นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์

หลักการ

องค์การบริหารส่วนตำบลกระโด ได้มีข้อกำหนดสำหรับการใช้งาน การดูแลรักษา และการป้องกันให้เหมาะสมกับลักษณะการดำเนินกิจการ ซึ่งการดูแลรักษาและการป้องกันมุ่งหมายไปในทางความมั่นคงปลอดภัย โดยมีหลักการสำคัญคือการธำรงไว้ซึ่ง การรักษาความลับของข้อมูล ความถูกต้องครบถ้วน และความสมบูรณ์พร้อมใช้ ดังนี้

การรักษาความลับ (Confidentiality) หมายถึง การป้องกันไม่ให้สินทรัพย์สามารถถูกเข้าถึงได้จากผู้ไม่มีสิทธิ โดยการเข้าถึงยังรวมถึงการถูกเปิดเผยและการจำแนกแจกจ่ายซึ่งสินทรัพย์นั้นด้วย ดังนั้น ในการรักษาความลับจำเป็นจะต้องมีการควบคุมทั้ง ทางกายภาพและทางเทคนิค โดยผู้ที่ไม่มีสิทธิจะต้องไม่สามารถเข้าถึงสินทรัพย์นั้นได้และสินทรัพย์จำเป็นจะต้องมีการจำแนกและกำหนดระดับความต้องการในการป้องกันไว้อย่างชัดเจน เพื่อให้ผู้ที่ถือครองสินทรัพย์ปฏิบัติได้ถูกต้องเหมาะสมกับระดับความต้องการนั้น

ความถูกต้องครบถ้วน (Integrity) หมายถึง การป้องกันไม่ให้สินทรัพย์ถูกเปลี่ยนแปลงแก้ไขทั้งที่มีเจตนาหรือไม่ก็ตามจากผู้ไม่มีสิทธิที่จะแก้ไขสินทรัพย์เหล่านั้น ดังนั้นการควบคุมและป้องกันจึงต้องประกอบด้วยการกำหนดสิทธิในการแก้ไข กำหนดสิทธิในการเข้าถึง และจำเป็นต้องอาศัยการตรวจสอบทั้งจากการทำรายการบัญชีสินทรัพย์และทางเทคนิคประกอบด้วย

ความสมบูรณ์พร้อมใช้ (Availability) หมายถึง การที่ผู้มีสิทธิสามารถเข้าใช้งานสินทรัพย์นั้นได้เมื่อยามต้องการใช้งาน ซึ่งมีทั้งในทางกายภาพและทางเทคโนโลยี ได้แก่ การให้บริการระบบจดหมายอิเล็กทรอนิกส์ที่จำเป็นจะต้องให้บริการตลอดเวลา ดังนั้น เมื่อผู้ใช้ต้องการจะรับหรือส่ง ระบบจำเป็นที่จะต้องสามารถให้บริการได้ตลอดเวลา เป็นต้น

นโยบายการปฏิบัติ

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

๒. องค์การบริหารส่วนตำบลกระโด มีการกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้ และความเสี่ยงที่ยอมรับไม่ได้ เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงที่เกิดขึ้นในการประเมินความเสี่ยงที่เกิดขึ้น

๓. องค์การบริหารส่วนตำบลกระโด จัดให้มีการทบทวนนโยบายอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๔. องค์การบริหารส่วนตำบลกระโด มีการกำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อรับมือ ตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

๕. องค์การบริหารส่วนตำบลกระโด มีการประเมินผลสัมฤทธิ์ของนโยบายที่ประกาศใช้ เพื่อนำมาปรับปรุงนโยบาย แผนกลยุทธ์ให้สอดคล้องกับภัยคุกคามในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต

๖. องค์การบริหารส่วนตำบลกระโด จัดให้มีทรัพยากร ด้านงบประมาณ ทรัพยากรบุคคล การบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการด้านความมั่นคงปลอดภัยขององค์กร

โครงสร้างทางด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์การบริหารส่วนตำบลกระโด

องค์การบริหารส่วนตำบลกระโดกำหนดมาตรการควบคุม กำกับและติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับส่วนงานต่าง ๆ ภายในสำนักงาน และเพื่อเป็นแนวทางการควบคุมอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอกให้เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) แบ่งเป็น ๒ ส่วน คือ

๑. การจัดโครงสร้างภายในองค์กร (Internal Organization)

องค์การบริหารส่วนตำบลกระโดมีกำหนดบทบาทหน้าที่ ความรับผิดชอบในการใช้ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมและมีความมั่นคงปลอดภัยทางไซเบอร์

๒. นโยบายการควบคุมอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอก (Computing Device and Teleworking Policy)

เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอกองค์การบริหารส่วนตำบลกระโด

นโยบายความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล

องค์การบริหารส่วนตำบลกระโดมีกระบวนการในการคัดเลือกบุคลากร ฝึกอบรมและควบคุมการปฏิบัติงานของบุคลากรในสำนักงานอย่างเหมาะสมตลอดระยะเวลาการจ้างงานและเพื่อให้เข้าใจถึงหน้าที่ความรับผิดชอบของตนในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศของสำนักงาน โดยคำนึงถึงก่อนการจ้างงาน, ระหว่างการจ้างงาน, การเปลี่ยนตำแหน่งหรือการสิ้นสุดการจ้างงาน

การบริหารจัดการสินทรัพย์

องค์การบริหารส่วนตำบลกระโดมีการระบุสินทรัพย์ที่สำคัญของสำนักงานและกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์จากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจเกิดขึ้นอย่างเหมาะสม โดยประกอบด้วย

๑. นโยบายการบริหารจัดการสินทรัพย์ (Asset Management Policy)

องค์การบริหารส่วนตำบลกระโดมีการระบุสินทรัพย์ที่สำคัญของสำนักงานและกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์อย่างเหมาะสม

๒. นโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy

เพื่อให้สารสนเทศได้รับการปกป้องที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้น ๆ ที่มีต่อสำนักงาน

๓. นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล

เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายสินทรัพย์สารสนเทศโดยไม่ได้รับอนุญาต

การควบคุมการเข้าถึง

องค์การบริหารส่วนตำบลกระโดมีนโยบายควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์สารสนเทศ สร้างความมั่นคงปลอดภัยให้กับการดำเนินงานของสำนักงาน ประกอบด้วย

๑. นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

สำนักงานกำหนดกฎเกณฑ์และควบคุมการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศของสำนักงาน, ปกป้องข้อมูลและสารสนเทศจากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

๒. นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control Policy)

เพื่อรักษาความมั่นคงปลอดภัยและป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๓. นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control Policy)

องค์การบริหารส่วนตำบลกระโดกำหนดกฎเกณฑ์ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศของสำนักงานจากผู้ที่ไม่ได้รับอนุญาต

การเข้ารหัสลับข้อมูล

องค์การบริหารส่วนตำบลกระโดมีนโยบายกำหนดแนวทางการเข้ารหัสลับข้อมูลและทำให้ระบบสารสนเทศรักษาไว้ซึ่งความลับของข้อมูล การพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและ เหมาะสม

นโยบายความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

องค์การบริหารส่วนตำบลกระโดกำหนดเป็นมาตรการควบคุมและป้องกัน และเป็นมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ พื้นที่ใช้งานระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบสารสนเทศ ข้อมูลซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับกับผู้ใช้งานและผู้ให้บริการภายนอก