คำสั่งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ที่ ๐๑๗/๒๕๕๓

เรื่อง แต่งตั้งคณะทำงานด้านการรักษาความปลอดภัยโครงสร้างเครือข่ายและข้อมูลสารสนเทศ

เพื่อให้ฝ่ายเครือข่ายคอมพิวเตอร์และการสื่อสารสามารถปฏิบัติการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของฝ่ายเครือข่ายคอมพิวเตอร์และการสื่อสาร ได้อย่างมีประสิทธิภาพ จึงเห็นควรให้มีการแต่งตั้ง คณะกรรมการรักษาความปลอดภัยโครงสร้างเครือข่ายและข้อมูลสารสนเทศ ซึ่งมีบทบาทหน้าที่ทางด้านการรักษาความปลอดภัยให้กับโครงสร้างเครือข่ายและความปลอดภัยข้อมูลสารสนเทศ ตลอดจนกำหนดนโยบายการรักษาความปลอดภัยระบบเครือข่ายและข้อมูลสารสนเทศให้ได้ตามมาตรฐานสากล โดยนำนโยบายมาตรฐาน เช่น ISO/IEC17799 หรือ ISACA CobiT Framework มาจัดการกับระบบในองค์กรให้มีความปลอดภัยในลักษณะบรรษัทภิบาล หรือที่เรียกว่า "Corporate Governance" คณะกรรมการฯประกอบด้วย

๑. ผู้ช่วยศาสตราจารย์นิวัตร จารุวาระกูล	ประธานคณะทำงาน
๒. นายนพชัย ทิพย์ไกรลาศ	รองประธานคณะทำงาน
๓. นายโยธิน หนูแดง	คณะทำงาน
๔. นายเชาวลิต สมบูรณ์พัฒนากิจ	คณะทำงาน
๕. นายปาโมกข์ รัตนตรัยาภิบาล	คณะทำงานและเลขานุการ

กำหนดให้คณะกรรมการรักษาความปลอดภัยโครงสร้างเครือข่ายและข้อมูลสารสนเทศดังกล่าวมีหน้าที่ดังต่อไปนี้

๑. กำหนดเป้าหมาย นโยบายด้านการรักษาความปลอดภัยข้อมูล โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ขององค์กร (Corporate Strategic Plan)
๒. จัดการพัฒนานโยบายด้านการรักษาความปลอดภัยข้อมูล Policy, Standard, Procedure and Guideline เพื่อให้องค์กรได้มาซึ่ง การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability) ยกตัวอย่าง การรับผิดชอบจัดทำแผน Information Security Awareness Training ให้กับบุคลากรขององค์กรที่ต้องใช้คอมพิวเตอร์ในการทำงานให้มีความรู้ความเข้าใจกับภัยอินเทอร์เน็ต
๓. จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่างๆ ที่อาจเกิดขึ้นกับระบบ โดยใช้ระบบเตือนผู้บุกรุก Intrusion Detection System (IDS), ระบบป้องกันผู้บุกรุก Intrusion

Prevention System (IPS) หรือระบบจัดการกำจัดไวรัส (Anti-Virus Systems) ตลอดจนวางแผน Business Continuity และ Disaster Recovery (BCP and DRP) เพื่อกู้ระบบยามฉุกเฉิน

๔. มีการบริหารความเสี่ยง (Risk Management) และการวิเคราะห์ความเสี่ยง (Risk Analysis) ที่อาจทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุรกิจขององค์กร

๕. นำเสนอผู้บริหารระดับสูงเช่น CIO หรือ CEO ในเรื่องของแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง ตลอดจนแผนการ Outsource ด้านความปลอดภัยข้อมูลเพื่อขอดำเนินการอนุมัติ และเพื่อให้ผู้บริหารระดับสูงมีความตระหนัก (Awareness) ในความสำคัญเรื่อง Information Security

๖. เป็นที่ปรึกษาด้านระบบความปลอดภัยข้อมูลให้กับแผนกอื่นๆ ที่ต้องใช้ IT ในการปฏิบัติงาน

๗. ติดต่อและรักษาความสัมพันธ์กับคู่ค้า, องค์กร หรือบุคคลภายนอกที่มีความเกี่ยวข้องกับเรื่องความปลอดภัยข้อมูลทั้งภาครัฐและเอกชนเช่น ตำรวจ, นักข่าว, Systems Integrator (SI), Outsourcer, Managed Security Services Provider (MSSP) และผู้ตรวจสอบ (Auditor)

๘. ออกข้อกำหนดในการจัดซื้อจัดจ้างระบบรักษาความปลอดภัยข้อมูลสารสนเทศ Requests for Proposal (RPF)

๙. จัดตั้งและควบคุมบริหารทีม Incident Response เพื่อให้สามารถปฏิบัติงานในยามที่เกิดภาวะฉุกเฉินขึ้นในองค์กร เช่น การระบาดของไวรัสคอมพิวเตอร์

๑๐. เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ๆ ทางด้าน Information Security อย่างสม่ำเสมอ

ทั้งนี้ ตั้งแต่วันที่ ๒ ตุลาคม ๒๕๕๓ เป็นต้นไป

สั่ง ณ วันที่ ๒ เดือน ตุลาคม พ.ศ. ๒๕๕๓

(ผู้ช่วยศาสตราจารย์นิวัตร จารุวาระกูล)

ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ