ที่ ศก ๐๐๓๒/ว 6000

ถึง อำเภอทุกอำเภอ โรงพยาบาลศรีสะเกษ โรงพยาบาลกันทรลักษ์ โรงพยาบาลชุมชน ทุกแห่ง

พร้อมนี้จังหวัดศรีสะเกษ ขอส่งสำเนาหนังสือสำนักงานเขตสุขภาพที่ ๑๐ ที่ สธ ๐๒๓๕/๑๒๕ ลงวันที่ ๒๗ มกราคม ๒๕๖๕ เรื่อง แจ้งนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของเขตสุขภาพที่ ๑๐ รายละเอียดตามเอกสารที่แนบสามารถดาวน์โหลดรายละเอียดได้ที่ (งานสารบรรณ) www.ssko.moph.go.th

จึงเรียนมาเพื่อโปรดทราบ

สำนักงานสาธารณสุขจังหวัดศรีสะเกษ
ศูนย์เทคโนโลยีสารสนเทศ
โทร ๐-๔๕๖๑-๖๐๔๐-๖ ต่อ ๓๐๘
โทรสาร ๐-๔๕๖๑-๖๐๔๒

ที่ สธ ๐๒๓๕/๑๒๕

สำนักงานเขตสุขภาพที่ ๑๐
เลขที่ ๙๐๐ หมู่ ๒ ถ.แจ้งสนิท
ต.แจระแม อ.เมืองอุบลราชธานี
จ.อุบลราชธานี ๓๔๐๐๐

๒๗ มกราคม ๒๕๖๕

เรื่อง แจ้งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของเขตสุขภาพที่ ๑๐

เรียน นายแพทย์สาธารณสุขจังหวัดทุกจังหวัด, ผู้อำนวยการโรงพยาบาลศูนย์, ผู้อำนวยการโรงพยาบาลทั่วไป ทุกแห่งในเขตสุขภาพที่ ๑๐, ผู้อำนวยการโรงพยาบาลพระศรีมหาโพธิ และผู้อำนวยการโรงพยาบาลมะเร็งอุบลราชธานี

สิ่งที่ส่งมาด้วย ประกาศสำนักงานปลัดกระทรวงสาธารณสุข เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของเขตสุขภาพที่ ๑๐ ลงวันที่ ๒๕ มกราคม ๒๕๖๕ จำนวน ๑ ชุด

ตามที่ เขตสุขภาพที่ ๑๐ ได้จัดทำประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของเขตสุขภาพที่ ๑๐ เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของหน่วยบริการทุกระดับในเขตสุขภาพที่ ๑๐ มีความมั่นคงปลอดภัย รวมทั้งป้องกันภัยจากการคุกคามต่าง ๆ ที่อาจก่อให้เกิดความเสียหาย และเพื่อป้องกันการกระทำที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศของเจ้าหน้าที่ซึ่งอาจเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ นั้น

ในการนี้ เขตสุขภาพที่ ๑๐ จึงขอให้ทุกหน่วยบริการยึดถือประกาศดังกล่าวข้างต้นเพื่อเป็นแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

จึงเรียนมาเพื่อโปรดทราบ และปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของเขตสุขภาพที่ ๑๐ ต่อไป

ขอแสดงความนับถือ

(นายสุวิทย์ โรจนศักดิ์โสธร)
ผู้อำนวยการสำนักงานเขตสุขภาพที่ ๑๐

○ ทราบ ✓ ทราบ
○ ขอพบ ○ ลงนัด
○ แจ้งผู้เกี่ยวข้อง
✓ ดำเนินการ
○ ประสาน.....
.....
.....

(นายพิเชฏฐ์ จงเจริญ)
นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน) ปฏิบัติราชการแทน
นายแพทย์สาธารณสุขจังหวัดศรีสะเกษ

กลุ่มงานยุทธศาสตร์และสารสนเทศ 1 กพ. 65
โทร ๐๔๕ ๔๓๕๑๓๔ โทรสาร ๐๔๕ ๔๓๕๑๓๓
ผู้ประสานงาน : ๑. นางหรรษา ชื่นชูผล โทร. ๐๘๙ ๘๔๕๒๒๕๕
๒. นางสาวเย็นฤดี ศรีพรม โทร. ๐๙๗ ๑๓๗๖๑๘๑

ประกาศสำนักงานปลัดกระทรวงสาธารณสุข

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของเขตสุขภาพที่ ๑๐

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานในเขตสุขภาพที่ ๑๐ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหาย และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ สำนักงานปลัดกระทรวงสาธารณสุข จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของเขตสุขภาพที่ ๑๐ ต่อไป

อาศัยอำนาจตามคำสั่งกระทรวงสาธารณสุขที่ ๑๑๐๖/๒๕๖๔ เรื่องกำหนดเขตสุขภาพและมอบหมายให้ผู้ตรวจราชการกระทรวงสาธารณสุขปฏิบัติงานในเขตสุขภาพ กระทรวงสาธารณสุข, พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ และด้วยความเห็นชอบของคณะกรรมการเทคโนโลยีสารสนเทศเขตสุขภาพที่ ๑๐ จึงออกประกาศไว้ ดังต่อไปนี้

๑. ประกาศนี้เรียกว่า “ประกาศสำนักงานปลัดกระทรวงสาธารณสุข เรื่องนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของเขตสุขภาพที่ ๑๐”

๒. บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

๓. นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของเขตสุขภาพที่ ๑๐ มีวัตถุประสงค์ ดังต่อไปนี้

๓.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของหน่วยงานในเขตสุขภาพที่ ๑๐ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๓.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในเขตสุขภาพที่ ๑๐ ได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๓.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงานในเขตสุขภาพที่ ๑๐ ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศ ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง

๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของเขตสุขภาพที่ ๑๐ กำหนดประเด็นสำคัญดังต่อไปนี้

๔.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๔.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์

เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๔.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งานตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งานเพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้งานระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๔.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเตอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่หน่วยงาน จัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำการควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๔.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

๔.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอพพลิเคชั่น ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอพพลิเคชั่นต่างๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) และระบบงานต่างๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๔.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบขอเจ้าหน้าที่ในการสำรองข้อมูลและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๔.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้ผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

๕. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๖. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แนบท้ายประกาศนี้

๗. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๕ มกราคม พ.ศ. ๒๕๖๕

(นายทวีศิลป์ วิษณุโยธิน)
ผู้ตรวจราชการกระทรวง ปฏิบัติราชการแทน
ปลัดกระทรวงสาธารณสุข

เอกสาร

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เขตสุขภาพที่ 10