



ประกาศสำนักงานสาธารณสุขอำเภอเกาะจันทร์
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานสาธารณสุขอำเภอเกาะจันทร์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้ง ป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและ การถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักงานสาธารณสุขอำเภอเกาะจันทร์และ เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่ เกี่ยวข้องได้ สำนักงานสาธารณสุขอำเภอเกาะจันทร์ จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสาธารณสุขอำเภอ เกาะจันทร์ มีวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศ ของ สำนักงานสาธารณสุขอำเภอเกาะจันทร์ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
๒. เพื่อเผยแพร่ประกาศนโยบายและข้อปฏิบัติให้เจ้าหน้าที่ทุกระดับในสังกัดของสำนักงาน สาธารณสุขอำเภอเกาะจันทร์และผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบ เข้าถึง เข้าใจ และถือปฏิบัติตามนโยบาย และแนวปฏิบัติอย่างเคร่งครัด
๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับของสำนักงานสาธารณสุขอำเภอเกาะจันทร์ ตระหนักถึงความสำคัญของ การรักษาความมั่นคงในการใช้งานด้านสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้อง มีการทบทวนนโยบายปีละหนึ่งครั้ง

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานสาธารณสุขอำเภอ เกาะจันทร์ กำหนดประเด็นสำคัญ ดังต่อไปนี้

๑. การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ
 - ๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการ ประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนด กฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจและสามารถ ปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของ ระบบสารสนเทศ
 - ๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งานอนุมัติ และกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้

/และต้องเก็บ...

และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งานโดยแสดงตัวตนด้วยชื่อผู้ใช้งานและต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน เพื่อให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่เข้าใช้งานต้องลงบันทึกเข้าใช้งาน โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งานและจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมมัลแวร์ประเภทต่างๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ต่างๆ

๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์ หรือแอปพลิเคชันต่างๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่างๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงาน รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

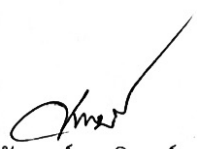
๒. การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูลและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓. ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของหน่วยงาน หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอกอย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๔. กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเอียด หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้คณะกรรมการรักษาความมั่นคงด้านสารสนเทศของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๒ ตุลาคม พ.ศ. ๒๕๖๖


(นายรัฐพงษ์ ภูมรินทร์)

สาธารณสุขอำเภอเกาะจันทร์