



ประกาศสำนักงานสาธารณสุขจังหวัดชลบุรี
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานสาธารณสุขจังหวัดชลบุรี พ.ศ. ๒๕๖๓

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานสาธารณสุขจังหวัดชลบุรี เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้น จากการใช้งาน ระบบสารสนเทศ และการสื่อสาร ในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจ ก่อให้เกิดความเสียหายแก่สำนักงานสาธารณสุขจังหวัดชลบุรี และหน่วยงานภายใต้สังกัด และเป็นความผิดตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และกฎหมายอื่นที่เกี่ยวข้องได้ สำนักงานสาธารณสุขจังหวัดชลบุรี จึงเห็นสมควรกำหนด นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นต่อไป

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศสำนักงานสาธารณสุขจังหวัดชลบุรี เรื่องนโยบายและแนวทางปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันนี้เป็นต้นไป

ข้อ ๓. บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้ง กับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสาธารณสุขจังหวัด ชลบุรี มีวัตถุประสงค์ ดังต่อไปนี้

๔.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศ ของสำนักงานสาธารณสุขจังหวัดชลบุรี ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ เพื่อเผยแพร่ประกาศนโยบายและข้อปฏิบัติให้เจ้าหน้าที่ทุกระดับในหน่วยงาน สังกัด สำนักงานสาธารณสุขจังหวัดชลบุรี และผู้ที่เกี่ยวข้องทั้งหมด ได้รับทราบ เข้าถึง เข้าใจและถือปฏิบัติ ตามนโยบายและแนวปฏิบัติ อย่างเคร่งครัด

๔.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานสาธารณสุขจังหวัดชลบุรี ตระหนักถึงความสำคัญ ของการรักษา ความมั่นคงในการใช้งานด้านสารสนเทศของสำนักงานสาธารณสุขจังหวัดชลบุรี ในการ ดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละหนึ่งครั้ง

ข้อ ๕. นโยบาย...

ข้อ ๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสาธารณสุขจังหวัดชลบุรี กำหนดประเด็นสำคัญดังต่อไปนี้

๕.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๕.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๕.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่าน การลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งาน และตรวจสอบการละเมิดความปลอดภัยเสมอ

๕.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่เข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่สำนักงานสาธารณสุขจังหวัดชลบุรีจัดสรรไว้ และมีการออกแบบ ระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อให้การควบคุม และป้องกันภัยคุกคาม ได้อย่างเป็นระบบ และมี ประสิทธิภาพ

๕.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่เข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมมัลแวร์ประเภทต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์ และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

๕.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึง จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๕.๒ การจัดทาระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทาระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๕.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๖. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าปิ่นการปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโดยกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๗. ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานสาธารณสุขจังหวัดชลบุรี พ.ศ. ๒๕๖๖ ตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๒ มีนาคม พ.ศ. ๒๕๖๗



นายอภิรัตน์ กัตัญญตานนท์
นายแพทย์สาธารณสุขจังหวัดชลบุรี