



นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์

องค์การบริหารส่วนตำบลสระ พ.ศ.๒๕๖๘

.....

๑. หลักการ

องค์การบริหารส่วนตำบลสระ ได้มีข้อกำหนดสำหรับการใช้งาน การดูแลรักษา และการป้องกันให้เหมาะสมกับลักษณะการดำเนินงาน ซึ่งการดูแลรักษาและการป้องกัน มุ่งหมายไปในทางความมั่นคงปลอดภัย โดยมีหลักการสำคัญคือการเข้ารหัส การรักษาความลับของข้อมูล ความถูกต้องครบถ้วน และความสมบูรณ์พร้อมใช้ ดังนี้

๑.๑ การรักษาความลับ (Confidentiality) หมายถึง การป้องกันไม่ให้สินทรัพย์สามารถถูกเข้าถึงได้จากผู้ไม่มีสิทธิ โดยการเข้าถึงยังรวมถึงการถูกเปิดเผยและการจำแนกแจกจ่ายซึ่งสินทรัพย์นั้นด้วย ดังนั้นในการรักษาความลับจำเป็นจะต้องมีการควบคุมทั้งทางกายภาพและทางเทคนิค โดยผู้ที่ไม่มีสิทธิจะต้องไม่สามารถเข้าถึงสินทรัพย์นั้นได้และสินทรัพย์จำเป็นจะต้องมีการจำแนก และกำหนดระดับความต้องการในการป้องกันไว้อย่างชัดเจน เพื่อให้ผู้ที่ถือครองสินทรัพย์ปฏิบัติได้ถูกต้องเหมาะสมกับระดับความต้องการนั้น

๑.๒ ความถูกต้องครบถ้วน (Integrity) หมายถึง การป้องกันไม่ให้สินทรัพย์ถูกเปลี่ยนแปลงแก้ไขทั้งที่มีเจตนาหรือไม่ก็ตามจากผู้ไม่มีสิทธิที่จะแก้ไขสินทรัพย์เหล่านั้น ดังนั้นการควบคุมและป้องกันจึงต้องประกอบด้วยกำหนดสิทธิในการแก้ไข กำหนดสิทธิในการเข้าถึงและจำเป็นต้องอาศัยการตรวจสอบทั้งจากการทำรายการบัญชีสินทรัพย์และทางเทคนิคประกอบด้วย

๑.๓ ความสมบูรณ์พร้อมใช้ (Availability) หมายถึง การที่ผู้ที่มีสิทธิสามารถเข้าใช้งานสินทรัพย์นั้นได้เมื่อยามต้องการใช้งาน ซึ่งมีทั้งในทางกายภาพและทางเทคโนโลยี ได้แก่ การให้บริการระบบจดหมายอิเล็กทรอนิกส์ที่จำเป็นจะต้องให้บริการตลอดเวลา ดังนั้น เมื่อผู้ใช้ต้องการจะรับหรือส่งระบบจำเป็นที่จะต้องสามารถให้บริการได้ตลอดเวลา เป็นต้น

๒. นโยบายการปฏิบัติ

๒.๑ องค์การบริหารส่วนตำบลสระ จัดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยการประเมินความเสี่ยงดังกล่าวพิจารณาถึงบริบทภายใน (Internal Context) บริบทภายนอก (External Context) ผู้ที่มีส่วนได้ส่วนเสีย (Interested Party) วิสัยทัศน์ พันธกิจ การเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ

๒.๒ องค์การบริหารส่วนตำบลสระ มีการกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้และความเสี่ยงที่ยอมรับไม่ได้ เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงที่เกิดขึ้นในการประเมินความเสี่ยงที่เกิดขึ้น

๒.๓ องค์การบริหารส่วนตำบลสระ จัดให้มีการทบทวนนโยบายอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๒.๔ องค์การบริหารส่วนตำบลสระ มีการกำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อรับมือตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

๒.๕ องค์การบริหารส่วนตำบลสระ มีการประเมินผลสัมฤทธิ์ของนโยบายที่ประกาศใช้ เพื่อนำมาปรับปรุงนโยบาย แผนกลยุทธ์ให้สอดคล้องกับยุคความในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต

๒.๖ องค์การบริหารส่วนตำบลสระ จัดให้มีทรัพยากร ด้านงบประมาณ ทรัพยากรบุคคล การบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการด้านความมั่นคงปลอดภัยของสำนักงาน

๓. โครงสร้างทางด้านการมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์การบริหารส่วนตำบลสระ

องค์การบริหารส่วนตำบลสระ กำหนดมาตรการควบคุม กำกับและติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับส่วนงานต่างๆ ภายในหน่วยงาน และเพื่อเป็นแนวทางการควบคุม อุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอกให้เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) แบ่งเป็น ๒ ส่วน คือ

๑. การจัดโครงสร้างภายในองค์กร (Internal Organization)

องค์การบริหารส่วนตำบลสระ มีกำหนดบทบาทหน้าที่ ความรับผิดชอบในการใช้ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม และมีความมั่นคงปลอดภัยทางไซเบอร์

๒. นโยบายการควบคุมอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอก (Computing Device and Teleworking Policy)

เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอกองค์การบริหารส่วนตำบลสระ

๔. นโยบายความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล

องค์การบริหารส่วนตำบลสระ มีกระบวนการในการคัดเลือกบุคลากร การฝึกอบรมและการควบคุม การปฏิบัติงานของบุคลากรในหน่วยงานอย่างเหมาะสมตลอดระยะเวลาการจ้างงาน และเพื่อให้เข้าใจถึงหน้าที่ ความ รับผิดชอบของตนในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศของหน่วยงาน โดยคำนึงถึงก่อน การจ้างงาน , ระหว่างการจ้างงาน , การเปลี่ยนตำแหน่ง หรือการสิ้นสุดการจ้างงาน

๕. การบริหารจัดการสินทรัพย์

องค์การบริหารส่วนตำบลสระ มีการระบุสินทรัพย์ที่สำคัญของหน่วยงานและกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์จากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจเกิดขึ้น อย่างเหมาะสม โดยประกอบด้วย

๑. นโยบายการบริหารจัดการสินทรัพย์ (Asset Management Policy)

องค์การบริหารส่วนตำบลสระ มีการระบุสินทรัพย์ที่สำคัญของสำนักงานและกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์อย่างเหมาะสม

๒. นโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy)

เพื่อให้สารสนเทศได้รับการปกป้องที่เหมาะสม โดยสอดคล้องกับสำคัญของสารสนเทศนั้นๆที่มีต่อองค์การบริหารส่วนตำบลสระ

๓. นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล

เพื่อป้องกันการเปิดเผยการเปลี่ยนแปลง แก้ไข การลบหรือการทำลายสินทรัพย์สารสนเทศโดยไม่ได้รับอนุญาต

๖. การควบคุมการเข้าถึงระบบสารสนเทศ

องค์การบริหารส่วนตำบลสระ มีนโยบายควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์สารสนเทศ สร้างความมั่นคงปลอดภัยให้กับ การดำเนินงานของหน่วยงานประกอบด้วย

๑. นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

องค์การบริหารส่วนตำบลสระ กำหนดกฎเกณฑ์และควบคุมการเข้าถึงข้อมูลและการใช้งาน ระบบสารสนเทศของสำนักงาน, ปกป้องข้อมูลและสารสนเทศจากการเข้าถึงโดยผู้ที่ไม่มีได้รับอนุญาต

๒. นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control Policy)

เพื่อรักษาความมั่นคงปลอดภัยและป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่มีได้รับอนุญาต

๓. นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control Policy)

องค์การบริหารส่วนตำบลสระ กำหนดกฎเกณฑ์ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือ แอปพลิเคชันและสารสนเทศของหน่วยงานจากผู้ที่ไม่ได้รับอนุญาต

๗. การเข้ารหัสลับของข้อมูล

องค์การบริหารส่วนตำบลสระ มีนโยบายกำหนดแนวทางการเข้ารหัสลับข้อมูลและทำให้ระบบ สารสนเทศรักษาไว้ซึ่งความลับของข้อมูล การพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และป้องกันการแก้ไข ข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและ เหมาะสม

๘. นโยบายความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

องค์การบริหารส่วนตำบลสระ กำหนดเป็นมาตรการควบคุมและป้องกัน และเป็นมาตรฐานความ มั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ พื้นที่ใช้งานระบบสารสนเทศ โดย พิจารณาตามความสำคัญของอุปกรณ์ระบบสารสนเทศ ข้อมูลซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษา ความลับ โดยมาตรการนี้จะมีผลบังคับกับผู้ใช้งานและผู้ให้บริการภายนอก

องค์การบริหารส่วนตำบลสระ
ตำบลสระ อำเภอยางชุมน้อย จังหวัดพะเยา