ประกาศองค์การบริหารส่วนตำบลสวี
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙

.....

ตามประกาศกรมส่งเสริมการปกครองท้องถิ่น เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมส่งเสริมการปกครองท้องถิ่น ลงวันที่ ๑๑ พฤศจิกายน ๒๕๖๘ เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การบริหารส่วนตำบลสวี เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์การบริหารส่วนตำบลสวี และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ องค์การบริหารส่วนตำบลสวีจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การบริหารส่วนตำบลสวี เพื่อเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยความเห็นชอบของนายกองค์การบริหารส่วนตำบลสวี โดยมีรายละเอียดดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศองค์การบริหารส่วนตำบลสวี เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ บรรดาประกาศ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การบริหารส่วนตำบลสวี มีวัตถุประสงค์ดังต่อไปนี้

๔.๑ เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานด้านสารสนเทศขององค์การบริหารส่วนตำบลสวี ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ เพื่อเผยแพร่และประกาศนโยบายและข้อปฏิบัติให้เจ้าหน้าที่ทุกระดับในหน่วยงาน และผู้ที่เกี่ยวข้องทั้งหมด ได้รับทราบ เข้าถึง เข้าใจและถือปฏิบัติตามนโยบายและแนวทางอย่างเคร่งครัด

๔.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์การบริหารส่วนตำบลสวี ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศขององค์การบริหารส่วนตำบลสวี ในการดำเนินงานและปฏิบัติอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละหนึ่งครั้ง

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การบริหารส่วนตำบลสวี กำหนดประเด็นสำคัญดังต่อไปนี้

๕.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๕.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศกำหนด

กฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานทุกระดับได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๕.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๕.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Log in) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน ก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ตโดยผ่านระบบรักษาความปลอดภัยตามที่องค์การบริหารส่วนตำบลสวีจัดสรรไว้ และมีการออกแบบระบบเครือข่าย โดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๕.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Log in) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งานต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่างๆ เพื่อไม่ใช้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่างๆ

๕.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่างๆ รวมถึง จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่างๆโ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๕.๒ การจัดทำระบบสำรองข้อมูลเพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่ และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๕.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๖ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๗ ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙ นี้

ประกาศ ณ วันที่ ๓ กรกฎาคม พ.ศ. ๒๕๖๙

(นายธวัชชัย ซื่อสัตย์)
นายกองค์การบริหารส่วนตำบลสวี

บันทึกข้อความ

ส่วนราชการ งานควบคุมภายในและตรวจสอบภายใน หน่วยตรวจสอบภายใน องค์การบริหารส่วนตำบลสวี

ที่ ชพ ๗๖๘๐๔/๐๕๐ **วันที่** ๒ กรกฎาคม ๒๕๖๙

เรื่อง ขออนุมัติและประกาศใช้ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การบริหารส่วนตำบลสวี พ.ศ. ๒๕๖๙

เรียน นายกองค์การบริหารส่วนตำบลสวี

๑. ต้นเรื่อง

ตามประกาศกรมส่งเสริมการปกครองท้องถิ่น เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น พ.ศ. ๒๕๖๘ ลงวันที่ ๑๑ พฤศจิกายน ๒๕๖๘ ข้อ ๕.๓ กำหนดให้หน่วยงานในสังกัดกรมส่งเสริมการปกครองท้องถิ่นต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ นั้น

๒. ข้อเท็จจริง

หน่วยตรวจสอบภายใน องค์การบริหารส่วนตำบลสวี จึงได้กำหนด นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การบริหารส่วนตำบลสวี พ.ศ. ๒๕๖๙ ขึ้น เพื่อเป็นแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศในคราวต่อไป

๓. ระเบียบ/ข้อกฎหมาย

๑. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๒. พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓. ประกาศกรมส่งเสริมการปกครองท้องถิ่น เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น พ.ศ. ๒๕๖๘ ลงวันที่ ๑๑ พฤศจิกายน ๒๕๖๘

๔. ข้อเสนอ/เพื่อพิจารณา

หน่วยตรวจสอบภายใน จึงขออนุมัติและประกาศใช้ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การบริหารส่วนตำบลสวี พ.ศ. ๒๕๖๙ ฉบับที่มีผลใช้บังคับตั้งแต่วันที่ ๓ กรกฎาคม ๒๕๖๙ เป็นต้นไป

จึงเรียนมาเพื่อโปรดพิจารณา

(นายนัฐวิชญ์ คงเย็น)
หัวหน้าหน่วยงานตรวจสอบภายใน

- ความเห็นปลัดองค์การบริหารส่วนตำบลสวี

เห็นควรพิจารณาอนุมัติ ประการใด

.....

.....

(ลงชื่อ) .....

(นางสาวจิระพันธุ์ พรหมขุนทอง)

ปลัดองค์การบริหารส่วนตำบลสวี

๔/๑/๖๑

- ความเห็นนายกองค์การบริหารส่วนตำบลสวี

(/) อนุมัติ

( ) ไม่อนุมัติ

(ลงชื่อ) .....

(นายธวัชชัย ซื่อสัตย์)

นายกองค์การบริหารส่วนตำบลสวี