



บันทึกข้อความ

ส่วนราชการ กลุ่มตรวจสอบภายใน ฝ่ายอำนวยการ โทร. ๐๒๕๕๐๔๑๐๒ โทรสาร ๐ ๒๕๕๐ ๔๑๐๑
ที่ สจ ๐๙๒๕.๐๑/ วันที่ ๒ มกราคม ๒๕๕๙

เรื่อง สรุปสาระสำคัญจากการเข้าร่วมประชุมความรู้เกี่ยวกับการจัดทำ GAP Analysis

เรียน ผู้อำนวยการกลุ่มตรวจสอบภายใน

ตามที่ข้าพเจ้า นางสาวศตวรรษ อ่างแก้ว นักวิชาการคอมพิวเตอร์ กลุ่มตรวจสอบภายใน ได้รับมอบหมายให้เข้าร่วมประชุม เรื่อง ความรู้เกี่ยวกับการจัดทำ GAP Analysis วันที่ ๒๒ ธันวาคม ๒๕๕๘ ณ กองแผนงาน กรมอนามัย นั้น

ในการนี้ ข้าพเจ้า ได้เข้าร่วมประชุมฯ ตามที่ได้รับมอบหมายเรียบร้อยแล้ว และขอสรุปสาระสำคัญดังนี้

วิทยากรจากสำนักงานรัฐบาลอิเล็กทรอนิกส์ ได้มีการบรรยายองค์ความรู้เรื่องต่าง ๆ ดังนี้

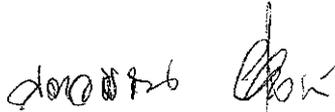
- วัตถุประสงค์และให้ความรู้เกี่ยวกับการจัดทำ GAP Analysis โดย สำนักงานรัฐบาลอิเล็กทรอนิกส์ โดยได้บรรยาย วัตถุประสงค์ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ดำเนินการตรวจสอบสภาพการบริหารจัดการระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ วิธีการ GAP Analysis ตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ หรือมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยที่เทียบเท่า และสอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ความรู้เกี่ยวกับการจัดทำ GAP Analysis สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ได้ให้บริการบำรุงรักษาระบบบริหารงานภายในกรมอนามัย (Intranet) ศูนย์ติดตามผลการปฏิบัติงาน กรมอนามัย (DOC) และระบบสารสนเทศอิเล็กทรอนิกส์กับกรมอนามัยตามพันธกิจของ สรอ. ต่อเนื่องมาเป็นประจำทุกปี โดยในปีงบประมาณ ๒๕๕๙ กรมอนามัยได้กำหนดข้อชี้แจงการดำเนินงาน ให้มีการตรวจสอบสภาพการบริหารจัดการระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภายในกลุ่มเทคโนโลยีสารสนเทศ กองแผนงาน กรมอนามัย ด้วยวิธีการ Gap Analysis ตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ดังนั้น สรอ. จึงดำเนินการตรวจสอบสภาพการบริหารจัดการระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เพื่อให้บรรลุวัตถุประสงค์ตามที่กรมอนามัยกำหนดไว้ ประโยชน์ของการทำ Gap Analysis - ทำให้ทราบถึงจุดอ่อนช่องโหว่ของการดำเนินงานในปัจจุบัน เมื่อเทียบกับข้อกำหนดของมาตรฐานสากล - ทำให้ทราบถึงแนวทางในการปรับปรุงการดำเนินงานในปัจจุบัน เพื่อเพิ่มความมั่นคงปลอดภัยของข้อมูล - ทำให้สามารถนำข้อมูลจาก Gap Analysis ไปเป็นข้อมูลในการทำแผนแม่บทเทคโนโลยีสารสนเทศได้

มาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ เป็นมาตรฐานที่พัฒนาขึ้นโดย ISO (International Organization for Standardization) ซึ่งเป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information security management system : ISMS) เพื่อสร้างความมั่นใจถึงความมีประสิทธิภาพและประสิทธิผลของระบบความมั่นคงปลอดภัยสารสนเทศขององค์กร รวมถึงการดำเนินการที่สอดคล้องตามข้อกำหนดด้านระบบความมั่นคงปลอดภัย ข้อกำหนด และระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้อง - A.๕ นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) - A.๖ โครงสร้างความปลอดภัยสารสนเทศ (Organization of Information Security) - A.๗ ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security) - A.๘ การบริหารจัดการทรัพย์สิน (Asset Management) - A.๙ การควบคุมการเข้าถึง (Access Control) - A.๑๐ การเข้ารหัสข้อมูล (Cryptography) - A.๑๑ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security) - A.๑๒ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security) - A.๑๓ ความมั่นคงปลอดภัยสำหรับการ

สื่อสารข้อมูล (Communications security) - A.๑๔ การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance) - A.๑๕ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) - A.๑๖ การบริหารจัดการเหตุการณ์ ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) - A.๑๗ ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management) - A.๑๘ ความสอดคล้อง (Compliance)

รายละเอียดอื่น ๆ ตามเอกสารที่แนบมาพร้อมนี้

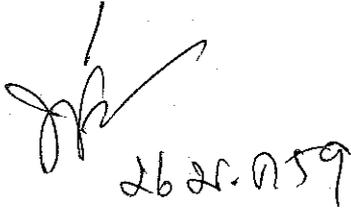
จึงเรียนมาเพื่อโปรดทราบ



(นางสาวศตวรรษ อ่างแก้ว)
นักวิชาการคอมพิวเตอร์


๕ ต.ค. ๕๙

- อรณ + สิ่งต่าง ๆ จากตัว ๒ (กรณี)
- สิ่งต่าง ๆ ในเอกสารแนบมา


๒๖ ต.ค. ๕๙

พิกัด 1

พิกัด 2  ๕ ต.ค. ๕๙

พิกัด 3

พิกัดแผนที่  ๕ ต.ค. ๕๙