รายงานผลการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

หน่วยรับตรวจ

กองพัฒนาระบบการประเมินผลกระทบสิ่งแวดล้อม (กพส.)

กิจกรรมที่ตรวจสอบ

ตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ.๒๕๖๕

ประเด็นการตรวจสอบ

ตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เกี่ยวกับศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม (Smart EIA Plus) ซึ่งประกอบด้วยระบบฐานข้อมูลรายงานการประเมินผลกระทบสิ่งแวดล้อม ระบบฐานข้อมูลผู้มีสิทธิจัดทำรายงานการประเมินผลกระทบสิ่งแวดล้อม ระบบฐานข้อมูลรายงานผลการปฏิบัติตามมาตรการป้องกันและแก้ไขผลกระทบสิ่งแวดล้อมและมาตรการติดตามตรวจสอบผลกระทบสิ่งแวดล้อม (รายงาน Monitor) และโมบายแอปพลิเคชัน (Smart EIA Plus)

วัตถุประสงค์ในการตรวจสอบ

๑. เพื่อให้ทราบว่าระบบการควบคุมภายใน มีความเหมาะสม เพียงพอ

๒. เพื่อให้ทราบว่าระบบฐานข้อมูล มีความมั่นคงปลอดภัย เป็นไปตามนโยบาย แผน มาตรการ แนวปฏิบัติด้านสารสนเทศของ สผ. หนังสือสั่งการ และระเบียบที่เกี่ยวข้อง

๓. เพื่อให้ทราบปัญหา อุปสรรค และเสนอแนวทางแก้ไข

ขอบเขตในการตรวจสอบ

๑. ศึกษาข้อมูลด้านระบบฐานข้อมูล และระบบงาน เบื้องต้นทั่วไป

๒. สอบทานแบบประเมินการควบคุมทั่วไป เช่น การกำหนดสิทธิการใช้งานของผู้ดูแลระบบและผู้ใช้งาน รวมถึงการมอบหมายงาน

๓. สอบทานเอกสารหลักฐานที่เกี่ยวข้อง เช่น

๓.๑ ระบบฐานข้อมูล

- คู่มือการปฏิบัติงานเกี่ยวกับระบบฐานข้อมูล ระบบงาน
- เอกสารที่เกี่ยวข้อง และสัญญาจ้างจัดทำระบบฐานข้อมูล

๔. สอบถามเจ้าหน้าที่ผู้ปฏิบัติงาน/ผู้รับผิดชอบระบบฐานข้อมูลฯ และระบบงานฯ

ระยะเวลาที่ตรวจสอบ

มิถุนายน – กรกฎาคม- ๒๕๖๕

ข้อมูลเบื้องต้น

สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม (สผ.) เป็นหน่วยงานรับผิดชอบหลัก เกี่ยวกับการประเมินผลกระทบสิ่งแวดล้อม ตามพระราชบัญญัติส่งเสริมและรักษาคุณภาพสิ่งแวดล้อมแห่งชาติ (ฉบับที่ ๒) พ.ศ.๒๕๖๑ โดย สผ. ได้ตระหนักถึงความสำคัญของการบริหารจัดการข้อมูลด้านการประเมินผลกระทบสิ่งแวดล้อม จึงได้ริเริ่มพัฒนาระบบฐานข้อมูลที่เกี่ยวข้องกับการดำเนินงานด้านการ

ประเมินผลกระทบสิ่งแวดล้อม ตั้งแต่ปี พ.ศ. ๒๕๕๖ - ๒๕๖๓ โดยได้พัฒนาศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม ประกอบด้วยระบบฐานข้อมูล และ โมบายแอปพลิเคชัน ดังนี้

๑. ระบบฐานข้อมูล จำนวน ๓ ระบบ

๑.๑. ระบบฐานข้อมูลรายงานการประเมินผลกระทบสิ่งแวดล้อม (รายงาน EIA) เป็นระบบที่เกี่ยวข้องกับกับยื่นเสนอรายงานการประเมินผลกระทบสิ่งแวดล้อมทางระบบอิเล็กทรอนิกส์ของเจ้าของโครงการหรือผู้รับมอบอำนาจ

๑.๒. ระบบฐานข้อมูลรายงานผลการปฏิบัติตามมาตรการป้องกันและแก้ไขผลกระทบสิ่งแวดล้อมและมาตรการติดตามตรวจสอบผลกระทบสิ่งแวดล้อม (รายงาน Monitor) เป็นระบบที่เกี่ยวข้องกับการเสนอรายงาน Monitor ทางระบบอิเล็กทรอนิกส์ของเจ้าของโครงการ (ผู้ดำเนินการ/ผู้ขออนุญาต)

๑.๓. ระบบฐานข้อมูลผู้มีสิทธิจัดทำรายงานการประเมินผลกระทบสิ่งแวดล้อม เป็นระบบที่เกี่ยวข้องกับการยื่นขอใบอนุญาตเป็นผู้มีสิทธิจัดทำรายงานฯ การต่ออายุใบอนุญาต การขอรับใบแทนอนุญาต ของผู้ชำนาญการ หรือ ผู้จัดทำรายงานอิสระ และนิติบุคคลผู้จัดทำรายงาน นอกจากนี้ ยังรวมถึงการขอผ่อนผัน และการขอเปลี่ยนแปลงผู้ชำนาญการหรือเจ้าหน้าที่ประจำของนิติบุคคลผู้จัดทำรายงาน

๒. โมบายแอปพลิเคชัน Smart EIA Plus จำนวน ๑ ระบบ

Smart EIA Plus เป็นแอปพลิเคชันเพื่อใช้งานค้นหาข้อมูลเกี่ยวกับข้อมูลเจ้าของโครงการที่ลงทะเบียนในระบบศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม ค้นหานิติบุคคลผู้มีสิทธิจัดทำรายงานการประเมินผลกระทบสิ่งแวดล้อม การติดตามสถานะรายงานการยื่นรายงาน/คำขอรับใบอนุญาตเป็นผู้มีสิทธิจัดทำรายงาน และแจ้งเรื่องร้องเรียน และอยู่ระหว่างการพัฒนาระบบการขอรับใบอนุญาตเป็นผู้มีสิทธิจัดทำรายงานการประเมินผลกระทบสิ่งแวดล้อม ให้สามารถยื่นคำขอ การแจ้ง และการออกใบอนุญาต/เอกสารทางราชการได้โดยวิธีการทางอิเล็กทรอนิกส์หรือการอนุมัติผ่านช่องทางอิเล็กทรอนิกส์ รวมทั้งพัฒนาระบบการเชื่อมโยงข้อมูลกับหน่วยงานที่เกี่ยวข้องกับการขอรับใบอนุญาตเป็นผู้มีสิทธิจัดทำรายงานการประเมินผลกระทบสิ่งแวดล้อม พร้อมกับการพัฒนาเว็ปไซต์ของกองพัฒนาระบบการวิเคราะห์ผลกระทบสิ่งแวดล้อม เพื่อให้สอดคล้องและเชื่อมโยงกับระบบศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม

ระบบศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม หรือ Smart EIA Plus ติดตั้งอยู่ที่ระบบคลาวด์กลางภาครัฐ : Government Data Center and Cloud service (GDCC) ซึ่งเป็นแม่ข่ายให้บริการข้อมูลของศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม ระบบศูนย์ข้อมูลฯ ดังกล่าว ลูกข่ายสามารถใช้งานระบบผ่าน ๓ ช่องทาง คือ ๑) PC Desktop หรือ Laptop ผ่านทาง Web browser ๒) Mobile Device อุปกรณ์ของเจ้าหน้าที่ หรือ ประชาชนทั่วไป ผ่านทาง Web browser และ Mobile Application ๓) Web Server แม่ข่ายจากหน่วยงานภายนอกที่เรียกใช้งานระบบศูนย์ข้อมูลฯ ผ่านทาง Partner API ซึ่ง สผ. ได้มีการเชื่อมโยงกับหน่วยงานภายนอก ได้แก่ ๑) สภาวิชาชีพวิทยาศาสตร์และเทคโนโลยี ๒) สถาบันการศึกษา ๓) กรมบัญชีกลาง ๔) กรมการปกครอง ๕) กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ๖) การนิคมอุตสาหกรรมแห่งประเทศไทย ๗) สำนักงานคณะกรรมการกำกับกิจการพลังงาน และ ๘) เชื่อมโยงข้อมูลนิติบุคคลกรมพัฒนาธุรกิจการค้า โดยใช้บริการศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐ (Government Data Exchange : GDX)

การใช้งานระบบศูนย์ข้อมูลฯ แบ่งได้ดังนี้

๑. ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย การเข้าใช้งานระบบศูนย์ข้อมูลฯ ระบบจะมีการตรวจสอบยืนยันตัวตนผ่านระบบฐานข้อมูล Active Directory ซึ่งระบบฐานข้อมูล Active Directory เป็น

แหล่งรวบรวมข้อมูลรายชื่อผู้ใช้งาน (Username) ติดตั้งอยู่ในระบบ Server ที่ สผ. เพื่อยืนยันตัวตนในการเข้าใช้งานระบบศูนย์ข้อมูลฯ

๒. ผู้ใช้งานทั่วไป สามารถลงทะเบียนผู้ใช้งานผ่านทาง Web Application ซึ่งต้องกำหนดรหัสผู้ใช้และรหัสผ่าน เพื่อเข้าใช้งานระบบ โดยสามารถเพิ่มข้อมูลส่วนตัว และแนบหลักฐานสำหรับยืนยันตัวตนของผู้ลงทะเบียน

๓. การใช้งานผ่าน Mobile Application : Smart EIA Plus ผู้ใช้งานทั่วไปสามารถค้นหาข้อมูล และติดตามสถานะรายงาน/คำขอ โดยใช้รหัสผู้ใช้ (Username) และ รหัสผ่าน (Password) ที่ลงทะเบียนไว้เพื่อยืนยันตัวตน

ผลการตรวจสอบ

๑. การตรวจสอบด้านการการควบคุมทั่วไป (IT General Control)

๑.๑ การตรวจสอบความปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental controls) พบว่ามีความเพียงพอ เหมาะสม ดังนี้

๑.๑.๑) ระบบศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม (Smart EIA Plus) ติดตั้งและทำงานบนเครื่องคอมพิวเตอร์แม่ข่ายที่ระบบคลาวด์กลางภาครัฐ : Government Data Center and Cloud service (GDCC) ซึ่งเป็นบริการของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) ดำเนินการร่วมกับบริษัท กสท โทรคมนาคม จำกัด (มหาชน) ในการรวมศูนย์การให้บริการเครื่องคอมพิวเตอร์เสมือน (Virtual Machine หรือ VM) สำหรับหน่วยงานภาครัฐที่มีความมั่นคงปลอดภัยและมีเสถียรภาพสูง ได้รับการรับรองมาตรฐาน ISO 27001 (มาตรฐานความมั่นคงปลอดภัยข้อมูลสารสนเทศ) , ISO 20000 (มาตรฐานด้านการบริหารบริการเทคโนโลยีสารสนเทศ) และ CSA STAR (มาตรฐานความปลอดภัยสำหรับระบบคลาวด์) รองรับการเชื่อมต่อเครือข่าย Public, Private และ GIN โดยมีทีมงานให้บริการตลอด ๒๔ ชั่วโมง

๑.๑.๒) ระบบฐานข้อมูล Active Directory สำหรับใช้ตรวจสอบยืนยันตัวตนรายชื่อผู้ใช้งานที่เกี่ยวข้องภายใน สผ. ซึ่งติดตั้งและทำงานบนเครื่องคอมพิวเตอร์แม่ข่าย สผ. ซึ่งสภาพแวดล้อมโดยทั่วไปของเครื่องคอมพิวเตอร์แม่ข่าย สผ. มีการจัดการและมีการควบคุมภายในที่ดี ดังนี้

- ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) สผ. มีตั้งอยู่ชั้น ๑๒ อาคารทิปโก้ ซึ่งมีความปลอดภัยจากเหตุอุทกภัยและการคุกคามจากภายนอก
- มีระบบสแกนลายนิ้วมือบันทึกการเข้า-ออก จำกัดสิทธิเฉพาะผู้ได้รับอนุญาตเท่านั้น
- มีการติดตั้งกล้องวงจรปิด (CCTV) เพื่อบันทึกภาพภายในห้องคอมพิวเตอร์แม่ข่าย (Server)
- มีการติดตั้งอุปกรณ์ป้องกันอัคคีภัย ระบบดับเพลิงอัตโนมัติ ถังดับเพลิงชนิดสารระเหย ใช้สำหรับห้องคอมพิวเตอร์แม่ข่าย (Server)
- อุปกรณ์อยู่ในตู้จัดเก็บอุปกรณ์เกี่ยวกับคอมพิวเตอร์ (Rack) สายไฟฟ้า สายสัญญาณมีการแยก และเดินสายไฟอย่างเป็นระเบียบ

- มีการติดตั้งอุปกรณ์สัญญาณเตือนภัย
- มีเครื่องสำรองไฟสำหรับกรณีไฟฟ้าดับ โดยสามารถสำรองไฟฟ้าได้ประมาณ ๑๕-๒๐ นาที
- มีเครื่องตรวจวัดอุณหภูมิ และความชื้น (Hygrometre)
- มีเครื่องปรับอากาศ ๔ เครื่อง สลับการทำงาน
- มีป้ายเตือนห้ามนำอาหาร และสัตว์ เข้าห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๑.๒ <u>การตรวจสอบด้านความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security) และความพร้อมใช้งาน (Availability)</u>

ระบบศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม (Smart EIA Plus) มีการรักษาความปลอดภัยและความพร้อมใช้งาน ที่เพียงพอ เหมาะสม ดังนี้

- มีการป้องกันการเข้าถึงระบบงานหรือบุกรุกโดยไม่ได้รับอนุญาต มีการป้องกันไวรัสและมัลแวร์ (Anti-Virus) ให้กับหน่วยงาน ซึ่งมีการอัพเดตฐานข้อมูล Virus/Malware อย่างสม่ำเสมอ โดยติดตั้ง Agent บนเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (VM) และผู้ใช้บริการ สามารถเลือกเปิด/ปิดโหมดป้องกันไวรัสและมัลแวร์ (Anti-Virus) ได้หากผู้ใช้งานมีการ download ไฟล์ที่มี Virus/Malware ระบบจะทำการบล็อกทันที
- มีระบบป้องกันการโจมตีประเภท DDoS (DDoS Protection) ให้กับหน่วยงานที่ใช้งานบนระบบ GDCC เพื่อป้องกันจากการถูกโจมตีในรูปแบบต่าง ๆ เช่น DNS Water Torture, Burst Attack, Zeros Day, Botnet หรือ Flood Attacks โดยเมื่อระบบตรวจพบว่ามีการโจมตีที่เครื่อง VM ระบบจะทำการหยุดทำงานของการโจมตี ทำให้เครื่อง VM ภายใต้ GDCC ปลอดภัย และสามารถใช้งานได้ต่อเนื่อง
- มีระบบป้องกันการบุกรุกเครือข่าย (Firewall) และ Web Application Firewall (WAF) ให้กับหน่วยงานที่ใช้งานอยู่บนระบบ GDCC สามารถกำหนด Customized rule Firewall ได้ทั้ง Deny/Accept และมี WAF (Web Application Firewall) เพื่อป้องกันการโจมตีหรือการ Hack เว็บไซต์หรือ Web Application ของหน่วยงาน
- ระบบมีการรักษาความปลอดภัยในการส่งข้อมูลด้วย SSL และในการบันทึกข้อมูลสำคัญ (Sensitive Data) ดำเนินการเข้ารหัสข้อมูล (Encryption)
- มีมาตรฐานรับรองความปลอดภัยสำหรับระบบคลาวด์ CSA STAR (Cloud Security Alliance (CSA) – Security, Trust & Assurance Registry (STAR)) ที่รองรับการเชื่อมต่อเครือข่าย Public, Private และ GIN โดยมีทีมงานให้บริการตลอด 24 ชั่วโมง
- มีการเก็บ Log ย้อนหลังไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ ประกอบด้วย ประวัติข้อมูลจราจรทางคอมพิวเตอร์ ที่ผ่านเข้าออก โดยมีบริการเรียกข้อมูล Log ให้หน่วยงานที่ใช้งานอยู่บน GDCC
- มีการสำรองข้อมูลให้กับหน่วยงานที่ใช้งานอยู่บนระบบ GDCC โดยมีการสำรองข้อมูลอัตโนมัติ เป็นรายวัน เก็บไว้ทั้งหมด ๗ วันย้อนหลัง และข้อมูลถูกเก็บไว้ทั้ง ๒ ศูนย์ข้อมูลของ GDCC
- มีการจัดทำสัญญาว่าจ้างการให้บริการและกำหนดเงื่อนไขต่างๆ ต่อผู้ให้บริการภายนอก (Outsource) ที่ช่วยในการบริหารจัดการด้านเทคโนโลยีสารสนเทศ

- มีการกำหนดกระบวนการในการติดตาม ดูแล ประสานงาน ประเมินผล รายงาน และตรวจสอบการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ
- มีการทดสอบระบบงานกับผู้ใช้งาน (User Acceptance Test) มีการอบรมหลักสูตรการใช้งานของผู้ดูแลระบบและผู้ใช้งานระบบ และมีการจัดทำคู่มือการใช้งาน

๑.๓ <u>การตรวจสอบความด้านความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)</u>

ศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อมมีข้อมูลที่มีความถูกต้องเชื่อถือได้ เนื่องจากศูนย์ข้อมูลฯ มีการเชื่อมโยงเพื่อตรวจสอบหรือใช้ข้อมูลกับหน่วยงานภายนอก ได้แก่ ๑) สภาวิชาชีพวิทยาศาสตร์และเทคโนโลยี ๒) สถาบันการศึกษา ๓) กรมบัญชีกลาง ๔) กรมการปกครอง ๕) กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ๖) การนิคมอุตสาหกรรมแห่งประเทศไทย ๗) สำนักงานคณะกรรมการกำกับกิจการพลังงาน และ ๘) เชื่อมโยงข้อมูลนิติบุคคล กรมพัฒนาธุรกิจการค้า โดยใช้บริการศูนย์กลางแลกเปลี่ยนข้อมูลภาครัฐ (Government Data Exchange : GDX)

๒. การตรวจสอบการปฏิบัติตามกฎหมายหรือระเบียบที่เกี่ยวข้อง (Reputation and Regulation)

ระบบศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม ได้ดำเนินการสอดคล้องกฎหมายหรือระเบียบที่เกี่ยวข้องอย่างเหมาะสม ในด้านกฎหมายและนโยบายภาครัฐที่เกี่ยวข้องกับการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล ได้แก่

- พระราชบัญญัติส่งเสริมและรักษาคุณภาพสิ่งแวดล้อมแห่งชาติ (ฉบับที่ ๒) พ.ศ.๒๕๖๑
- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐
- พระราชบัญญัติอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ.๒๕๕๘
- กรอบการกำกับดูแลข้อมูล (Data Governance Framework)
- ระเบียบการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation (GDPR)

ประกอบกับ สผ. มีการกำหนดนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) และขั้นตอนการปฏิบัติงานที่เกี่ยวข้อง ประกอบด้วย

- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๔
- แผนบริหารความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศของ สผ. ปีงบประมาณ พ.ศ.๒๕๖๕-๒๕๖๖
- มาตรการและวิธีการปฏิบัติภายใต้นโยบายข้อมูล สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม
- แผนปฏิบัติการดิจิทัล สำนักงานนโยบายแลแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม พ.ศ.๒๕๖๓-๒๕๖๕ (ฉบับปรับปรุง พ.ศ.๒๕๖๔)
- นโยบายข้อมูล สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม

อย่างไรก็ตาม ศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม มีข้อตรวจพบที่ควรทบทวน/ปรับปรุงเพิ่มเติม ดังนี้

ข้อตรวจพบที่ควรทบทวน/ปรับปรุงเพิ่มเติม ดังนี้

๑) การตรวจสอบด้านความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security) และความพร้อมใช้งาน (Availability)

ข้อตรวจพบ

จากการสุ่มตรวจสอบ กตภ. ได้ทดลองลงทะเบียนเข้าใช้งานในฐานะเจ้าของโครงการ โดยการลงทะเบียนได้ระบุเลขประจำตัวประชาชน ระบบได้กำหนดให้ใส่ชื่อ นามสกุล แต่ระบบไม่ได้ทำการตรวจสอบความถูกต้องของชื่อ นามสกุล ให้ถูกต้องตรงกันกับเลขที่ประจำตัวประชาชน (ระบบได้มีการเชื่อมโยงข้อมูลกับกรมการปกครองแล้ว) อาจจะส่งผลให้เกิดความเสี่ยง กรณีผู้ไม่ประสงค์ดีสามารถเข้ามาในระบบและก่อความเสียหายได้ และทำให้ปริมาณหรือจำนวนผู้เข้าใช้งานที่ไม่เกี่ยวข้องเพิ่มขึ้น

สาเหตุ

- ความรู้ ความเข้าใจ ความเชื่อมั่นว่าระบบศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม มีการควบคุม/การตรวจสอบความถูกต้อง ตอนขอรายงานข้อมูลผ่านระบบฯ แล้ว น่าจะควบคุมเพียงพอและเหมาะสม

ผลกระทบ

- อาจจะส่งผลให้เกิดความเสี่ยง กรณีผู้ไม่ประสงค์ดีสามารถเข้ามาในระบบและก่อความเสียหายได้ และทำให้ปริมาณหรือจำนวนผู้เข้าใช้งานที่ไม่เกี่ยวข้องเพิ่มขึ้น

ข้อเสนอแนะ

เห็นควรให้ กพส. ประสาน ผู้รับจ้างในการกำหนดให้มีการควบคุม/ตรวจสอบ การลงทะเบียนเข้าใช้งาน โดยการระบุเลขที่ประจำตัวประชาชน ระบุชื่อ และนามสกุล ให้ถูกต้องตรงกัน จึงจะสามารถลงทะเบียนเข้าใช้งานได้

๒) การตรวจสอบการปฏิบัติตามกฎหมายหรือระเบียบที่เกี่ยวข้อง (Reputation and Regulation)

ข้อตรวจพบ

จากการสอบทานการดำเนินการของศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม ตามประกาศ สผ. เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม พ.ศ.๒๕๖๔ มีรายละเอียดควรทบทวนดังนี้

๒.๑) ระบบศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม มีการกำหนดสิทธิการเข้าถึงข้อมูลของเจ้าหน้าที่รับผิดชอบในส่วนงาน ๓ ระบบ ซึ่งเจ้าหน้าที่ที่ได้รับมอบสิทธิสามารถเพิ่มข้อมูล แก้ไข และลบข้อมูล ตามสิทธิและงานที่ได้รับตามภารกิจและผู้ใช้งาน ระบบมีการกำหนดและควบคุมการเข้าถึงข้อมูล ดังนี้

- สิทธิอ่านอย่างเดียว (Read-only)
- สิทธิเพิ่มข้อมูล (Create)
- สิทธิแก้ไขข้อมูล (Edit)
- สิทธิลบข้อมูล (Delete)
- สิทธิอนุมัติ/อนุญาต (Approve/Authorize)

จากการตรวจสอบผู้รับผิดชอบระบบฯ มีการมอบหมายงานตามภารกิจของแต่ละส่วนแต่ยังไม่มีการมอบหมายเจ้าหน้าที่ทำหน้าที่ดูแลระบบ และเจ้าหน้าที่ผู้นำเข้าข้อมูล และผู้ตรวจสอบความถูกต้อง

ของข้อมูลเป็นลายลักษณ์อักษร ตามประกาศ สผ. เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สผ. พ.ศ. ๒๕๖๔ ส่วนที่ ๑๕ แนวปฏิบัติในการพัฒนาและปรับปรุงระบบสารสนเทศให้มีความปลอดภัย

สาเหตุ

- ความรู้ความเข้าใจ ที่คลาดเคลื่อนต่อการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผลกระทบ

- อาจจะส่งผลให้เกิดความเสี่ยง การเข้าถึงระบบงานหรือบุกรุกโดยไม่ได้รับอนุญาต หรือผู้ไม่ประสงค์ดีสามารถเข้ามาในระบบและก่อความเสียหายได้

ข้อเสนอแนะ

เห็นควรให้ผู้รับผิดชอบระบบกำหนดเจ้าหน้าที่ทำหน้าที่ดูแลระบบ ผู้นำเข้าข้อมูล และผู้ตรวจสอบ ความถูกต้องของข้อมูลเป็นลายลักษณ์อักษร เพื่อเป็นการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศให้มีความมั่นคงและปลอดภัย

๒.๒) การควบคุมการใช้งานระบบศูนย์ข้อมูลการประเมินผลกระทบสิ่งแวดล้อม รายละเอียดดังนี้

๒.๒.๑) การใช้งานระบบไม่มีการกำหนดระยะเวลาในการเชื่อมต่อระบบ (Limitation of connection time) ที่ใช้ในการปฏิบัติงานระบบสารสนเทศ หลังจากผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ อาจทำให้เกิดความเสี่ยงจากการเข้าสู่ระบบโดยไม่ได้รับอนุญาต

สาเหตุ

- เนื่องจากผู้ใช้งานระบบมีทั้งบุคคลภายนอก และบุคคลภายใน การกำหนดระยะในการเชื่อมต่อระบบขณะใช้งานให้มีความเหมาะสมค่อนข้างทำได้ยาก รวมทั้งการไม่กำหนดระยะเวลาในการเชื่อมต่อระบบเจ้าหน้าที่ผู้รับผิดชอบโครงการมองว่าเป็นการอำนวยความสะดวกและจูงใจให้ผู้รับบริการเข้าใช้งานเพื่อรับบริการทางดิจิทัล

ผลกระทบ

- อาจทำให้เกิดความเสี่ยงจากการเข้าสู่ระบบโดยไม่ได้รับอนุญาต

ข้อเสนอแนะ

เห็นควรให้ประสานผู้รับจ้างในการกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ที่ใช้ในการปฏิบัติงานระบบ ให้เหมาะสมกับระบบงาน เพื่อลดความเสี่ยงและป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

๒.๒.๒) การบริหารจัดการรหัสผ่านของระบบศูนย์ข้อมูลการประเมินผลระบุให้กำหนดรหัสผ่านอย่างน้อย ๖ ตัวอักษร ซึ่งการกำหนดรหัสผ่านดังกล่าวอาจยังไม่มีคุณภาพ และความปลอดภัย รัดกุม

เพียงพอ จากการทดสอบการกำหนดรหัสผ่านในกรณีลืมรหัสผ่าน โดยใช้เฉพาะตัวเลข หรือตัวอักษรไทย หรือตัวอักษรอังกฤษ อย่างน้อย ๖ ตัวเลข โดยไม่มีการผสมตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และตัวขระพิเศษต่างๆ สามารถกำหนดรหัสผ่านทดแทนได้

ข้อเสนอแนะ

เห็นควรให้ผู้รับผิดชอบระบบ แจ้งแนวทาง/วิธีการกำหนดรหัสผ่านหรือเปลี่ยนแปลงรหัสผ่านให้มีความปลอดภัย รัดกุม ยากต่อการคาดเดา รวมทั้งแจ้งให้ทราบถึงหน้าที่ความรับผิดชอบของผู้ใช้งาน ตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม พ.ศ.๒๕๖๔ เพื่อจำกัด ควบคุม ป้องกันการเข้าถึง การเปิดเผย ล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

เจ้าหน้าที่ผู้รับผิดชอบ

ผู้ตรวจสอบ : นายเทพจินดา แก้ววิจิตร์	นักวิชาการตรวจสอบภายในปฏิบัติการ
ผู้สอบทาน : น.ส.นันท์นภัส มูลกำบิล	ผอ.กตภ.