แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติด้านเทคโนโลยีสารสนเทศ สำนักบรรณสารสนเทศ พ.ศ. ๒๕๖๗

จัดทำโดย

สำนักบรรณสารสนเทศ มหาวิทยาลัยสุโขทัยธรรมาธิราช

พ.ศ. ๒๕๖๗

คำนำ

ในยุคที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการดำเนินงานและการให้บริการในองค์กรต่าง ๆ การเตรียมความพร้อมเพื่อรับมือกับสถานการณ์ฉุกเฉินที่เกิดจากภัยพิบัติด้านเทคโนโลยีสารสนเทศจึงเป็นสิ่งที่จำเป็นอย่างยิ่งที่จะต้องทำการป้องกันและปัญหาในด้านต่าง ๆ ที่อาจจะเกิดขึ้นจากสถานการณ์ที่ไม่แน่นอน ซึ่งส่งผลกระทบต่อการดำเนินงานตามภารกิจขององค์กร หรืออาจจะทำให้ไม่สามารถบริการได้อย่างต่อเนื่อง ดังนั้นการจัดทำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติด้านเทคโนโลยีสารสนเทศ ของสำนักบรรณสารสนเทศ เพื่อเป็นกรอบและแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อข้อมูล ฐานข้อมูล และสารสนเทศของสำนักบรรณสารสนเทศ เพื่อป้องกันความเสียหายและลดผลกระทบที่อาจจะเกิดขึ้นต่อข้อมูล จึงทำให้มั่นใจได้ว่า การดำเนินงานด้านเทคโนโลยีสารสนเทศของสำนักบรรณสารสนเทศจะดำเนินงานได้ต่อเนื่อง แม้อยู่ในสถานการณ์ฉุกเฉิน

สำนักบรรณสารสนเทศถือว่าข้อมูล ฐานข้อมูล และสารสนเทศต่าง ๆ ของสำนักบรรณสารสนเทศ เป็นทรัพย์สินที่สำคัญ จึงได้จัดทำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติด้านเทคโนโลยีสารสนเทศ สำนักบรรณสารสนเทศขึ้น เพื่อใช้เป็นเครื่องมือในการดำเนินงาน ดูแลรักษา ตลอดจนแก้ไขปัญหาที่จะเกิดขึ้นกับข้อมูลและสารสนเทศอันเป็นทรัพย์สินที่สำคัญให้เกิดความมั่นคงปลอดภัยอย่างเป็นระบบและมีประสิทธิภาพสูงสุด เกิดประโยชน์สูงสุดต่อการการเรียนการสอนของมหาวิทยาลัยต่อไป

(กัลยาณี ศุภดิษฐ์)
หัวหน้าศูนย์เทคโนโลยีบรรณสารสนเทศ
กรกฎาคม ๒๕๖๗

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติด้านเทคโนโลยีสารสนเทศ
สำนักบรรณสารสนเทศ พ.ศ. ๒๕๖๗

ข้อมูล ฐานข้อมูล และสารสนเทศ ถือเป็นทรัพย์สินที่สำคัญของมหาวิทยาลัย จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ให้เกิดประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ สำนักบรรณสารสนเทศได้ตระหนักถึงความสำคัญของข้อมูล ฐานข้อมูล และสารสนเทศของมหาวิทยาลัย ซึ่งอาจมีปัจจัยจากภายนอกหรือปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลสารสนเทศรวมทั้งอุปกรณ์เกิดผลเสียหายได้

สำนักบรรณสารสนเทศ ได้จัดทำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติด้านเทคโนโลยีสารสนเทศขึ้น เพื่อใช้เป็นกรอบและแนวทางในการดูแลรักษาและแก้ไขปัญหาที่เกิดขึ้น ที่จะส่งผลกระทบและเป็นอันตรายต่อข้อมูล ฐานข้อมูล และสารสนเทศที่สำคัญของมหาวิทยาลัย โดยความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ขัดข้อง การถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจ ไฟฟ้าขัดข้อง เป็นต้น

๑.๑ กรณีการป้องกันไวรัสล้มเหลว

๑.๑.๑ กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

๑.๑.๒ วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

๑.๑.๓ ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

๑.๑.๔ ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

๑.๑.๕ กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุให้เจ้าหน้าที่สำนักทราบ หรือกรณีมีเหตุอันทำให้งานด้านเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้สำนักจะต้องประกาศให้ทุกหน่วยงานทราบ

๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว

๑.๒.๑ กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall

๑.๒.๒ ผู้ดูแลระบบแจ้งผู้บังคับบัญชาตามลำดับขั้นตอนดังนี้ หัวหน้าฝ่ายแจ้งและทำบันทึกแจ้งหัวหน้าศูนย์เทคโนโลยีบรรณสาร เพื่อจัดทำบันทึกในการขอความอนุเคราะห์แก้ไขปัญหาผ่านผู้อำนวยการสำนักบรรณสารสนเทศ เสนอต่อผู้อำนวยการสำนักคอมพิวเตอร์และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ทราบโดยด่วน

๑.๒.๓ ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

๑.๓ กรณีการเชื่อมโยงเครือข่ายล้มเหลว

๑.๓.๑ ดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

๑.๓.๒ หากสายเคเบิ้ลชำรุดเสียหายหรือขาดให้รีบแจ้งผู้บังคับบัญชาตามลำดับขั้นตอนดังนี้ หัวหน้าศูนย์เทคโนโลยีบรรณสาร เพื่อจัดทำบันทึกในการขอความอนุเคราะห์แก้ไขปัญหาผ่านผู้อำนวยการสำนัก

บรรณสารสนเทศ เสนอต่อผู้อำนวยการสำนักคอมพิวเตอร์และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ทราบ พร้อมติดต่อบริษัทผู้รับจ้างดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว

๑.๓.๓ หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางจุด ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคาร และ switch ที่ติดตั้งอยู ณ อาคารนั้น ๆ

๑.๔ กรณีอุปกรณ์หรือเครื่องคอมพิวเตอร์ขัดข้อง

๑.๔.๑ แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

๑.๔.๒ เร่งดำเนินการจัดหาอุปกรณ์มาเปลี่ยนใหม่และนำข้อมูลที่ได้สำรองไว้มากู้คืนข้อมูล (Data Recovery) โดยเร็ว

๑.๔.๓ ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

๑.๕ กรณีไฟฟ้าขัดข้อง

๑.๕.๑ ระบบสารสนเทศมีเครื่องสำรองไฟฟ้า UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ไม่น้อยกว่า ๔ ชั่วโมง

๑.๕.๒ หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชาตามลำดับขั้นตอนดังนี้ หัวหน้าศูนย์เทคโนโลยีบรรณสาร เพื่อจัดทำบันทึกในการขอความอนุเคราะห์แก้ไขปัญหาผ่านผู้อำนวยการสำนักบรรณสารสนเทศ เสนอต่อผู้อำนวยการสำนักคอมพิวเตอร์และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ทราบ เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

๑.๕.๓ ระบบสำรองไฟฟ้ามีการทดสอบการใช้งานของระบบทุก ๆ วันจันทร์ เวลา ๐๘.๓๐ น. และมีการบำรุงรักษาและตรวจเช็คความพร้อมของอุปกรณ์ทุก ๆ ๓ เดือน

๒. สถานการณ์ฉุกเฉินที่เกิดจากภัยและเหตุการณ์ที่ไม่สามารถคาดการณ์ได้

๒.๑ กรณีไฟไหม้

๒.๑.๑ หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

๒.๑.๒ หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร

๒.๑.๓ หากปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ภายหลังจากการดับเพลิงเรียบร้อยแล้ว ให้รีบดำเนิน สำรวจและจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาทดแทนเพื่อให้การปฏิบัติงานดำเนินต่อไปได้

๒.๑.๔ ตรวจสอบระบบตรวจดับไฟและ/หรือระบบดับไฟอัตโนมัติ พร้อมทั้งอบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๒.๒ กรณีแผ่นดินไหว/อาคารถล่ม

๒.๒.๑ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร

๒.๒.๒ ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้

๒.๒.๓ เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสารสนเทศสามารถดำเนินการต่อไปได้

๒.๓ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

๒.๓.๑ กรณีที่ไม่สามารถเข้ามาปฏิบัติงาน ณ สถานที่ตั้งได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งหัวหน้าศูนย์เทคโนโลยีบรรณสาร เพื่อจัดทำบันทึกในการขอความอนุเคราะห์แก้ไขปัญหาผ่านผู้อำนวยการสำนักบรรณสารสนเทศ เสนอต่อผู้อำนวยการสำนักคอมพิวเตอร์และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ทราบ เพื่อดำเนินการหาวิธีแก้ไขปัญหาที่เกิดขึ้น

๒.๓.๒ หลังเหตุการณ์ความไม่สงบและสามารถเข้ามาปฏิบัติงาน ณ สถานที่ตั้งได้ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าวหากพบความชำรุดเสียหาย ให้แจ้งหัวหน้าศูนย์เทคโนโลยีบรรณสาร เพื่อจัดทำบันทึกในการขอความอนุเคราะห์แก้ไขปัญหาผ่านผู้อำนวยการสำนักบรรณสารสนเทศ เสนอต่อผู้อำนวยการสำนักคอมพิวเตอร์และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ทราบ พร้อมดำเนินการซ่อมแซมแก้ไข หากไม่สามารถใช้งานได้จะต้องจัดหาอุปกรณ์ทดแทนเร่งด่วนตามความจำเป็น

๓. สถานการณ์ฉุกเฉินที่เกิดจากบุคคล

๓.๑ กรณีโจรกรรมทรัพย์สิน

๓.๑.๑ ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน

๓.๑.๒ สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย

๓.๑.๓ ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน เพื่อผู้ใช้งานระบบงานสามารถใช้ระบบงานต่าง ๆ ได้โดยเร็ว

๓.๒ กรณีโจรกรรมข้อมูล

๓.๒.๑ ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน

๓.๒.๒ สำรวจตรวจสอบรายการข้อมูลที่สูญหาย

๓.๒.๓ ทางผู้ดูแลระบบ ตรวจสอบช่องโหว่ความปลอดภัย และอัพเดทระบบเพื่อปิดช่องโหว่ต่าง ๆ

๓.๒.๔ ในกรณีที่นำข้อมูลสำคัญที่ก่อให้เกิดความเสียหายแก่ทางราชการให้ดำเนินการแจ้งเรื่อง ไปยัง กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)

๓.๓ กรณีผู้ปฏิบัติงานไม่สามารถปฏิบัติงานได้

๓.๓.๑ แจ้งผู้บังคับบัญชาทราบ

๓.๓.๒ ปฏิบัติตามคู่มือการปฏิบัติงาน (Workflow) หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

๔. การกำหนดผู้รับผิดชอบ

๔.๑ ผู้บริหาร รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหาและสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๔.๑.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

๔.๑.๒ ผู้อำนวยการสำนักคอมพิวเตอร์

๔.๑.๓ ผู้อำนวยการสำนักบรรณสารสนเทศ

๔.๒ ผู้รับผิดชอบการปฏิบัติงานระบบเครือข่าย ห้องแม่ข่ายและศูนย์ข้อมูล ดำเนินการภายใต้ความรับผิดชอบของสำนักคอมพิวเตอร์ ในการรับผิดชอบการปฏิบัติงาน ระบบเครือข่าย ห้องแม่ข่ายและศูนย์ข้อมูล ได้แก่

๔.๒.๑ อาจารย์ ดร.ศรันย์ นาคฌนอม ผู้อำนวยการสำนักคอมพิวเตอร์ โทรศัพท์ ๐๘ ๐๐๓๙ ๗๗๘๘

๔.๒.๒ นายเสกสรรค์ ปิ่นเจริญ หัวหน้าฝ่ายเครือข่ายคอมพิวเตอร์ โทรศัพท์ ๐๖ ๕๙๙๗ ๘๒๕๖

๔.๓ ผู้รับผิดชอบระบบสารสนเทศและฐานข้อมูล รับผิดชอบการปฏิบัติงานระบบสารสนเทศ และฐานข้อมูล ได้แก่

๔.๓.๑ อาจารย์ ดร.ศรันย์ นาคฌนอม ผู้อำนวยการสำนักคอมพิวเตอร์ โทรศัพท์ ๐๘ ๐๐๓๙ ๗๗๘๘

๔.๓.๒ นางสาวศิวาพร รุขชาติ ตำแหน่ง หัวหน้าฝ่ายปฏิบัติการประมวลผล โทรศัพท์ ๐๘ ๙๒๐๕ ๓๕๕๘

๔.๓.๓ นางวัลลภาภรณ์ มัสอูดี ตำแหน่ง หัวหน้าฝ่ายวิเคราะห์และพัฒนาระบบ โทรศัพท์ ๐๘ ๙๗๘๖ ๙๙๕๗

๔.๔ ผู้รับผิดชอบการประสานงานหน่วยงานที่เกี่ยวข้อง และการบริการเทคนิค ได้แก่

๔.๔.๑ อาจารย์ ดร.ศรันย์ นาคฌนอม ผู้อำนวยการสำนักคอมพิวเตอร์ โทรศัพท์ ๐๘ ๐๐๓๙ ๗๗๘๘

๔.๔.๒ นางสาวศศิธร สายนภา ตำแหน่ง หัวหน้าฝ่ายบริการงานคอมพิวเตอร์ โทรศัพท์ ๐๘ ๑๘๑๘ ๖๕๑๖

๔.๕ ผู้รับผิดชอบการสำรวจตรวจสอบรายการทรัพย์สิน ได้แก่

๔.๕.๑ อาจารย์ ดร.ศรันย์ นาคฌนอม ผู้อำนวยการสำนักคอมพิวเตอร์ โทรศัพท์ ๐๘ ๐๐๓๙ ๗๗๘๘

๔.๕.๒ นายหัสนัย ริยาพันธ์ หัวหน้าสำนักงานเลขานุการ โทรศัพท์ ๐๘ ๗๐๒๐ ๖๕๙๑

๔.๕.๓ นายอำนาจ ธรรมกิจ หัวหน้าศูนย์ฝึกอบรมเทคโนโลยีสารสนเทศ โทรศัพท์ ๐๘ ๙๔๕๒ ๐๘๓๐

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบมีประสิทธิภาพมีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานราชการให้เกิดประโยชน์สูงสุดจึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉินเพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

สำนักบรรณสารสนเทศได้จัดทำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบในด้านเทคโนโลยีสารสนเทศ เพื่อเป็นกรอบและแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบในด้านเทคโนโลยีสารสนเทศ ภายใต้แนวคิดของแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบในด้านเทคโนโลยีสารสนเทศของสำนักคอมพิวเตอร์ มหาวิทยาลัย ดังนี้

๑. แนวทางป้องกันและการเตรียมการขั้นต้น

๒. การเตรียมความพร้อม

๓. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

๔. มาตรการการป้องกันและการแก้ปัญหาภัยพิบัติ

๕. ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๖. แผนการสำรองและกู้คืนระบบกลับสู่สภาพปกติ

๗. การติดตามและรายงานผล

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อฐานข้อมูล และข้อมูลสารสนเทศของมหาวิทยาลัย โดยมีรายละเอียดดังนี้

๑. แนวทางป้องกันและการเตรียมการขั้นต้น

๑.๑ การประกาศแผน (Activation)

มหาวิทยาลัยมีการประกาศใช้แผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเป็นทางการ เพื่อให้บุคลากรของมหาวิทยาลัยทราบและปฏิบัติอย่างเคร่งครัด โดยที่มีเอกสารยืนยันที่แสดงให้เห็นว่าบุคลากรทุกคนทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางปฏิบัติตามแผนด้วย โดยที่เมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการสำนักคอมพิวเตอร์จะทำการแจ้งให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ของมหาวิทยาลัยทราบเพื่อพิจารณาและประกาศใช้แผนต่อไป

๑.๒ กระบวนการดำเนินงาน (Procedure)

สำนักคอมพิวเตอร์เตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติ โดยที่เมื่อเกิดเหตุการณ์ฉุกเฉินขึ้นต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ ระบุที่มาของผู้บุกรุกหรือยุติเหตุการณ์ที่เกิดขึ้นได้ทันเวลาและถูกต้องระบบงานต่าง ๆ ที่มีความสำคัญจะต้องมีการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืนระบบเมื่อมีปัญหาเกิดขึ้น

๑.๓ การติดต่อสื่อสาร (Communication) ในการติดต่อมีการจัดทำข้อมูลบัญชีรายชื่อสำหรับการติดต่อกับหน่วยงานภายนอกที่เกี่ยวข้อง เพื่อใช้สำหรับการติดต่อด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้าส่วนภูมิภาค สถานีตำรวจภูธร สถานีตำรวจดับเพลิง เป็นต้น มีการประสานงานกับศูนย์รักษาความปลอดภัยของมหาวิทยาลัยเพื่อประสานงานกับสถานีตำรวจดับเพลิงเกี่ยวกับเรื่องแผนที่อาคารและเส้นทางเดินในอาคาร

๑.๔ การจัดเตรียมอุปรณ์ที่จำเป็น

ในการเตรียมพร้อมเพื่อการรับภัยพิบัติที่อาจจะเกิดขึ้นต่อด้านเทคโนโลยีสารสนเทศของสำนักคอมพิวเตอร์ ซึ่งเป็นหน่วยงานกลางในการดูแลและให้บริการด้านคอมพิวเตอร์ มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีที่คอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยจัดเตรียมอุปกรณ์ดังต่อไปนี้

๑) แผ่นติดตั้งระบบปฏิบัติการ ระบบปฏิบัติการเครือข่าย และแผ่นติดตั้งระบบงานที่สำคัญ

๒) เทปสำรองข้อมูลและระบบงานที่สำคัญ

๓) แผ่นโปรแกรม Antivirus/Spyware

๔) แผ่น Driver อุปกรณ์ต่าง ๆ

๕) ระบบการสำรองไฟฉุกเฉิน

๖) อุปกรณ์สำรองอื่น ๆ ที่เกี่ยวข้องของคอมพิวเตอร์

๑.๕ การสำรองข้อมูล (Backup) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับข้อมูล ซึ่งอาจจะสูญหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุก/ทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำเอาข้อมูลที่มีปัญหากลับมาใช้งานปกติได้ โดยที่มีนโยบายการสำรองข้อมูลระบบงานคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and Information Technology Continuity Plan Policy)

๑.๖ การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ โดยที่ผู้ใช้งานจำเป็นต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเทอร์เน็ต เพื่อไม่ให้เป็น

ช่องทางให้ผู้ที่ไม่หวังดีเข้ามาทำการบุกรุกหรือทำลายระบบได้ โดยที่มีนโยบายในการป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious Software Protection Policy)

๑.๗ การป้องกันและการแก้ไขปัญหาที่เกิดขึ้นจากกระแสไฟฟ้า เพื่อป้องกันและแก้ปัญหาจากกระแสไฟฟ้าที่อาจก่อให้เกิดความเสียหายแก่ระบบสารสนเทศ และอุปกรณ์คอมพิวเตอร์ ดำเนินการดังต่อไปนี้

๑) ติดตั้งเครื่องสำรองไฟฟ้าและแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับ

๒) อุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนที่เป็นเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๓๐-๖๐ นาที

๓) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๔) เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้งานระบบรีบทำการบันทึกข้อมูลที่ยังใช้งานค้างอยู่ทันที พร้อมกับปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

๑.๘ การป้องกันการบุกรุกและภัยคุกคามทางด้านคอมพิวเตอร์เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ มีแนวทางดังต่อไปนี้

๑) มาตรการการเข้าออกในห้องควบคุมระบบเครือข่ายคอมพิวเตอร์และการป้องกันความเสียหายโดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากมีความจำเป็นให้เจ้าหน้าที่ของสำนักคอมพิวเตอร์ที่มีหน้าที่เกี่ยวข้องเป็นผู้รับผิดชอบในการนำพา การเข้าออกห้องควบคุมระบบเครือข่ายคอมพิวเตอร์จะต้องมีการทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้าออกและมีการติดตั้งเครื่องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต

๓) สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยที่มีการเปิดใช้งาน Firewall ตลอดเวลา

๔) มีการติดตั้ง Proxy Server เป็นการเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

๕) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนระบบเครือข่ายอินเทอร์เน็ตของมหาวิทยาลัย เพื่อสังเกตข้อมูลว่ามีมากผิดปกติหรือไม่ หรือการเรียกใช้ระบบสารสนเทศที่มีความถี่ในการเรียกใช้ผิดปกติ เพื่อสรุปหาสาเหตุและป้องกันต่อไป

๖) การดำเนินการตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ เป็นการช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๑.๙ การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว การจัดเตรียมวัสดุที่จำเป็น อุปกรณ์และเครื่องมือที่จำเป็นในกรณีที่เกิดแผ่นดินไหว โดยเตรียมอุปกรณ์ดังต่อไปนี้

๑) เตรียมอุปกรณ์ยังชีพ ไฟฉาย ยารักษาโรค และแจ้งให้ทุกคนทราบที่เก็บ

๒) ฝึกซ้อมการปฐมพยาบาลเบื้องต้นเพื่อแก้ปัญหาในยามฉุกเฉิน

๓) ควรทราบตำแหน่งสะพานไฟฟ้า วาล์วถังแก๊ส และน้ำประปา

๔) ไม่ควรวางของหนักไว้บนชั้นที่สูง หรือบนหลังตู้

๕) ผูกหรือยึดติดเฟอร์นิเจอร์ที่มีน้ำหนักไว้กับผนัง

๖) ศึกษาแผนการฝึกซ้อม การอพยพในยามฉุกเฉิน กำหนดจุดรวมพลที่ชัดเจนของแต่ละชั้น แต่ละหน่วยงาน

๒. การเตรียมความพร้อม

๒.๑ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์ และข้อมูลเกิดจากความเสียหายเมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก การเตรียมความพร้อมในขั้นนี้เป็นการเตรียมความพร้อมและแก้ปัญหาที่เกิดจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางในการดำเนินการเบื้องต้นเพื่อลดความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟฟ้าดับ หม้อไฟระเบิด

๒) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้า ๓๐ นาที

๓) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพใช้งานได้เสมอ

๔) เมื่อกระแสไฟฟ้าดับให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีแล้วปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

๒.๒ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดไฟไหม้เป็นการป้องกันและแก้ปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศ อุปกรณ์คอมพิวเตอร์ กำหนดแนวทางการแก้ปัญหาเบื้องต้นเพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศดังนี้

๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้

๒) ติดตั้งเครื่องดับเพลิงในทุกชั้นของอาคาร เพื่อการควบคุมเพลิงในเบื้องต้น

๓) ให้มีการสำรองฐานข้อมูลเดือนละครั้งเป็นอย่างน้อย

๒.๓ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความสียหายเมื่อเกิดน้ำท่วม น้ำรั่วเป็นการป้องกันสถานการณ์และแก้ไขปัญหาจากน้ำท่วม น้ำรั่ว ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากน้ำท่วม น้ำรั่ว

๒) มีการตรวจสอบระบบท่อประปา ฝ้าเพดานห้องควบคุมระบบเครือข่ายเพื่อให้มีความปลอดภัยต่อการรั่วซึม

๓) ให้มีการสำรองฐานข้อมูลเดือนละครั้งเป็นอย่างน้อย

๒.๔ การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัส ดำเนินการดังนี้

๑) มีการติดตั้ง Firewall ซึ่งทำหน้าที่การกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก

๒) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสเครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

๓) อัพเดทโปรแกรมกำจัดไวรัสทุก ๆ ๑ เดือน เป็นอย่างน้อย (Update Patch)

๔) ให้เจ้าหน้าที่สำนักคอมพิวเตอร์แจ้งข้อมูลเตือนภัยคอมพิวเตอร์อย่างต่อเนื่อง สม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสเบื้องต้น

๒.๕ การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย เพื่อเป็นการเสริมสร้างระบบความปลอดภัยให้กับระบบสารสนเทศ และระบบเครือข่าย มีแนวทางการดำเนินการ ดังนี้

๑) กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

๒) หากว่าบุคคลใดที่ไม่มีอำนาจหน้าที่เกี่ยวข้องจำเป็นต้องเข้าไปในห้องควบคุมเครือข่าย จะต้องให้เจ้าหน้าที่ของสำนักคอมพิวเตอร์ซึ่งเป็นผู้ดูแลระบบเครือข่ายเป็นผู้รับผิดชอบนำพาเข้าออก และคอยกำกับดูแลตลอดระยะเวลาปฏิบัติงาน สำหรับประตูเข้าออกมีการติดตั้งระบบ Access Control โดยใช้ Key Card และโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๓) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดระยะเวลา

๔) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการบริการอินเทอร์เน็ตและกลั่นกรองข้อมูลที่มาจากเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๕) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตของมหาวิทยาลัยเพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและทำการป้องกันต่อไป

๖) มีการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเทอร์เน็ตหรือระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๒.๖ การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ เจ้าหน้าที่แผนกต่าง ๆ ขาดทักษะความรู้ความเข้าใจในเครื่องมือ อุปกรณ์คอมพิวเตอร์ การเตรียมการชี้แจงให้เจ้าหน้าที่มีความรู้ความเข้าใจด้านฮาร์ดแวร์ (Hardware) และด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงที่เกิดขึ้นให้น้อยที่สุด

๑) สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ของหน่วยงาน เพื่อช่วยกำกับดูและถ่ายทอดความรู้แก่เพื่อนร่วมงาน

๒) วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์ จัดทำคู่มือการบริหารความเสี่ยงระบบสารสนเทศเพื่อเป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

๒.๗ การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว การเตรียมความพร้อมในขั้นนี้ ให้เริ่มตั้งแต่ปัจจุบันเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เพื่อเตรียมการต่าง ๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

๑) ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัย จากหน่วยงานที่เกี่ยวข้องและข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก แนวทาง/มาตรการปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ กฎหมายที่เกี่ยวข้องเชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่าง ๆ ทั้งหน่วยงานภายในและต่างประเทศ คือ

- กรมอุตุนิยมวิทยา: ข้อมูลพยากรณ์อากาศ ข้อมูลอุณหภูมิ ข่าวเตือนภัย
- ศูนย์เตือนภัยพิบัติแห่งชาติ : การแจ้งเตือนล่วงหน้า ที่ www.ndwc.thaigov.go.th
- กรมทรัพยากรธรณี : ข้อมูลพื้นที่เสี่ยงภัยจากดินถล่ม/แผ่นดินไหว ที่ www.dmr.go.th
- หน่วยงานสำรวจเชิงภูมิศาสตร์ ประเทศสหรัฐอเมริกา : ข้อมูลสถานการณ์แผ่นดินไหวทั่วโลกที่ www.earthquake.usgs.gov
- กรมป้องกันและบรรเทาสาธารณภัย : การแจ้งเตือนภัย ข้อมูลพื้นที่เสี่ยงภัย มาตรการและแนวทางปฏิบัติ ที่ www.disaster.go.th

๒) การสังเกตพฤติกรรมของสัตว์มีสัตว์หลายชนิดมีการรับรู้และแสดงท่าทางออกมาก่อนการเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้าเป็นชั่วโมงหรือเป็นวันก็ได้ เช่น

- สัตว์เลี้ยง สัตว์บ้านทั่วไปที่ตกใจตื่น เช่น สุนัข เป็ด ไก่ เป็นต้น
- แมลงสาบวิ่งเพ่นพ่าน
- งูและหนูวิ่งออกจากที่อยู่อาศัย
- ปลากระโดดขึ้นมาจากผิวน้ำ

๓) การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

- ประสานงานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม กำหนดวิธีปฏิบัติทุกขั้นตอน
- ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุอุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม
- สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร น้ำ สำหรับบุคลากร
- สำรวจจัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์อย่างมีประสิทธิภาพเมื่อเกิดภัย
- จัดเตรียมยานพาหนะเพื่ออพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่าง ๆ

๔) การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

- สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้มีการปรับปรุงแก้ไขให้ใช้ประโยชน์ใน อาคารให้ถูกต้องตามระเบียบ กฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่อ อาคารตามความเหมาะสม
- อาคารที่ทำการดัดแปลง ก่อสร้าง โดยที่ไม่ถูกต้องตามแบบแปลน เจ้าหน้าที่ที่รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้ผู้ครอบครองอาคารดำเนินการแก้ไขหรือรื้อถอนเพื่อความปลอดภัย

๕) การปฏิบัติขั้นเตรียมการ

- ซักซ้อมแผนป้องกันและบรรเทาภัย
- สำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย และกำหนดมาตรการในการผจญภัย

- อบรมให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่มบุคลากร

- รายงานผลการปฏิบัติการ

๒.๘ การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วง/ก่อจลาจลเพื่อติดตามสถานการณ์และรวบรวมข้อมูลข่าวสาร ประเมินสถานการณ์จากการชุมชนประท้วงและก่อการจราจล เตรียมการต่าง ๆ ที่จำเป็นดังนี้

- หาข่าวจากแหล่งข่าวต่าง ๆ เช่น วิทยุ โทรทัศน์ ตำรวจ หรือหน่วยงานอื่นที่เกี่ยวข้อง

- จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ และมอบหมายการปฏิบัติหน้าที่แก่ผู้เกี่ยวข้อง

- ตรวจสอบระบบไฟฟ้า เครื่อง Generator น้ำมันเชื้อเพลิง และระบบปั๊มน้ำ ให้อยู่ในสภาพพร้อมใช้งาน

- ตรวจสอบระบบ CCTV เพื่อเตรียมพร้อมเกี่ยวกับระบบรักษาความปลอดภัย

๓. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

สำนักบรรณสารสนเทศ มหาวิทยาลัยสุโขทัยธรรมาธิราช จัดเตรียมทีมงานและมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้นดังต่อไปนี้

๓.๑ ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจนการติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติการผู้รับผิดชอบได้แก่

อธิการบดี (CEO)

รองอธิการบดี ฝ่ายบริการวิชาการ ทำนุบำรุงศิลปวัฒนธรรมและวิเทศสัมพันธ์

ผู้อำนวยการสำนักบรรณสารสนเทศ

การดำเนินนโยบายและแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติด้านเทคโนโลยีสารสนเทศเมื่อเกิดสถานการณ์ฉุกเฉินภายใต้การกำกับดูแลเรื่องระบบรักษาความปลอดภัย โดยสำนักคอมพิวเตอร์ เมื่อเกิดปัญหาในการปฏิบัติงานให้รายงานตามลำดับขั้นดังนี้ ผู้ปฏิบัติงานหรือผู้ดูแลระบบแจ้งหัวหน้าฝ่าย/ศูนย์ หัวหน้าศูนย์เทคโนโลยีบรรณสาร เพื่อจัดทำบันทึกในการขอความอนุเคราะห์แก้ไขปัญหาผ่านผู้อำนวยการสำนักบรรณสารสนเทศ เสนอต่อผู้อำนวยการสำนักคอมพิวเตอร์และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ทราบ

๓.๒ ระดับปฏิบัติการ

๓.๒.๑ ทีมบริหารจัดการกู้คืนข้อมูล/ระบบของสำนักบรรณสารสนเทศ มีหน้าที่หลักในการบริหารจัดการและประสานงานกับหน่วยงานที่เกี่ยวข้องในการกู้คืนข้อมูล/ระบบ มีผู้รับผิดชอบ คือ

๑.	นางกัลยาณี ศุภดิษฐ์	เบอร์ติดต่อ	๐๘๑-๗๗๗-๓๒๓๑
๒.	นางสาวชลลดา หงษ์งาม	เบอร์ติดต่อ	๐๙๔-๔๑๖-๕๙๒๖
๓.	นายสมชาย บุญปัญญา	เบอร์ติดต่อ	๐๙๒-๔๑๕-๕๙๙๘
๔.	นายอาเขต แก้วสว่าง	เบอร์ติดต่อ	๐๙๓-๕๒๕-๖๔๕๓
๕.	นายสมพงษ์ ปภาวีระวงศ์	เบอร์ติดต่อ	๐๘๖-๘๑๑-๘๘๔๖

๓.๒.๒ ทีมกู้คืนเครือข่าย ทำหน้าที่ดูแลกู้คืนเครือข่ายให้กลับมาใช้งานได้ปกติ มีผู้รับผิดชอบคือ

๑.	นายเสกสรรค์ ปิ่นเจริญ	เบอร์ติดต่อ	๐๘๑-๕๘๑-๕๔๑๐
๒.	นางสุมณฑา สุขชานุลักษ์	เบอร์ติดต่อ	๐๙๕-๕๐๖-๖๐๙๑
๓.	นายจักรพรรดิ นิลพันธ์	เบอร์ติดต่อ	๐๖๒-๒๗๙-๗๘๘๙
๔.	นายเฉลิมพล จันทะบาล	เบอร์ติดต่อ	๐๘๔-๑๑๑-๖๓๓๙
๕.	นางสาวธุวนัน เสน่ห์จันทร์	เบอร์ติดต่อ	๐๘๙-๐๖๐-๘๐๒๗

๓.๒.๓ ทีมกู้คืน Application ทำหน้าที่ติดตั้งกู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน มีผู้รับผิดชอบ คือ

๑.	นางกัลยาณี ศุภดิษฐ์	เบอร์ติดต่อ	๐๘๑-๗๗๗-๓๒๓๑
๒.	นางสาวชลลดา หงษ์งาม	เบอร์ติดต่อ	๐๙๔-๔๑๖-๕๙๒๖
๓.	นายสมชาย บุญปัญญา	เบอร์ติดต่อ	๐๙๒-๔๑๕-๕๙๙๘
๔.	นายอาเขต แก้วสว่าง	เบอร์ติดต่อ	๐๙๓-๕๒๕-๖๔๕๓
๕.	นายสมพงษ์ ปภาวีระวงศ์	เบอร์ติดต่อ	๐๘๖-๘๑๑-๘๘๔๖

๓.๒.๔ ทีมประเมินความเสียหายทำหน้าที่ให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมหาอุปกรณ์มาทดแทนมีผู้รับผิดชอบ คือ

๑.	นางสาวนภัสสร สังวรวิตร์	เบอร์ติดต่อ	๐๘๙-๗๘๖-๙๙๕๗
๒.	นายสุรเชษฐ์ มูลสาร	เบอร์ติดต่อ	๐๘๙-๙๒๕-๒๙๐๕
๓.	นางสาวระพีพรรณ แก้วประชุม	เบอร์ติดต่อ	๐๘๑-๒๘๕-๓๘๓๕
๔.	นางสาวสุวิมล ศรีสุราช	เบอร์ติดต่อ	๐๙๖-๘๘๗-๘๒๔๗
๕.	นายจักรพรรดิ นิลพันธ์	เบอร์ติดต่อ	๐๖๒-๔๗๙-๗๘๘๙
๖.	นางสาวธุวนัน เสน่ห์จันทร์	เบอร์ติดต่อ	๐๘๙-๐๖๐-๘๐๒๗
๗.	นายวุฒินันท์ พลโลก	เบอร์ติดต่อ	๐๘๐-๔๔๓-๘๘๗๕

๓.๒.๕ ทีมอาคารสถานที่ ทีมจัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร เครื่องปรับอากาศให้พร้อมใช้งาน มีผู้รับผิดชอบ คือ

๑.	นายกันตภณ ขันถม	เบอร์ติดต่อ	๐๘๑-๓๐๒-๕๖๘๔
๒.	นายจักรพรรดิ นิลพันธ์	เบอร์ติดต่อ	๐๖๒-๔๗๙-๗๘๘๙
๓.	นางโชติกา นาคทองคำ	เบอร์ติดต่อ	๐๘๙-๔๘๓-๔๒๓๙
๔.	นางสาวมาลินี ไมตรีสวัสดิ์	เบอร์ติดต่อ	๐๘๖-๐๔๗-๑๒๓๗
๕.	นางธัญนันท์ พฤกษา	เบอร์ติดต่อ	๐๘๖-๕๒๖-๘๐๑๒
๖.	นายเอกรัตน์ วิโรจนกุล	เบอร์ติดต่อ	๐๘๕-๑๑๔-๑๗๒๔

๓.๒.๖ ทีมการจัดการทั่วไป เป็นทีมประสานงานช่วยเหลือทีมอื่น ให้บรรลุวัตถุประสงค์การในการทำงาน มีผู้รับผิดชอบ คือ

๑.	นางสาววรัมภา จินาทอง	เบอร์ติดต่อ	๐๘๑-๘๔๙-๙๕๐๔
๒.	นางสาวนพวรรณ วงษ์ศรีแก้ว	เบอร์ติดต่อ	๐๘๘-๐๘๑-๑๗๕๕

๓.๒.๗ ทีมแก้ไขปัญหาเบื้องต้น กรณีเกิดไฟไหม้ห้องควบคุมระบบ ทำหน้าที่แก้ปัญหาเบื้องต้นควบคุมการดำเนินงานการดับเพลิง โดยใช้อุปกรณ์ที่สำนักคอมพิวเตอร์จัดหาไว้ ผู้รับผิดชอบ คือ

๑.	นายจักรพรรดิ นิลพันธ์	เบอร์ติดต่อ	๐๖๒-๔๗๙-๗๘๘๙
๒.	นางสาวธุวนัน เสน่ห์จันทร์	เบอร์ติดต่อ	๐๘๙-๐๖๐-๘๐๒๗
๓.	นางโชติกา นาคทองคำ	เบอร์ติดต่อ	๐๘๙-๔๘๓-๔๒๓๙

๓.๒.๘ ทีมแก้ปัญหาเบื้องต้นในกรณีที่ไฟดับ หรือหม้อแปลงไฟฟ้าระเบิด ทำหน้าที่ป้องกันไม่ให้เกิดความเสียหายกับระบบงาน ต้องดำเนินการสำรองข้อมูลที่สำคัญ จากเครื่องสำรองไฟฟ้าที่สามารถให้พลังงานอยู่ ผู้รับผิดชอบ คือ

๑.	นายจักรพรรดิ นิลพันธ์	เบอร์ติดต่อ	๐๖๒-๔๗๙-๗๘๘๙
๒.	นางสาวธุวนัน เสน่ห์จันทร์	เบอร์ติดต่อ	๐๘๙-๐๖๐-๘๐๒๗
๓.	นางโชติกา นาคทองคำ	เบอร์ติดต่อ	๐๘๙-๔๘๓-๔๒๓๙

๓.๒.๙ ทีมแก้ไขปัญหาเบื้องต้น กรณีเกิดน้ำท่วม ทำหน้าที่ป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยจะต้องปิดระบบที่อาจเกิดผลกระทบจากการเกิดน้ำท่วมทุกระบบ/ดำเนินการสูบน้ำออก/ตรวจสอบการรั่วซึม ผู้รับผิดชอบ คือ

๑.	นายจักรพรรดิ นิลพันธ์	เบอร์ติดต่อ	๐๖๒-๔๗๙-๗๘๘๙
๒.	นางสาวธุวนัน เสน่ห์จันทร์	เบอร์ติดต่อ	๐๘๙-๐๖๐-๘๐๒๗
๓.	นางโชติกา นาคทองคำ	เบอร์ติดต่อ	๐๘๙-๔๘๓-๔๒๓๙

๓.๒.๑๐ ทีมแก้ไขปัญหาอันเนื่องมาจากการเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์ ทำหน้าที่กู้คืนระบบให้สามารถทำงานได้ตามปกติ รวมทั้งหาสาเหตุ อุดช่องโหว่ด้านระบบเครือข่าย ผู้รับผิดชอบ คือ

๑.	นายจักรพรรดิ นิลพันธ์	เบอร์ติดต่อ	๐๖๒-๔๗๙-๗๘๘๙
๒.	นายเฉลิมพล จันทะบาล	เบอร์ติดต่อ	๐๘๔-๑๑๑-๖๓๓๙
๓.	นางสุมณฑา สุขชานุลักษ์	เบอร์ติดต่อ	๐๙๕-๕๐๖-๖๐๙๑
๔.	นายกันตินันท์ แสงวัฒนรัตน์	เบอร์ติดต่อ	๐๖๑-๖๒๕-๖๔๑๕
๕.	นายธนกฤต ทองสืบสาย	เบอร์ติดต่อ	๐๖๕-๕๙๔-๒๙๓๘
๖.	นายดิลก พุ่มสุวรรณ์	เบอร์ติดต่อ	๐๘๐-๖๐๐-๕๙๐๗

๓.๒.๑๑ ทีมสำรองและกู้คืนข้อมูล (Backup & Recovery) ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล ฟื้นฟูระบบข้อมูลจากความเสียหายเพื่อให้กลับมาใช้งานใหม่ได้ทันที ผู้รับผิดชอบ คือ

๑.	นางสุมณฑา สุขชานุลักษ์	เบอร์ติดต่อ	๐๙๕-๕๐๖-๖๐๙๑
๒.	นายจักรพรรดิ นิลพันธ์	เบอร์ติดต่อ	๐๖๒-๔๗๙-๗๘๘๙
๓.	นายเฉลิมพล จันทะบาล	เบอร์ติดต่อ	๐๘๔-๑๑๑-๖๓๓๙
๔.	นางสาวนภัสสร สังวรวิตร์	เบอร์ติดต่อ	๐๘๑-๘๑๓-๕๙๐๖
๕.	นายวีระพล มาทะเล	เบอร์ติดต่อ	๐๙๒-๔๕๖-๙๘๒๕
๖.	นายกันตินันท์ แสงวัฒนรัตน์	เบอร์ติดต่อ	๐๖๑-๖๒๕-๖๔๑๕
๗.	นายเอกรัตน์ วิโรจนกุล	เบอร์ติดต่อ	๐๘๕-๑๑๔-๑๗๒๔
๘.	นายดิลก พุ่มสุวรรณ์	เบอร์ติดต่อ	๐๘๐-๖๐๐-๕๙๐๗
๙.	นายอำนาจ ธรรมกิจ	เบอร์ติดต่อ	๐๘๙-๒๕๒-๐๘๓๐

๓.๒.๑๒ ทีมแก้ไขปัญหาเนื่องจากแผ่นดินไหว ทำหน้าที่ในการแจ้งต่อผู้บังคับบัญชา เตรียมการแจ้งเจ้าหน้าที่ไฟฟ้า ผู้รับผิดชอบ คือ

๑.	นายจักรพรรดิ นิลพันธ์	เบอร์ติดต่อ	๐๖๒-๔๗๙-๗๘๘๙
๒.	นางโชติกา นาคทองคำ	เบอร์ติดต่อ	๐๘๙-๔๘๓-๔๒๓๙
๓.	นายทรงกลด พัฒนโชติ	เบอร์ติดต่อ	๐๘๖-๒๒๑-๕๑๘๕
๔.	นางสาวภัทรวดี เย็นนภา	เบอร์ติดต่อ	๐๙๙-๓๒๙-๘๘๘๕
๕.	นายอภิชาติ เชื้อวงศ์	เบอร์ติดต่อ	๐๘๙-๗๙๖-๔๐๐๗
๖.	นางสาวฉันทนา บุญไชย	เบอร์ติดต่อ	๐๘๕-๙๙๗-๐๘๘๘
๗.	นางสาวอนัญญา เกษแก้ว	เบอร์ติดต่อ	๐๙๐-๑๒๓-๗๙๕๔

๓.๒.๑๓ ทีมแก้ไขปัญหาอันเกิดจากการชุมนุมประท้วง จลาจล ทำหน้าที่ในการแจ้งต่อผู้บังคับบัญชา เตรียมการ

๑.	นายจักรพรรดิ นิลพันธ์	เบอร์ติดต่อ	๐๖๒-๔๗๙-๗๘๘๙
๒.	นางโชติกา นาคทองคำ	เบอร์ติดต่อ	๐๘๙-๔๘๓-๔๒๓๙
๓.	นายทรงกลด พัฒนโชติ	เบอร์ติดต่อ	๐๘๖-๒๒๑-๕๑๘๕
๔.	นางสาวภัทรวดี เย็นนภา	เบอร์ติดต่อ	๐๙๙-๓๒๙-๘๘๘๕
๕.	นายอภิชาติ เชื้อวงศ์	เบอร์ติดต่อ	๐๘๙-๗๙๖-๔๐๐๗
๖.	นางสาวฉันทนา บุญไชย	เบอร์ติดต่อ	๐๘๕-๙๙๗-๐๘๘๘
๗.	นางสาวอนัญญา เกษแก้ว	เบอร์ติดต่อ	๐๙๐-๑๒๓-๗๙๕๔

๔. มาตรการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศของมหาวิทยาลัย จึงได้กำหนดแนวทางให้บุคลากรปฏิบัติดังนี้ คือ

๔.๑ กรณีเครื่องลูกข่าย (Client)

๑) กรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการได้หรือใช้ระบบสารสนเทศได้ตามปกติให้เจ้าหน้าที่แจ้งเหตุให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศของหน่วยงานทราบ หรือกรณีอันเกิดจากศูนย์ข้อมูล (Data Center) ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์ข้อมูล (Data Center) หรือสำนักคอมพิวเตอร์จะต้องประกาศให้ทุกหน่วยงานในมหาวิทยาลัยทราบ

๒) กรณีที่เกิดขัดข้องอันเนื่องจากไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายอันอาจจะแพร่กระจายไปยังจุดอื่นในระบบเครือข่าย ให้ผู้รับผิดชอบดำเนินการตัดการเชื่อมโยงเครือข่ายออกจากเครื่องนั้นโดยเร็ว หรือในกรณีที่เกรงว่าเหตุการณ์ที่เกิดจะเป็นอันตรายแก่หน่วยงานภายในอาคารที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้องในเบื้องต้นให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกไปก่อน

๓) ให้เจ้าหน้าที่ด้านไอทีที่เกี่ยวข้องของหน่วยงานตรวจสอบและดำเนินการแก้ไขปัญหาเบื้องต้น หรือหากไม่สามารถแก้ไขปัญหาได้ให้แจ้งเหตุขัดข้องต่อผู้บังคับบัญชาทราบเพื่อดำเนินการในขั้นต่อไป

๔.๒ เครื่องแม่ข่ายบริการ (Server) มาตรการในการป้องกันและแก้ไขปัญหา คือ

๑) ดำเนินการตัดการเชื่อมต่อเครือข่ายโดยเร็ว ปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญในการให้บริการ

๒) หากไฟฟ้าดับหรือไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย โดยให้พิจารณาตามลำดับความสำคัญของการให้บริการ

๓) ตัดระบบจ่ายไฟ หรือในกรณีที่ไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดเพื่อควบคุมเพลิงดำเนินการตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ในที่ที่ปลอดภัย

๔) กรณีที่ไฟไหม้ให้ใช้น้ำยาฉีดควบคุมเพลิงโดยเร็ว

๕) รีบขนย้ายเครื่องไว้ในที่ที่ปลอดภัย

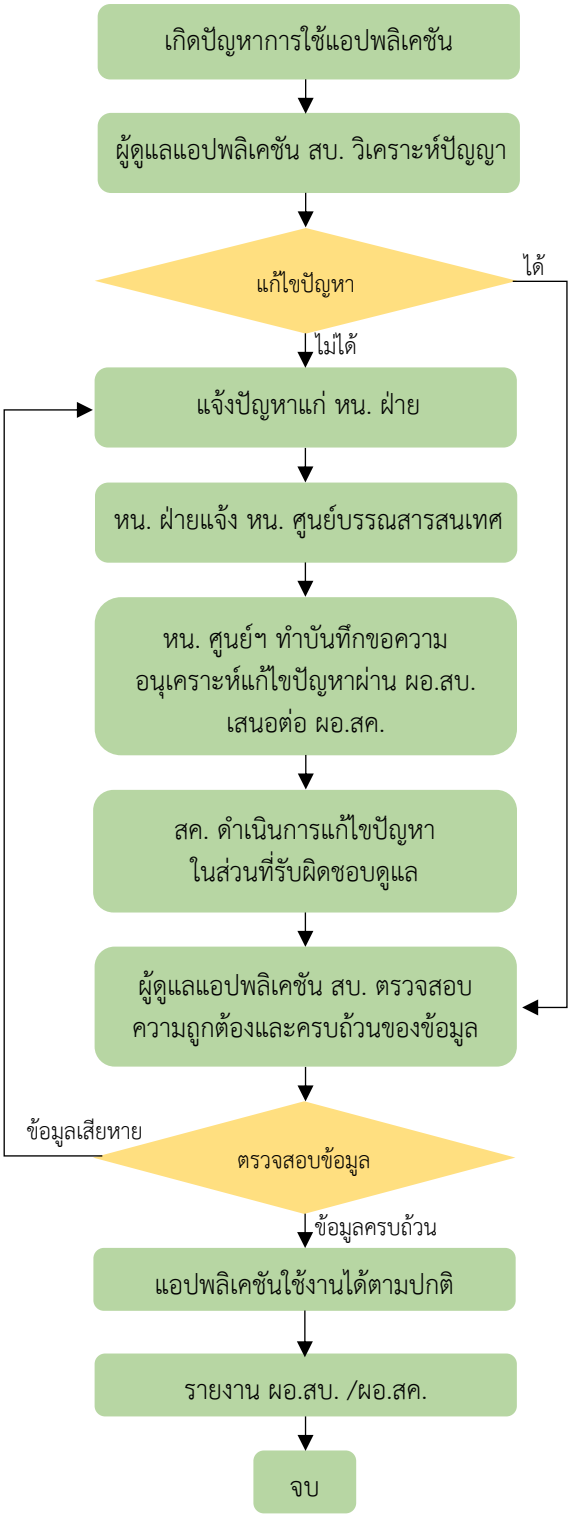
๖) ประสานงานขอความช่วยเหลือจากหน่วยงานภายนอกที่รับผิดชอบหรือบริษัทที่ปรึกษาในการดูแลเครื่องคอมพิวเตอร์โดยเร็ว

๗) กรณีที่อุปกรณ์ฮาร์ดแวร์เสียให้ดำเนินการโดยรีบหาอุปกรณ์สำรองหรือแจ้งบริษัทที่รับผิดชอบให้นำอุปกรณ์เปลี่ยนโดยเร็วที่สุด

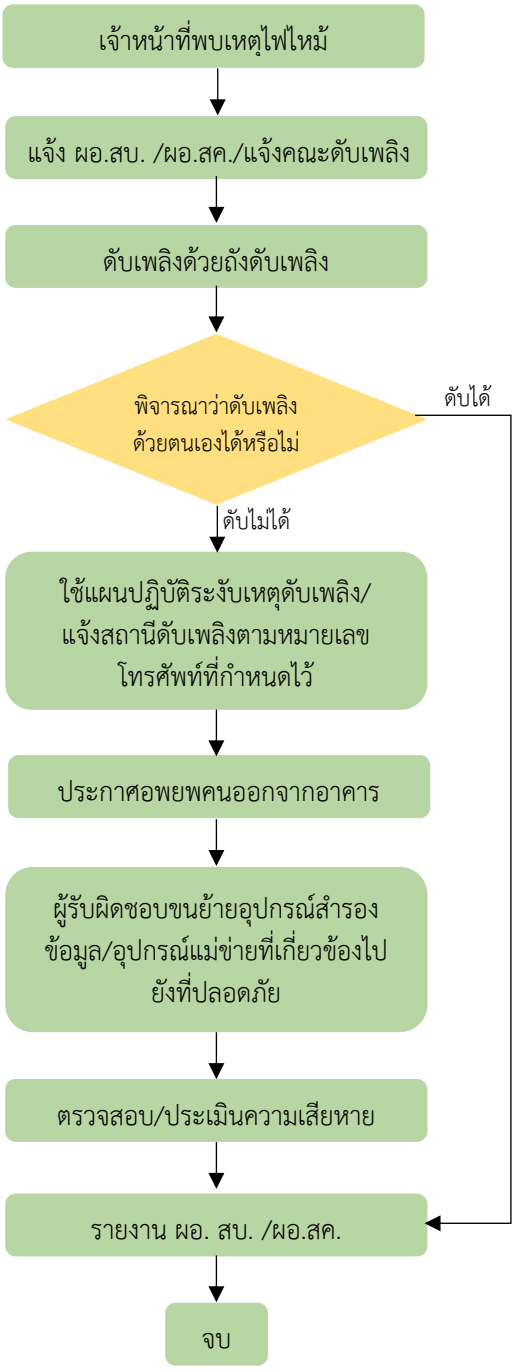
๘) ให้ผู้ดูแลระบบจัดทำรายงานแจ้งผู้อำนวยการสำนักคอมพิวเตอร์ทราบโดยเร็ว

๕. Flowchart

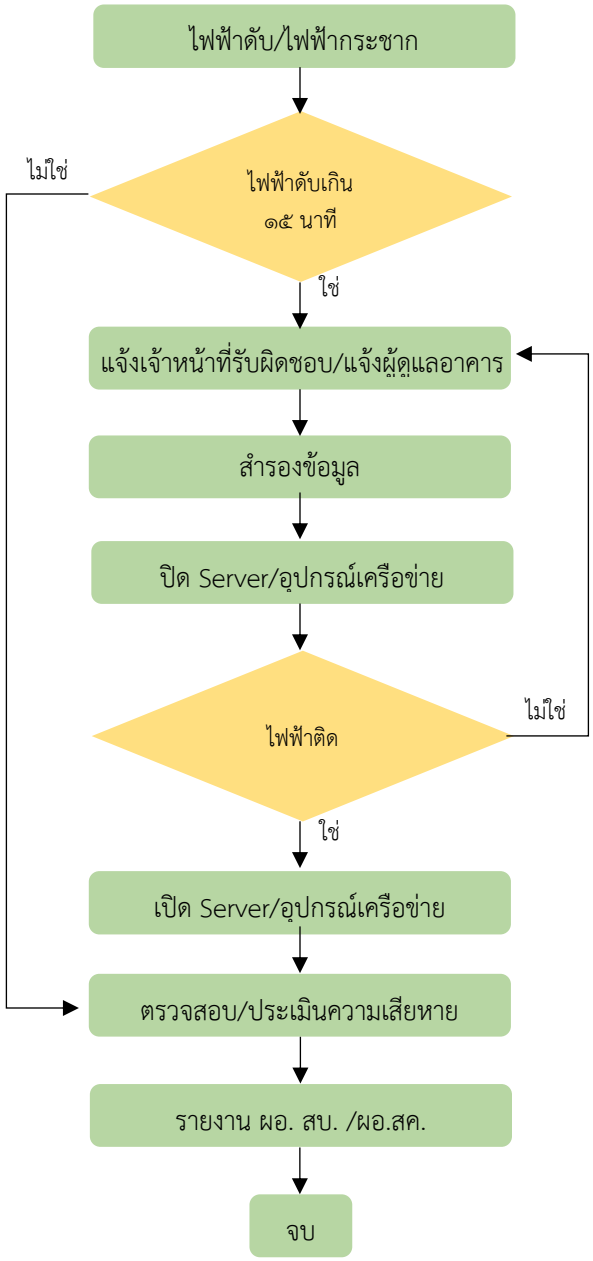
ขั้นตอนปฏิบัติงานการเกิดกรณีเกิดภัยพิบัติด้านเทคโนโลยีของสำนักบรรณสารสนเทศ



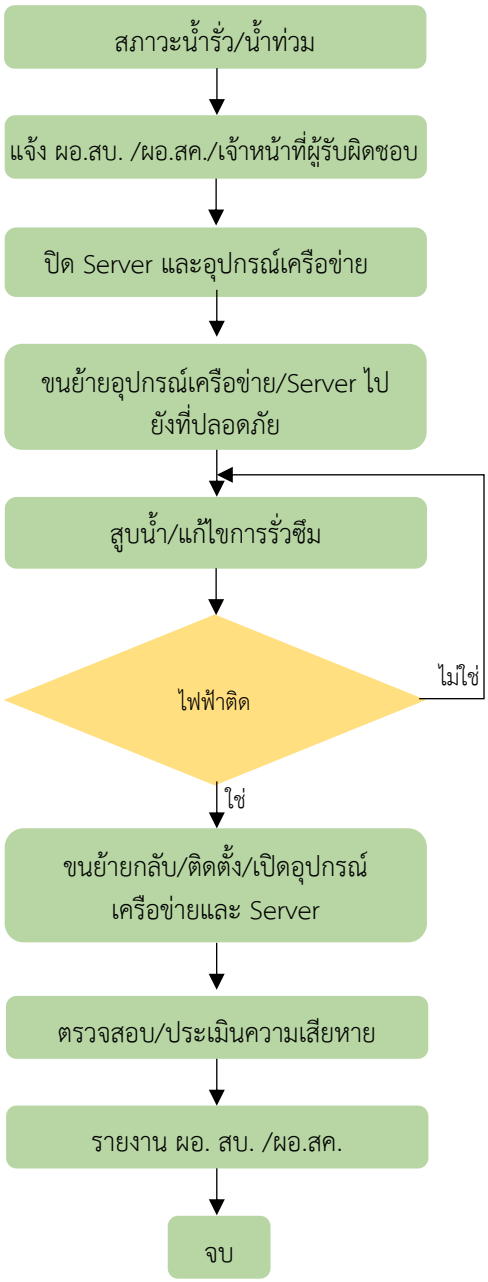
ขั้นตอนการปฏิบัติงานกรณีเกิดไฟไหม้



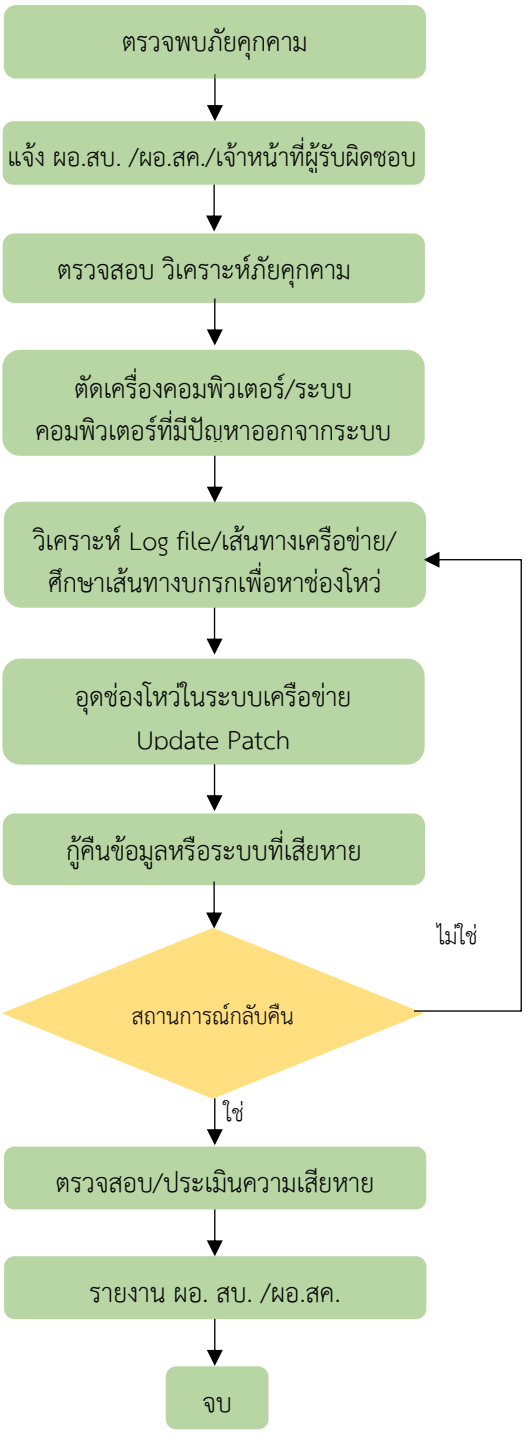
ขั้นตอนการปฏิบัติงานกรณีไฟดับ/ไฟกระชาก/หม้อแปลงไฟฟ้าระเบิด



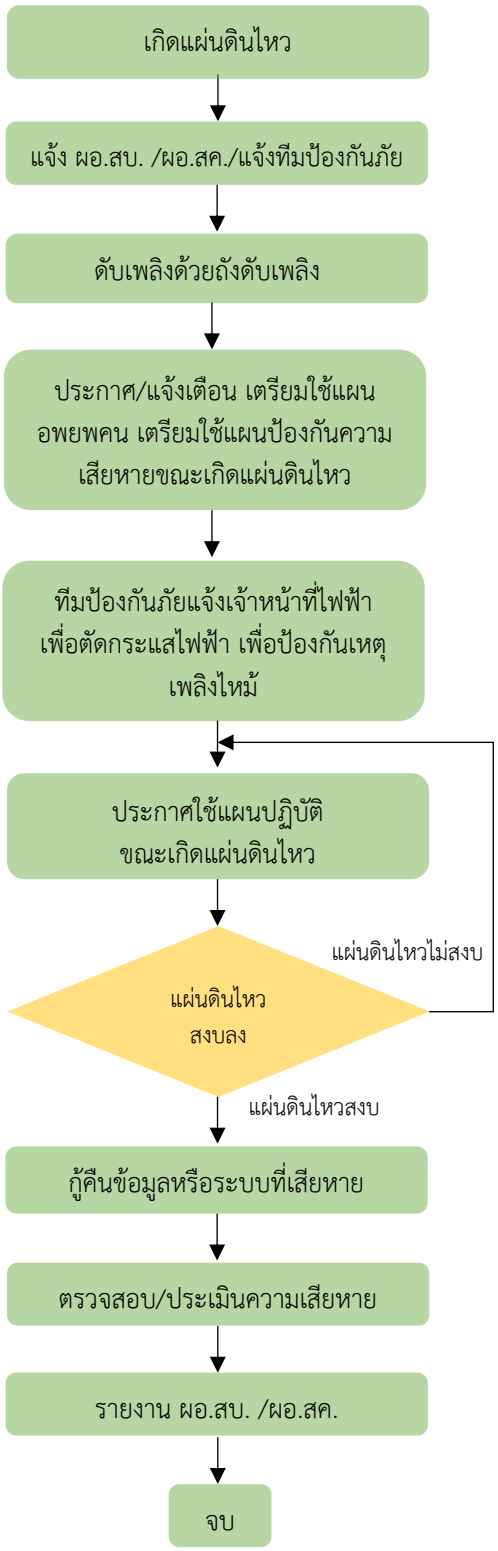
ขั้นตอนการปฏิบัติงานกรณีน้ำท่วม



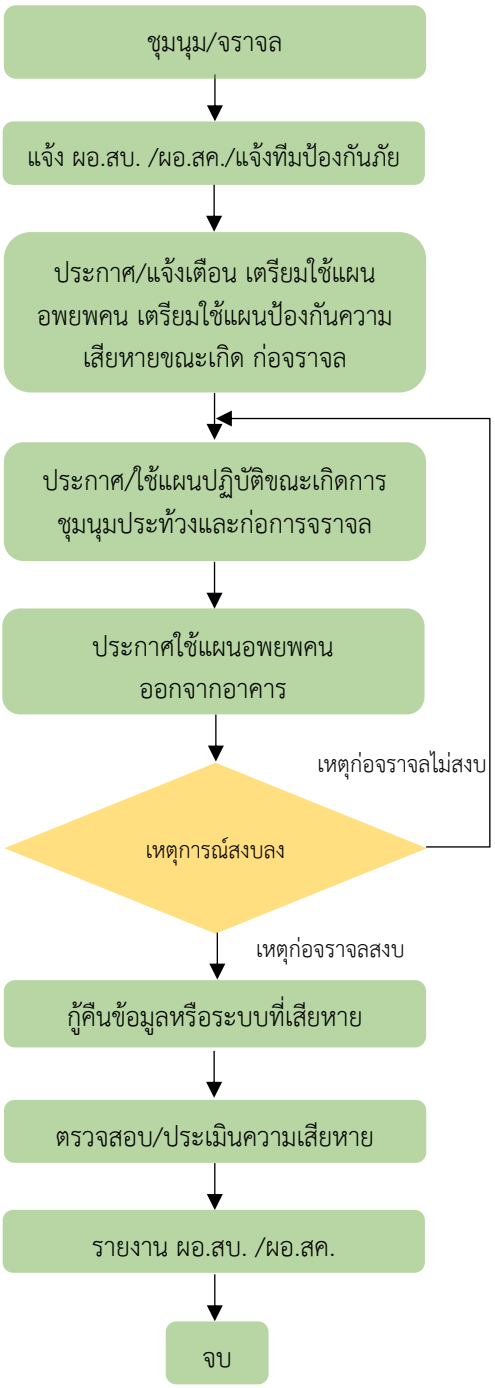
ขั้นตอนการปฏิบัติงานกรณีโดนเจาะระบบหรือตรวจพบภัยคุกคาม



ขั้นตอนการปฏิบัติงานกรณีเกิดแผ่นดินไหว



ขั้นตอนการปฏิบัติงานกรณีเกิดการชุมนุมประท้วงก่อการจราจล



แผนการสำรองและกู้คืนข้อมูล

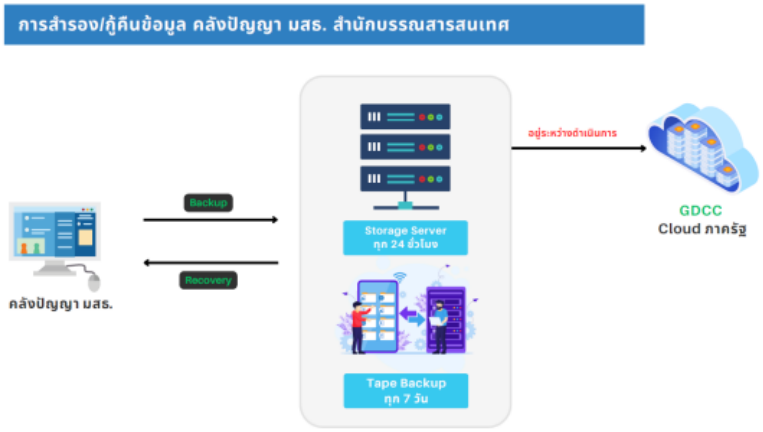
สำนักบรรณสารสนเทศ ได้มีการจัดทำแผนการสำรองและกู้คืนข้อมูลขึ้น จากการวิเคราะห์ความเสี่ยงการดำเนินงานในกรณีเกิดภัยพิบัติด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถเข้าถึงข้อมูลได้อย่างต่อเนื่อง (Continuity of Service) ในสถานการณ์ต่าง ๆ เพื่อป้องกันข้อมูลเสียหายและการสูญหาย กรณีเกิดเหตุฉุกเฉินจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้น เพื่อเตรียมความพร้อมในการกู้คืนระบบสารสนเทศให้สามารถดำเนินการเปิดให้บริการโดยเร็วที่สุด และเพื่อให้มั่นใจได้ว่าสำนักบรรณสารสนเทศ มีความพร้อมที่จะเผชิญสภาวะวิกฤติ

แผนการสำรองข้อมูล แบ่งเป็น ๓ รูปแบบ คือ

๑) การทำ Snapshot คอมพิวเตอร์แม่ข่ายเสมือนทั้งระบบ ทุก ๒๔ ชั่วโมง โดยจะเก็บข้อมูลสำรองไว้บน Storage Server สามารถกู้คืนข้อมูลย้อนกลับได้ ๑๔ วัน

๒) การสำรองข้อมูลลงเทปสำรองข้อมูล (Tape Backup) โดยสำรองข้อมูลทุก ๗ วัน และนำเทปสำรองข้อมูลไปเก็บไว้ที่ปลอดภัย โดยสำรองข้อมูล ๘ เวอร์ชั่น สามารถกู้คืนข้อมูลย้อนหลังได้ ๖๐ วัน

๓) การทำแผนติดตั้ง DR Site ไว้ที่ Cloud ภาครัฐ เพื่อสำรองข้อมูลจากระบบหลัก และใช้งานทดแทนระบบหลักในกรณีที่เกิดจากสาเหตุต่าง ๆ เช่น ภัยธรรมชาติ ไฟฟ้าดับ (ภายในปีงบประมาณ พ.ศ. ๒๕๖๗)



ในการกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) ซึ่งโดยปกติแล้วเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณจะต้องอยู่ในสภาพพร้อมใช้งานที่รองรับการให้บริการกับเครื่องลูกข่ายได้ตลอดระยะเวลา ๒๔ ชั่วโมง แต่ถ้าหากไม่สามารถให้บริการจะต้องกู้คืนระบบให้เร็วที่สุด หรือสามารถดำเนินการเท่าที่ทำได้ แผนนี้เป็นวิธีการที่จะทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม ซึ่งเมื่อระบบเสียหายหรือระบบหยุดการทำงานให้ดำเนินการดังนี้

๑) จัดหาอุปกรณ์ใหม่แทน

๒) ทำการเปลี่ยนอุปกรณ์ในส่วนที่เสียหาย

๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้แล้วเสร็จภายใน ๒ วัน หรือ ๔๘ ชั่วโมง

๔) ดำเนินการขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่น เพื่อนำมาใช้ชั่วคราว

๕) นำเอา Backup Tape, CD-ROM, Hard disk ที่สำรองข้อมูลเอาไว้กลับมาทำการ Restore โดยใช้ทีมงานกู้ระบบดำเนินการกู้ระบบกลับคืนมาโดยเร็วที่สุดภายใน ๔๘ ชั่วโมง

๖) ตรวจสอบระบบปฏิบัติการ ฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง จากภัยพิบัติดังกล่าวไม่ใช่เพียงแต่ Hardware เท่านั้น เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม นอกจากนี้ ยังรวมถึงการที่ถูกเจาะระบบหรือเกิดไวรัสคอมพิวเตอร์ซึ่งมีผลต่อระบบงานด้านเทคโนโลยีสารสนเทศ สำนักคอมพิวเตอร์จึงมีแผนในการที่จัดทำการสำรองแหล่งข้อมูลที่ไซต์สำรอง เพื่อเตรียมการในการให้บริการด้านเทคโนโลยีสารสนเทศเพื่อให้มีความต่อเนื่องอยู่เสมอ

แผนการดำเนินการ

๑) สำรวจความต้องการของระบบสำรอง
๒) สำรวจไซต์สำรองที่เหมาะสม
๓) ทำการประเมินความเสี่ยงจากสิ่งต่าง ๆ การจัดหามาตรการด้าน Risk Management
๔) ดำเนินการจัดลำดับผลกระทบขององค์กร
๕) การจัดทำแผนในการกู้คืน
๖) การวางแผน การตั้งทีมงาน ลำดับของการทำงานภายหลังที่ระบบได้รับความเสียหาย
๗) การฝึกอบรมบุคลากร เพื่อให้รับทราบในเรื่องของหน้าที่และการฝึกอบรมด้านเทคนิค
๘) ดำเนินการทดสอบแผนกู้คืนระบบสู่สภาพปกติ (Disaster Recovery Plan) ปีละ ๑ ครั้ง
๙) ปรับปรุงแผนการกู้คืนระบบสู่สภาพปกติ (Disaster Recovery Plan)

๗. การติดตามและรายงานผล

ให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินงานหรือการตรวจสอบต่อผู้บังคับบัญชา คือ ผู้อำนวยการสำนักบรรณสาร ผู้อำนวยการสำนักคอมพิวเตอร์ทราบ ให้ผู้อำนวยการสำนักคอมพิวเตอร์รายงานผลดังกล่าวต่อรองอธิการบดีฝ่ายเทคโนโลยีสารสนเทศ (CIO) และอธิการบดี (CEO) ทราบเป็นประจำทุกเดือน และให้รายงานปัญหา การแก้ปัญหาให้ทราบทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้ในข้างต้น เพื่อที่จะนำมาทำการปรับปรุงและพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ เพื่อให้นำมาใช้งานได้ทันท่วงทีในกรณีที่อาจจะเกิดภัยพิบัติต่อไป