือแจ้งผลการพิจารณา	ข้อมูลรั่วไหลจากเครื่องคอมพิวเตอร์	สูง	🔒 ห้ามมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์	🔒 กำหนดรหัสผ่านเข้าใช้เครื่องคอมพิวเตอร์ ที่คาดเดายาก และเปลี่ยนรหัสทุก ๙๐ วัน	🔒 ห้ามบุคคลอื่นเข้าใกล้บริเวณเครื่องคอมพิวเตอร์ หากจำเป็น ต้องมีเจ้าหน้าที่ดูแลอย่างใกล้ชิด

ขั้นตอน	ทรัพย์สินสารสนเทศ (information asset)	ความเสี่ยงที่สำคัญ	ระดับความเสี่ยง	ประเภท : มาตรการ		
				เชิงองค์กร	เชิงเทคนิค	ทางกายภาพ
๓. เปิดเผย	หนังสือชี้แจงข้อเท็จจริง	ข้อมูลอาจรั่วไหลในขั้นตอนการรับส่งหนังสือชี้แจงข้อเท็จจริงภายในและระหว่างหน่วยงาน	สูง	🔒 กำหนดชั้นความลับ และปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ. ๒๕๔๔ อย่างเคร่งครัด	🔒 ไม่นำข้อมูลเข้าสู่ระบบคอมพิวเตอร์	🔒 เก็บคำขอในตู้เหล็กมีกุญแจล็อคและให้นายทะเบียนข้อมูลข่าวสารลับเป็นผู้ควบคุมกุญแจ
		ทิ้งเอกสารฉบับร่าง โดยไม่มีการทำลาย	สูง	🔒 แจ้งแนวปฏิบัติให้ทำลายเอกสารฉบับร่างด้วยเครื่องทำลายเอกสาร ห้ามทิ้งโดยไม่มีการทำลาย	🔒 ใช้เครื่องย่อยกระดาษทำลายเอกสารฉบับร่างที่หมดความจำเป็น	🔒 หมั่นตรวจตรามิให้มีร่างเอกสารถูกทิ้งปะปนในถังขยะหรือร่วงหล่น
		พิมพ์ชื่อ นามสกุล ที่อยู่ ของผู้ขอข้อมูลไม่ถูกต้อง	สูง	ตรวจทานความถูกต้องของชื่อ นามสกุล ที่อยู่ ในหนังสือแจ้งผลการพิจารณาสองครั้ง (double check)	ใช้วิธีคัดลอกข้อมูลจากไฟล์เรื่องเดิมไว้บน clipboard แล้ววางในไฟล์หนังสือแจ้งผลการพิจารณา	ระวังไม่ให้นิ้วโดนปุ่มบนแป้นพิมพ์โดยไม่ตั้งใจ
	ไฟล์หนังสือชี้แจงข้อเท็จจริง	ข้อมูลรั่วไหลจากเครื่องคอมพิวเตอร์	สูง	🔒 ห้ามให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์	🔒 กำหนดรหัสผ่านเข้าใช้เครื่องคอมพิวเตอร์ ที่คาดเดายาก และเปลี่ยนรหัสทุก ๙๐ วัน	🔒 ห้ามบุคคลอื่นเข้าใกล้บริเวณเครื่องคอมพิวเตอร์ หากจำเป็นต้องมีเจ้าหน้าที่ดูแลอย่างใกล้ชิด

หมายเหตุ

๑. ต้องมีการเสริมสร้างความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย

๒. ต้องมีการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสมให้ข้าราชการ พนักงานราชการ และผู้ปฏิบัติงานที่เกี่ยวข้องกับการเข้าถึง เก็บรวบรวม เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ขอข้อมูลข่าวสาร ทราบและถือปฏิบัติ

๓. ต้องทบทวนมาตรการเมื่อมีเหตุละเมิดข้อมูลส่วนบุคคล และเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

๔. ต้องปฏิบัติตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ประวัติการแก้ไข

รุ่นเอกสาร	วันที่แก้ไข	ผู้จัดทำ	การแก้ไข
๑.๑	๑๖ กรกฎาคม ๒๕๖๗	ส่วนข้อมูลข่าวสารและบริการร่วม กองกลาง	เพิ่มติมมาตรการป้องกันการโจมตีทางไซเบอร์ของระบบ e-Request
๑.๐	๑๙ มิถุนายน ๒๕๖๗	ส่วนข้อมูลข่าวสารและบริการร่วม กองกลาง	ร่างแรก