



แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เทศบาลตำบลกกโก ประจำปีงบประมาณ พ.ศ. ๒๕๖๙



เทศบาลตำบลกกโก
อำเภอเมืองลพบุรี จังหวัดลพบุรี



ประกาศเทศบาลตำบลกกโก
เรื่อง แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เทศบาลตำบลกกโก
ประจำปีงบประมาณ พ.ศ.๒๕๖๙

.....

ตามที่เทศบาลตำบลกกโก ได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เทศบาลตำบลกกโก ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ เพื่อนำไปใช้เป็นกรอบแนวทางการบริหารจัดการ ความเสี่ยง เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ควบคุม แก้ไขความเสี่ยงและปัญหาจากภัยพิบัติ ด้านเทคโนโลยี สารสนเทศที่อาจเกิดขึ้น และเพิ่มประสิทธิภาพให้กับระบบสารสนเทศ ของเทศบาลตำบลกกโก

เพื่อนำไปใช้เป็นกรอบแนวทางการบริหารจัดการความเสี่ยง เตรียมความพร้อมและรองรับ สถานการณ์ฉุกเฉิน ควบคุม แก้ไขความเสี่ยงและปัญหาจากภัยพิบัติด้านเทคโนโลยี สารสนเทศที่อาจเกิดขึ้น และเพิ่มประสิทธิภาพให้กับระบบสารสนเทศ ของเทศบาลตำบลกกโก จึงจัดทำแผนบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ เทศบาลตำบลกกโก ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ขึ้น เพื่อหาวิธีการป้องกัน ปัญหาที่อาจเกิดขึ้น อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงาน การบริหารจัดการ ความเสี่ยงระบบสารสนเทศของเทศบาลตำบลกกโก

ทั้งนี้ ตั้งแต่วันที่ ๒๕ กันยายน ๒๕๖๙ เป็นต้นไป

ประกาศ ณ วันที่ ๒๕ เดือน กันยายน พ.ศ. ๒๕๖๙

(นายก่องณ อุ้นสกุล)
นายกเทศมนตรีตำบลกกโก

คำนำ

เทศบาลตำบลกกโกตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่อาจเกิดขึ้น ไม่ว่าจะเป็นความเสี่ยงที่เกิดขึ้นจากธรรมชาติหรือการกระทำของมนุษย์ เช่น อัคคีภัย อุทกภัย ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ การบุกรุกหรือโจมตีจากภายนอก การก่อวินาศกรรมจาก Hacker หรือ การเจาะทำลาย ระบบจาก Cracker ไวรัสคอมพิวเตอร์ สถานการณ์ความไม่สงบ สถานการณ์โรคระบาด เป็นต้นซึ่งสามารถสร้าง ความเสียหายให้กับฐานข้อมูล ระบบสารสนเทศ โปรแกรมซอฟต์แวร์ ตลอดจนอุปกรณ์ คอมพิวเตอร์ ของเทศบาลตำบลกกโก

เทศบาลตำบลกกโก จึงจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เทศบาลตำบล กกโก ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ เพื่อนำไปใช้เป็นกรอบแนวทางการบริหารจัดการความเสี่ยง เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ควบคุม แก้ไขความเสี่ยงและปัญหาจากภัยพิบัติด้าน เทคโนโลยี สารสนเทศที่อาจเกิดขึ้น และเพิ่มประสิทธิภาพให้กับระบบสารสนเทศ ของเทศบาลตำบลกกโก

คณะกรรมการบริหารศูนย์เทคโนโลยีสารสนเทศ

เทศบาลตำบลกกโก

กันยายน ๒๕๖๙

สารบัญ

คำนำ	ก
สารบัญ	ข
บทที่ ๑ บทนำ	๑
๑. หลักการและเหตุผล	๑
๒. วัตถุประสงค์	๑
๓. ขอบเขตการดำเนินการ	๒
บทที่ ๒ ความหมายและกรอบการบริหารความเสี่ยง	๓
๑. ความหมายของการบริหารความเสี่ยง	๓
๒. กรอบการบริหารความเสี่ยง	๓
บทที่ ๓ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก	๙
๑. วิเคราะห์สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ	๙
๒. ปัจจัยความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๒
๓. ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๓
๔. การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๑๔
๕. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ	๒๒
บทที่ ๔ แผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)	๒๙
เทศบาลตำบลกกโก	
๑. การดำเนินการป้องกันภัยพิบัติ	๒๙
๒. การเตรียมความพร้อม	๓๔
๓. การกำหนดผู้รับผิดชอบ	๓๕
๔. กระบวนการแก้ไขปัญหายภัยพิบัติ	๓๖
๕. การกู้คืนระบบ	๔๙
๖. การซ่อมแผนการแก้ไขความเสี่ยง	๕๒
๗. การติดตามและรายงานผล	๕๒
ภาคผนวก	๕๔

บทที่ ๑

บทนำ

๑. หลักการและเหตุผล

เทศบาลตำบลกกโกมีภารกิจในการให้บริการสาธารณะและอำนวยความสะดวกให้กับประชาชนในท้องที่ ตั้งแต่การแจ้งเกิด, การแจ้งตาย, การขึ้นทะเบียนผู้พิการ, ขึ้นทะเบียนผู้สูงอายุ, ขึ้นทะเบียนเด็กแรกเกิด, การรับเรื่องร้องเรียนร้องทุกข์ ฯลฯ เป็นต้น ตามอำนาจหน้าที่ ตามพระราชบัญญัติเทศบาล พ.ศ. ๒๔๙๖ แก้ไขเพิ่มเติมถึงฉบับที่ ๑๔ และปัจจุบันเทศบาลตำบลกกโก ได้นำเอาระบบเทคโนโลยีสารสนเทศและสื่อสารเข้ามามีบทบาทสำคัญต่อการปฏิบัติงานของหน่วยงาน ฉะนั้นเพื่อให้การนำเอาระบบเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานเกิดประโยชน์สูงสุด และลดโอกาสความเสียหายที่อาจเกิดขึ้น จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงาน การบริหารจัดการความเสี่ยงระบบสารสนเทศของเทศบาลตำบลกกโกและตามนโยบายของนายกเทศมนตรีตำบลกกโก ต้องการให้เทศบาลตำบลกกโกก้าวเข้าสู่เป็นท้องถิ่นดิจิทัล หรือเป็นเมืองอัจฉริยะ (Smart City) ที่เป็นเมืองที่ใช้ประโยชน์จากเทคโนโลยีและนวัตกรรมที่ทันสมัยและชาญฉลาด เพื่อเพิ่มประสิทธิภาพของการให้บริการและการบริหารจัดการเมือง ลดค่าใช้จ่ายและการใช้ทรัพยากรของเมืองและประชากรเป้าหมาย โดยเน้นการออกแบบที่ดี และการมีส่วนร่วมของภาคธุรกิจและภาคประชาชนในการพัฒนาเมือง ภายใต้แนวคิด “กกโกเมืองน่าอยู่ อนุรักษ์เขตชุมชนวัฒนธรรม เกษตรกรรมนำเศรษฐกิจ มีคุณภาพชีวิตที่ดีทุกชุมชน”

มีวัตถุประสงค์เพื่อใช้เป็นแนวทางตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศของเทศบาลตำบลกกโก ด้วยการคาดการณ์ล่วงหน้าในกรณีที่มีความเสี่ยงนั้นเกิดขึ้นจริงและนำ แนวทางจัดการความเสี่ยงนี้ไปใช้ในดำเนินการ เป็นการช่วยเสริมสร้างความมั่นคงปลอดภัยระบบสารสนเทศ และความมั่นคงปลอดภัยทางด้านไซเบอร์ให้มีความแข็งแกร่งต่อการถูกโจมตีจาก Hacker และช่วยให้การพัฒนาทางด้านเทคโนโลยีสารสนเทศและการสื่อสารของกกโก มีขีดความสามารถในการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางตามยุทธศาสตร์กกโก เพื่อเป็นมาตรฐานในการรักษาความปลอดภัยระบบสารสนเทศของเทศบาลตำบลกกโก จึงได้จัดทำแผนบริหาร ความเสี่ยงด้านเทคโนโลยีสารสนเทศขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติในการบริหารจัดการความเสี่ยง การป้องกัน แก้ไขปัญหา และลดความเสียหาย อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมการปกครอง ท้องถิ่น และเป็นแนวทางที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ด้วยการคาดการณ์ล่วงหน้าในกรณีที่มีความเสี่ยงนั้นเกิดขึ้นจริงและนำแนวทางจัดการความเสี่ยงไปดำเนินการแก้ไขปัญหา และเพื่อให้แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สามารถบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ จึงได้ปรับปรุงและทบทวนแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ขึ้น

๒. วัตถุประสงค์

๑) เพื่อให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศภายในเทศบาลตำบลกกโกมีประสิทธิภาพ และมีความยืดหยุ่นในการปรับตัว ลดโอกาสที่จะก่อให้เกิดความเสียหายต่อระบบสารสนเทศ

๒) เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของ เทศบาลตำบลกกโก

๓) เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงและปัญหาจากภัยพิบัติด้านเทคโนโลยีสารสนเทศ

๔) เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

๓. ขอบเขตการดำเนินการ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เทศบาลตำบลกกโก ดำเนินการภายในขอบเขตงาน ดังนี้

- ๑) ศึกษาขั้นตอนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ๒) วิเคราะห์สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก
- ๓) ระบุประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก
- ๔) วิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก
- ๕) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก
- ๖) จัดทำแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก

บทที่ ๒

ความหมายและกรอบการบริหารความเสี่ยง

๑. ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือ ลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ หมายถึง ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำเทคโนโลยีสารสนเทศมาใช้ หรือมีการเปลี่ยนแปลงเทคโนโลยีหรือนวัตกรรมต่าง ๆ อย่าง เฉียบพลัน ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุ ของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการ ประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของ ความเสี่ยงที่ได้จากการ ประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลง อยู่ในระดับ ที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลด ความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อป้องกัน การควบคุมเพื่อให้ ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

๒. กรอบการบริหารความเสี่ยง

กรอบการบริหารความเสี่ยงตามแนวทางของ COSO (Committee of Sponsoring Organization) ประกอบด้วย ๘ ขั้นตอน ดังนี้

๒.๑ การกำหนดวัตถุประสงค์ (Objective Setting)

การกำหนดวัตถุประสงค์ที่ชัดเจนคือขั้นตอนแรกสำหรับกระบวนการบริหารความเสี่ยง องค์กรควร มั่นใจว่า วัตถุประสงค์ที่กำหนดมีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้

๒.๒ การระบุความเสี่ยง (Risk Identification)

เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งปัจจัยเสี่ยงที่เกิดจากภายในและภายนอกองค์กร เช่น นโยบายการบริหารงาน บุคลากร ระบบสารสนเทศ ระเบียบข้อบังคับ เป็นต้น ซึ่งความเสี่ยงของทุก องค์กรอาจ แบ่งได้เป็น ๔ ประเภท ได้แก่

๑) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) เป็นความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ และการปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบายเป้าหมายกลยุทธ์โครงสร้างองค์กร ทรัพยากรและสภาพแวดล้อมอันส่งผลกระทบต่อวัตถุประสงค์หรือเป้าหมายองค์กร

๒) ความเสี่ยงด้านการดำเนินงาน (Operational Risk) เป็นความเสี่ยงที่เกิดจากการปฏิบัติงาน ขั้นตอน อันเนื่องมาจากขาดการกำกับดูแลที่ดีหรือขาดการควบคุมภายในที่ดี โดยครอบคลุมถึงปัจจัย ที่เกี่ยวข้องกับกระบวนการ อุปกรณ์ เทคโนโลยีสารสนเทศ บุคลากร และความปลอดภัยของทรัพย์สิน ทุกๆ

๓) ความเสี่ยงด้านการเงิน (Financial Risk) เป็นความเสี่ยงที่เกี่ยวข้องกับทางการเงิน สภาพ คล่องทางการเงิน ความสามารถในการทำสรุปรายรับรายจ่าย, การรายงานทางการเงินและสถานะทางการเงิน

๔) ความเสี่ยงด้านกฎระเบียบ (Compliance Risk) เป็นความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับ

ทั้งนี้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้จัดทำคู่มือบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ และแบ่งประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ ๘ ประเภท ดังนี้

๑) ความเสี่ยงด้านข้อมูล (Information Risk) หมายถึง ความเสี่ยงที่เกิดจากข้อมูลต่างๆ ในระบบ เทคโนโลยีสารสนเทศ ไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลง โดย บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผล ที่ผิดพลาดโดยอาจมี สาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจ เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access Risk) ทำให้ข้อมูลที่จัดเก็บรั่วไหล อาจทำให้เกิดการ ฟ้องร้องได้ หรือมีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่าง ต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากไม่มีการ ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ ยังรวมถึงความเสี่ยง เกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Backup) ที่สำคัญ คือ เพื่อไม่ให้ข้อมูล เกิดการสูญ หาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูล สำรอง (Information Back-Up) การกู้คืนข้อมูล (Information Recovery)

๒) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึงความเสี่ยงที่เกิดจากการเลือกใช้ หรือความเสี่ยงจากการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง การถูกผู้ไม่หวังดี ทำลายระบบ (Hacker) การควบคุมการ Reversion software ไม่เพียงพอ การที่ Software ที่ใช้ อยู่ Out of date ความเสี่ยงที่เกิดจากการเลือกใช้ Software platforms ความเสี่ยงที่เกิดจากการควบคุม การเปลี่ยนแปลง (Change control) ไม่เหมาะสมเพียงพอ ความเสี่ยงที่ไม่ได้กำหนดขั้นตอนการอนุมัติการใช้งาน Software การไม่ได้จัดทำ ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Document operating procedures) ความเสี่ยงจากการไม่แยก ระบบสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน (Separation of development, test and operation facilities) เป็นต้น

๓) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) หมายถึง ความเสี่ยงที่เกิดจาก ความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ที่ไม่เหมาะสม ความเสี่ยงใน เรื่องของการจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่เหมาะสมกับลักษณะของงานและขององค์กร ที่ต้องมีการจัดหา เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหา

และติดตั้งอุปกรณ์ เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการ และเหมาะสม กับงบประมาณ หรือความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงจากการที่อุปกรณ์ เทคโนโลยีสารสนเทศหมดอายุไปเอง ความเสี่ยงจากการไม่ได้กำหนด หรือกำหนดกระบวนการอนุมัติใช้อุปกรณ์ เทคโนโลยีสารสนเทศไม่ชัดเจน

๔) ความเสี่ยงด้านบุคลากร (People Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับ การดำเนินงานด้านเทคโนโลยีสารสนเทศในเรื่องของการกำหนดโครงสร้าง การมอบหมายงานในหน้าที่ให้แก่ บุคลากรด้านเทคโนโลยีสารสนเทศที่มีความเหมาะสม คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการ ถ่ายทอดเทคโนโลยีสารสนเทศ และสามารถถ่ายทอดความรู้ให้แก่ผู้ใช้งานด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ทั้งนี้ ยังรวมถึงการที่ขาดแผนการฝึกอบรมด้านเทคโนโลยีสารสนเทศให้กับเจ้าหน้าที่ของหน่วยงาน อย่างทั่วถึง ทั้งในส่วนของผู้ดูแลระบบ (Administration) ผู้พัฒนาระบบ (Developer/Programmer) และผู้ใช้งาน ทั่วไป (User) อย่างสม่ำเสมอ

๕) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่เกิดจากมนุษย์ เช่น วาตภัย อุทกภัย ไฟฟ้า น้ำท่วม

กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การไม่มีระบบรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย และการก่อการร้าย เป็นต้น

๖) ความเสี่ยงด้านเครือข่ายสื่อสาร (Network Communication Risk) หมายถึง ความเสี่ยงที่เกิด จากระบบเครือข่ายสื่อสารขัดข้อง ไม่มีระบบเครือข่ายสื่อสารสำรอง ความเสี่ยงที่เกิดจากไม่ได้กำหนดคุณสมบัติ ทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดในการบริหารจัดการสำหรับบริหารเครือข่ายทั้งหมดที่ องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่ายโดยที่บริการเครือข่ายเหล่านี้จะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก การบำรุงรักษาอุปกรณ์เครือข่าย สื่อสารไม่สม่ำเสมอ การไม่มีรายชื่อและข้อมูลสำหรับติดต่อหน่วยงานอื่นกรณีมีความจำเป็น เช่น บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) เป็นบริษัทที่ควรรวมระหว่าง บริษัท ทีโอที จำกัด (มหาชน) หรือ TOT กับ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) (CAT Telecom Public Company Limited) ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ให้กับเทศบาลตำบลกกโก ความเสี่ยงที่ผู้ดูแลระบบไม่มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย

และดูแลรักษาความมั่นคงปลอดภัย สำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่ายรวมทั้งสารสนเทศต่าง ๆ ที่ส่งผ่านทางเครือข่าย เป็นต้น

๗) ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing) หมายถึง ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำ โครงการด้านเทคโนโลยีสารสนเทศต่างๆ เช่น ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่ กำหนดไว้ เป็นต้น

๘) ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk) หมายถึง ความเสี่ยงที่เกิดจาก กระบวนการทางงานด้านเทคโนโลยีสารสนเทศที่ไม่เป็นไปตามมาตรฐานสากล ซึ่งส่งผลให้ขาดการนำ Best Practice ที่ดีมาใช้งาน

๒.๓ การประเมินความเสี่ยง (Risk Assessment)

เป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๑) การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาส ที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้ง เกณฑ์เชิงปริมาณ และเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมาก ที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยง อาจกำหนดเป็นเกณฑ์ ๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๒) การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยง แต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรง หรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมี ความรุนแรงแตกต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับ มาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบ และมิติ โอกาสของความเสี่ยงที่จะเกิดขึ้น

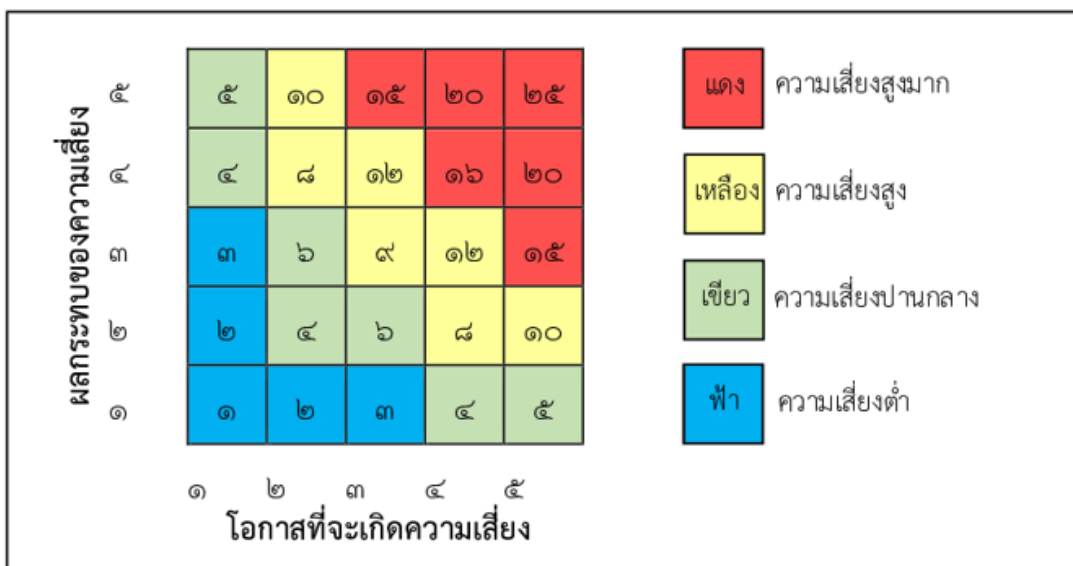
เกณฑ์การประเมินผลกระทบ เป็นดังนี้

<u>ระดับ</u>	<u>การประเมิน</u>
๑	น้อยมาก
๒	น้อย
๓	ปานกลาง
๔	สูง
๕	สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง เป็นดังนี้

<u>ระดับ</u>	<u>การประเมิน</u>
๑	เกิดขึ้นน้อยมาก
๒	เกิดขึ้นน้อย
๓	เกิดขึ้นปานกลาง
๔	เกิดขึ้นสูง
๕	เกิดขึ้นสูงมาก

๓) การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและ ผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยง สูงสุดที่จะต้องบริหารจัดการก่อน



ภาพตัวอย่างการวิเคราะห์ความเสี่ยง

๔ การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กรเพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมากหรือสูง มาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๒.๔ การตอบสนองความเสี่ยง (Risk Response)

ในการควบคุมและบรรเทาความเสี่ยง จะขึ้นอยู่กับค่าระดับความเสี่ยงที่ประเมินได้ ทางเลือกในการควบคุมหรือบรรเทาความเสี่ยงจะมีด้วยกัน ๔ ทางเลือก ดังนี้

๑) การยอมรับความเสี่ยง (Acceptance) กรณีที่ค่าระดับความเสี่ยงอยู่ในบริเวณสีฟ้า ผู้ประเมิน ความเสี่ยงสามารถยอมรับความเสี่ยงได้ กรณีการยอมรับความเสี่ยงยังหมายรวมถึง

- กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเขียว สีเหลือง หรือ สีแดง ก็ตาม แต่หน่วยงาน ยังไม่สามารถระบุมาตรการที่เหมาะสมได้ จึงอาจต้องยอมรับความเสี่ยงไว้ก่อน ในภายหลังเมื่อได้มาตรการที่เหมาะสมแล้ว จึงเสนอมาตรการเพื่อหาทางลดความเสี่ยงให้ลดลงมาอยู่ในระดับสีฟ้า เป็นต้น

- กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเขียว สีเหลือง หรือ สีแดง แต่หน่วยงานพบว่าการ จัดการกับความเสี่ยงนี้จะมีค่าใช้จ่ายที่ค่อนข้างสูงและไม่คุ้มค่าที่จะลงทุน จึงเห็นสมควรให้ยอมรับความเสี่ยงและไม่ดำเนินการใด ๆ

๒) การเลี่ยงความเสี่ยง (Avoidance) คือ การหาหนทางที่เหมาะสมเพื่อหลีกเลี่ยงความเสี่ยงที่พบนั้น เช่น หากพบว่าการนำทรัพย์สินไปตั้งไว้ในบริเวณที่มีความเสี่ยงต่อการสูญหาย ก็ควรจะหลีกเลี่ยงโดยการนำไปจัดเก็บไว้ในสถานที่ที่ปลอดภัย, การตัดสินใจที่จะแลกเปลี่ยนข้อมูลสำคัญกับองค์กรหนึ่งผ่านทางระบบออนไลน์ เมื่อพบว่าองค์กรนั้นยังไม่มีมาตรการความมั่นคงปลอดภัยที่ดีเพียงพอ ก็อาจยับยั้งการตัดสินใจนั้น โดยหลีกเลี่ยง ความเสี่ยงไปใช้วิธีการแลกเปลี่ยนแบบ Manual แทน การหาหนทางที่เหมาะสมกว่า ควรพิจารณาว่าความเสี่ยง ลดลงมาอยู่ในระดับที่ยอมรับได้หรือไม่ เช่น ตกอยู่ในบริเวณสีฟ้าหรือไม่

๓) การโอนย้ายความเสี่ยง (Transfer) คือ การให้หน่วยงานอื่นเป็นผู้รับความเสี่ยงหรือดำเนินการ แทน เช่น การใช้ Outsource เรื่องการพัฒนาระบบให้หน่วยงานภายนอกโดยการทำสัญญาดูแลรักษาฮาร์ดแวร์ อุปกรณ์เครือข่าย การซื้อประกันภัยจากหน่วยงานภายนอก การโอนย้ายความเสี่ยง ควรพิจารณาว่า ผู้ดำเนินการ สามารถจัดการความเสี่ยงนั้นได้เป็นอย่างดีหรือไม่ ระดับความเสี่ยงที่เกิดจาก

ผู้ดำเนินการแทน ควรจะอยู่ในระดับที่ หน่วยงานยอมรับได้ หากผู้ดำเนินการแทนไม่สามารถทำได้ดี ความเสี่ยงจะตกกลับมาที่หน่วยงานเอง

๔) การลดความเสี่ยง (Reduction) คือ การหาทางลดค่าความเสี่ยงที่อาจตกอยู่ในบริเวณ สีเขียว สีเหลือง หรือ สีแดงก็ตาม ให้ลงมาอยู่ในระดับที่น้อยลง กรณีที่หน่วยงานสามารถลดความเสี่ยงลงมาอยู่ในบริเวณ สีฟ้าได้ หน่วยงานสามารถยอมรับความเสี่ยงได้และไม่ต้องทำอะไรเพิ่มเติม แต่หากอยู่ในบริเวณ สีเขียว หน่วยงานยัง ต้องคอยคุมความเสี่ยงไว้ (เพื่อป้องกันการเลื่อนระดับไปสู่ระดับที่สูงขึ้น) เมื่อมีการประเมินระดับความเสี่ยงในหัวข้อ ที่แล้ว หน่วยงานต้องพิจารณาค่าระดับความเสี่ยงนั้นและ ละตัดสินใจว่าจะใช้ทางเลือกใด (จาก ๑ ใน ๔ ทางเลือก) เพื่อจัดการกับความเสี่ยงที่ประเมินนั้น

๒.๕ การวิเคราะห์ (Cost – Benefit)

เป็นการวิเคราะห์ประมาณการต้นทุน/ค่าใช้จ่ายในการดำเนินการแผนบริหารความเสี่ยงและการประมาณการมูลค่าของผลกระทบจากความเสียหายที่ลดลงเมื่อเทียบกับไม่ดำเนินการใดๆ

๒.๖ กิจกรรมการควบคุม (Control Activities)

การกำหนดกิจกรรมและการปฏิบัติต่าง ๆ เพื่อช่วยลดหรือควบคุมความเสี่ยง เพื่อสร้างความมั่นใจ ว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้อง และทำให้การดำเนินงานบรรลุวัตถุประสงค์และเป้าหมาย องค์กร ป้องกันและลดระดับความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับ

๒.๗ สารสนเทศและการสื่อสาร (Information and Communication)

องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยงต่อไป ตามกรอบและขั้นตอนการปฏิบัติที่องค์กรกำหนด

๒.๘ การติดตามประเมินผล (Monitoring)

องค์กรจะต้องมีการติดตามผล เพื่อให้ทราบถึงผลการดำเนินงานว่าเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

บทที่ ๓

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ของเทศบาลตำบลกกโก

๑. วิเคราะห์สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

๑.๑ สภาพแวดล้อมภายใน

๑.๑.๑ อุปกรณ์คอมพิวเตอร์

๑.๑.๑.๑ เครื่องคอมพิวเตอร์แม่ข่าย

ลำดับ	รายการ	จำนวน	หน่วย
๑	เครื่องคอมพิวเตอร์แม่ข่าย ติดตั้ง Server สำนักงานเทศบาลตำบลกกโก	๑	เครื่อง

๑.๑.๑.๒ อุปกรณ์คอมพิวเตอร์สำนักงานและอุปกรณ์เครือข่าย

ลำดับ	รายการ	จำนวน	หน่วย
๑	คอมพิวเตอร์ตั้งโต๊ะ	๖๔	เครื่อง
๒	คอมพิวเตอร์โน้ตบุ๊ก	๑๑	เครื่อง
๓	เครื่องพิมพ์	๖๖	เครื่อง
๔	เครื่องสำรองไฟฟ้า (UPS)	๒๐	เครื่อง
๕	อุปกรณ์กระจายสัญญาณเครือข่าย (Switching)	๗	เครื่อง
๖	อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)	๗	เครื่อง
๗	เครื่องถ่ายเอกสาร	๑	เครื่อง

*ข้อมูลอุปกรณ์คอมพิวเตอร์ ณ วันที่ ๓๑ สิงหาคม ๒๕๖๙

๑.๑.๒ ระบบสารสนเทศ

๑) ระบบเว็บไซต์เทศบาลตำบลกกโก (www.kokko.go.th) เป็นระบบบริหารจัดการเว็บไซต์, ประชาสัมพันธ์และเปิดเผยข้อมูลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.๒๕๔๐ และเพื่อความโปร่งใสในการบริหารงานราชการของเทศบาลตำบลกกโก

๒) ระบบ Intranet เทศบาลตำบลกกโก ประกอบด้วยระบบสารสนเทศ ได้แก่

- ระบบจองห้องประชุม เป็นระบบทำรายการจองใช้ห้องประชุมและตรวจสอบรายการใช้ห้องประชุมของเทศบาลตำบลกกโก
- ระบบปฏิทินกิจกรรม เป็นระบบแจ้งกิจกรรมของเทศบาลตำบลกกโก เช่น การประชุมประจำเดือนของเทศบาลตำบลกกโก
- ระบบ e-Book เป็นระบบเผยแพร่และดาวน์โหลดหนังสืออิเล็กทรอนิกส์ของเทศบาลตำบลกกโก
- เว็บบอร์ด เป็นระบบเว็บบอร์ดสำหรับพูดคุย ตอบข้อซักถามของระหว่างประชาชนหรือบุคคลภายนอกกับบุคลากรในหน่วยงาน
- ระบบสร้าง QR Code เป็นระบบสำหรับสร้าง QR Code สำหรับดาวน์โหลดไฟล์และเชื่อมโยงไปยังหน้าเว็บเพจที่กำหนด

๓) ระบบบริหารจัดการเอกสารแบบรวมศูนย์ (Document Management System : DMS) เป็นระบบบริหารจัดการข้อมูลเอกสาร จัดเก็บและเรียกดูข้อมูลในรูปแบบไฟล์ดิจิทัล

๔) ระบบป้องกันไวรัสคอมพิวเตอร์ เป็นโปรแกรมสำหรับป้องกันการบุกรุกโจมตีคอมพิวเตอร์และ เครือข่ายจากไวรัสคอมพิวเตอร์

๕) ระบบติดตาม (Monitor) ระบบเครือข่ายคอมพิวเตอร์ เทศบาลตำบลกกโก เป็น ระบบแสดงสถานะของเครือข่ายอินเทอร์เน็ต และอินเทอร์เน็ต

๖) ระบบจัดเก็บข้อมูลอุปกรณ์เครือข่ายคอมพิวเตอร์ เทศบาลตำบลกกโก เป็นระบบแสดงสถานะการทำงานของอุปกรณ์เครือข่ายคอมพิวเตอร์

๗) ระบบ Web Conference เทศบาลตำบลกกโก เป็นระบบการประชุมทางไกลผ่านเครือข่ายอินเทอร์เน็ต

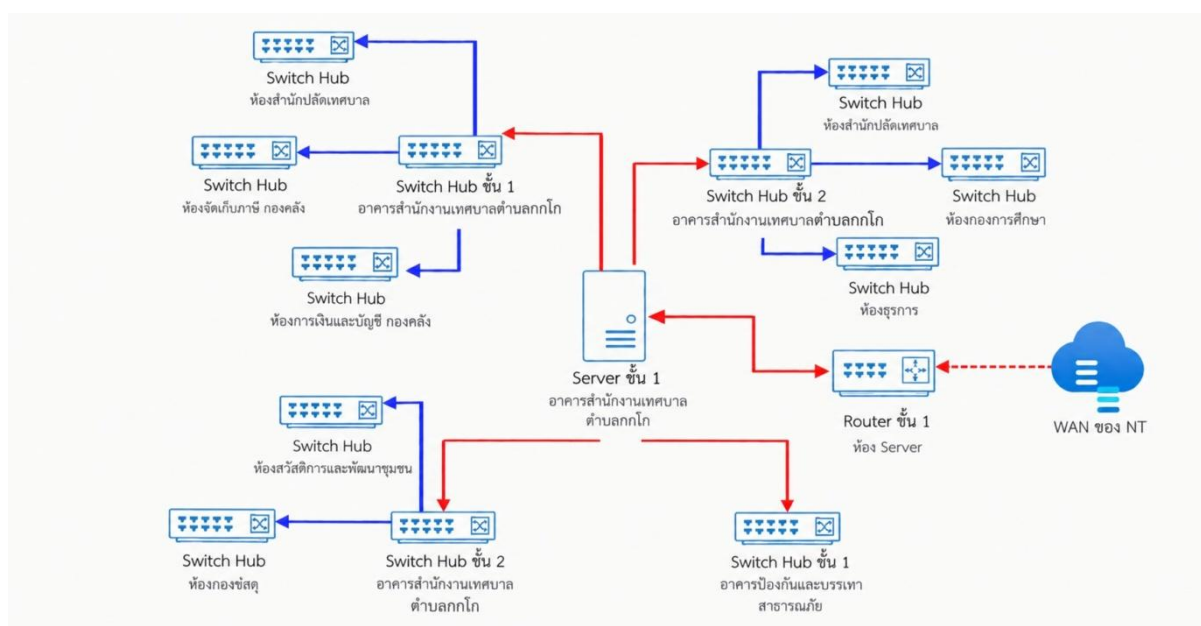
๘) ระบบจองห้องประชุม Conference เทศบาลตำบลกกโก เป็นระบบสำหรับจองใช้ ระบบ Web Conference ของเทศบาลตำบลกกโก

๙) ระบบสารบรรณอิเล็กทรอนิกส์ เป็นระบบงานสารบรรณของเทศบาลตำบลกกโก สำหรับบันทึกรับ-ส่งหนังสือราชการ

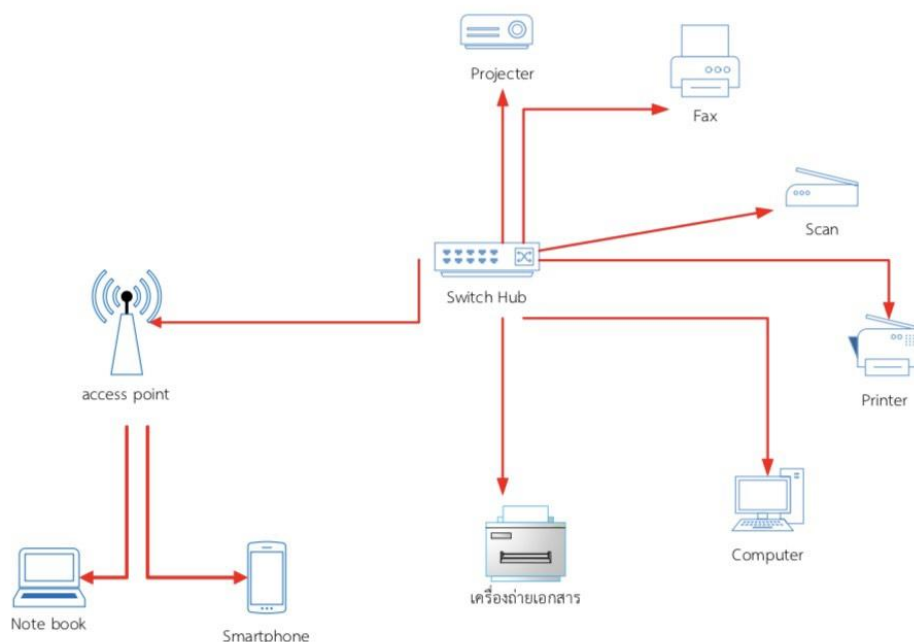
๑๐) ระบบไปรษณีย์อิเล็กทรอนิกส์ เป็นระบบไปรษณีย์อิเล็กทรอนิกส์ของเทศบาลตำบลกกโกที่ให้บริการแก่บุคลากรในสังกัด

๑๑) ระบบช่วยตอบข้อความ ตอบคำถาม ให้ข้อมูล ในรูปแบบ Chat Bot (Facebook, line OA, ฯลฯ) เพื่อบริหารข้อมูลของเทศบาลตำบลกกโกทั้งแบบอัตโนมัติและแบบ manual หรือเจ้าหน้าที่ตอบคำถามด้วยตัวเองในระบบ Chat Bot แก่ประชาชนและผู้ติดต่อประสานงานกับเทศบาลตำบลกกโก

๑๒) ระบบเว็บไซต์กกโก (www.กกโก.คอม) เป็นเว็บไซต์ที่ประชาสัมพันธ์และให้ความรู้เกี่ยวกับประวัติศาสตร์กกโก, สถานที่ท่องเที่ยว และสินค้า OTOP ให้กับนักท่องเที่ยวและประชาชนทั่วไปที่สนใจ และเป็นการช่วยกระตุ้นเศรษฐกิจในท้องถิ่น แม้ว่าเทศบาลตำบลกกโกไม่มีแหล่งท่องเที่ยว แต่ส่วนใหญ่จะมีที่พักอาศัยและร้านอาหาร ทำให้เกิดเศรษฐกิจหมุนเวียนในพื้นที่



รูปภาพ โครงข่ายเน็ตเวิร์ค ภาพรวมของเทศบาลตำบลกกโก



รูปภาพ ผังอุปกรณ์เครือข่าย อาคารสำนักงานเทศบาลตำบลกกโกและอาคารป้องกันและบรรเทาสาธารณภัย

๑.๑.๔ บุคลากร

เทศบาลตำบลกกโกมีบุคลากรปฏิบัติงานประจำศูนย์เทคโนโลยีสารสนเทศท้องถิ่น ดังนี้

ตำแหน่ง	จำนวนบุคลากร	
	กรอบอัตรากำลัง	ที่มีอยู่จริง
๑. ปลัดเทศบาล (นักบริหารงานท้องถิ่น ระดับต้น/กลาง)	๑	๑
๒. รองปลัดเทศบาล (นักบริหารงานท้องถิ่น ระดับต้น/กลาง)	๑	๑
๓. หัวหน้าสำนักงาน ระดับต้น/กลาง	๑	๑
๔. นักจัดการงานทั่วไป ระดับปฏิบัติการ/ชำนาญการ	๒	๒
๕. เจ้าพนักงานธุรการ ระดับปฏิบัติงาน/ชำนาญการ	๔	๔
๖. นักวิเคราะห์นโยบายและแผน	๑	๑
๗. ผู้ช่วยนักพัฒนาการท้องถิ่น	๑	๑
๘. ผู้ช่วยนักประชาสัมพันธ์	๑	๑
รวม	๑๒	๑๒

* ข้อมูลบุคลากร ณ วันที่ ๑ สิงหาคม ๒๕๖๙

๑.๒ สภาพแวดล้อมภายนอก

๑.๒.๑ ระบบสายสัญญาณ การใช้งานระบบสัญญาณอินเทอร์เน็ตของเทศบาลตำบลไชยปราการใช้งานผ่าน ๒ เครือข่าย ได้แก่

๑) สัญญาณอินเทอร์เน็ตของบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) เป็นบริษัทที่ควรรวมระหว่าง บริษัท ทีโอที จำกัด (มหาชน) หรือ TOT กับ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) (CAT Telecom Public Company Limited) เป็นเครือข่ายหลักสำหรับการใช้งาน ของเทศบาลตำบลกกโกในส่วนกลางมีการใช้งานจำนวน ๔ วงจร โดยมีรายละเอียดดังนี้

๑.๑) วงจรเดิมของบริษัท ทีโอที จำกัด (มหาชน) หรือ TOT มีจำนวน ๒ วงจร ได้แก่ วงจรหลักแบบ leased Line Internet (Fixed IP จำนวน ๔ IP) มีความเร็วเฉลี่ยในการวิ่งความเร็วในประเทศ ดาว์นโหลด ๑๐๐ Mbps การอัปโหลด ๑๐๐ Mbps วิ่งความเร็วต่างประเทศ ดาว์นโหลด ๒๐ Mbps การ อัปโหลด ๒๐ Mbps และวงจรสำรองมีความเร็วเฉลี่ยในการดาว์นโหลด ๑๐๐๐ Mbps การอัปโหลด ๗๐๐ Mbps สำหรับในส่วนภูมิภาคจะมีความเร็วในการดาว์นโหลดและอัปโหลดแตกต่างกันในแต่ละจังหวัด

๑.๒) วงจรเดิมของบริษัท กสท โทรคมนาคม จำกัด (มหาชน) (CAT Telecom Public Company Limited) มีจำนวน ๒ วงจร ได้แก่ วงจรหลักแบบ Fixed IP จำนวน ๕ IP มีความเร็วเฉลี่ยความเร็ว ดาว์นโหลด ๗๐ Mbps การอัปโหลด ๑๐ Mbps และอีกวงจรความเร็วอินเทอร์เน็ต ดาว์นโหลด ๑๐๐๐ Mbps การอัปโหลด ๒๐๐ Mbps สำหรับในส่วนภูมิภาคจะมีความเร็วในการดาว์นโหลดและอัปโหลดแตกต่างกันในแต่ละจังหวัด

๒) สัญญาณสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) มีการใช้งานในส่วนกลาง โดยใช้เชื่อมต่อกับสำนักทะเบียน กรมการปกครอง และกรมบัญชีกลาง มีความเร็วเฉลี่ยในการดาว์นโหลดและ อัปโหลด ๒ Mbps

๑.๒.๒ ระบบไฟฟ้า

เทศบาลตำบลไชยปราการมีการใช้ไฟฟ้าจากการไฟฟ้าส่วนภูมิภาคอำเภอฝาง เมื่อเกิดเหตุ ไฟฟ้าขัดข้อง อาจส่งผลกระทบต่ออุปกรณ์คอมพิวเตอร์และระบบสารสนเทศของเทศบาลได้ ซึ่งได้มีการ ติดตั้งเครื่องสำรองไฟฟ้า เพื่อสำรองไฟฟ้า (UPS) สำหรับอุปกรณ์คอมพิวเตอร์ ของเทศบาลตำบลกกโก ใช้ขนาด ๑ kVA ดังนี้

๑) ห้อง Server ศูนย์เทคโนโลยีสารสนเทศ ของเทศบาลตำบลกกโก จำนวน ๑ เครื่อง สามารถสำรองไฟฟ้าได้เป็นเวลาไม่น้อยกว่า ครึ่งชั่วโมง ขึ้นอยู่กับการใช้กระแสไฟที่อุปกรณ์

๒) คอมพิวเตอร์ตั้งโต๊ะที่ใช้ในงานสำนักงาน มีการใช้งานเครื่องสำรองไฟฟ้า จำนวน ๓๒ เครื่อง

๓) ห้องระบบกล้องโทรทัศน์วงจรปิด CCTV ของเทศบาลตำบลกกโก จำนวน ๒ เครื่อง

๒. ปัจจัยความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ปัจจัยที่จะก่อให้เกิดความเสียหายด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก ได้แก่

๑) ปัจจัยภายนอก ได้แก่

๑.๑) ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่ กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัย ความชื้นและอุณหภูมิที่ไม่เหมาะสม แผลงสัตว์กัดแทะ เป็นต้น

๑.๒) การโจรกรรมอุปกรณ์คอมพิวเตอร์

๑.๓) ระบบการเชื่อมโยงเครือข่ายขัดข้อง

๑.๔) ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๑.๕) การบุกรุกหรือโจมตีจากภายนอก การก่อวินาศกรรมจาก Hacker หรือการเจาะทำลายระบบ จาก Cracker

๑.๖) ไวรัสคอมพิวเตอร์

๑.๗) ระบบเสียหายจากภัยสงคราม/เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

๑.๘) สถานการณ์โรคระบาดโรคติดต่ออุบัติใหม่

๒) ปัจจัยภายใน ได้แก่

๒.๑) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๓. ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากการศึกษาสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก สามารถ จำแนกประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก ได้ดังนี้

๑) ความเสี่ยงด้านข้อมูล (Information Risk) เป็นความเสี่ยงที่ส่งผลให้ข้อมูลต่างๆ ในระบบ เทคโนโลยี สารสนเทศ ไม่ถูกต้องครบถ้วน ไม่สามารถใช้ข้อมูลได้ตามปกติ และฐานข้อมูลสูญหาย ได้แก่

- ๑.๑) การบุกรุกหรือโจมตีจากภายนอก
- ๑.๒) ไวรัสคอมพิวเตอร์หรือ Malware ทำลายข้อมูล
- ๑.๓) การบันทึกข้อมูลไม่ถูกต้องครบถ้วน

๒) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) เป็นความเสี่ยงที่ส่งผลให้การทำงานของโปรแกรมต่างๆ ผิดปกติ ได้แก่

- ๒.๑) การบุกรุกหรือโจมตีจากภายนอก
- ๒.๒) ไวรัสคอมพิวเตอร์หรือ Malware บุกรุกและทำลายระบบ
- ๒.๓) การใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้อง ๒.๔) ซอฟต์แวร์หมดอายุ

๓) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) ได้แก่

- ๓.๑) การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม
- ๓.๒) การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่มีมาตรฐาน

๔) ความเสี่ยงด้านบุคลากร (People Risk) ได้แก่

- ๔.๑) ขาดแคลนบุคลากรปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

๕) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) เป็นความเสี่ยง ที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยจากมนุษย์ ได้แก่

- ๕.๑) อัคคีภัย
- ๕.๒) อุทกภัย/น้ำรั่วซึม
- ๕.๓) แผ่นดินไหว
- ๕.๔) ความชื้นและอุณหภูมิที่ไม่เหมาะสม
- ๕.๕) แมลงสัตว์กัดแทะอุปกรณ์
- ๕.๖) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ
- ๕.๗) ภัยสงคราม/เหตุจลาจล และสถานการณ์ความไม่สงบ
- ๕.๘) สถานการณ์โรคระบาด
- ๕.๙) การโจรกรรมอุปกรณ์คอมพิวเตอร์

๖) ความเสี่ยงด้านเครือข่ายสื่อสาร (Network Communication Risk) ได้แก่

- ๖.๑) การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต
- ๖.๒) การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง

๗) ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing) ได้แก่

- ๗.๑) การพัฒนา/บำรุงรักษาระบบไม่ทันกำหนด หรือไม่ปฏิบัติตามสัญญาจ้าง
- ๗.๒) การรักษาความลับของข้อมูล

๘) ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk) เป็นความเสี่ยงที่เกิดจากกระบวนการ ทำงานด้านเทคโนโลยีสารสนเทศที่ไม่เป็นไปตามมาตรฐานสากล ได้แก่

- ๘.๑) ระบบสารสนเทศไม่สอดคล้องกับระเบียบกฎหมายใหม่

๔. การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโกสามารถวิเคราะห์และประเมินระดับความเสี่ยง ได้ดังนี้

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส x ความรุนแรง)
IT๑	การบุกรุกหรือโจมตีจากภายนอก	ความเสี่ยงด้านข้อมูล และ ความเสี่ยงด้านโปรแกรม คอมพิวเตอร์	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย	- Hacker - Cracker - การโจมตีการให้บริการ (denial of service/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - การจัดหา พัฒนา และการบำรุงรักษาระบบสารสนเทศขาด ความมั่นคงปลอดภัย	ฐานข้อมูล, ระบบสารสนเทศ และ โปรแกรมซอฟต์แวร์ ได้รับ ความเสียหายไม่สามารถ ใช้งานได้ ตามปกติ	๒ x ๔ = ๘
IT๒	ไวรัสคอมพิวเตอร์หรือ Malware ทำลายข้อมูลและระบบ	ความเสี่ยงด้านข้อมูล และ ความเสี่ยงด้านโปรแกรม คอมพิวเตอร์	ผู้ใช้งานภายในองค์กรนำอุปกรณ์ที่มีไวรัสหรือ Malware มาเชื่อมต่อกับคอมพิวเตอร์ หรือเปิดอ่านอีเมลที่มีไวรัสหรือ Malware หรือดาวน์โหลดไฟล์ไวรัสมาจากเว็บไซต์	- ไวรัส/ Malware - ขาดความระมัดระวังในการเปิดใช้งานอุปกรณ์บันทึกข้อมูล การเปิดอ่านอีเมล หรือ การดาวน์โหลดไฟล์จากเว็บไซต์	ฐานข้อมูล, ระบบสารสนเทศ และ โปรแกรม ซอฟต์แวร์ได้รับความ เสียหายไม่สามารถใช้งาน ได้ตามปกติ	๒ x ๔ = ๘
IT๓	การบันทึกข้อมูลไม่ถูกต้อง ครบถ้วน	ความเสี่ยงด้านข้อมูล	ผู้ใช้งานนำข้อมูลที่ไม่ถูกต้องหรือไม่ครบถ้วนเข้าสู่ระบบ ตลอดทั้งมีการเข้าใช้งานระบบโดยใช้ User/password ของบุคคลอื่นเพื่อเข้าถึงข้อมูลและเปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	- ขาดความระมัดระวังและความเข้าใจในการบันทึกข้อมูล - การอำพรางหรือสวมรอยผู้ใช้งาน - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับ อนุญาต	ระบบฐานข้อมูลที่ไม่ครบถ้วนถูกต้อง ไม่สามารถนำข้อมูลมาใช้ประโยชน์	๒ x ๔ = ๘

๔. การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโกสามารถวิเคราะห์และประเมินระดับความเสี่ยง ได้ดังนี้

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส x ความรุนแรง)
IT๔	การใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ถูกต้อง	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย เช่น MS Office	- การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - ขาดงบประมาณ/ไม่มีการตั้งงบประมาณสำหรับจัดซื้อซอฟต์แวร์	หน่วยงานอาจถูกฟ้องร้อง เรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	๑ X ๓ = ๓
IT๕	ซอฟต์แวร์หมดอายุ	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	ซอฟต์แวร์ที่ใช้อยู่หมดอายุ (Out of date) ทำให้ไม่สามารถใช้งานซอฟต์แวร์ได้	- ขาดงบประมาณ/ไม่มีการตั้งงบประมาณสำหรับจัดซื้อซอฟต์แวร์	ไม่สามารถใช้งานซอฟต์แวร์ได้	๑ X ๓ = ๓
IT๖	การติดตั้งอุปกรณ์เทคโนโลยี สารสนเทศ ในพื้นที่ที่ไม่เหมาะสม	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	การติดตั้งอุปกรณ์ในพื้นที่ที่เกิดความเสียหาย/ชำรุดได้ง่าย หรือติดตั้งในจุดที่ไม่สามารถใช้งานได้ หรือจุดอับสัญญาณ	- สภาพแวดล้อม แสงแดด น้ำฝน ต้นไม้ ทำให้อุปกรณ์ได้รับความเสียหาย - ฝาผนัง เสาค้ำพัง ต้นไม้ ปิดบังสัญญาณเครือข่าย	- อุปกรณ์เทคโนโลยีเสื่อมสภาพ/ชำรุด - ผู้ใช้งานไม่สามารถใช้งานอุปกรณ์ได้เต็มประสิทธิภาพ	๒ X ๓ = ๖
IT๗	เครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่มีมาตรฐาน	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	ใช้อุปกรณ์ที่ไม่มีมาตรฐานเพียงพอ เกิดการชำรุดได้ง่าย และไม่มีความปลอดภัยเพียงพอ	- การนำเครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่มีมาตรฐานมาใช้งาน	เครื่องคอมพิวเตอร์และอุปกรณ์เกิดการชำรุดได้ง่าย และขาดความมั่นคงปลอดภัย	๑ X ๓ = ๓

๔. การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโกสามารถวิเคราะห์และประเมินระดับความเสี่ยง ได้ดังนี้

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส x ความรุนแรง)
IT๘	ขาดแคลนบุคลากรปฏิบัติงานด้านเทคโนโลยีสารสนเทศ	ความเสี่ยงด้านบุคลากร	การขาดแคลนบุคลากรด้านเทคโนโลยีสารสนเทศ อาจทำให้การทำงานหยุดชะงัก หากบุคลากร ผู้รับผิดชอบไม่สามารถมา ปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน	- หน่วยงานขาดแคลนบุคลากร - การย้าย หรือออกจากราชการโดยไม่มีบุคลากรมาทดแทน	การพัฒนาระบบ ,ควบคุม ระบบ และงานด้าน เทคโนโลยีสารสนเทศเกิด ความล่าช้า	$3 \times 2 = 6$
IT๙	อัคคีภัย	ความเสี่ยงด้านกายภาพและสิ่ง แวดล้อม	การเกิดไฟไหม้อาคาร ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้	ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง	ระบบคอมพิวเตอร์และระบบเครือข่ายได้รับความเสียหายทั้งหมดหรือ บางส่วน	$1 \times 5 = 5$
IT๑๐	อุทกภัย/น้ำรั่วซึม	ความเสี่ยงด้านกายภาพและ สิ่งแวดล้อม	การเกิดน้ำท่วมจนต้องดำเนินการตัดกระแสไฟฟ้าและไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้ หรือน้ำรั่วซึมเข้าสู่ห้องคอมพิวเตอร์	น้ำท่วมซึ่งเป็นภัยธรรมชาติ หรือน้ำรั่วซึมเข้าสู่ห้องคอมพิวเตอร์	- ระบบคอมพิวเตอร์และระบบเครือข่ายได้รับความเสียหายทั้งหมดหรือ บางส่วนจากน้ำท่วม - ไม่สามารถใช้งานระบบ คอมพิวเตอร์ได้เนื่องจาก การตัดกระแสไฟฟ้า	$2 \times 5 = 10$

๔. การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโกสามารถวิเคราะห์และประเมินระดับความเสี่ยง ได้ดังนี้

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส x ความรุนแรง)
IT๑๑	แผ่นดินไหว	ความเสี่ยงด้านกายภาพ และ สิ่งแวดล้อม	การเกิดภัยธรรมชาติ แผ่นดินไหว อาคารได้รับความเสียหายและไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้	ภัยธรรมชาติ	ระบบคอมพิวเตอร์และระบบเครือข่ายได้รับความเสียหายทั้งหมดหรือ บางส่วน	$๒ \times ๓ = ๖$
IT๑๒	ความชื้นและอุณหภูมิที่ไม่ เหมาะสม	ความเสี่ยงด้านกายภาพ และ สิ่งแวดล้อม	ปัญหาความชื้น อุณหภูมิที่ไม่เหมาะสมภายในห้องคอมพิวเตอร์ แม่ข่าย ส่งผลให้ระบบคอมพิวเตอร์ได้รับความเสียหายทั้งหมดหรือบางส่วน	ระบบควบคุมความชื้นภายใน ห้องคอมพิวเตอร์แม่ข่ายทำงาน ผิดปกติ/ชำรุด	ระบบคอมพิวเตอร์และระบบเครือข่ายได้รับความเสียหายทั้งหมดหรือ บางส่วน	$๑ \times ๕ = ๕$
IT๑๓	แมลงสัตว์กัดแทะ อุปกรณ์	ความเสี่ยงด้านกายภาพ และ สิ่งแวดล้อม	แมลงสัตว์กัดแทะอุปกรณ์ เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์	สัตว์กัดแทะประเภทหนู หรือ แมลง	เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ได้รับความเสียหาย	$๒ \times ๔ = ๘$
IT๑๔	ระบบกระแสไฟฟ้า ขัดข้อง/ไฟฟ้าดับ	ความเสี่ยงด้านกายภาพ และ สิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือ เกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูล	แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	- เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ลูกข่าย ไม่สามารถเปิดใช้งานได้ และได้รับความเสียหาย/ชำรุด - ระบบฐานข้อมูล ระบบสารสนเทศไม่สามารถใช้งานได้	$๒ \times ๔ = ๘$

๔. การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโกสามารถวิเคราะห์และประเมินระดับความเสี่ยง ได้ดังนี้

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส x ความรุนแรง)
			สารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ		และอาจทำให้ ข้อมูลสารสนเทศบางส่วน เกิดการสูญหาย	
IT๑๕	ภัยสงคราม/เหตุจลาจล และ สถานการณ์ความไม่สงบ	ความเสี่ยงด้านกายภาพ และ สิ่งแวดล้อม	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ หรือเกิดการบุกรุกและปิดล้อมหน่วยงาน	การชุมนุมประท้วง การจลาจล และก่อการร้าย	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ได้รับความเสียหาย ไม่สามารถใช้งานได้ ซึ่งเป็นผลกระทบมาจากการบุกรุกและปิดล้อมสถานที่ หรือการตัดไฟฟ้า เป็นต้น	๓ x ๔ = ๑๒
IT๑๖	สถานการณ์	ความเสี่ยงด้านกายภาพ และ สิ่งแวดล้อม	การเกิดสถานการณ์โรคระบาด จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	โรคระบาด โรคติดต่อที่ส่งผลกระทบต่อการเดินทางและ ทำงานของบุคลากร	ผู้ใช้งานและผู้ดูแลระบบ ไม่สามารถปฏิบัติงานที่หน่วยงานได้ตามปกติ	๒ x ๓ = ๖
IT๑๗	การโจรกรรมเครื่องคอมพิวเตอร์ และ อุปกรณ์	ความเสี่ยงด้านกายภาพ และ สิ่งแวดล้อม	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงานได้	- การลักทรัพย์ - ขาดการดูแลรักษาความปลอดภัย	เครื่องคอมพิวเตอร์และอุปกรณ์ไม่สามารถทำงานได้ตามปกติ	๑ x ๔ = ๔

๔. การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโกสามารถวิเคราะห์และประเมินระดับความเสี่ยง ได้ดังนี้

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส x ความรุนแรง)
IT๑๘	การเชื่อมต่อระบบเครือข่าย อินเทอร์เน็ต ชัดข้อง	ความเสี่ยงด้านเครือข่ายสื่อสาร	ไม่สามารถเชื่อมต่อเครือข่ายอินเทอร์เน็ตได้	- สายสัญญาณอินเทอร์เน็ตขาด/ชำรุด - สัญญาณอินเทอร์เน็ตจากผู้ให้บริการขัดข้อง	ไม่สามารถใช้งานระบบอินเทอร์เน็ต	๒ x ๔ = ๘
IT๑๙	การเชื่อมต่อระบบเครือข่าย อินทราเน็ต ชัดข้อง	ความเสี่ยงด้านเครือข่ายสื่อสาร	ไม่สามารถเข้าใช้ระบบงานในเครือข่ายอินทราเน็ตได้	- สายสัญญาณอินทราเน็ตชำรุด/ขัดข้อง - ระบบสารสนเทศ/ฐานข้อมูลที่ใช้ภายในเครือข่ายอินทราเน็ตขัดข้อง	ผู้ใช้งานไม่สามารถใช้งาน ระบบอินทราเน็ตได้	๒ x ๔ = ๘
IT๒๐	ผู้รับจ้าง (Outsource) พัฒนา/ บำรุงรักษา ระบบไม่ทันกำหนดหรือไม่เป็นไปตามสัญญาจ้าง	ความเสี่ยงจากการว่าจ้างหรือ จัดจ้างผู้ให้บริการภายนอก	ผู้รับจ้างพัฒนา/บำรุงรักษาระบบไม่ทันภายในระยะเวลาที่กำหนดหรือไม่เป็นไปตามข้อกำหนดการว่าจ้าง การปรับปรุงแก้ไขงานไม่ทันภายในระยะเวลาที่กำหนดตลอดทั้งระบบสารสนเทศขาดความมั่นคงปลอดภัย	- Outsource ขาดบุคลากร - การเปลี่ยนแปลงตัวเจ้าหน้าที่ ของ Outsource ทำให้งานไม่ต่อเนื่อง/เกิดข้อผิดพลาด - ความเข้าใจในงานไม่ตรงกัน	- การพัฒนา/บำรุงรักษาระบบไม่ทันกำหนดหรือไม่เป็นไปตามสัญญาจ้าง - ระบบสารสนเทศถูกเข้าถึงโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูล	๒ x ๔ = ๘

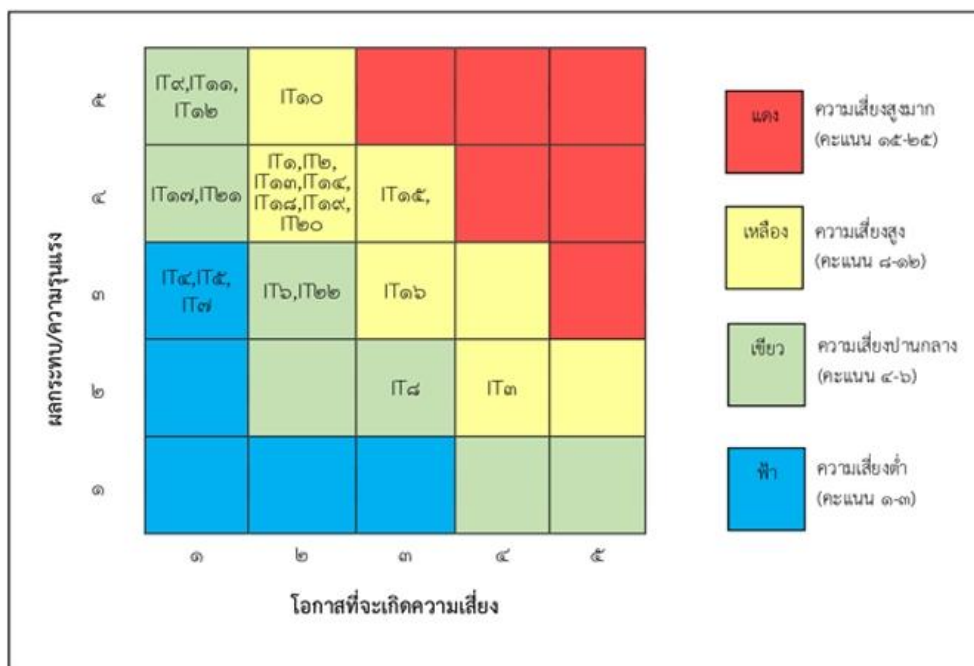
๔. การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโกสามารถวิเคราะห์และประเมินระดับความเสี่ยง ได้ดังนี้

รหัส	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ	ระดับความเสี่ยง (โอกาส x ความรุนแรง)
IT๒๑	ผู้รับจ้าง (Outsource) ไม่รักษาความลับของข้อมูล	ความเสี่ยงจากการว่าจ้างหรือ จัดจ้างผู้ให้บริการภายนอก	ผู้รับจ้างไม่รักษาความลับของข้อมูล เกิดการรั่วไหลของข้อมูล ไปยังบุคคลภายนอก	- Outsource ไม่ดูแลรักษา ข้อมูลให้เป็นความลับ - Outsource ที่หมดสัญญาเข้า ใช้งานระบบสารสนเทศโดยไม่ได้ รับอนุญาต	เกิดข้อมูลรั่วไหล เช่น ข้อมูลสารสนเทศ ข้อมูลระบบ ตลอดจนข้อมูล ส่วน บุคคล ตาม พ.ร.บ คื้มครองข้อมูลส่วนบุคคล	๑ x ๔ = ๔
IT๒๒	ระบบสารสนเทศไม่สอดคล้อง ทันสมัยกับระเบียบกฎหมาย	ความเสี่ยงด้านกระบวนการ ทำงาน	การปฏิบัติตามขั้นตอนใช้งานระบบสารสนเทศไม่ทันสมัยกับระเบียบกฎหมายในปัจจุบัน	- มีการพัฒนาระบบสารสนเทศก่อนประกาศหรือปรับปรุงระเบียบกฎหมายที่ใช้ในปัจจุบัน	การใช้งานระบบสารสนเทศในบางขั้นตอน ไม่สอดคล้อง/ทันสมัยกับ ระเบียบกฎหมาย	๒ x ๓ = ๖

จากการวิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก สามารถนำมาอธิบายด้วยแผนภาพการวิเคราะห์ความเสี่ยง ซึ่งแสดงความสัมพันธ์ระหว่างโอกาส ที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยงต่อองค์กร โดยกำหนดระดับความเสี่ยงเป็น ๔ ระดับ ดังนี้

- | | |
|-----------------------------------|----------------|
| ๑) ความเสี่ยงสูงมาก (คะแนน ๑๕-๒๕) | มีจำนวน ๐ ข้อ |
| ๒) ความเสี่ยงสูง (คะแนน ๘-๑๒) | มีจำนวน ๑๑ ข้อ |
| ๓) ความเสี่ยงปานกลาง (คะแนน ๔-๖) | มีจำนวน ๘ ข้อ |
| ๔) ความเสี่ยงต่ำ (คะแนน ๑-๓) | มีจำนวน ๓ ข้อ |



รูปภาพ แผนภาพการวิเคราะห์ความเสี่ยง

๕. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เมื่อทำการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลไชยปราการแล้ว จึงจัดเรียงระดับความเสี่ยงจากความเสี่ยงสูงไปความเสี่ยงต่ำ กำหนดกลยุทธ์การจัดการ ความเสี่ยงและแนวทางการดำเนินการจัดการความเสี่ยง ดังนี้

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง		กลยุทธ์การจัดการ ความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
		ระดับ	คะแนน		
๑	IT๑๕ ภัยสงคราม/เหตุ จลาจล และ สถานการณ์ความไม่สงบ	ความเสี่ยงสูง	๑๒	การลดความเสี่ยง	- มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ - จัดทำแผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย
๒	IT๑๐ อุทกภัย/น้ำท่วม	ความเสี่ยงสูง	๑๐	การลดความเสี่ยง	- ติดตั้งระบบแจ้งเตือนน้ำท่วมเข้าสู่ห้องคอมพิวเตอร์แม่ข่าย - มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ - จัดทำแผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย
๓	IT๑๐ สถานการณ์โรค ระบาด	ความเสี่ยงสูง	๙	การลดความเสี่ยง	- เตรียมความพร้อม เครื่องมือและอุปกรณ์การทำงานให้เป็นอิเล็กทรอนิกส์ เพื่อรองรับนโยบาย Work From Home - จัดทำแผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย
๔	IT๑ การบุกรุกหรือโจมตี จากภายนอก	ความเสี่ยงสูง	๘	การลดความเสี่ยง	- สแกนหาจุดอ่อนและอัปเดต Patch โดยใช้ซอฟต์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่ - ติดตั้ง Firewall และตรวจสอบการตั้งค่า Policy, Log ของ Firewall อย่างสม่ำเสมอ

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง		กลยุทธ์การจัดการ ความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
		ระดับ	คะแนน		
					- ติดตั้ง Proxy Server ซึ่งกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ - จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่าย อินเทอร์เน็ตและ อินทราเน็ต เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบ เทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สืบหาสาเหตุ และป้องกันต่อไป - ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัปเดตอย่างสม่ำเสมอและปิดพอร์ตที่ไม่มี การใช้งาน - กำหนด password เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต - ป้องกันการปลอมแปลง IP address โดยการกรอง packet ที่มาจากภายนอก โดยการนำ ระบบ DMZ มากรอง IP ที่จะเข้ามายังระบบเครือข่าย - ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOS และ DDOS - ประกาศใช้นโยบายการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ และการควบคุมการรักษา ความ ปลอดภัย ด้านเทคโนโลยีสารสนเทศ - จัดทำแผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย
๕	IT๒ ไวรัสมัลแวร์หรือ Malware ทำลาย ข้อมูลและระบบ	ความเสี่ยงสูง	๘	การลดความเสี่ยง	- ระมัดระวังการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ โดยการสแกนหาไวรัส ก่อนเปิด และไม่เปิด ไฟล์ที่นามสกุลแปลก - ระมัดระวังในการเปิด E-mail โดยไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา - ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต - ปิดการใช้งานฟังก์ชัน Autoplay เพื่อป้องกันไม่ให้ไวรัสที่แพร่ระบาดผ่านทางสื่อเก็บข้อมูลแบบ พกพาใช้เป็นช่องทางในการรันไฟล์ไวรัสโดยอัตโนมัติ - จัดทำแผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง		กลยุทธ์การจัดการ ความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
		ระดับ	คะแนน		
๖	IT๓ การบันทึกข้อมูลไม่ ถูกต้อง ครบถ้วน	ความเสี่ยงสูง	๘	การลดความเสี่ยง	- กำหนดให้มีการอบรมผู้ใช้งานระบบสารสนเทศ - จัดทำคู่มือการใช้งานระบบสารสนเทศ เพื่อให้ผู้ใช้งานระบบบันทึกข้อมูล ได้ถูกต้องครบถ้วนตรง ตามวัตถุประสงค์ของระบบสารสนเทศ - มีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศและฐานข้อมูล เพื่อให้การเข้าถึงข้อมูลเป็นไปตาม สิทธิของผู้ใช้งาน - ผู้ใช้งานระบบเก็บรักษา username และ password ไว้เป็นความลับ/ ไม่ให้ผู้อื่นทราบ - ประกาศใช้นโยบายการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ และการ ควบคุมการรักษา ความ ปลอดภัย ด้านเทคโนโลยีสารสนเทศ
๗	IT๑๓ แมลงสัตว์กัดแทะ อุปกรณ์	ความเสี่ยง ปานกลาง	๘	การลดความเสี่ยง	- ไม่นำอาหารหรือเครื่องดื่มมารับประทานหรือเก็บไว้ในบริเวณที่มีอุปกรณ์ คอมพิวเตอร์ - ใช้ท่อห่อหุ้มสายไฟฟ้าหรือสายสัญญาณ เพื่อป้องกันการกัดแทะ - จัดทำแผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย
๘	IT๑๔ ระบบกระแสไฟฟ้า ชัดข้อง/ ไฟฟ้าดับ	ความเสี่ยงสูง	๘	การลดความเสี่ยง	- ติดตั้งเครื่องสำรองไฟฟ้าให้กับเครื่องคอมพิวเตอร์แม่ข่าย - ติดตั้งเครื่องสำรองไฟฟ้าให้กับเครื่องคอมพิวเตอร์สำนักงาน และเมื่อเกิด กระแสไฟฟ้าดับ ให้รีบ บันทึกข้อมูลและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ ต่อพ่วงต่าง ๆ - บำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ - จัดทำแผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง		กลยุทธ์การจัดการ ความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
		ระดับ	คะแนน		
๙	IT๑๘ การเชื่อมต่อระบบ เครือข่ายอินเทอร์เน็ต ชัดข้อง	ความเสี่ยงสูง	๘	การลดความเสี่ยง	- จัดให้มีเครือข่ายอินเทอร์เน็ตจำนวนไม่น้อยกว่า ๒ เครือข่าย ได้แก่ เครือข่ายหลัก และ เครือข่ายสำรอง - บำรุงดูแลรักษาและตรวจสอบการทำงานอุปกรณ์เครือข่ายให้พร้อมใช้งานเสมอ - เมื่อเครือข่ายอินเทอร์เน็ตขัดข้อง ให้ทำการตรวจสอบอุปกรณ์และสายสัญญาณเครือข่าย อินเทอร์เน็ต/สอบถามผู้ให้บริการเครือข่าย อินเทอร์เน็ต เพื่อหาสาเหตุการขัดข้อง - จัดทำแผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย
๑๐	IT๑๙ การเชื่อมต่อระบบ เครือข่ายอินเทอร์เน็ตขัดข้อง	ความเสี่ยงปานกลาง	๘	การลดความเสี่ยง	- บำรุงดูแลรักษาและตรวจสอบการทำงานอุปกรณ์เครือข่ายให้พร้อมใช้งานเสมอ - เมื่อเครือข่ายอินเทอร์เน็ตขัดข้อง ให้ทำการตรวจสอบระบบสารสนเทศ อุปกรณ์เครือข่าย สายสัญญาณ และเครื่องคอมพิวเตอร์แม่ข่ายในระบบเครือข่ายอินเทอร์เน็ต เพื่อหาสาเหตุการ ขัดข้อง - จัดทำแผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย
๑๑	IT๒๐ ผู้รับจ้าง(Outsource) พัฒนา/บำรุงรักษา ระบบไม่ทันกำหนด หรือไม่ปฏิบัติตาม สัญญาจ้าง	ความเสี่ยงสูง	๘	การลดความเสี่ยง	- กำหนดเงื่อนไขสัญญาจ้างให้ชัดเจน ทั้งรายละเอียดงาน จำนวนและคุณสมบัติของบุคลากร และข้อกำหนดด้านความมั่นคงปลอดภัย - ตรวจสอบงานจ้างตามข้อกำหนดของสัญญาจ้าง
๑๒	IT๖ การติดตั้งอุปกรณ์ เทคโนโลยีสารสนเทศ ในพื้นที่ไม่เหมาะสม	ความเสี่ยงปานกลาง	๖	การหลีกเลี่ยงความเสี่ยง	- มีการสำรวจความเหมาะสมจุดติดตั้งอุปกรณ์ก่อนการติดตั้ง - บำรุงดูแลรักษาอุปกรณ์ และตรวจสอบให้อยู่ในสภาพพร้อมใช้งานเสมอ

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง		กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
		ระดับ	คะแนน		
๑๓	IT๘ ขาดแคลนบุคลากร ปฏิบัติงานด้าน เทคโนโลยีสารสนเทศ	ความเสี่ยงปานกลาง	๖	การโอนย้ายความเสี่ยง	- จัดหา Outsource ด้านเทคโนโลยีสารสนเทศมาช่วยปฏิบัติงาน
๑๔	IT๒๒ ระบบสารสนเทศ สอดคล้องทันสมัยกับ ระเบียบกฎหมาย	ความเสี่ยงปานกลาง	๖	การลดความเสี่ยง	- ผู้ดูแลระบบมีการทบทวน/ปรับปรุงระบบสารสนเทศให้สอดคล้องทันสมัยกับระเบียบกฎหมาย ที่เกี่ยวข้องอย่างน้อย ๑ ครั้ง/ปี - เมื่อมีการจัดทำโครงการพัฒนา/ปรับปรุงระบบสารสนเทศ ให้เสนอโครงการ ให้คณะกรรมการ พิจารณาและจัดหาระบบคอมพิวเตอร์ของ สก. พิจารณาความเหมาะสมและให้ความเห็นชอบ ก่อนการจัดหาระบบสารสนเทศ
๑๕	IT๑๙ อัคคีภัย	ความเสี่ยงปานกลาง	๕	การลดความเสี่ยง	- กำหนดเวรรักษาการณ์รักษาความปลอดภัย - ติดตั้งระบบตรวจจับควัน แจ้งเตือนเมื่อเกิดควันไฟไหม้ - ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย - จัดทำเครื่องหมายระบุลำดับความสำคัญของอุปกรณ์คอมพิวเตอร์แม่ข่ายเพื่อประสิทธิภาพใน การเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน - มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ - จัดทำแผนแก้ไขปัญหายุ่งยากด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง		กลยุทธ์การจัดการ ความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
		ระดับ	คะแนน		
๑๖	IT๑๑ แผ่นดินไหว	ความเสี่ยง ปานกลาง	๕	การลดความเสี่ยง	- มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ - จัดทำแผนแก้ไขปัญหายุ่งยากด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย
๑๗	IT๑๒ ความชื้นและอุณหภูมิ ที่ไม่เหมาะสม	ความเสี่ยง ปานกลาง	๕	การลดความเสี่ยง	- ติดตั้งระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่ เหมาะสมกับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย - ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศให้ใช้งานได้ตลอด ๒๔ ชม. - มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ - จัดทำแผนแก้ไขปัญหายุ่งยากด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย
๑๘	IT๑๒ การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยง ปานกลาง	๔	การลดความเสี่ยง	- ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่าย ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่าย - ติดตั้งระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตน (Finger Scan) และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ - ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกพื้นที่ และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง - จัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่ มิดชิดเมื่อไม่ได้ใช้งาน

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง		กลยุทธ์การจัดการ ความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
		ระดับ	คะแนน		
					- มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้อีกสถานที่ (DR Site) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้ - จัดทำแผนแก้ไขปัญหายภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็น แนวทางปฏิบัติเมื่อเกิดภัย
๑๙	IT๒๑ ผู้รับจ้าง(Outsource) ไม่รักษา ความลับของ ข้อมูล	ความเสี่ยง ปานกลาง	๔	การลดความเสี่ยง	- กำหนดเงื่อนไขสัญญาจ้างให้ชัดเจน ครอบคลุมข้อตกลงการรักษาความลับของข้อมูล และ ข้อกำหนดด้านความมั่นคงปลอดภัย - ทำการเปลี่ยน password การเข้าใช้ระบบ เมื่อเปลี่ยนตัวผู้รับจ้างหรือการว่าจ้างเสร็จสิ้น
๒๐	IT๔ การใช้ซอฟต์แวร์ที่ไม่มี ลิขสิทธิ์ ถูกต้อง	ความเสี่ยงต่ำ	๓	การยอมรับ ความเสี่ยง	- จัดหาซอฟต์แวร์ ตามคุณลักษณะพื้นฐานการจัดหาอุปกรณ์และระบบคอมพิวเตอร์ของ กระทรวงดิจิทัลฯ - เมื่อมีการจัดทำโครงการจัดหาซอฟต์แวร์ ให้เสนอโครงการ ให้คณะกรรมการพิจารณาและ จัดหาระบบคอมพิวเตอร์ของ สก. พิจารณาความเหมาะสมและให้ความเห็นชอบก่อนการจัดหา ซอฟต์แวร์
๒๑	IT๕ ซอฟต์แวร์หมดอายุ	ความเสี่ยงต่ำ	๓	การยอมรับ ความเสี่ยง	- บำรุงรักษาระบบสารสนเทศ/ซอฟต์แวร์ และตรวจสอบอายุซอฟต์แวร์ หากพบว่าใกล้หมดอายุ ให้ทำการต่ออายุหรือจัดซื้อซอฟต์แวร์ใหม่ตามความเหมาะสม
๒๒		ความเสี่ยงต่ำ	๓	การยอมรับ ความเสี่ยง	- จัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ ตามคุณลักษณะพื้นฐานการจัดหาอุปกรณ์และระบบ คอมพิวเตอร์ของกระทรวงดิจิทัลฯ - เมื่อมีการจัดทำโครงการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ ให้เสนอโครงการให้คณะกรรมการพิจารณาและจัดหาระบบคอมพิวเตอร์ของ สก. พิจารณาความเหมาะสมและ ให้ความเห็นชอบก่อนการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์

บทที่ ๔

แผนแก้ไขปัญหากลยุทธ์ด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

เทศบาลตำบลกกโก

แผนแก้ไขปัญหากลยุทธ์ด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เป็นแผนในการ แก้ไข ความเสี่ยงจากภัยพิบัติที่ อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ทั้งในส่วนองภัยที่มีสาเหตุมาจาก ธรรมชาติและภัยที่ เกิดจากการกระทำของมนุษย์ เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของ ระบบเทคโนโลยีสารสนเทศ เตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินและลดความเสียหายที่อาจจะเกิดแก่ ระบบเทคโนโลยีสารสนเทศ เป็นแนวทาง ในการดำเนินงานให้แก่บุคลากรให้สามารถบริหารจัดการความไม่ แน่นอนที่จะเกิดขึ้นกับองค์กรได้อย่างเป็นระบบ และมีประสิทธิภาพ

จากแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของเทศบาลตำบลไชยปราการ นำมาจัดทำ แผนแก้ไขปัญหากลยุทธ์ด้านเทคโนโลยีสารสนเทศ โดยมีขั้นตอนการดำเนินการ ดังนี้

๑. การดำเนินการป้องกันภัยพิบัติ
๒. การเตรียมความพร้อม
๓. การกำหนดผู้รับผิดชอบ
๔. กระบวนการแก้ไขปัญหากลยุทธ์
๕. การกู้คืนระบบ
๖. การซ่อมแผนการแก้ไขความเสี่ยง
๗. การติดตามและรายงานผล

๑. การดำเนินการป้องกันภัยพิบัติ

จากการวิเคราะห์ความเสี่ยงในรูปแบบต่างๆ ที่อาจเกิดขึ้น เพื่อให้การบริหารที่มีการป้องกันและ แก้ไข ตลอดจนการจัดการกับระบบเทคโนโลยีสารสนเทศให้เป็นไปอย่างมีประสิทธิภาพ ในกรณีที่เกิดเหตุการณ์ ที่ไม่ปลอดภัยหรือ ภัยพิบัติขึ้น จึงกำหนดแนวทางการดำเนินการเบื้องต้น ดังนี้

๑.๑) การตรวจสอบ วิเคราะห์ และสรุปสาเหตุเบื้องต้น การสังเกตอาการหรือเหตุอันผิดปกติ มี ๒ องค์ประกอบ คือ

(๑) ทางกายภาพ สภาพอันผิดปกติ เช่น กลิ่น อุณหภูมิ ไฟฟ้าดับ เสียง อาการสั้น

(๒) การทำงานของระบบ เช่น ไม่สามารถเข้าระบบงานได้ ระบบทำงานช้ากว่าปกติ โดย ไม่มี สาเหตุ ระบบไม่ทำงานผิดพลาดแต่มีข้อความแจ้งเหตุอันผิดปกติ

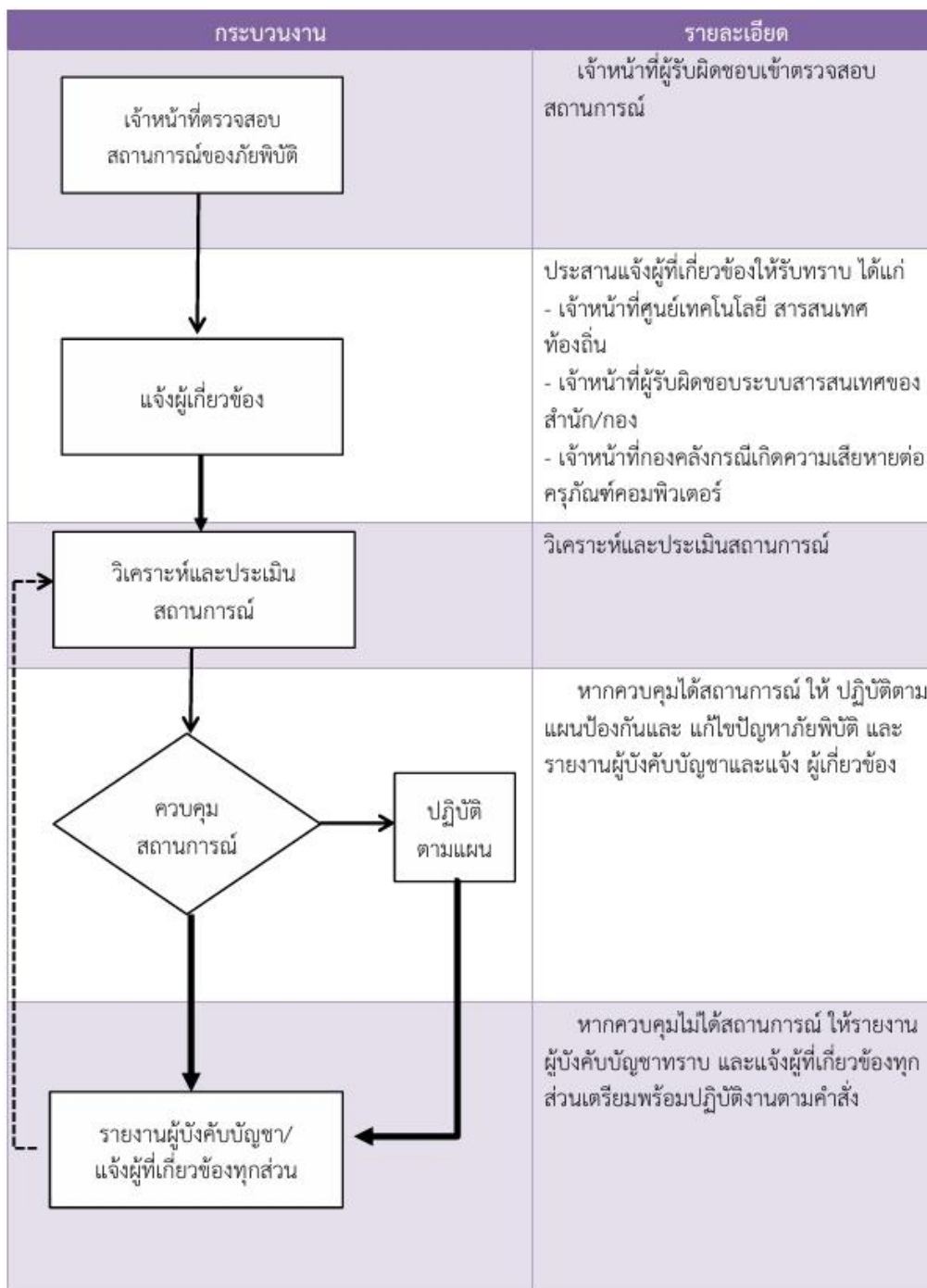
๑.๒) การแจ้งเหตุ

(๑) แจ้งเหตุการณ์เร่งด่วน ประสานแจ้งผู้ที่เกี่ยวข้องโดยตรง ได้แก่ เจ้าหน้าที่ศูนย์ เทคโนโลยี สารสนเทศท้องถิ่น เทศบาลตำบลไชยปราการ

(๒) แจ้งเหตุการณ์ปกติ สรุปสาเหตุและจัดทำรายงานแจ้งไปยังผู้ที่เกี่ยวข้อง และ เจ้าหน้าที่ ผู้รับผิดชอบรายงานผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

- ๑.๓) การประเมินสถานการณ์ โดยการแจ้งผู้รับผิดชอบหรือเจ้าหน้าที่ที่ประจำ ณ จุดเกิดเหตุ
- ๑.๔) ปฏิบัติตามแผนแก้ไขปัญหายับยั้งด้านเทคโนโลยีสารสนเทศ

แนวทางการดำเนินการเบื้องต้น



เทศบาลตำบลกกโกมีการดำเนินการบริหารจัดการความเสี่ยงและป้องกันภัยด้าน เทคโนโลยี สารสนเทศที่เกิดขึ้นและมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก ดังนี้

๑) การบุกรุกหรือโจมตีจากภายนอก

ภัยจากการบุกรุกหรือโจมตีจากภายนอกเพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายฐานข้อมูล หรือการก่อกวนจาก Hacker หรือการเจาะทำลายระบบจาก Cracker ดำเนินการ ดังนี้

๑.๑) สแกนหาจุดอ่อนและอัปเดต Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยใช้ซอฟต์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

๑.๒) ติดตั้ง Firewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและ อินทราเน็ตสามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของกรมส่งเสริมการปกครอง ท้องถิ่นได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

๑.๓) ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตของเทศบาลตำบลกกโกและกลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์

๑.๔) จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและ อินทราเน็ตของเทศบาลตำบลกกโก เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือ การเรียกใช้ระบบเทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกัน ต่อไปที่ไม่มีการใช้งาน

๑.๕) ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัปเดตอย่างสม่ำเสมอ และปิด พอร์ต

๑.๖) ป้องกันการปลอมแปลง IP address โดยการกรอง packet ที่มาจากภายนอก โดยการนำระบบ DMZ มากรอง IP ที่จะเข้ามายังระบบเครือข่าย

๑.๗) ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOS และ DDOS

๒) ไวรัสคอมพิวเตอร์หรือ Malware

๒.๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอและต้องใช้โปรแกรมเพื่อ ตรวจสอบหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๒.๒) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

๒.๒.๑) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

๒.๒.๒) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย

๒.๒.๓) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๒.๓) ใช้ความระมัดระวังในการเปิด E-mail

๒.๓.๑) ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

๒.๓.๒) ลบ E-mail ที่ทันทีถ้าไม่ทราบแหล่งที่มา

๒.๔) ปิดการใช้งานฟังก์ชัน Autoplay เพื่อป้องกันไม่ให้ไวรัสที่ แพร่ระบาดผ่านทางสื่อเก็บข้อมูลแบบพกพาใช้เป็นช่องทางในการรันไฟล์ไวรัสโดยอัตโนมัติ

๓) อัคคีภัย

- ๓.๑) กำหนดเวรรักษาการณ์รักษาความปลอดภัย
- ๓.๒) ติดตั้งระบบตรวจจับควัน แจ้งเตือนเมื่อเกิดควัน/ไฟไหม้
- ๓.๓) ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย
- ๓.๔) จัดทำเครื่องหมายระบุลำดับความสำคัญของอุปกรณ์คอมพิวเตอร์แม่ข่ายเพื่อประสิทธิภาพ

ในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

- ๓.๕) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site)
- ๓.๖) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๔) อุทกภัย/น้ำรั่วซึม

- ๔.๑) เจ้าหน้าที่ที่เกี่ยวข้อง ติดตามข่าวสารภัยพิบัติตามสถานการณ์ที่เกิดขึ้น
- ๔.๒) ติดตั้งระบบแจ้งเตือนน้ำรั่วซึมเข้าสู่ห้องคอมพิวเตอร์แม่ข่าย
- ๔.๓) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site) ใช้งานได้

๕) แผ่นดินไหว

- ๕.๑) เจ้าหน้าที่ที่เกี่ยวข้อง ติดตามข่าวสารภัยพิบัติตามสถานการณ์ที่เกิดขึ้น
- ๕.๒) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site)
- ๕.๓) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๖) ความชื้นและอุณหภูมิที่ไม่เหมาะสม

- ๖.๑) ติดตั้งระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ใน สภาวะที่เหมาะสมกับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย
- ๖.๒) ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศให้ใช้งานได้ตลอด ๒๔ ชม.
- ๖.๓) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site)
- ๖.๔) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๗) แมลงสัตว์กัดแทะอุปกรณ์

- ๗.๑) ไม่นำอาหารหรือเครื่องดื่มมารับประทานหรือเก็บไว้ในบริเวณที่มีอุปกรณ์คอมพิวเตอร์
- ๗.๒) ใช้ท่อห่อหุ้มสายไฟฟ้าหรือสายสัญญาณ เพื่อป้องกันการกัดแทะ

๘) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

- ๘.๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่ อาจเกิดขึ้นกับ อุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วน of เครื่อง คอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์สำนักงาน
- ๘.๒) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษา เครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ
- ๘.๓) เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้อุปกรณ์คอมพิวเตอร์สำนักงานบันทึกข้อมูลที่ยังค้างอยู่ ทันที และปิดเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่าง ๆ

๘.๔) สำรองข้อมูลที่สำคัญบนสื่อที่สามารถจัดเก็บข้อมูลได้อย่างเหมาะสม (DVD, CD, External Harddisk, Handy drive ฯลฯ)

๙) ภัยสงคราม/เหตุจลาจล และสถานการณ์ความไม่สงบ

๙.๑) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site)

๙.๒) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๑๐) การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์

๑๐.๑) กำหนดเวรรักษาการณ์รักษาความปลอดภัย

๑๐.๒) ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่าย ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่าย

๑๐.๓) ติดตั้งระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบ ยืนยันตัวตน (Finger Scan) และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

๑๐.๔) ติดตั้งกล้องโทรทัศน์วงจรปิดให้ครอบคลุมทุกพื้นที่ และส่งสัญญาณภาพมาไว้ที่จอภาพที่ ศูนย์ระบบกล้องโทรทัศน์วงจรปิด ของเทศบาลตำบลกกโก

๑๐.๕) จัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน

๑๐.๖) มีการสำรองข้อมูลไว้มากกว่า ๑ Backup และคัดลอกข้อมูลไปเก็บไว้ที่อีกสถานที่ (DR Site)

๑๐.๗) จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้เมื่อระบบหลักไม่สามารถใช้งานได้

๑๑) การเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง

๑๑.๑) จัดให้มีเครือข่ายอินเทอร์เน็ตจำนวนไม่น้อยกว่า ๒ เครือข่าย ได้แก่ เครือข่ายหลัก และเครือข่ายสำรอง

๑๑.๒) บำรุงดูแลรักษาและตรวจสอบการทำงานของอุปกรณ์เครือข่ายให้พร้อมใช้งานเสมอ

๑๑.๓) เมื่อเครือข่ายอินเทอร์เน็ตขัดข้อง ให้ทำการตรวจสอบอุปกรณ์และสายสัญญาณ เครือข่ายอินเทอร์เน็ต/สอบถามผู้ให้บริการเครือข่ายอินเทอร์เน็ต เพื่อหาสาเหตุการขัดข้อง

๑๒) การเชื่อมต่อระบบเครือข่ายอินทราเน็ตขัดข้อง

๑๒.๑) บำรุงดูแลรักษาและตรวจสอบการทำงานของอุปกรณ์เครือข่ายให้พร้อมใช้งานเสมอ

๑๒.๒) เมื่อเครือข่ายอินทราเน็ตขัดข้อง ให้ทำการตรวจสอบระบบสารสนเทศ อุปกรณ์ เครือข่ายสายสัญญาณ และเครื่องคอมพิวเตอร์แม่ข่ายในระบบเครือข่ายอินทราเน็ต เพื่อหาสาเหตุการขัดข้อง

๑๓) สถานการณ์โรคระบาด

ปัจจุบันสถานการณ์การแพร่ระบาดอย่างรวดเร็วและต่อเนื่องของเชื้อไวรัส COVID-๑๙ มีแนวโน้มสร้างภาวะชะงักงันให้กับหน่วยงานและส่งผลกระทบเหมือนกับการบุกรุกทางด้านไซเบอร์หรือเป็นภัยพิบัติทางธรรมชาติ หน่วยงานต้องควบคุมสถานการณ์โดยสร้างความเชื่อมั่นในการควบคุมโรคให้กับบุคลากรและสามารถปฏิบัติงานได้อย่างต่อเนื่อง โดยใช้เครื่องมือดิจิทัลเพื่อทำงานร่วมกันในการควบคุม ความปลอดภัย และมีเครือข่ายรองรับมาตรการกักกันต่างๆ และข้อจำกัดการเดินทาง ในเบื้องต้นหน่วยงานที่ ยังไม่มีความสามารถนำระบบทำงานแบบระยะไกลมาปรับใช้ได้นั้น อาจต้องแก้ไขโดยการการระบุข้อกำหนด กรณีการใช้

งาน เช่น การส่งข้อความทันทีเพื่อสื่อสารทั่วไป การแชร์ไฟล์ หรือการประชุม และการเข้าถึง แอปพลิเคชันต่างๆ ขององค์กร เช่น ระบบสารสนเทศต่างๆ และเตรียมการด้านความปลอดภัยทั้งหมดเพื่อให้ เข้าถึงแอปพลิเคชันและข้อมูลได้อย่างปลอดภัย ใช้ช่องทางดิจิทัลเป็นช่องทางหลักในการติดต่อสื่อสารกับ บุคลากรและหน่วยงานอื่นที่เกี่ยวข้องนำแพลตฟอร์มดิจิทัลมาใช้ติดต่อสื่อสาร เช่น เว็บไซต์ หรือแอปพลิเคชันต่างๆ โซเชียลมีเดีย แต่การติดต่อแบบออฟไลน์ยังคงมีบทบาทสำคัญ การทำงานร่วมกันในสถานที่ทำงาน การประชุมผ่านวิดีโอและไลฟ์สตรีมมิ่ง สร้างแหล่งข้อมูลหลักที่เชื่อถือได้ให้แก่องค์กร และการเตรียมแผน รับมือตอนกลับเข้าสู่โหมดการดำเนินงานในภาวะปกติขององค์กร ซึ่งความวิตกกังวลดังกล่าวบรรเทาลงได้ หากองค์กรสามารถใช้ประโยชน์จากข้อมูลมาช่วยในการตัดสินใจได้ดีขึ้น และสื่อสารความคืบหน้าของสถานการณ์อย่างมีประสิทธิภาพต่อพนักงาน องค์กรสามารถนำเสนอเนื้อหาที่คัดสรรมาจากแหล่งที่มาภายในและภายนอกองค์กร เพื่อให้คำแนะนำแก่พนักงานนำไปปรับใช้ได้ โดยแหล่งข้อมูลเหล่านี้จะรวมไปถึง ข้อมูล ข่าวสารของรัฐบาลท้องถิ่น หน่วยงานและองค์กรด้านสาธารณสุขระหว่างประเทศ เช่น องค์การอนามัยโลก (WHO) แจ้งขอความช่วยเหลือและขอรับการดูแลพิเศษในกรณีเกิดเหตุฉุกเฉินได้

๒. การเตรียมความพร้อม

๒.๑) การจัดเตรียมอุปกรณ์ที่จำเป็น

- ๒.๑.๑) แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย แผ่นติดตั้งระบบงานที่สำคัญ
- ๒.๑.๒) สำรองข้อมูลและระบบงานที่สำคัญ
- ๒.๑.๓) แผ่นโปรแกรม antivirus/spyware
- ๒.๑.๔) แผ่น driver อุปกรณ์ต่างๆ
- ๒.๑.๕) ระบบสำรองไฟฉุกเฉิน
- ๒.๑.๖) อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

๒.๒) การสำรองข้อมูล (Backup)

เทศบาลตำบลกกโก มีการสำรองข้อมูลระบบสารสนเทศจากเครื่องคอมพิวเตอร์ แม่ข่ายภายในห้อง Server ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น เทศบาลตำบลกกโก และศูนย์ข้อมูล (Data Center) โดยเครื่องคอมพิวเตอร์แม่ข่ายสำหรับสำรองข้อมูล (Backup Server) ทำการสำรองข้อมูล แบบอัตโนมัติ ดังนี้

๒.๒.๑) สำรองข้อมูลรายวัน ทำการสำรองข้อมูลแบบ Virtual Machine วันละ ๑ ครั้ง ในช่วงเวลา ๒๒.๐๐ - ๒๓.๐๐ น. หลังจากทำการสำรองข้อมูลแล้วจะตรวจสอบข้อมูลที่สำรองไว้ว่าสามารถ ใช้งานได้ปกติหรือไม่ ถ้าไม่สามารถใช้งานได้ให้ดำเนินการแก้ไข และถ้าสามารถใช้งานได้จะดำเนินการจัดเก็บไฟล์ข้อมูลสำรองในสื่อบันทึกข้อมูล หลังจากนั้นการสำรองข้อมูลจะดำเนินการเฉพาะส่วนที่มีการเปลี่ยนแปลง จากการสำรองข้อมูลครั้งล่าสุดแบบ Incremental Backup

๒.๒.๒) สำรองข้อมูลทุกๆ ๑๕ วัน ทำการสำรองข้อมูลทุกๆ ๑๕ วัน ช่วงเวลา ๐๑.๐๐ - ๐๓.๐๐ น. ซึ่งเป็นการสำรองข้อมูลทั้งหมดแบบ Full Backup หลังจากทำการสำรอง ข้อมูลแล้ว จะตรวจสอบข้อมูลที่สำรองไว้ว่าสามารถใช้งานได้ปกติหรือไม่ ถ้าไม่สามารถใช้งานได้ให้ดำเนินการ แก้ไข และถ้าสามารถใช้งานได้จะดำเนินการจัดเก็บไฟล์ข้อมูลสำรองในเทปแม่เหล็ก

๓.การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

๓.๑) ระดับนโยบาย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) เทศบาลตำบลกกโกรับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตามการกำกับดูแล

๓.๒) ระดับอำนวยการ

การแก้ไขปัญหาจากภัยพิบัติ มีหน้าที่ในควบคุม ตรวจสอบ กำกับดูแลการประเมินสถานการณ์และตัดสินใจในกรณีที่ฝ่ายปฏิบัติงาน ประเมินสถานการณ์และรายงานการประเมินเบื้องต้นว่าอาจไม่สามารถควบคุมสถานการณ์ได้ จำเป็นจะต้องปฏิบัติงานนอกเหนือจาก แผนป้องกันแก้ไขปัญหาจากภัยพิบัติ ที่กำหนดไว้ หรือสถานการณ์ยังไม่เกิดแต่มีสภาวะการณ์หรือแนวโน้มที่อาจเกิดขึ้น รายงานผลต่อ ผู้บังคับบัญชาประกอบด้วย

๓.๒.๑) ปลัดเทศบาล

๓.๒.๒) หัวหน้าสำนักปลัดเทศบาล

๓.๓) ระดับปฏิบัติ

ดำเนินการตามแผนป้องกันและแก้ไขปัญหาเกี่ยวกับภัยพิบัติรายงานผลการดำเนินการตามแผนฯ ทบทวนแผนฯ ประเมินสถานการณ์ ติดต่อประสานงานฝ่ายต่างๆ ที่เกี่ยวข้อง รวมทั้งขอรับการ สนับสนุนจากหน่วยงานภายนอกหรือบริษัทคู่สัญญา ดังนี้

๓.๓.๑) ด้านฐานข้อมูล ระบบสารสนเทศ ประกอบด้วย

- ผู้อำนวยการกลุ่มงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ ได้แก่ หัวหน้าสำนักปลัดเทศบาล เป็นต้น
- เจ้าหน้าที่กลุ่มงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ สำนักปลัดเทศบาล

๓.๓.๒) ด้านระบบงานคอมพิวเตอร์ ประกอบด้วย

- ผู้อำนวยการกลุ่มงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ ได้แก่ หัวหน้าสำนักปลัดเทศบาล เป็นต้น
- เจ้าหน้าที่กลุ่มงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ สำนักปลัดเทศบาล

๓.๓.๓) ด้านสนับสนุนการแก้ไขปัญหาจากภัยพิบัติ มีหน้าที่ในการสนับสนุนการแก้ไขปัญหาจากภัยพิบัติตามที่

ฝ่ายปฏิบัติงานแก้ไขปัญหาจากภัยพิบัติร้องขอ ประกอบด้วย

- ผู้อำนวยการกลุ่มงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ ได้แก่ หัวหน้าสำนักปลัดเทศบาล เป็นต้น
- เจ้าหน้าที่กลุ่มงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ สำนักปลัดเทศบาล

๔. กระบวนการแก้ไขปัญหาภัยพิบัติ

๔.๑) ข้อปฏิบัติกรณีเกิดการบุกรุกหรือโจมตีจากภายนอก

การบุกรุกหรือโจมตีจากภายนอกเป็นการสร้างความเสียหายให้แก่ระบบเทคโนโลยี สารสนเทศซึ่งอาจเป็นการเจาะระบบเครือข่าย หรือการโจมตีระบบสารสนเทศ จึงมีข้อปฏิบัติ ดังนี้

๔.๑.๑) กรณีโดนเจาะระบบเครือข่าย

กระบวนการงาน	รายละเอียด
ตรวจสอบพบว่าระบบเครือข่ายหรือระบบงานทำงานไม่ปกติ	- ตรวจสอบพบว่าระบบเครือข่ายหรือระบบงานทำงานไม่ปกติ
ตรวจสอบ Log File จาก Firewall, IPS, Firewall Analysis, Switch, Server	- ฝ่ายปฏิบัติตรวจสอบ Log File จาก อุปกรณ์ Firewall IPS, Firewall Analysis, Switch
วิเคราะห์สาเหตุ ลักษณะการโจมตี ผลกระทบ และความรุนแรง	- วิเคราะห์สาเหตุที่ทำให้ระบบ เครือข่ายหรือระบบงานไม่ปกติ ลักษณะการโจมตีประเภทการโจมตี ผลกระทบและความรุนแรง
ปิดช่องโหว่ ปรับตั้งค่า Firewall Policy	- ปิดช่องโหว่ที่เป็นช่องทางเข้าโจมตี โดยการปรับตั้งค่า Firewall Policy
ทดสอบระบบ	- ทดสอบระบบเครือข่ายหรือระบบงานว่าทำงานเป็นปกติหรือไม่
การทำงานของระบบเป็นปกติ	ไม่ใช่
รายงานให้ผู้บังคับบัญชา	- หากพบว่าระบบมีการทำงานปกติ แล้ว ให้รวบรวมข้อมูล รายงานให้ฝ่าย บริหารทราบ

๔.๑.๒) กรณีโดนโจมตีระบบสารสนเทศ

กระบวนการงาน	รายละเอียด
ระบบสารสนเทศถูกโจมตี ↓	- ตรวจสอบจากอุปกรณ์ Firewall พบว่าระบบสารสนเทศมีการใช้งาน สูงผิดปกติ
ตรวจสอบ Log File จาก Firewall ↓	- ฝ่ายปฏิบัติการตรวจสอบ Log File จาก อุปกรณ์ Firewall เพื่อตรวจสอบ IP ต้นทางที่โจมตี และวิเคราะห์ลักษณะ การโจมตี
ปิดกั้น IP ที่มีการโจมตีเข้ามายังระบบสารสนเทศ และเฝ้าระวังการโจมตี ↓	- ปรับตั้ง Policy เพื่อปิดกั้น IP ที่มี การโจมตีเข้ามายังระบบสารสนเทศ และเฝ้าระวังว่ามี IP เพิ่มเติมหรือไม่ - ปิดช่องทางที่เป็นช่องทางเข้าโจมตี โดยการปรับตั้งค่า Firewall Policy
การทำงานของระบบเป็นปกติ ↓	- ตรวจสอบว่ายังมีการโจมตีอยู่หรือไม่
ใช่ รายงานให้ผู้บังคับบัญชา ↓	- ปรับตั้งค่า Policy ให้ตรวจจับ พฤติกรรมและ IP ที่มาจากต้นทาง เดียวกันเป็นพิเศษ
รายงานให้ผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหาร ทราบ

๔.๒) ข้อปฏิบัติการณีเครื่องแม่ข่ายหรืออุปกรณ์ขัดข้อง

กระบวนการงาน	รายละเอียด
ตรวจสอบพบเครื่องแม่ข่ายขัดข้อง	- ตรวจสอบในโปรแกรม Monitoring พบว่าเครื่องแม่ข่ายไม่ทำงาน (ขึ้น สัญลักษณ์สีแดง)
Service ทำงานปกติ เครื่องแม่ข่ายไม่ทำงาน	- ตรวจสอบ Service ทำงานเป็นปกติ หรือไม่ - หาก Service ทำงานปกติแสดงว่า เครื่องแม่ข่ายไม่ทำงาน
ตรวจสอบสาเหตุที่ Service ไม่ทำงาน ตรวจสอบสาเหตุที่ เครื่องแม่ข่ายไม่ทำงาน	- หาก Service ไม่ทำงานให้ตรวจสอบ สาเหตุที่ Service ไม่ทำงาน - หากเครื่องแม่ข่ายไม่ทำงานให้ ตรวจสอบสาเหตุที่เครื่องแม่ข่าย ไม่ ทำงาน
สามารถแก้ไขได้ แก้ไขเครื่องแม่ข่าย/ Service ให้สามารถ ทำงานได้ตามปกติ	- ประเมินสถานการณ์ว่าสามารถแก้ไข ปัญหาได้หรือไม่ - หากแก้ไขได้ให้ดำเนินการแก้ไขให้ เครื่องแม่ข่าย
ไม่ใช่ แจ้งบริษัทคู่สัญญาดำเนินการแก้ไข	- หากไม่สามารถแก้ไขได้ ให้แจ้งบริษัท คู่สัญญาดำเนินการ เปลี่ยนอุปกรณ์/ แก้ไข
รายงานให้ผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๓) ข้อปฏิบัติกรณีข้อมูลได้รับความเสียหาย

กรณีตรวจพบข้อมูลในเครื่องคอมพิวเตอร์แม่ข่ายได้รับความเสียหาย ข้อมูลสูญหายไม่ครบถ้วน มีข้อปฏิบัติ ดังนี้

กระบวนการงาน	รายละเอียด
ตรวจสอบพบข้อมูลใน เครื่องคอมพิวเตอร์ แม่ข่ายสูญหายไม่ครบถ้วน	- ตรวจสอบพบข้อมูลในเครื่อง คอมพิวเตอร์แม่ข่ายสูญหาย ไม่ ครบถ้วน
ตรวจสอบวัน เวลา ที่ข้อมูลสูญหาย	- ตรวจสอบวัน เวลา ที่ข้อมูลสูญหาย และระบบที่มีข้อมูลสูญ หาย
ประเมินค่าความเสียหาย	- ประเมินสถานการณ์ว่าสามารถแก้ไข ได้หรือไม่ - หากแก้ไขได้ ให้นำข้อมูลที่สำรองไว้ มา Restore ในเครื่อง ทดสอบ
สามารถแก้ไขได้ ใช่ กู้ข้อมูล	- ทำการกู้คืนข้อมูลไปยังระบบที่ ตรวจสอบพบว่าข้อมูลสูญหาย
ไม่ใช่ แจ้งบริษัทคู่สัญญาดำเนินการแก้ไข	- หากไม่สามารถแก้ไขได้ ให้แจ้งบริษัท คู่สัญญาดำเนินการแก้ไขข้อมูล
รายงานให้ผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหาร ทราบ

๔.๔) ข้อปฏิบัติกรณีเกิดอัคคีภัย

กระบวนการงาน	รายละเอียด
ระบบตรวจสอบพบควัน ↓ เกิดเพลิงไหม้ ↓ ไม่ใช่	- ระบบไฟฟ้าดับ ระบบแจ้งเตือนภัย Alert Alarm แจ้งว่าตรวจพบควัน (Smoke Detector)
เกิดเพลิงไหม้ → ใช่ ระบบ Pyrogen ปล่อยองเคมีดับเพลิง ↓ เจ้าหน้าที่ดับเพลิง ควบคุมพื้นที่เพลิงไหม้	- ฝ่ายปฏิบัติตรวจสอบประเมินเหตุการณ์ว่าเกิด เพลิงไหม้หรือไม่ แจ้งฝ่ายอำนวยการฝ่าย สนับสนุนทราบให้บุคลากรออกจากพื้นที่ แจ้งฝ่าย ป้องกันและบรรเทาสาธารณภัย - หากเกิดเพลิงไหม้พนักงานดับเพลิงจะใช้ระบบ Pyrogen ฉีด พ่นลองเคมีดับเพลิงในอาคาร
ตรวจสอบแหล่งที่มาของควัน ↓	- หากไม่เกิดเพลิงไหม้ ให้ฝ่ายปฏิบัติตรวจสอบ แหล่งที่มาของ ควันและประเมินสถานการณ์ของ ควันและประเมินสถานการณ์ และแจ้งให้ฝ่าย อำนวยการทราบ
พบแหล่ง กำเนิดควัน ↓ ไม่ใช่ ปิดอุปกรณ์ทั้งหมด ↓ แจ้งบริษัทคู่สัญญา ↓ รายงานให้ผู้บังคับบัญชา	- หากตรวจสอบพบแหล่งที่มาของควัน ให้ ประเมินสถานการณ์ ว่าสามารถควบคุมและแก้ไข ได้หรือไม่ - หากตรวจสอบไม่พบแหล่งที่มาของควันให้ทำ การปิดอุปกรณ์ ทั้งหมด ปิดเครื่องปรับอากาศแล ระบบไฟฟ้า - หากตรวจพบแหล่งกำเนิดควันแต่ไม่สามารถ แก้ไขปัญหาได้ ให้ ปิดอุปกรณ์ทั้งหมด ปิด เครื่องปรับอากาศ และระบบไฟฟ้า - หากตรวจพบแหล่งกำเนิดควัน และสามารถ แก้ไขปัญหาได้ ให้ ปิดอุปกรณ์ที่ทำให้เกิดควัน
สามารถ แก้ปัญหาได้ ↓ ใช่ ปิดอุปกรณ์ที่ทำให้เกิดควัน ↓ แจ้งบริษัทคู่สัญญา ↓ รายงานให้ผู้บังคับบัญชา	- หากตรวจพบแหล่งกำเนิดควันแต่ไม่สามารถ แก้ไขปัญหาได้ ให้ ปิดอุปกรณ์ทั้งหมด ปิด เครื่องปรับอากาศ และระบบไฟฟ้า - หากตรวจพบแหล่งกำเนิดควัน และสามารถ แก้ไขปัญหาได้ ให้ ปิดอุปกรณ์ที่ทำให้เกิดควัน
แจ้งบริษัทคู่สัญญา ↓ รายงานให้ผู้บังคับบัญชา	- แจ้งบริษัทคู่สัญญาให้มาตรวจสอบ หรือถ้าหมด สัญญาก็จัดหา บริษัทที่มีความชำนาญเฉพาะเข้า มาตรวจสอบความเสียหายของ อุปกรณ์และ ซ่อมแซม - รวบรวมข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๕) ข้อปฏิบัติกรณีเกิดอุทกภัย (น้ำท่วม)

กระบวนการงาน	รายละเอียด
ประเมินสถานการณ์น้ำ มีโอกาสดเกิดน้ำท่วม	- ฝ่ายปฏิบัติงานติดตามข่าวสารและประกาศจาก ศูนย์ป้องกันและแก้ไขปัญหายภัยพิบัติแห่งชาติ - ฝ่ายปฏิบัติประเมินสถานการณ์และวิเคราะห์ความ น่าจะเป็นที่ อาจเกิดน้ำท่วมบริเวณห้องควบคุม ระบบ
แจ้งผู้บังคับบัญชา ↓ เครื่องย้ายอุปกรณ์	- รวบรวมข้อมูล สถานการณ์น้ำท่วมและแนวโน้มที่ อาจเกิดน้ำท่วมให้ฝ่ายบริหารทราบ - ขอความเห็นชอบในการย้ายอุปกรณ์ไปยัง ห้องควบคุมสำรอง
ใช่ ↓ ย้ายอุปกรณ์ไปยังชั้น ๓ หรือชั้นบนสุดของ แต่ละอาคาร พร้อมติดตั้งและทดสอบระบบ	- แจ้งบริษัทคู่สัญญา (MA) ดำเนินการย้ายอุปกรณ์ - ปิดระบบ/ปิดอุปกรณ์ทั้งหมด - ดำเนินการย้าย ติดตั้ง ทดสอบระบบ
ประเมินสถานการณ์น้ำสถานะเข้าสู่ภาวะปกติ	- ฝ่ายปฏิบัติงาน ติดตาม ข่าวสาร และประเมิน สถานการณ์ว่า สถานการณ์เข้าสู่ภาวะปกติ
แจ้งผู้บังคับบัญชา ↓ เครื่องย้ายอุปกรณ์กลับ	- รวบรวมข้อมูล สถานการณ์น้ำท่วมให้ฝ่ายบริหาร ทราบ - ขอความเห็นชอบในการย้ายอุปกรณ์กลับ ห้องควบคุมระบบ (Server Room)
ใช่ ↓ ย้ายอุปกรณ์กลับห้องควบคุมระบบ/ ติดตั้ง ทดสอบระบบ	- แจ้งบริษัทคู่สัญญา (MA) ดำเนินการย้ายอุปกรณ์ - ปิดระบบ/ปิดอุปกรณ์ทั้งหมด - ดำเนินการย้าย ติดตั้ง ทดสอบระบบ
รายงานให้ผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหารทราบ

หมายเหตุ : กำหนดให้ใช้ชั้นบนสุดของแต่ละอาคารเป็น ห้องเก็บอุปกรณ์ และให้ชั้น ๓ อาคารสำนักงาน เทศบาลตำบลกกโก

๔.๖) ข้อปฏิบัติกรณีเกิดน้ำรั่วซึม

กระบวนการงาน	รายละเอียด
ระบบแจ้งเตือน Water Leak (น้ำรั่ว)	- ระบบแจ้งเตือนภัย Alert Alarm แจ้ง ว่าตรวจพบน้ำ (Water Leak) ในพื้นที่ ห้องควบคุมระบบ (Server Room)
สามารถแก้ไขได้ ใช่ → ชีบน้ำบริเวณที่รั่วซึม	- ฝ่ายปฏิบัติงานแก้ไขปัญหามาจากภัย พิบัติ ดำเนินการเปิดพื้นและชีบน้ำให้แห้ง
ไม่ใช่ ↓ แจ้งฝ่ายอำนวยการทราบ	- ฝ่ายปฏิบัติงานแจ้งฝ่ายอำนวยการ ทราบปัญหาและขออนุญาตปิดอุปกรณ์ ทั้งหมด
ปิดอุปกรณ์ เครื่องปรับอากาศและ ระบบไฟฟ้าภายในห้องควบคุมระบบ (Server Room)	- ฝ่ายปฏิบัติงานดำเนินการปิดอุปกรณ์ ทั้งหมด ปิดระบบไฟฟ้าและ เครื่องปรับอากาศ
แจ้งบริษัทคู่สัญญา MA	- แจ้งบริษัทคู่สัญญา MA หรือผู้รับจ้าง ระบบดำเนินการแก้ไข
สถานการณ์เข้าสู่ภาวะปกติ	- ตรวจสอบสถานการณ์ หากเข้าสู่ ภาวะปกติ แจ้งฝ่ายอำนวยการทราบ และขอเปิดระบบ
แจ้งบริษัทคู่สัญญา MA	- เปิดระบบไฟฟ้า ระบบ เครื่องปรับอากาศ รอให้อุณหภูมิอยู่ที่ ๒๕ °C แล้วเปิดอุปกรณ์ทั้งหมด
รายงานให้ผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๗) ข้อปฏิบัติการณีเกิดแผ่นดินไหว

กระบวนการงาน	รายละเอียด
ได้รับแจ้งว่าอาจเกิดเหตุแผ่นดินไหว	- ได้รับแจ้งจากหน่วยงานที่เกี่ยวข้อง แจ้งว่าจะเกิดเหตุแผ่นดินไหว
เกิดเหตุแผ่นดินไหว ไม่ใช่ → นำอุปกรณ์จัดเก็บและสำรองข้อมูลออกปิดระบบ ทั้งหมด ใช่ ↓ อพยพออกนอกอาคาร	- ประเมินสถานการณ์หากเกิดเหตุ แผ่นดินไหวขึ้นแล้วให้อพยพออกนอก อาคาร - หากยังไม่เกิดขึ้นแต่ได้รับการแจ้ง เตือนให้นำอุปกรณ์สำรองข้อมูลออก จากห้องควบคุมระบบและปิดระบบ ทั้งหมด
ตรวจสอบความเสียหาย และความพร้อมใช้งาน	- รอเหตุการณ์สงบหรือพ้นระยะเวลาที่ ได้รับแจ้งว่าอาจเกิดแผ่นดินไหวให้ ดำเนินการตรวจสอบความเสียหาย และความพร้อมใช้งานของอุปกรณ์
อุปกรณ์ชำรุดเสียหาย ไม่พร้อมใช้งาน ไม่ใช่ → เปิดระบบทั้งหมดและนำอุปกรณ์จัดเก็บและสำรองข้อมูลติดตั้งที่เดิม ใช่ ↓	- ตรวจสอบอุปกรณ์ทั้งหมดว่าได้รับ ความเสียหายหรือไม่หากไม่ได้รับความเสียหายให้ประเมินความพร้อมใช้งาน หากมีความพร้อมใช้งานให้เปิดระบบ ทั้งหมดดังเดิม
แจ้งบริษัทคู่สัญญาหรือผู้รับจ้างเข้ามาดำเนินการแก้ไข	- กรณีอุปกรณ์ได้รับความเสียหายให้ แจ้งบริษัทคู่สัญญาบำรุงรักษาระบบมา ตรวจสอบดำเนินการแก้ไขหรือจัดหาอุปกรณ์มาทดแทน
รายงานให้ผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหาร ทราบ

๔.๘) ข้อปฏิบัติการณืไฟฟ้าดับ

กระบวนการงาน	รายละเอียด
ไฟฟ้าดับ	- ระบบแจ้งเตือนภัย Alert Alarm แจ้ง ว่าไฟฟ้าดับ (Main Power FAIL)
เครื่องกำเนิดไฟฟ้าทำงาน ใช่ ตรวจสอบน้ำมันเครื่อง กำเนิดไฟฟ้ากับกองช่าง (ไม่น้อยกว่า ๕๐%) เผื่อระวังจนกว่า ระบบไฟฟ้าเป็นปกติ ไม่ใช่	- ตรวจสอบเครื่องกำเนิดไฟฟ้าว่า ทำงานหรือไม่ - กรณีที่เครื่องกำเนิดไฟฟ้าทำงานให้ ฝ่ายปฏิบัติตรวจสอบปริมาณน้ำมันและ แจ้งกองคลัง สำรองน้ำมันหากมีน้ำมัน น้อยกว่า ๕๐% และเผื่อระวังจนกว่า ระบบไฟฟ้าจะเป็นปกติ
UPS ปริมาณมาก กว่า ๗๐% ใช่ ไฟฟ้าดับนานกว่า ๓๐ นาที ไม่ใช่ ใช่/แน่ใจ	- กรณีเครื่องกำเนิดไฟฟ้าไม่ทำงาน ฝ่ายปฏิบัติตรวจสอบ UPS ว่าปริมาณ ไฟฟ้าสำรองมากกว่า ๗๐% และให้ สอบถาม การไฟฟ้าส่วนภูมิภาคฝาง ถึง ระยะเวลาที่ไฟฟ้าจะกลับเป็นปกติ - หากไฟฟ้าดับน้อยกว่า ๓๐ นาที ให้ เผื่อระวังจนกว่าระบบไฟฟ้าจะเป็นปกติ
ปิดอุปกรณ์ทั้งหมด	- ปิดอุปกรณ์หากปริมาณไฟฟ้าสำรอง ของ UPS น้อยกว่า ๗๐% หรือไฟฟ้า ดับนานกว่า ๓๐ นาที หรือไม่แน่ใจ สถานการณ์
ปิดอุปกรณ์ทั้งหมด เปิดอุปกรณ์ทั้งหมด/ ทดสอบการทำงาน	- เมื่อ ระบบ ไฟ ฟ้า เป็น ปกติ ให้ เปิด ระบบ ไฟ ฟ้า เครื่องปรับอากาศ และให้ อุณหภูมิอยู่ที่ ๒๕ °C - แล้วเปิดอุปกรณ์ทั้งหมดและทดสอบ การทำงานให้เป็นปกติ
รายงานให้ผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๙) ข้อปฏิบัติกรณีเกิดภัยสงคราม/เหตุจลาจล และสถานการณ์ความไม่สงบ

กรณีเกิดภัยสงคราม/เหตุจลาจล และสถานการณ์ความไม่สงบ และได้มีการปิดล้อมสถานที่ ปฏิบัติงาน มีข้อปฏิบัติ ดังนี้

กระบวนการงาน	รายละเอียด
ได้รับข่าวว่าอาจถูกปิดล้อมสถานที่ปฏิบัติงาน)	- ได้รับแจ้งจากหน่วยงานที่เกี่ยวข้อง แจ้งว่าจะ เกิดเหตุปิดล้อมสถานที่ปฏิบัติงาน
↓	
ติดตามข่าว ฝ้าระวังและเตรียมความพร้อม	- ประสานหน่วยงานที่เกี่ยวข้องจัดเตรียม สถานที่ปฏิบัติงานสำรอง
↓	
เกิดเหตุปิดล้อมสถานที่ปฏิบัติงาน	- ประเมินสถานการณ์ รอคำสั่งจากฝ่ายบริหาร ให้ย้ายสถานที่ปฏิบัติงาน
↓	
ย้ายสถานที่ปฏิบัติ/ ย้ายเครื่องแม่ข่าย ระบบ Intranet ไปยัง Data Center	- ดำเนินการติดตั้งอุปกรณ์เครือข่าย เครื่อง คอมพิวเตอร์และอุปกรณ์ต่อพ่วงสำหรับ ปฏิบัติงาน ณ สถานที่ปฏิบัติงานสำรอง - ย้ายเครื่องแม่ข่าย ที่ห้องปฏิบัติงานสำรอง
↓	
ประเมินสถานการณ์	- ประเมินสถานการณ์ว่าเข้าสู่ภาวะปกติหรือไม่ - รอคำสั่งจากฝ่ายบริหารให้ย้ายสถานที่ ปฏิบัติงาน
↓	
เหตุการณ์ปกติ	
↓	
ย้ายสถานที่ปฏิบัติงานกลับมายังสำนักงาน/ย้ายเครื่องแม่ข่าย กลับมายังห้องควบคุม	- หากเหตุการณ์เข้าสู่ภาวะปกติให้ดำเนินการ ย้ายสถานที่ปฏิบัติงานกลับมายังเทศบาลตำบล ไชยปราการ ตรวจสอบอุปกรณ์ให้สามารถใช้ งานตามปกติ - ย้ายเครื่องแม่ข่าย Intranet กลับมายัง ห้องควบคุม
↓	
รายงานให้ผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหารทราบ

๔.๑๐) ข้อปฏิบัติกรณีเกิดการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง

กระบวนการงาน	รายละเอียด
ระบบเครือข่ายอินเทอร์เน็ตไม่สามารถใช้งานได้ ↓	- ตรวจพบระบบเครือข่ายอินเทอร์เน็ตขัดข้อง ไม่สามารถใช้งานได้
ตรวจสอบอุปกรณ์เครือข่ายและสายสัญญาณอินเทอร์เน็ต ↓ เกิดเหตุขัดข้องสถานที่ปฏิบัติงาน ↓ ใช่	- ตรวจสอบอุปกรณ์เครือข่ายและสายสัญญาณ อินเทอร์เน็ตหากพบปัญหาให้ดำเนินการแก้ไข
ไม่ใช่ ↓ สอบถามผู้ให้บริการเครือข่ายอินเทอร์เน็ต ↓ ตรวจพบปัญหาและแก้ไข ↓ ไม่ใช่	- หากไม่พบปัญหา ว่าเกิดจากอุปกรณ์ เครือข่ายและสายสัญญาณอินเทอร์เน็ตภายใน เทศบาลตำบลไชยปราการ ให้สอบถามผู้ให้บริการเครือข่ายอินเทอร์เน็ต - หากพบปัญหา ว่าเกิดจากผู้ให้บริการ เครือข่ายอินเทอร์เน็ตให้ผู้ให้บริการเครือข่ายอินเทอร์เน็ตดำเนินการแก้ไขปรับปรุงให้แล้วเสร็จโดยไว
ใช่ ↓ รายงานให้ผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ผู้ฝ่ายบริหารทราบ

๔.๑๑) ข้อปฏิบัติกรณีเกิดการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตขัดข้อง

กระบวนการงาน	รายละเอียด
ระบบเครือข่ายอินเทอร์เน็ตไม่สามารถใช้งานได้ ↓	- ตรวจพบระบบเครือข่ายอินเทอร์เน็ตขัดข้อง ไม่สามารถใช้งานได้
ตรวจสอบอุปกรณ์เครือข่ายและสายสัญญาณอินเทอร์เน็ต ↓ ตรวจพบปัญหาและแก้ไข ↓ ไม่ใช่ สอบถามผู้ให้บริการเครือข่ายอินเทอร์เน็ต ↓ ไม่ใช่ ตรวจพบปัญหาและแก้ไข ↓ ใช่ รายงานให้ผู้บังคับบัญชา	- ตรวจสอบอุปกรณ์เครือข่ายและสายสัญญาณ อินเทอร์เน็ตหากพบปัญหาให้ดำเนินการแก้ไข - หากไม่พบปัญหา ว่าเกิดจากอุปกรณ์ เครือข่ายและสายสัญญาณอินเทอร์เน็ต ให้ ตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายในระบบ เครือข่ายอินเทอร์เน็ต - หากพบปัญหา ว่าเกิดจากเครื่องคอมพิวเตอร์ แม่ข่ายในระบบเครือข่ายอินเทอร์เน็ต อินเทอร์เน็ตขัดข้อง ให้ดำเนินการแก้ไขตาม กรณีเครื่องแม่ข่ายหรืออุปกรณ์ขัดข้อง - รวบรวมข้อมูลรายงานให้ฝ่ายบริหารทราบ

๔.๑๒) ข้อปฏิบัติกรณีเกิดสถานการณ์โรคระบาดในสถานที่ปฏิบัติงาน

กระบวนการงาน	รายละเอียด
รับแจ้งข่าวเกิดโรคระบาด/ติดตามข่าว	- ได้รับแจ้งจากหน่วยงานที่เกี่ยวข้อง เกี่ยวกับ สถานการณ์โรคระบาด
↓ ประเมินสถานการณ์อินเทอร์เน็ต	- ประเมินสถานการณ์เตรียมสถานที่ปฏิบัติงาน สำรอง/การทำงานที่บ้าน (WFH) และรอคำสั่ง จากฝ่ายบริหารห้ามเข้าพื้นที่เขตโรคระบาด ฯลฯ
มีเครื่องมือสำหรับการปฏิบัติงานนอกสถานที่ ไม่ใช่ แจ้งผู้เกี่ยวข้อง ↑	- หากไม่พบปัญหา ว่าเกิดจากอุปกรณ์ เครือข่ายและสายสัญญาณอินเทอร์เน็ต ให้ ตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายในระบบ เครือข่ายอินเทอร์เน็ต - หากพบปัญหา ว่าเกิดจากเครื่องคอมพิวเตอร์ แม่ข่ายในระบบ เครือข่ายอินเทอร์เน็ต อินเทอร์เน็ตขัดข้อง ให้ดำเนินการแก้ไขตาม กรณีเครื่องแม่ข่ายหรืออุปกรณ์ขัดข้อง
↓ ปฏิบัติงานนอกสถานที่	- หากมีความพร้อมในส่วน of เครื่องมือ สำหรับการปฏิบัติงานนอกสถานที่ ให้ ปฏิบัติงานนอกสถานที่
↓ รายงานให้ผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหารทราบ

๕. การกู้คืนระบบ

การกู้คืนระบบเมื่อเกิดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วย การกู้คืนระบบเครื่อง คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และการกู้คืนระบบสารสนเทศและฐานข้อมูล ซึ่งมีขั้นตอน ดังนี้

๑) การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติระบบเครื่อง คอมพิวเตอร์ แม่ข่ายและอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ ตลอดเวลา หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อให้ระบบการทำงานของ เครื่อง คอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

- ๑.๑) จัดหาอุปกรณ์ ชิ้นส่วนเพื่อทดแทนและเปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
- ๑.๒) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้แล้วเสร็จภายใน ๒๔ ชั่วโมง
- ๑.๓) จัดหาอุปกรณ์คอมพิวเตอร์ทดแทนจากหน่วยงานอื่นมาใช้ในการชั่วคราว
- ๑.๔) นำสื่อที่ได้จัดเก็บข้อมูลที่สำรองไว้กลับมา Restore
- ๑.๕) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่น ๆ ที่เกี่ยวข้อง

กระบวนการงาน	รายละเอียด
ระบบเครื่องคอมพิวเตอร์แม่ข่ายและ อุปกรณ์เครือข่าย เสียหายหรือหยุดทำงาน	- เกิดภัยด้านเทคโนโลยีสารสนเทศส่งผลให้ ระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ เครือข่าย ได้รับความเสียหายหรือหยุดทำงาน
จัดหาอุปกรณ์/ชิ้นส่วนเพื่อทดแทนและเปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย ซ่อมบำรุงอุปกรณ์	- เมื่อพบความเสียหาย ให้จัดหาอุปกรณ์/ ชิ้นส่วนเพื่อทดแทนและเปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหายโดยซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้แล้วเสร็จภายใน ๒๔ ชั่วโมง - หรือจัดหาอุปกรณ์คอมพิวเตอร์ทดแทนจาก หน่วยงานอื่นมาใช้ในการชั่วคราว
ซ่อมบำรุงอุปกรณ์	- นำสื่อที่ได้จัดเก็บข้อมูลที่สำรองไว้กลับมา Restore
ซ่อมบำรุงอุปกรณ์	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหารทราบ

๒) การกู้คืนระบบสารสนเทศและฐานข้อมูลให้สู่สภาวะปกติ ดังนี้

- ๒.๑) ตรวจสอบวันเวลาที่ข้อมูลสูญหาย
- ๒.๒) คัดลอกไฟล์สำรองข้อมูล ที่ทำการ Backup ไว้ในแต่ละวันเพื่อใช้ในการ Restore ข้อมูล
- ๒.๓) ปิดระบบสารสนเทศที่ต้องการกู้คืนข้อมูล
- ๒.๔) ทำการกู้คืนข้อมูล Restore
- ๒.๕) เปิดใช้งานระบบสารสนเทศ
- ๒.๖) ตรวจสอบข้อมูลที่ได้ทำการกู้คืนโดยผู้ดูแลระบบ
- ๒.๗) แจ้งผู้ใช้งานให้ดำเนินการตรวจสอบข้อมูลหลังจาก Restore

กระบวนการงาน	รายละเอียด
ระบบสารสนเทศและฐานข้อมูล เสียหายหรือหยุดทำงาน	- เกิดภัยด้านเทคโนโลยีสารสนเทศส่งผลให้ ระบบสารสนเทศและฐานข้อมูล ได้รับความ เสียหาย หรือหยุดทำงาน
ตรวจสอบวันเวลาที่ข้อมูลสูญหาย	- ตรวจสอบวันเวลาที่ข้อมูลสูญหาย
คัดลอกไฟล์สำรองข้อมูล	- ทำการคัดลอกไฟล์สำรองข้อมูล
ปิดระบบสารสนเทศที่ต้องการกู้คืนข้อมูล	- ปิดระบบสารสนเทศที่ต้องการกู้คืนข้อมูล
นำข้อมูลที่สำรองไว้มา Restore	- เตรียมไฟล์ Database ที่ทำการ Backup ไว้ ในแต่ละวันเพื่อใช้ในการ Restore ข้อมูล - ทำการกู้คืนข้อมูล Restore
เปิดระบบสารสนเทศ	- เปิดใช้งานระบบสารสนเทศ
ตรวจสอบข้อมูลที่ได้ทำการกู้คืน	- ตรวจสอบข้อมูลที่ได้ทำการกู้คืนโดยผู้ดูแล ระบบ
แจ้งผู้ใช้งานตรวจสอบข้อมูล	- แจ้งผู้ใช้งานให้ดำเนินการตรวจสอบข้อมูล หลังจาก Restore
รายงานผู้บังคับบัญชา	- รวบรวมข้อมูล รายงานให้ฝ่ายบริหารทราบ

ในส่วนของระยะเวลาการกู้คืนข้อมูลของระบบสารสนเทศและระบบเครือข่าย (Network) คำนึงถึง ความสำคัญ จำเป็นและความเหมาะสมในแต่ละภารกิจของเทศบาลตำบลกกโก ดังนี้

๑) ระบบเว็บไซต์เทศบาลตำบลกกโก (www.kokko.go.th) กำหนดระยะเวลากู้คืนข้อมูล ภายในเวลา ๒๔ ชั่วโมง

๒) ระบบสารสนเทศสำหรับสนับสนุนการปฏิบัติงานของเทศบาลตำบลกกโก ที่มีความ สำคัญต่อการปฏิบัติงานประจำค่อนข้างมาก เช่น ระบบ Intranet ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น กำหนดระยะเวลากู้คืนข้อมูล ภายในเวลา ๒๔ ชั่วโมง

๓) ระบบสารสนเทศเพื่อการบริหารจัดการภายในเทศบาลตำบลกกโก (ERP) เช่น ระบบ เบิกจ่ายเงินค่าเช่าบ้านข้าราชการ ระบบพัสดุและครุภัณฑ์ เป็นต้น กำหนดระยะเวลากู้คืนข้อมูลภายในเวลา ๔๘ ชั่วโมง

๔) ระบบ Network เมื่อเกิดความขัดข้องไม่สามารถทำงานได้ตามปกติ จะดำเนินการแก้ไขให้สามารถ ใช้งานได้ตามปกติภายในเวลา ๔ ชั่วโมง และหากต้องมีการเปลี่ยนหรือซ่อมแซมอุปกรณ์จะดำเนินการให้แล้วเสร็จโดยเร็วที่สุด เพราะไม่ได้มีอุปกรณ์สำรอง

ทั้งนี้ สามารถแสดงระยะเวลาเป้าหมายในการกู้คืนข้อมูลของระบบเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก

ลำดับ	ระบบสารสนเทศ	ระยะเวลาเป้าหมายในการกู้คืนข้อมูล (ชั่วโมง)		
		๒๔	๔๘	๗๒
๑	ระบบเว็บไซต์เทศบาลตำบลกกโก (www.kokko.go.th)	/		
๒	ระบบ Intranet	/		
๓	ระบบเว็บไซต์กกโก (www.กกโก.com)	/		
๔	ระบบติดตาม (Monitor) ระบบเครือข่ายคอมพิวเตอร์ ของเทศบาลตำบลกกโก	/		
๕	ระบบจัดเก็บข้อมูลอุปกรณ์เครือข่ายคอมพิวเตอร์เทศบาลตำบลกกโก	/		
๖	ระบบจองห้องประชุม Conference ของเทศบาลตำบลกกโก	/		
๗	ระบบสารบรรณอิเล็กทรอนิกส์ (e-saraban)	/		
๘	ระบบไปรษณีย์อิเล็กทรอนิกส์	/		
๙	ระบบช่วยตอบข้อความ ตอบคำถาม ในรูปแบบ Chat Bot ที่มีการโต้ตอบแบบ Auto และแบบ Manual		/	
๑๐	ระบบศูนย์ข้อมูล (Big Data)	/		

๖. การซ้อมแผนการแก้ไขความเสี่ยง

เพื่อเป็นการเตรียมความพร้อมรับมือกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงกำหนดแผนการซ้อม การแก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ จากสถานการณ์ฉุกเฉิน/พิบัติภัย โดยกำหนดให้มีการซ้อมแผนร่วมกับฝ่ายป้องกันและบรรเทาสาธารณภัย จำนวน ๑ ครั้งต่อปี ซึ่งมีขั้นตอน ดังนี้

๑) เตรียมการซ้อมแผนการแก้ไขปัญหาจากภัยพิบัติ

๑.๑) เลือกประเภทของภัยพิบัติที่จะดำเนินการซ้อมแผน ซึ่งเป็นภัยพิบัติที่ปรากฏตาม แผน แก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ได้แก่ กรณีอัคคีภัย กรณีแผ่นดินไหว กรณีน้ำท่วม กรณีน้ำรั่ว กรณีเครื่องแม่ข่ายหรืออุปกรณ์ขัดข้อง กรณีไฟฟ้าดับ กรณีโดนเจาะระบบเครือข่าย กรณีโดนโจมตีระบบสารสนเทศ กรณีโดนปิดล้อมสถานที่ปฏิบัติงาน กรณีข้อมูลได้รับความเสียหาย กรณีเกิด โรคระบาดในสถานที่ปฏิบัติงาน

๑.๒) กำหนดวัน เวลา ในการซ้อมแผนการแก้ไขปัญหาจากภัยพิบัติ

๑.๓) ประชุมเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อเตรียมการซ้อมแผนการแก้ไขปัญหาจากภัยพิบัติ

๒) ดำเนินการซ้อมแผนการแก้ไขปัญหาจากภัยพิบัติ ตามกรณีที่เกิดขึ้น

เทศบาลตำบลกกโก ได้กำหนดขั้นตอนการซ้อมแผนการแก้ไขปัญหาจากภัยพิบัติ ใน ๒ กรณี ได้แก่ กรณีอัคคีภัยและกรณีน้ำรั่ว ดังนี้

๒.๑) กรณีเกิดน้ำรั่ว ดำเนินการ ดังนี้

๒.๑.๑) ตรวจสอบการทำงานของระบบตรวจสอบและแจ้งเตือนภายในห้อง ควบคุมทั้งหมด

๒.๑.๒) เปิดพื้นที่ห้องเพื่อดูแนวสายตรวจจับน้ำรั่ว

๒.๑.๓) จำลองเหตุการณ์การเกิดน้ำรั่วซึม โดยการนำน้ำมาหยดลงบนสายตรวจจับน้ำรั่ว

๒.๑.๔) อุปกรณ์ตรวจจับน้ำรั่ว จะแสดงพิกัดที่ตรวจสอบพบน้ำรั่ว

๒.๑.๕) ระบบตรวจจับน้ำรั่ว จะส่งข้อความเตือน Water Leak Alarm

๒.๑.๖) ทำการตรวจสอบ วิเคราะห์และประเมินว่าสามารถแก้ไขปัญหได้หรือไม่ กรณีที่แก้ไขได้ให้นำผ้าไปซับน้ำบริเวณที่มีน้ำรั่ว รอจนกว่าระบบจะแจ้งเตือนว่า Water Leak back to normal และกรณีที่ไม่สามารถแก้ไขได้ให้ดำเนินการตามแนวทางปฏิบัติการแก้ไขปัญหาน้ำรั่ว ตามแผนแก้ไข ปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๒.๒) กรณีเกิดอัคคีภัย จะดำเนินการซ้อมแผนในส่วนที่ตรวจจับพบควันเท่านั้น เพื่อให้เกิดความปลอดภัยกับระบบมากที่สุด และเกิดผลกระทบกับส่วนอื่น ๆ น้อยที่สุด ซึ่งดำเนินการ ดังนี้

๒.๒.๑) ตรวจสอบการทำงานของระบบตรวจสอบและแจ้งเตือนภายในห้อง ควบคุมทั้งหมด

๒.๒.๒) จำลองเหตุการณ์การเกิดอัคคีภัย โดยการนำสเปรย์ควันมาฉีดที่บริเวณท่อตรวจจับควัน

๒.๒.๓) ระบบตรวจจับควัน จะตรวจสอบพบควัน

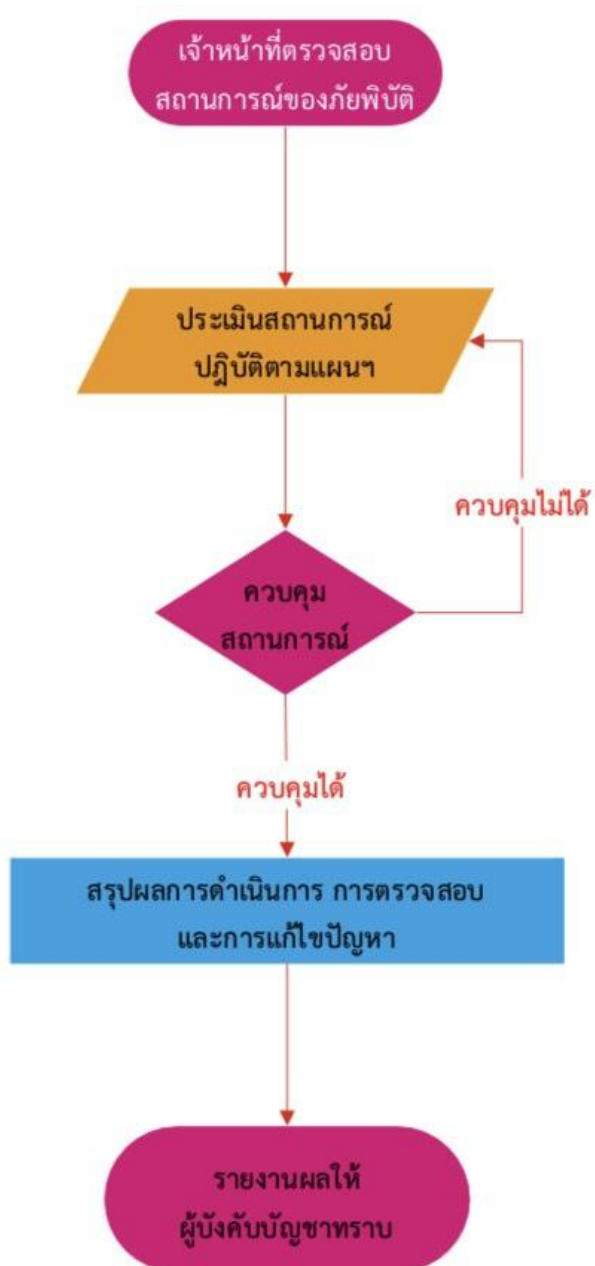
๒.๒.๔) ระบบตรวจจับควัน จะส่งข้อความเตือน SMOKE DETECTOR

๒.๒.๕) ทำการตรวจสอบ วิเคราะห์และประเมินสถานการณ์ว่าสามารถแก้ไขปัญหได้หรือไม่ กรณีแก้ไขไม่ได้ให้แจ้งบุคลากรภายในศูนย์เทคโนโลยีสารสนเทศท้องถิ่นออกจากพื้นที่และปฏิบัติตามแนวทางปฏิบัติการแก้ไข ปัญหาจากอัคคีภัย ตามแผนแก้ไขปัญหาภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๗. การติดตามและรายงานผล

เมื่อเกิดภัยพิบัติด้านระบบเทคโนโลยีสารสนเทศ ให้เจ้าหน้าที่ผู้รับผิดชอบรายงานการเกิดปัญหา และ ผลการแก้ไขให้ทราบในทันที ตามกระบวนการในการป้องกันและแก้ไขปัญหภัยพิบัติ ตามแผนแก้ไขปัญหภัย พิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) พร้อมทั้งสรุปรายงานผลการดำเนินการ การตรวจสอบ และการแก้ไขปัญหาต่าง ๆ ให้ผู้บังคับบัญชาทราบ

ขั้นตอนการติดตามและรายงานผล



ภาคผนวก



คำสั่งเทศบาลตำบลกกโก

ที่ ๒๔๙/๒๕๖๙

เรื่อง แต่งตั้งคณะกรรมการบริหารศูนย์เทคโนโลยีสารสนเทศ ของเทศบาลตำบลกกโก

ตามพระราชบัญญัติกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัย และเชื่อถือได้” ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษรองค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของเทศบาลตำบลกกโก ประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ในการรักษาความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์ ของเทศบาลตำบลกกโก ซึ่งข้าราชการ เจ้าหน้าที่ บุคลากร ของเทศบาลตำบลกกโก และบุคคลภายนอกที่ปฏิบัติงานร่วมกับเทศบาลตำบลกกโกจะต้องปฏิบัติตามอย่างเคร่งครัด นั้น

ดังนั้น เพื่อให้การบริหารจัดการและการใช้งานระบบเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้อง และภัยคุกคามต่างๆ เทศบาลตำบลกกโก จึงแต่งตั้งคณะกรรมการบริหารศูนย์เทคโนโลยีสารสนเทศ ของเทศบาลตำบลกกโก และเพื่อให้คณะกรรมการเป็นปัจจุบัน จึงแต่งตั้งคณะกรรมการบริหารศูนย์เทคโนโลยีสารสนเทศ เทศบาลตำบลกกโก ประกอบด้วย

๑. กรรมการที่ปรึกษาบริหารจัดการบริหารศูนย์เทคโนโลยีสารสนเทศ ของเทศบาลตำบล กกโก ประกอบไปด้วย

- | | | |
|-----------------------------------|------|-----------------|
| ๑.๑ นายกเทศมนตรีตำบลกกโก | เป็น | ประธานที่ปรึกษา |
| ๑.๒ รองนายกเทศมนตรีตำบลกกโก | เป็น | ที่ปรึกษา |
| ๑.๓ ที่ปรึกษานายกเทศมนตรีตำบลกกโก | เป็น | ที่ปรึกษา |
| ๑.๔ เลขานุการนายกเทศมนตรีตำบลกกโก | เป็น | ที่ปรึกษา |

มีหน้าที่ ให้คำปรึกษา วางแผน กำหนดหรือให้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ, แผนปฏิบัติการดิจิทัล, แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ฯลฯ ที่เกี่ยวข้องให้เป็นไปตามข้อกำหนด/ระเบียบ/ข้อบังคับ เพื่อให้ระบบเทคโนโลยีสารสนเทศของเทศบาลตำบล กกโก เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ ของเทศบาลตำบลกกโก

//๒. คณะกรรมการ...

๒. คณะกรรมการบริหารศูนย์เทคโนโลยีสารสนเทศ ของเทศบาลตำบลกกโก ประกอบไปด้วย

๒.๑ ปลัดเทศบาลตำบลกกโก	เป็น	ประธานกรรมการ
๒.๒ รองปลัดเทศบาลตำบลกกโก	เป็น	รองประธานกรรมการ
๒.๓ หัวหน้าสำนักปลัดเทศบาล	เป็น	กรรมการ
๒.๔ ผู้อำนวยการกองคลัง	เป็น	กรรมการ
๒.๕ ผู้อำนวยการกองช่าง	เป็น	กรรมการ
๒.๖ ผู้อำนวยการกองการศึกษา	เป็น	กรรมการ
๒.๗ หัวหน้าฝ่ายปกครอง หรือ ผู้แทน	เป็น	กรรมการ
๒.๘ หัวหน้าฝ่ายบริหารงานทั่วไป หรือ ผู้แทน	เป็น	กรรมการ
๒.๙ นักวิเคราะห์นโยบายและแผน	เป็น	กรรมการ
๒.๑๐ นักจัดการงานทั่วไป	เป็น	กรรมการ / เลขานุการ

มีหน้าที่

๑) ให้คำปรึกษาและอำนวยความสะดวกในการปฏิบัติงานแก่คณะทำงานบริหารจัดการบริหารศูนย์เทคโนโลยีสารสนเทศระดับสำนัก/กอง ต่างๆ ให้เกิดประสิทธิภาพและตรงตามวัตถุประสงค์ของกรรมการที่ปรึกษา

๒) เป็นกรรมการและคณะทำงานการบริหารจัดการบริหารศูนย์เทคโนโลยีสารสนเทศ ของเทศบาลตำบลกกโก

๓) ต้องกำหนดระเบียบเทศบาลตำบลกกโก ว่าด้วยการใช้งานระบบเครือข่ายและระบบคอมพิวเตอร์ ให้ผู้ใช้บริการทั้งภายในองค์กรและภายนอกองค์กรที่เข้ามาใช้บริการระบบเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย เพื่อไม่ให้เกิดการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ.๒๕๖๐ และเป็นการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ จากผู้ใช้บริการระบบเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก

๔) ต้องตรวจสอบภายในด้านความมั่นคงปลอดภัยด้านสารสนเทศ ของเทศบาลตำบลกกโก เพื่อให้ระบบเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ ของเทศบาลตำบล กกโก

๕) ติดตามประเมินผลการใช้งานระบบเครือข่ายและคอมพิวเตอร์ของผู้ใช้งานระบบเครือข่ายและคอมพิวเตอร์ของเทศบาลตำบลกกโก หรือนโยบายอื่นที่เกี่ยวข้อง ให้เกิดประโยชน์และไม่ผิดกฎหมาย

๖) ควรมีการกำหนดแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ, แผนปฏิบัติการดิจิทัล, แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของเทศบาลตำบลกกโก ฯลฯ ที่เกี่ยวข้องให้เป็นไปข้อกฎหมาย/ระเบียบ/ข้อบังคับ ที่เกี่ยวข้อง ไปตามความเหมาะสมของสถานการณ์ปัจจุบัน

๓. คณะกรรมการบริหารจัดการบริหารศูนย์เทคโนโลยีสารสนเทศระดับปฏิบัติ ประกอบไปด้วย

๓.๑ หัวหน้าฝ่ายปกครอง หรือ ผู้แทน	เป็น	ประธานกรรมการ
๓.๒ หัวหน้าฝ่ายบริหารงานทั่วไป หรือ ผู้แทน	เป็น	รองประธานกรรมการ
๓.๓ นักวิเคราะห์นโยบายและแผน	เป็น	กรรมการ
๓.๔ นักทรัพยากรบุคคล	เป็น	กรรมการ
๓.๕ นิติกร	เป็น	กรรมการ

๓.๖	เจ้าพนักงานจัดเก็บรายได้	เป็น	กรรมการ
๓.๗	เจ้าพนักงานธุรการ (กองคลัง)	เป็น	กรรมการ
๓.๘	เจ้าพนักงานธุรการ (กองการศึกษา)	เป็น	กรรมการ
๓.๙	เจ้าพนักงานธุรการ (สำนักปลัดเทศบาล)	เป็น	กรรมการ
๓.๑๐	นักจัดการงานทั่วไป (สำนักปลัดเทศบาล)	เป็น	กรรมการ/เลขานุการ

มีหน้าที่

๑) นำระเบียบเทศบาลตำบลกกโก ว่าด้วยการใช้งานระบบเครือข่ายและระบบคอมพิวเตอร์ แผนนโยบาย และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ, แผนปฏิบัติการดิจิทัล, แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของเทศบาลตำบลกกโก จะเป็นแผนหรือนโยบายอื่น ที่ทางคณะกรรมการบริหารศูนย์เทคโนโลยีสารสนเทศได้ กำหนดนโยบายนำไปปฏิบัติ

๒) ช่วยควบคุม และดูแลการใช้งานระบบเครือข่ายคอมพิวเตอร์, ระบบคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศ หรือการพัฒนาระบบสารสนเทศของเทศบาลตำบลกกโกให้เป็นไปตามนโยบายและแนวทางปฏิบัติ

๓) การใช้อินเทอร์เน็ตจุดใดที่เข้าใช้งานไม่ได้ หรือการใช้งานระบบสารสนเทศอื่นๆ ที่เข้าใช้งานไม่ได้หรือมีปัญหา ให้แจ้งมายังงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ สำนักปลัด

๔) เมื่อมีความต้องการเพิ่มจุดเข้าใช้อินเทอร์เน็ตหรือขยายเครือข่ายของระบบเครือข่ายอินเทอร์เน็ตของสำนักงานเทศบาลตำบลกกโก ให้สำนัก/กอง/ฝ่าย/งาน ให้ประสานงานเป็นลายลักษณ์อักษร มายังงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ ฝ่ายบริหารงานทั่วไป สำนักปลัด แต่ถ้าต้องการเปลี่ยนสายหรือเข้าแลนใหม่ ให้แจ้งมายังงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ สำนักปลัด

๕) ถ้ามีหรือต้องการให้ซ่อมหรือตรวจเช็คระบบคอมพิวเตอร์เบื้องต้นให้ยกเครื่องคอมพิวเตอร์, เครื่องปริ้นเตอร์ หรืออุปกรณ์ต่อพ่วงมายังงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ สำนักปลัด

๖) ถ้ามีบุคคลภายนอกที่ต้องการใช้สัญญาณอินเทอร์เน็ตของสำนักงานเทศบาลตำบลกกโก ให้แจ้งงานส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศ ฝ่ายบริหารงานทั่วไป สำนักปลัด เพื่อขอรับคู่มือหรือรหัสอินเทอร์เน็ต

๔. คณะทำงานด้าน IT Support ประกอบไปด้วย

๔.๑	นายนิติ อาสกุล ตำแหน่ง เจ้าพนักงานธุรการชำนาญงาน	เป็น	ประธานคณะทำงาน
๔.๒	นางสาวอังคณา คังสิน ตำแหน่ง ผู้ช่วยพัฒนาการท่องเที่ยว	เป็น	คณะทำงาน
๔.๔	นางสาวจิณห์จุฑา ขำละเอียด ตำแหน่ง พนักงานจ้างทั่วไป	เป็น	คณะทำงาน
๔.๕	นางสาวจิตธนา ตันปกรณ ตำแหน่ง พนักงานจ้างเหมาบริการ	เป็น	คณะทำงาน
๔.๖	นายวิษณุศวรรษ มาตรง ตำแหน่ง พนักงานจ้างเหมาบริการ	เป็น	คณะทำงาน

มีหน้าที่

๑) ดูแลรักษา จัดการ แก้ไข ซ่อมแซม ทางด้านระบบเทคโนโลยีสาร, ระบบเครือข่าย, Server และระบบสัญญาณอินเทอร์เน็ต และบำรุงรักษาเครื่องใช้อุปกรณ์คอมพิวเตอร์ ตลอดจน Software และ Hardware ขององค์กรให้อยู่ในสภาพที่ดี และพร้อมใช้งานอยู่ตลอดเวลา

๒) วิเคราะห์การแก้ไขปัญหาเบื้องต้นให้กับผู้ขอใช้บริการ

๓) ออกแบบและวางระบบเครือข่ายและระบบสัญญาณอินเทอร์เน็ต

๔) ดำเนินงานตามนโยบายของคณะกรรมการบริหารศูนย์เทคโนโลยีสารสนเทศ

๕. กรรมการควบคุมกำกับและอนุญาตการใช้อินเทอร์เน็ตของเทศบาลตำบลกกโก ประกอบไปด้วย

๕.๑ นายกเทศมนตรีตำบลกกโก	เป็น	CEO/ผู้บริหารสูงสุด
๕.๒ ปลัดเทศบาลตำบลกกโก	เป็น	CIO/ผู้บริหารศูนย์ฯ
๕.๓ รองปลัดเทศบาลตำบลกกโก	เป็น	ผู้อำนวยการศูนย์ฯ
๕.๔ หัวหน้าสำนักปลัดเทศบาล	เป็น	ผู้ดูแลศูนย์ฯ

โดยมีอำนาจหน้าที่ ให้พิจารณาตรวจสอบ กลั่นกรองผู้ขอรับบริการ การใช้งานระบบเครือข่ายและระบบคอมพิวเตอร์ของเทศบาลตำบลกกโก ให้เป็นไปตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของเทศบาลตำบลกกโกให้ผู้ใช้บริการทั้งภายในองค์กรและภายนอกองค์กรที่เข้ามาใช้บริการระบบเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย เพื่อไม่ให้เกิดการกระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และเป็นการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ จากผู้ใช้บริการระบบเทคโนโลยีสารสนเทศของเทศบาลตำบลกกโก

ให้ผู้ที่ได้รับการแต่งตั้งปฏิบัติหน้าที่ตามระเบียบของทางราชการโดยเคร่งครัด ไม่ให้เกิดความเสียหายแก่ทางราชการได้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๕ เดือน กันยายน พ.ศ. ๒๕๖๙



(นายก่อภณ ฮั่นสกุล)

นายกเทศมนตรีตำบลกกโก

