บันทึกข้อความ

ส่วนราชการ กลุ่มตรวจสอบภายใน ฝ่ายตรวจสอบ ๒ โทร. ๐ ๒๕๙๐ ๔๖๒๘ โทรสาร ๐ ๒๕๙๐ ๔๑๐๑

ที่ สธ ๐๙๒๕.๐๔/ ๑๙๔ **วันที่** ๙ กันยายน ๒๕๕๗

เรื่อง สรุปผลการประชุม เรื่อง ระบบฐานข้อมูลระบบคอมพิวเตอร์และเครือข่าย กรมอนามัย

เรียน ผู้อำนวยการกลุ่มตรวจสอบภายใน

ตามที่ นางสาวอรวรรณ ศรีสงคราม นักวิชาการตรวจสอบภายในชำนาญการและนางสาวศตวรรณ อ่างแก้ว นักวิชาการคอมพิวเตอร์ กลุ่มตรวจสอบภายใน ไดรับมอบหมายให้เข้าร่วมประชุม เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมอนามัย วันที่ ๔-๕ กันยายน ๒๕๕๗ ณ ห้องประชุมกำธร สุวรรณกิจ อาคาร ๑ ชั้น ๑ นั้น

ในการนี้ ข้าพเจ้า ได้เข้าร่วมประชุมตามที่ได้รับมอบหมายเรียบร้อยแล้ว และได้ขอสรุปสาระสำคัญ การประชุมในวันที่ ๔-๕ กันยายน ๒๕๕๗ หัวข้อเรื่อง การพัฒนานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมอนามัย และ Information Security Control Audit and Evaluation และ Becoming ISO ๒๗๐๐๑ Certified โดยอาจารย์ ดร.ศุภกร กังพิศดารและ Chuchpon Kunachattrathorn ดังนี้

๑. ISO ๒๗๐๐๑ คือแนวทางหรือวิธีการเกี่ยวกับเรื่องความเสี่ยงด้านสารสนเทศเพื่อการกำหนด นโยบาย และกระบวนการทำงาน รวมทั้งเพื่อเลือกการควบคุมที่เหมาะสมในการบริหารความเสี่ยงด้วย หัวใจสำคัญของระบบบริหารความปลอดภัยสารสนเทศนั้นอยู่ที่ ๓ ปัจจัยหลักโดยพื้นฐานดังต่อไปนี้

๑.๑ ข้อมูลส่วนตัว ข้อมูลสำคัญขององค์กร การรักษาความปลอดภัยด้านข้อมูลไม่ให้ถูกขโมย ลักลอบนำไปใช้ ดัดแปลง หรือทำให้เกิดข้อผิดพลาดอื่นใด ซึ่งสำหรับหลายหน่วยงานอาจเป็นอันตรายระดับวิกฤติได้ ซึ่งข้อมูลนี้ไม่เพียงเฉพาะข้อมูลสำคัญขององค์กรแต่ยังรวมถึงข้อมูลส่วนตัว ของลูกค้าหรือบุคคลที่สามที่เกี่ยวข้องอื่นๆ ด้วย

๑.๒ การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่างๆ การบริหารความเสี่ยงจากเหตุการณ์และปัจจัยต่างๆ ซึ่งปัจจุบันมีการคำนึงถึงการตั้งไซต์สำรอง ในลักษณะของศูนย์สำรองข้อมูลและดำเนินการกู้คืนระบบภายหลังภัยพิบัติหรือ Disaster Recovery Center (DRC) ซึ่งมีความสำคัญมากในหลายธุรกิจเช่น ธุรกิจการเงิน หรือบริการด้านสุขภาพ เพราะข้อมูลเหล่านั้นมีความสำคัญยิ่งยวดต่อความสามารถในการดำเนินธุรกิจให้ ต่อเนื่องต่อไปได้ (Business continuity)

๑.๓ บริหารระบบเพื่อป้องกันความปลอดภัยของข้อมูล รายละเอียดการบริหารระบบเพื่อป้องกันความปลอดภัยของข้อมูล ซึ่งหัวข้อนี้นับเป็นหนึ่งในรายละเอียดหลักของเนื้อหาในร่างมาตรฐาน ISO ๒๗๐๐๐ ทั้งหมดก็ว่าได้ โดยครอบคลุมตั้งแต่นโยบาย แผน กลยุทธ์ การตรวจวัด การบริหาร และการควบคุมการปฏิบัติการ

๒.ปัจจัยในการพิจารณาความปลอดภัยของระบบสารสนเทศ

๒.๑ ความลับของข้อมูล (Confidentiality)

๒.๒ ความถูกต้องสมบูรณ์ของข้อมูล (Integrity)

๒.๓ ความพร้อมใช้งานของข้อมูล (Availability)

๒.๔ การยืนยันตัวตนของผู้ใช้ (Authentication)

๒.๕ การควบคุมสิทธิในการใช้งานของผู้ใช้ (Authorization)

๒.๖ การไม่สามารถปฏิเสธการกระทำ (Non repudiation)

๓.ตัวอย่างโปรแกรมที่ช่วยใช้การตรวจสอบความปลอดภัย Software ของ Microsoft

Microsoft security compliance manager เครื่องมือฟรีจากทีม Microsoft Solution Accelerators ที่ช่วยให้องค์กรสามารถกำหนดค่าและจัดการเดสก์ท็อป, ดาต้าเซ็นเตอร์ และระบบคลาวด์ โดยการใช้นโยบายกลุ่ม (Group Policy) และระบบ System Center Configuration Manager (SCCM) ได้อย่างรวดเร็วโดย SCM รวมคำแนะนำพื้นฐาน (Baselines) ด้านความปลอดภัยและคำแนะนำใหม่ล่าสุดสำหรับ Exchange Server ๒๐๐๗ และ ๒๐๑๐ เพื่อให้เกิดความปลอดภัยในการใช้งานสารสนเทศของ กรมอนามัย

จึงเรียนมาเพื่อโปรดทราบและได้แนบเอกสารการประชุมมาพร้อมนี้ด้วย จะเป็นพระคุณ

(นางสาวอรวรรณ ศรีสงคราม)
นักวิชาการตรวจสอบภายในชำนาญการ

8-9-57

(นางพรรณี เทียนทอง)
ผู้อำนวยการกลุ่มตรวจสอบภายใน