แผนปฏิบัติการป้องกันและแก้ไขปัญหา
ด้านความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2566 - 2570)
องค์การบริหารส่วนจังหวัดขอนแก่น

ประกาศองค์การบริหารส่วนจังหวัดขอนแก่น
เรื่อง ประกาศใช้แผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์
พ.ศ.๒๕๖๖ - ๒๕๗๐

.....

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และคำสั่งสำนักนายกรัฐมนตรี ที่ ๒๓๙/๒๕๖๓ เรื่อง มอบหมายและมอบอำนาจให้รองนายกรัฐมนตรี และรัฐมนตรีประจำสำนักนายกรัฐมนตรี ปฏิบัติหน้าที่ประธานกรรมการในคณะกรรมการต่างๆ ตามกฎหมาย และระเบียบสำนักนายกรัฐมนตรี และตามมติคณะรัฐมนตรีข้างต้น จึงออกประกาศแจ้งการใช้นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๖ - ๒๕๗๐) เพื่อเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

องค์การบริหารส่วนจังหวัดขอนแก่นจึงได้จัดทำแผนปฏิบัติการรป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๖ - ๒๕๗๐) ขึ้น เพื่อเป็นกรอบในการดำเนินงานของหน่วยงานและแสดงถึงความพร้อมของหน่วยงานในการตอบสนองต่อการป้องกันภัยคุกคามทางไซเบอร์ในส่วนของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งคณะกรรมการระบบเทคโนโลยีสารสนเทศและการสื่อสารองค์การบริหารส่วนจังหวัดขอนแก่นพิจารณาให้ความเห็นชอบ “ร่าง” แผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖- ๒๕๗๐ ในคราวประชุมครั้งที่ ๑/๒๕๖๖ เมื่อวันที่ ๗ ธันวาคม ๒๕๖๖

จึงประกาศมาเพื่อทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๙ เดือน ธันวาคม พ.ศ. ๒๕๖๖

(นายพงษ์ศักดิ์ ตั้งวานิชกพงษ์)
นายกองค์การบริหารส่วนจังหวัดขอนแก่น

สารบัญ

ส่วนที่ ๑
บทสรุปสำหรับผู้บริหาร

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

แนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและ กรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าว ไปใช้บังคับ

คำสั่งสำนักนายกรัฐมนตรี ที่ ๒๓๙/๒๕๖๓

ตามคำสั่งสำนักนายกรัฐมนตรี ที่ ๒๓๙/๒๕๖๓ เรื่อง มอบหมายและมอบอำนาจให้รองนายกรัฐมนตรี และรัฐมนตรีประจำสำนักนายกรัฐมนตรี ปฏิบัติหน้าที่ประธานกรรมการในคณะกรรมการต่างๆ ตามกฎหมาย และระเบียบสำนักนายกรัฐมนตรี และตามมติคณะรัฐมนตรีข้างต้น จึงออกประกาศแจ้งการใช้นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) เพื่อเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

องค์การบริหารส่วนจังหวัดขอนแก่นจึงได้จัดทำแผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) ขึ้น เพื่อเป็นกรอบในการดำเนินงานของหน่วยงานและแสดงถึงความพร้อมของหน่วยงานในการตอบสนองต่อการป้องกันภัยคุกคามทางไซเบอร์ในส่วนของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ส่วนที่ ๒
ความสอดคล้องกับแผน ๓ ระดับ

๒.๑ ยุทธศาสตร์ชาติ (แผนระดับที่ ๑)

๒.๑.๑ ยุทธศาสตร์ชาติ ด้านความมั่นคง

เป้าหมายที่ ๓ กองทัพ หน่วยงานด้านความมั่นคง ภาครัฐ ภาคเอกชนและภาคประชาชน มีความพร้อมในการป้องกันและแก้ไขปัญหาความมั่นคง

เป้าหมายที่ ๔ ประเทศไทยมีบทบาทด้านความมั่นคงเป็นที่ชื่นชมและได้รับ การยอมรับโดยประชาคมระหว่างประเทศ

เป้าหมายที่ ๕ การบริหารจัดการความมั่นคงมีผลสำเร็จที่เป็นรูปธรรมอย่างมี ประสิทธิภาพ

๒.๑.๒ ประเด็นยุทธศาสตร์ ข้อ ๔.๒ การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

ข้อ ๔.๒.๑ การแก้ไขปัญหาความมั่นคงในปัจจุบัน

ข้อ ๔.๒.๒ การติดตาม เฝ้าระวัง ป้องกัน และแก้ไขปัญหาที่อาจอุบัติขึ้นใหม่

๒.๒ แผนระดับที่ ๒

๒.๒.๑ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นยุทธศาสตร์ด้านความมั่นคง

ข้อ ๓.๒ แผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

๒.๒.๒ แผนปฏิรูปประเทศด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ ประเด็นยุทธศาสตร์แผนปฏิรูปประเทศด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ

ข้อ ๕.๕ การปฏิรูปการบริหารจัดการความปลอดภัยไซเบอร์ /กิจการอวกาศ และระบบและเครื่องมือด้านการสื่อสารมวลชนและโทรคมนาคมเพื่อสนับสนุนภารกิจการป้องกัน บรรเทาสาธารณภัย ภายใต้

กิจกรรมที่ ๑ การปกป้องคุ้มครองและรักษาความมั่นคงปลอดภัยไซเบอร์ ของโครงสร้างพื้นฐานสำคัญด้านสารสนเทศของประเทศ

๒.๒.๓ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒

ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศ สู่ความมั่งคั่งและยั่งยืน

แนวทางการพัฒนาที่ ๓.๒ การพัฒนาเสริมสร้างศักยภาพการป้องกัน ประเทศ เพื่อเตรียมความพร้อมในการรับมือภัยคุกคาม ทั้งการทหารและภัยคุกคามอื่น ๆ

ยุทธศาสตร์ที่ ๗ การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์

แนวทางการพัฒนาที่ ๓.๕ การพัฒนาเศรษฐกิจดิจิทัล

๒.๒.๔ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๒ - ๒๕๖๕) นโยบายที่ ๑๐ เสริมสร้างความมั่นคงปลอดภัยไซเบอร์ รองรับวัตถุประสงค์

๓.๔.๕ เพื่อพัฒนาศักยภาพของภาครัฐ และส่งเสริมบทบาทและความเข้มแข็งของทุกภาคส่วนในการรับมือกับภัยคุกคามทุกรูปแบบที่กระทบกับความมั่นคง แผนที่ ๑๕ การป้องกันและแก้ไขความมั่นคงทางไซเบอร์

๒.๓ แผนระดับที่ ๓ ที่เกี่ยวข้อง

๒.๓.๑ นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ ๒๕๖๑ - ๒๕๘๐)

ยุทธศาสตร์ที่ ๖ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล แผนงาน

ข้อ ๓ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัลและการทำธุรกรรมออนไลน์

๒.๓.๒ แผนปฏิบัติการด้านดิจิทัลเพื่อเศรษฐกิจและสังคมระยะ ๕ ปี (พ.ศ. ๒๕๖๒ - ๒๕๖๕)

เป้าหมายที่ ๕ สร้างความเชื่อมั่น

ประเด็นขับเคลื่อน ๕.๑ การเสริมสร้างความมั่นคงปลอดภัยไซเบอร์

เป้าหมายที่ ๖ พัฒนากำลังคนดิจิทัล ประเด็นขับเคลื่อน

๖.๑ การพัฒนากำลังคนและประชาชนสู่ยุคดิจิทัล

๒.๓.๓ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ ๒๕๖๐ - ๒๕๖๕)

ประเด็นยุทธศาสตร์ที่ ๑ เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

ประเด็นยุทธศาสตร์ที่ ๒ ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๓ ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

ประเด็นยุทธศาสตร์ที่ ๔ เสริมสร้างระบบเศรษฐกิจดิจิทัล

ประเด็นยุทธศาสตร์ที่ ๕ สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๖ เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

๒.๓.๔ แผนเตรียมพร้อมแห่งชาติ (พ.ศ. ๒๕๖๐-๒๕๖๕)

ยุทธศาสตร์ที่ ๓ การเสริมสร้างความร่วมมือ การเตรียมพร้อมรับมือภัยคุกคามกับต่างประเทศ

กลยุทธ์ ข้อ ๔ เสริมสร้างความสัมพันธ์และความร่วมมือการเตรียมพร้อมด้านวิกฤตการณ์ความมั่นคงกับต่างประเทศ อาทิ การก่อวินาศกรรม การก่อการร้าย ภัยความมั่นคงทางไซเบอร์ ภัยความมั่นคงทางอวกาศ โรคติดต่ออุบัติใหม่ ให้สอดคล้องกับนโยบายรัฐบาล นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ และยุทธศาสตร์ความมั่นคงเฉพาะด้านที่เกี่ยวข้อง

๒.๓.๕ นโยบายและแผนปฏิบัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ.๒๕๖๕-๒๕๗๐)

ยุทธศาสตร์ที่ ๑ สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Capacity)

กลยุทธ์ที่ ๑.๑ เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ ๑.๒ สร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ ๑.๓ ส่งเสริมการวิจัยและพัฒนาและนวัตกรรมด้านความมั่นคง

ยุทธศาสตร์ที่ ๒ บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)

กลยุทธ์ที่ ๒.๑ ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและภาคเอกชน

กลยุทธ์ที่ ๒.๒ ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม

ยุทธศาสตร์ที่ ๓ สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Resilience)

กลยุทธ์ที่ ๓.๑ กำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

กลยุทธ์ที่ ๓.๒ กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ที่ ๓.๓ ปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ

ยุทธศาสตร์ที่ ๔ สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน (Standard)

กลยุทธ์ที่ ๔.๑ เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ ๔.๒ ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม

กลยุทธ์ที่ ๔.๓ ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์

ส่วนที่ ๓ สาระสำคัญ
แผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)
องค์การบริหารส่วนจังหวัดขอนแก่น

๓.๑ การประเมินสถานการณ์ ปัญหา ความจำเป็น

ปัจจุบันเทคโนโลยีดิจิทัลมีบทบาทสำคัญในการเป็นเครื่องมืออำนวยความสะดวกแก่การดำรงชีวิตประจำวัน โดยรายงานของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union :ITU) พบว่า ปี พ.ศ. ๒๕๖๑ มีจำนวนผู้ใช้อินเทอร์เน็ต คิดเป็นร้อยละ ๕๑ ของประชากรทั่วโลก โดยคาดว่า ภายในปี พ.ศ. ๒๕๖๖ จะมีจำนวนผู้ใช้งานอินเทอร์เน็ต เพิ่มขึ้นถึงร้อยละ ๗๐ ของประชากรทั่วโลก

ผลสำรวจพฤติกรรมผู้ใช้งานอินเทอร์เน็ตในประเทศไทยปี พ.ศ. ๒๕๖๑ โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (สพธอ.) พบว่า ประเทศไทยก้าวสู่สังคมดิจิทัลอย่างเต็มรูปแบบแล้ว

ซึ่งค่าเฉลี่ยของการใช้งานอินเทอร์เน็ตของคนไทยเติบโตเพิ่มขึ้นมากกว่าปีที่ผ่านมาถึง ๓ เท่า

ทั้งนี้ ความก้าวหน้าทางเทคโนโลยีดิจิทัล โดยเฉพาะอย่างยิ่งการใช้อินเทอร์เน็ตมาพร้อมกับความท้าทายและภัยคุกคามทางไซเบอร์ซึ่งมีหลากหลายรูปแบบ ไม่ว่าจะเป็นการเผยแพร่ ข้อมูลที่ไม่เป็นจริง การพยายามบุกรุกเข้าระบบ การโจมตีสภาพการใช้งานของระบบ การพัฒนาโปรแกรมที่ไม่พึงประสงค์ และการสร้างหน้าเว็บไซต์ปลอมเพื่อหลอกลวงหาผลประโยชน์ เป็นต้น อันก่อให้เกิดความเสียหายแก่ประเทศชาติ ภาคธุรกิจ และปัจเจกบุคคล

จากข้อมูลสถิติภัยคุกคามทางไซเบอร์ของไทย ปี พ.ศ. ๒๕๖๑ รวบรวมโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) พบว่าความพยายามบุกรุกเข้าระบบสารสนเทศ (Intrusion Attempts) เป็นภัยคุกคามไซเบอร์ อันดับ ๑ ของประเทศไทย คิดเป็นสัดส่วนร้อยละ ๔๓ จากจำนวนภัยคุกคาม ทั้งหมด ๒,๕๒๐ เหตุการณ์

นอกจากนี้ ผลจากการสำรวจความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ ในปี พ.ศ. ๒๕๕๙ และ พ.ศ. ๒๕๖๑ ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เพื่อวิเคราะห์ถึงสถานการณ์ ปัญหา อุปสรรค และการรับมือกับภัยคุกคามไซเบอร์ของประเทศไทย โดยมีหลักการพิจารณา

๑) การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์

๒) การปกป้องดูแลอุปกรณ์สารสนเทศ

๓) ความสามารถในการตรวจพบเหตุภัยคุกคาม

๔) การรับมือภัยคุกคาม

๕) การกู้คืนระบบหลังเกิดเหตุ

พบว่า การรับมือภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐและภาคเอกชนมากกว่า ๕๐๐ หน่วยงาน มีค่าเฉลี่ยในระดับต่ำ จากสถานการณ์ภัยคุกคามไซเบอร์ข้างต้นที่เกิดขึ้นอย่างรวดเร็วและรุนแรงขึ้นทุกปี การขาดแคลนบุคลากรที่ปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อันส่งผลต่อความสามารถในการดำเนินการ จนส่งผลให้ถูกโจมตีทางไซเบอร์และส่งผลต่อเศรษฐกิจของประเทศไทยอย่างมหาศาล ถึงแม้ว่าจะมีการลงทุนในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เพิ่มสูงขึ้น แต่ในประเทศไทยเองยังขาดแคลนบุคลากรและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ ทำให้ต้องพึ่งพาบุคลากรและผลิตภัณฑ์จากต่างประเทศ ดังนั้น จึงมีความจำเป็นต้องกำหนดนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ในการเสริมสร้างศักยภาพในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนตอบสนองต่อเหตุภัยคุกคามและฟื้นฟูระบบให้กลับคืนสู่สภาวะปกติอย่างทันท่วงที

๓.๒ สาระสำคัญ

วิสัยทัศน์การรักษาความมั่นคงปลอดภัยไซเบอร์ คือ
“ให้บริการและให้ความร่วมมือเพื่อความมั่นคงปลอดภัยไซเบอร์”

นโยบายการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๑ การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

๑) จัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยจัดโครงสร้างองค์กร พร้อมกำหนดอำนาจ บทบาทหน้าที่และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ที่มีประสิทธิภาพ โดยองค์การบริหารส่วนจังหวัดขอนแก่นได้ดำเนินการ ดังนี้

- ประกาศองค์การบริหารส่วนจังหวัดขอนแก่น เรื่อง ปรับปรุงแผนอัตรากำลัง ๓ ปี ประจำปีงบประมาณ พ.ศ.๒๕๖๔-๒๕๖๖ (ครั้งที่ ๑๒) และการปรับปรุงโครงสร้างส่วนราชการจากกองยุทธศาสตร์และงบประมาณ เป็นสำนักยุทธศาสตร์และงบประมาณ
- คำสั่งที่ ๔๔๒๔/๒๕๖๕ เรื่อง การมอบหมายอำนาจหน้าที่และความรับผิดชอบของข้าราชการและพนักงานจ้าง สังกัดสำนักยุทธศาสตร์และงบประมาณ ลงวันที่ ๓ พฤศจิกายน ๒๕๖๕
- คำสั่งที่ ๙๒๒/๒๕๖๖ เรื่อง การมอบหมายอำนาจหน้าที่และความรับผิดชอบของบุคลากรสังกัดสำนักยุทธศาสตร์และงบประมาณ (แก้ไขครั้งที่ ๑) ลงวันที่ ๑๓ กุมภาพันธ์ ๒๕๖๖
- คำสั่งที่ ๓๐๑๔/๒๕๖๖ เรื่อง การมอบหมายอำนาจหน้าที่และความรับผิดชอบของบุคลากรสังกัดสำนักยุทธศาสตร์และงบประมาณ (แก้ไขครั้งที่ ๒) ลงวันที่ ๘ มิถุนายน ๒๕๖๖

กำหนดให้ฝ่ายสถิติข้อมูลและสารสนเทศ ส่วนบริการและเผยแพร่วิชาการ สำนักยุทธศาสตร์และงบประมาณ มีหน้าที่รับผิดชอบงานจัดทำคำสั่ง ประกาศ งานด้านเทคโนโลยีสารสนเทศ งานระบบสารสนเทศเพื่อการพัฒนาองค์กรและการพัฒนาจังหวัด และมอบหมายให้ หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศทำหน้าที่ควบคุม กำกับ และตรวจสอบควบคุมความเสี่ยงในชั้นแรก (Business Unit หรือ First Line of Defense)

๒) กำหนดให้เจ้าหน้าที่ตำแหน่งนักวิชาการคอมพิวเตอร์ สังกัดฝ่ายสถิติข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และงบประมาณ รับผิดชอบบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือกับภัยคุกคามทางไซเบอร์ มีบทบาทหน้าที่และความรับผิดชอบ ดังนี้

- มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด
- มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)
- บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงที่องค์กรมี และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการหน่วยงานเป็นวาระประจำ
- ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์
- ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้เรื่องความเสี่ยงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้านภัยคุกคามทางไซเบอร์

๓.๒.๒ กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยงรวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้

๑. การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรมเพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

๑. การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

๒. การใช้ Checklist

๓. การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

๔. การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

๕. การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสียรวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๒. การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๒.๑ การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

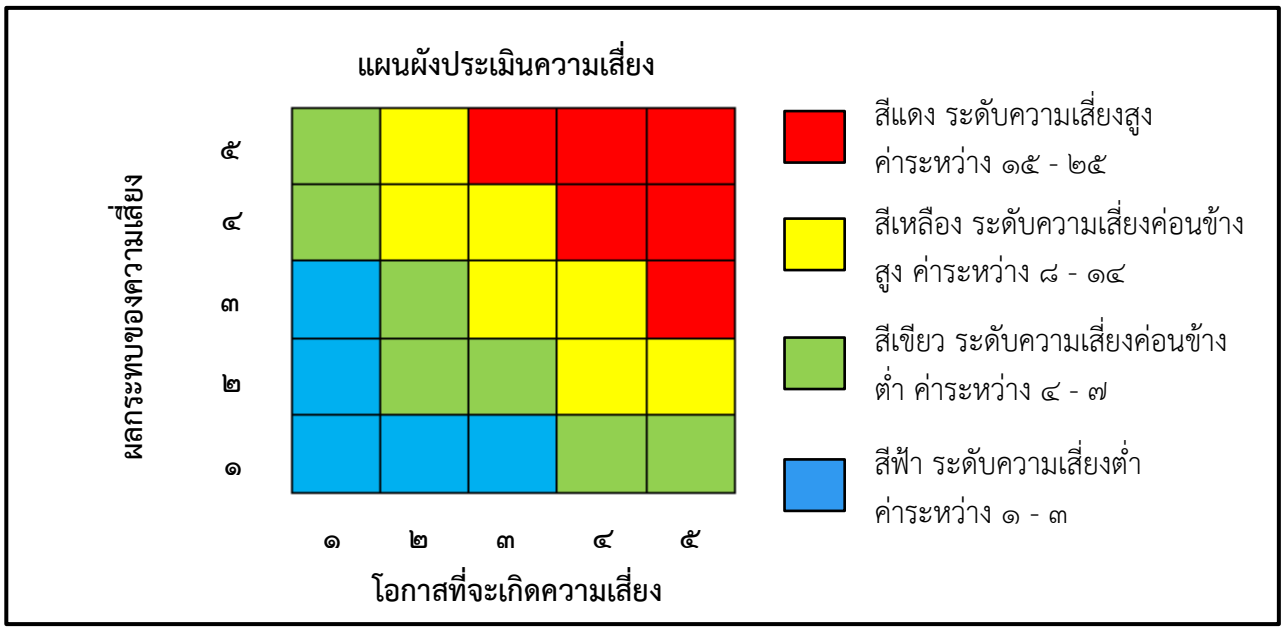
เกณฑ์การประเมินผลกระทบ เป็นดังนี้

ระดับ	การประเมิน
๑	น้อยมาก
๒	น้อย
๓	ปานกลาง
๔	สูง
๕	สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยงเป็นดังนี้

ระดับ	การประเมิน
๑	เกิดขึ้นน้อยมาก
๒	เกิดขึ้นน้อย
๓	เกิดขึ้นปานกลาง
๔	เกิดขึ้นสูง
๕	เกิดขึ้นสูงมาก

๒.๓ การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังรูปที่ ๑



รูปที่ ๑ แสดงแผนผังประเมินความเสี่ยง

๒.๔ การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๓. การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

๓.๑ ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

๓.๒ การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

๓.๓ การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๓.๔ การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก

๔. การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยงเมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

๔.๑ พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๔.๒ เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๔.๓ กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๔.๔ ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วย การรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๕. การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

๖. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

องค์การบริหารส่วนจังหวัดขอนแก่นได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้เป็น ๕ ประเภท ดังนี้

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัยอัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร
(Hardware and Data Communication Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Alware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กรความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูลดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆจึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

๗. การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกันเพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิดหากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่นอุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงานองค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

๘. ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศขององค์การบริหารส่วนจังหวัดขอนแก่นได้แก่

๑. ปัจจัยภายนอก ได้แก่

๑.๑ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๑.๒ การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

๑.๕ ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๒. ปัจจัยภายใน ได้แก่

๒.๑ ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร

๒.๓ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๙. การประเมินความเสียหาย

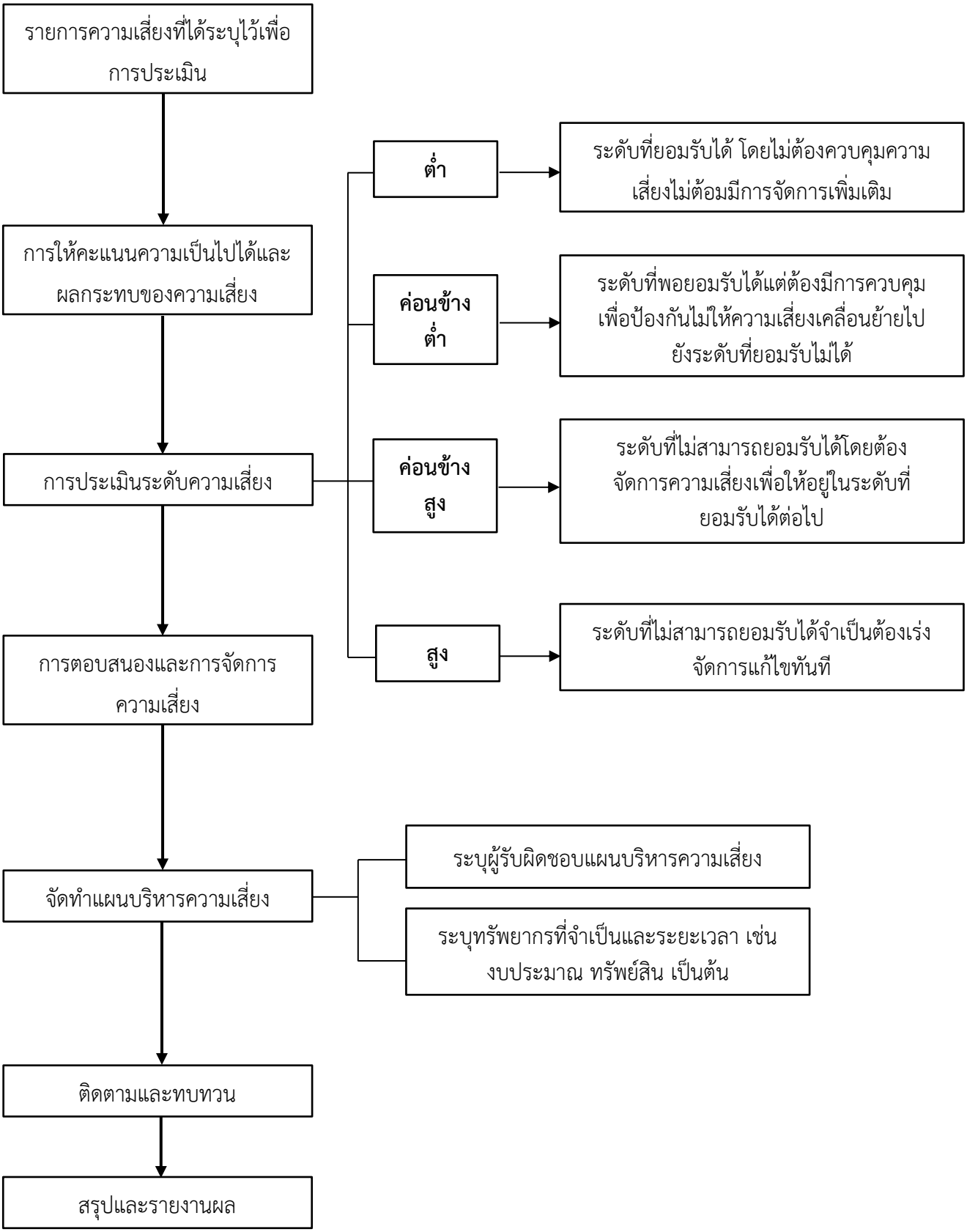
๑. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ การถูกเจาะหรือลักลอบ (Hack) ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒. ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

๑๐. การวิเคราะห์การบริหารจัดการความเสี่ยง

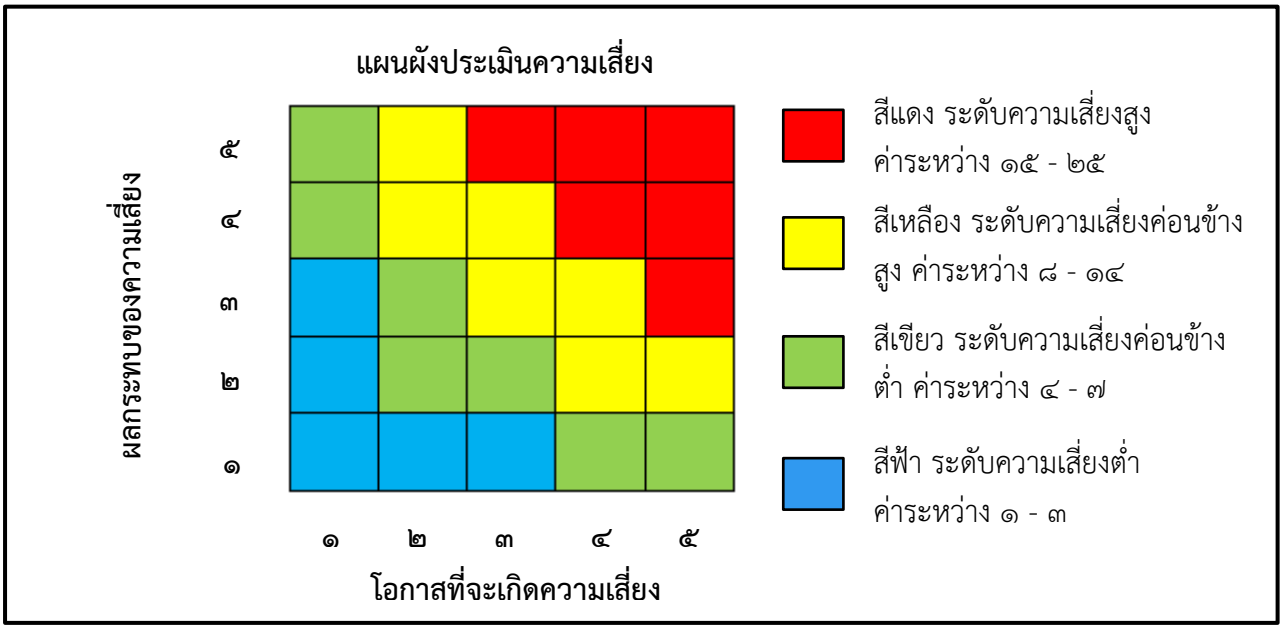
องค์การบริหารส่วนจังหวัดขอนแก่น ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. ๒๕๖๗ ให้สอดคล้องกับแผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) กระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

๑. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



๒. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ ผลสรุป การกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้



ตารางที่ ๑ ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
๑	ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	๓	๕	๑๕
๒	เสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๓	๕	๑๕
๓	ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	๓	๔	๑๒
๔	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๒	๕	๑๐

๓. การวิเคราะห์โอกาส ผลกระทบ และการตอบสนองความเสี่ยง

(๓) รหัสความเสี่ยง	(๔) โครงการ/กิจกรรม/ภารกิจ อปท. ที่สำคัญ	(๕) วัตถุประสงค์	(๖) ผู้รับผิดชอบ	(๗) ความเสี่ยง	(๘) ประเภท ความเสี่ยง	(๙) คะแนนโอกาส	(๑๐) คะแนนผลกระทบ	(๑๑) คะแนนความเสี่ยง (๙) x (๑๐)	(๑๒) วิธีการตอบสนองความเสี่ยง
๑	ป้องกันความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดีหรือ Hacker	๑. เพื่อป้องกันระบบเครือข่ายโดนโจมตีโดย Hacker ๒. ป้องกันการโจมตีการให้บริการ(Denial of Services/ DOS) ๓. ป้องกันการดักจับข้อมูลผ่านระบบเครือข่าย ๔. ป้องกันการโจรกรรมข้อมูลที่สำคัญหรือลักลอบแก้ไขเปลี่ยนแปลงข้อมูล	สำนักยุทธศาสตร์และงบประมาณ	๑. ระบบเครือข่ายโดนโจมตีโดย Hacker ๒. การโจมตีการให้บริการ (Denial of Services/ DOS) ๓. การดักจับข้อมูลผ่านระบบเครือข่าย ๔. การโจรกรรมข้อมูลที่สำคัญ หรือลักลอบแก้ไขเปลี่ยนแปลงข้อมูล	๑. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Technology Risks) ๒. ความเสี่ยงด้านความน่าเชื่อถือขององค์กร (Reputational Risks)	๓	๕	สูง ๓ x ๕ = ๑๕	การถ่ายโอน (Transfer)
๒	ลดความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๑. ระบบคอมพิวเตอร์แม่ข่ายใช้งานได้เต็มประสิทธิภาพ ๒. ลดความเสี่ยงของความเสียหายของข้อมูลและการกู้คืนข้อมูล	สำนักยุทธศาสตร์และงบประมาณ	๑. ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ ๒. เสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล	เทคโนโลยีสารสนเทศ (Technology Risks)	๓	๕	สูง ๓ x ๕ = ๑๕	การถ่ายโอน (Transfer)

(๓) รหัสความเสี่ยง	(๔) โครงการ/กิจกรรม/ภารกิจ อปท. ที่สำคัญ	(๕) วัตถุประสงค์	(๖) ผู้รับผิดชอบ	(๗) ความเสี่ยง	(๘) ประเภท ความเสี่ยง	(๙) คะแนนโอกาส	(๑๐) คะแนนผลกระทบ	(๑๑) คะแนนความเสี่ยง (๙) x (๑๐)	(๑๒) วิธีการตอบสนองความเสี่ยง
๓	ป้องกันความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	๑. เพื่อสร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network ๒. เพื่อให้ผู้ใช้บริการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง ๓. ป้องกันการเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูล โดยไม่ได้ รับอนุญาต ๔. ป้องกันข้อมูลหายหรือมีการแก้ไขโดยไม่ทราบสาเหตุ	สำนักยุทธศาสตร์และงบประมาณ	๑. การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต ๒. ข้อมูลหาย หรือมีการแก้ไขโดยไม่ทราบสาเหตุ ๓. ผู้ใช้งานใช้งานไม่เหมาะสมและเกินความจำเป็น ๔. อุปกรณ์ทำงานช้าลง หรือไม่สามารถใช้งานได้	๑. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Technology Risks)	๓	๔	ค่อนข้างสูง ๓ x ๔ = ๑๒	การถ่ายโอน (Transfer)

(๓) รหัสความเสี่ยง	(๔) โครงการ/กิจกรรม/ภารกิจ อปท. ที่สำคัญ	(๕) วัตถุประสงค์	(๖) ผู้รับผิดชอบ	(๗) ความเสี่ยง	(๘) ประเภท ความเสี่ยง	(๙) คะแนนโอกาส	(๑๐) คะแนนผลกระทบ	(๑๑) คะแนนความเสี่ยง (๙) x (๑๐)	(๑๒) วิธีการตอบสนองความเสี่ยง
๔	ป้องกันความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๑. เพื่อป้องกันไฟฟ้าขัดข้อง หรือแรงดันไฟฟ้าไม่คงที่ ๒. เพื่อป้องกันแหล่งกำเนิดไฟฟ้าดับ ๓. เพื่อจัดหาเครื่องสำรองไฟฟ้าเพิ่มเติม ๔. เพื่อบำรุงรักษาเครื่องสำรองไฟฟ้า	สำนักยุทธศาสตร์และงบประมาณ	๑. การเกิดกระแสไฟฟ้าขัดข้องหรือเกิดแรงดันไฟฟ้าไม่คงที่ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายอาจได้รับความเสียหาย จากแรงดันไฟฟ้าที่ไม่คงที่	เทคโนโลยีสารสนเทศ (Technology Risks)	๒	๕	ค่อนข้างสูง ๒ x ๕ = ๑๐	การควบคุม (Treat)

๓.๒.๓ นโยบายและแผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์

- มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด
- มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)
- บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงที่องค์กรมี และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการหน่วยงานเป็นวาระประจำ
- ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์
- ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้เรื่องความเสี่ยงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้านภัยคุกคามทางไซเบอร์

๓.๒.๓.๑ นโยบายรักษาความปลอดภัยระบบสารสนเทศ

การรักษาความปลอดภัยระบบสารสนเทศ องค์การบริหารส่วนจังหวัดขอนแก่น กำหนดขึ้นเพื่อเป็นแนวทางในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดขอนแก่นให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC ๒๗๐๐๑ (มาตรฐานที่มักจะถูกนำมาใช้เพื่อยกระดับความปลอดภัยให้กับระบบคอมพิวเตอร์และเครือข่ายมากที่สุด)

นโยบายรักษาความปลอดภัยระบบสารสนเทศ องค์การบริหารส่วนจังหวัดขอนแก่นประกอบด้วย ๔ ด้าน โดยมีรายละเอียดดังต่อไปนี้

๑. ด้านการพิสูจนตัวตน (Authentication) กรณีใช้สัญญาณอินเทอร์เน็ต

๑.๑ ผู้ใช้งานต้องรักษาข้อมูลชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง

๑.๒ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากชื่อผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

๑.๓ ผู้ใช้งานสามารถเปลี่ยนรหัสผ่าน (Password) เพื่อความปลอดภัย

๑.๔ ผู้ใช้งานคอมพิวเตอร์และสัญญาณอินเทอร์เน็ตทุกคนต้องระบุตัวตนในการใช้งานผ่านระบบสารสนเทศทุกครั้ง (Authentication) ทั้งนี้แบ่งผู้ใช้เป็น 2 กลุ่ม คือ

๑.๔.๑ No-Authentication สำหรับผู้บริหารไม่ต้องกรอกชื่อและรหัสผ่าน แต่ระบุตัวตนด้วยหมายเลขเครื่องคอมพิวเตอร์ที่ใช้ (mac address) ที่ระบบได้บันทึกค่าไว้แล้ว

๑.๔.๒ Authentication ผู้ใช้งานทั่วไปต้องกรอกชื่อและรหัสผ่านทุกครั้งก่อนใช้งาน

๑.๕ การเข้าใช้งานระบบ (log in) หนึ่งครั้งระบบกำหนดให้สามารถใช้งานอยู่ในระบบได้ ๘ ชั่วโมง หากผู้ใช้งานต้องการใช้งานน้อยกว่า ให้ทำการออกจากระบบ (log out) ทุกครั้ง

๒. ด้านการบริหารจัดการระบบสารสนเทศ (Information System Management**)**

๒.๑ กำหนดสิทธิให้ผู้ดูแลระบบและผู้ที่เกี่ยวข้อง สามารถเข้า-ออก ห้องสารสนเทศ

๒.๒ กำหนดสิทธิให้ผู้ดูแลระบบและผู้ที่เกี่ยวข้อง สามารถบริหารจัดการระบบสารสนเทศ

๒.๓ กำหนดให้มีการตรวจสอบการทำงานของระบบสารสนเทศเป็นประจำ

๒.๔ กำหนดให้มีการสำรองข้อมูลทุกสัปดาห์ ในส่วนของฐานข้อมูลเว็บไซต์ และข้อมูลการจราจรข้อมูลทางคอมพิวเตอร์ (Log file)

๓. ด้านความปลอดภัยของไฟร์วอลล์ (Firewall)

๓.๑ สำนักยุทธศาสตร์และงบประมาณเป็นส่วนราชการที่กำกับ ดูแล บริหารจัดการระบบสารสนเทศ

๓.๒ กำหนดการให้บริการหรือไม่ให้บริการเว็บไซต์ (Block) เช่น Block Bittorrent

๓.๓ เก็บข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ ไม่น้อยกว่า ๙๐ วัน

๓.๔ เปิดพอร์ตการเชื่อมต่อ (Service) ที่จำเป็นต่อการให้บริการเท่านั้น เช่น HTTP, HTTPS, FTP, RDP, SSH, PING

๔. ด้านความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server)

๔.๑ กำหนดสิทธิให้ผู้ดูแลระบบและผู้ที่เกี่ยวข้องในการเข้า-ออก ห้องสารสนเทศ

๔.๒ ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใดๆ ต่ออุปกรณ์ที่ติดตั้งตามส่วนราชการต่าง ๆ โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๔.๓ จัดทำแผนผังระบบเครือข่าย (Network Diagram) เพื่อเป็นประโยชน์ต่อการบริหารจัดการและพัฒนาระบบในอนาคต

๔.๔ ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่ายในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของระบบ

๔.๕ ผู้ดูแลระบบจะต้องตรวจสอบการทำงานของเครื่องแม่ข่ายอย่างสม่ำเสมอ เพื่อป้องกันการถูกบุกรุกจากเครือข่ายภายนอก

๓.๒.๓.๒ ข้อกำหนดที่เกี่ยวข้อง

การกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่ม

- ผู้ดูแลระบบ
- ผู้ใช้งานระบบ

การทบทวนสิทธิ

- ลาออก
- เปลี่ยนตำแหน่ง
- โอน ย้าย
- สิ้นสุดการจ้าง

ลำดับชั้นความลับ และการเข้าถึงข้อมูล

จัดแบ่งลำดับชั้นความลับของข้อมูล	จัดแบ่งระดับชั้นการเข้าถึง
- ข้อมูลลับที่สุด - ข้อมูลลับมาก - ข้อมูลลับ - ข้อมูลทั่วไป	- ระดับชั้นสำหรับผู้บริหาร - ระดับชั้นสำหรับผู้ดูแลระบบ - ระดับชั้นสำหรับผู้ปฏิบัติงาน - ระดับชั้นสำหรับผู้ใช้งานทั่วไป

แนวทางการควบคุมการเข้าถึงและการแบ่งระดับชั้นและสิทธิการเข้าถึง

- ระดับผู้ดูแลระบบ มีหน้าที่ในการควบคุมการเข้าถึงข้อมูล รวมไปถึงวิธีการทำลายข้อมูล
- ระดับเจ้าของข้อมูล มีหน้าที่ตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง
- ระดับผู้ปฏิบัติงาน มีหน้าที่ในการบันทึก ตรวจสอบ ปรับปรุง และรายงานข้อมูล
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป มีสิทธิในการใช้ข้อมูลตามสิทธิที่มอบให้เท่านั้น

การใช้งานเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของหน่วยงาน

๑. การใช้งานทั่วไป

- ผู้ใช้งานต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน
- ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว
- ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องตรวจสอบไวรัสก่อนใช้งาน

๒. การสำรองข้อมูลและการกู้คืน

- ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลไว้บนสื่อบันทึกอื่น ๆ
- ผู้ใช้งานมีหน้าที่เก็บรักษาข้อมูล การสำรองข้อมูลให้เก็บไว้ในที่เหมาะสม

๓. การใช้งานระบบอินเทอร์เน็ต

- การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัส
- ไม่ใช้ระบบอินเทอร์เน็ตขององค์การบริหารส่วนจังหวัดหาประโยชน์ในเชิงพาณิชย์
- ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงาน
- ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมละเมิดลิขสิทธิ์
- การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น ที่ยั่วยุ หรือ ให้ร้าย
- ออกจากระบบเครือข่าย และปิดเว็บบราวเซอร์ทุกครั้งเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๔. การใช้งานเครือข่ายสังคมออนไลน์

- อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ ตามที่ได้กำหนดไว้เท่านั้น
- ผู้ใช้งานต้องตระหนักถึงความมั่นคงปลอดภัยในการใช้งาน และต้องรับผิดชอบหากเกิดความเสียหาย
- ไม่อนุญาตให้ใช้งานเผยแพร่ข้อมูลที่เป็นความลับ และมีผลกระทบต่อบุคคลอื่น
- ให้ใช้งานเครือข่ายสังคมออนไลน์ได้เท่าที่จำเป็นโดยไม่เบียดบังเวลาปฏิบัติงาน
- หากเกิดปัญหาจากการใช้งาน ต้องแจ้งผู้ดูแลระบบโดยเร็วเพื่อดำเนินการตามความเหมาะสม

๓.๒.๓.๓ แผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์

๑. การเตรียมความพร้อมด้านบุคลากร งบประมาณ และโครงสร้างพื้นฐานด้านไอที

- **กำหนดหน้าที่ความรับผิดชอบ**

มอบหมายให้นักวิชาการคอมพิวเตอร์ ฝ่ายสถิติข้อมูลและสารสนเทศ ส่วนบริการและเผยแพร่วิชาการ สำนักยุทธศาสตร์และงบประมาณ เป็นผู้รับผิดชอบในการดูแลบำรุงรักษาโครงสร้างพื้นฐานด้านไอที ประสานความร่วมมือกับบุคลากรของส่วนราชการในสังกัดองค์การบริหารส่วนจังหวัดขอนแก่น เพื่อกำหนดแนวทางในองค์กรมีความมั่นคงปลอดภัยทางไซเบอร์

- **กำหนดขั้นตอนในการควบคุมป้องกันและรับมือสถานการณ์ผิดปกติที่เกิดขึ้น**

๑) เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ป้องกันเครือข่าย (Firewall) สม่ำเสมอ

๒) เรียงลำดับความสำคัญและแก้ไขปัญหาที่เกิดขึ้นตามการแจ้งเตือน

๓) ฝ่ายสถิติข้อมูลและสารสนเทศจะต้องติดตามข่าวสาร ศึกษาแนวทางการป้องกันด้านความมั่นคงปลอดภัยทางไซเบอร์ จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) สม่ำเสมอ

- **การสำรองข้อมูลสม่ำเสมอ**

กำหนดการสำรองข้อมูลทุกวัน สำรองข้อมูลที่เพิ่มขึ้น (Incremental backup) และสำรองแบบเต็ม (Full Backup)

๒. การรับมือเมื่อเกิดเหตุ

- ตรวจสอบว่าฐานข้อมูลได้รับความเสียหายหรือไม่ หากข้อมูลไม่เสียหายให้ทำการกู้คืนข้อมูลอย่างแม่นยำและรวดเร็วที่สุดที่เป็นไปได้
- เปลี่ยนรหัสผ่าน
- กำหนดสิทธิ์การเข้าถึงเครื่องแม่ข่ายทั้งหมด
- ตรวจสอบการตั้งค่าระบบ
- ตรวจสอบหาร่องรอยหรือสาเหตุที่เกิดจาก

๓. การดำเนินการหลังถูกภัยคุกคาม

- กู้คืนข้อมูล
- หากเกินการรับมือของหน่วยงาน ให้ขอความช่วยเหลือจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

องค์การบริหารส่วนจังหวัดขอนแก่น

ฝ่ายสถิติข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และงบประมาณ

043-239256 || strategy@kkpao.go.th