คู่มือการบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ

(Business Continuity and Availability Management)

สารบัญ

บทนำ

1. บทนำ

แผนความต่อเนื่อง หรือเรียกว่า “Business Continuity Plan (BCP) จัดทำขึ้นเพื่อให้โรงพิมพ์ตำรวจสามารถนำไปใช้ในการตอบสนองและปฏิบัติงานในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ ไม่ว่าจะเกิดจากภัยธรรมชาติ อุบัติเหตุ หรือการมุ่งร้ายต่อองค์กร เช่น อัคคีภัย ไฟฟ้าดับ ชุมนุมประท้วง การจลาจล ผู้ก่อการร้าย เป็นต้น โดยสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินดังกล่าว ส่งผลให้โรงพิมพ์ตำรวจต้องหยุดการดำเนินงาน หรือไม่สามารถให้บริการได้อย่างต่อเนื่อง

หากโรงพิมพ์ตำรวจไม่มีกระบวนการรองรับการดำเนินงานอย่างต่อเนื่อง อาจส่งผลกระทบที่อาจเกิดขึ้นต่อโรงพิมพ์ตำรวจ ในด้านต่าง ๆ เช่น ไม่ว่าจะเป็นผลกระทบด้านการให้บริการ สังคม ชุมชน และสิ่งแวดล้อม แผนความต่อเนื่องจึงเป็นสิ่งสำคัญที่จะช่วยให้โรงพิมพ์ตำรวจ สามารถรับมือกับเหตุการณ์ฉุกเฉินที่ไม่คาดคิด และทำให้กระบวนการที่สำคัญ สามารถกลับมาดำเนินการได้อย่างปกติ หรือตามระดับการให้บริการที่กำหนดได้ในระยะเวลาที่เหมาะสม ซึ่งจะช่วยให้สามารถลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อโรงพิมพ์ตำรวจ

การจัดทำแผนการบริหารความต่อเนื่องทางธุรกิจของโรงพิมพ์ตำรวจ ได้ประยุกต์ข้อกำหนดระบบ Business Continuity Management (BCM) โดยมีสาระสำคัญเกี่ยวกับกระบวนการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planing : BCP)

2. วัตถุประสงค์

2.1 เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่อง

2.2 เพื่อให้หน่วยงานเตรียมความพร้อมล่วงหน้าในการรับมือกับสภาวะวิกฤติ หรือเหตุการณ์ฉุกเฉินที่เกิดขึ้น

2.3 ลดผลกระทบจากการหยุดชะงักในการดำเนินธุรกิจ และบรรเทาความเสียหายให้อยู่ในระดับที่ยอมรับได้

2.4 เพื่อให้ผู้รับบริการ เจ้าหน้าที่ หน่วยงานรัฐวิสาหกิจ หน่วยงานภาครัฐ และผู้มีส่วนได้ส่วนเสีย มีความเชื่อมั่นในศักยภาพของหน่วยงาน แม้หน่วยงานต้องเผชิญกับเหตุการณ์ร้อยแรง และส่งผลกระทบจนทำให้การดำเนินธุรกิจต้องหยุดชะงัก

3. องค์ประกอบของเอกสาร

องค์ประกอบของเอกสารประกอบด้วยสาระสำคัญ 4 ส่วนหลัก ดังต่อไปนี้

3.1 การบริหารจัดการทรัพย์สินค้านเทคโนโลยีสารสนเทศ

3.2 การบริหารจัดการคอนฟิกุเรชั่น

3.3 การบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศ

3.4 การบริหารจัดการความต่อเนื่องทางธุรกิจ

การบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ

(IT Asset Management)

การบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ

(IT Asset Management)

1. วัตถุประสงค์

1.1. เพื่อใช้เป็นแนวทางในการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

1.2 เพื่อให้การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศมีมาตรฐานและถือปฏิบัติในแนวทางเดียวกัน

2. นิยามและคำจำกัดความ

• ปีปฏิทิน หมายถึง ปีพุทธศักราชโดยเริ่มตั้งแต่วันที่ 1 มกราคม ถึง วันที่ 31 ธันวาคมของทุกปี

• ปีงบประมาณ หมายถึง ปีพุทธศักราช โดยเริ่มตั้งแต่วันที่ 1 ตุลาคม ปีก่อนปัจจุบัน ถึงวันที่ 30 กันยายน ของปีปัจจุบัน

• ผู้มีส่วนได้ส่วนเสีย หมายถึง ผู้รับผิดชอบ พนักงาน ผู้ส่งมอบ คู่ค้า ลูกค้า และผู้มีส่วนได้ส่วนเสีย

• ทรัพย์สินด้านเทคโนโลยีสารสนเทศ คือ

1) ทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ระบบ คอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบดิจิทัล และระบบรักษาความปลอดภัยดิจิทัล

2) ทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

3) ทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลดิจิทัล ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

• รายการทรัพย์สิน ประกอบด้วย

1) ชื่อเครื่องแม่ข่าย
2) ชื่อระบบปฏิบัติการ (Operating System) และเวอร์ชั่น
3) ชื่อระบบงาน (Application) และเวอร์ชั่น
4) เจ้าของทรัพย์สิน (Owner)
5) ประเภทอุปกรณ์ ยี่ห้อ รายละเอียดทางเทคนิค (Specification)
6) หมายเลขอ้างอิงของฮาร์ดแวร์ (Serial Number) และหมายเลขอ้างอิงของซอฟต์แวร์ (Software License)
7) สถานที่ตั้ง
8) วันที่เริ่มติดตั้ง
9) ประเภทการครอบครอง (ซื้อหรือเช่า)
10) รายละเอียดผู้ให้บริการหรือผู้บำรุงรักษา
11) วันที่บำรุงรักษาล่าสุด
12) วันสิ้นสุดการใช้งานตามสัญญา (warranty) และวันสิ้นสุดการรับประกันการใช้งาน (support contract)
13) วันสิ้นสุดการให้บริการจากผู้ผลิต (end of support)

3. หน้าที่ความรับผิดชอบ

หมวดนโยบายแผนและสารสนเทศ

- จัดทำและวางแผนการจัดหาทรัพย์สินด้านเทคโนโลยีสารสนเทศ
- จัดทำและบำรุงรักษาทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ
- บริหารจัดการวงจรทรัพย์สินด้านเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ
- พัฒนาและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับมาตรฐาน กระบวนการที่เกี่ยวข้อง
- ให้คำแนะนำ และเป็นที่ปรึกษากับเจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศในการบริหารจัดการ ทรัพย์สินเทคโนโลยีสารสนเทศตลอดวงจรชีวิตของทรัพย์สิน (Plan, Purchase, Implement, Utilize and retire)
- ให้คำแนะนำหน่วยงานเจ้าของทรัพย์สินด้านเทคโนโลยีสารสนเทศให้มีความเข้าใจในการใช้งานทรัพย์สินเทคโนโลยีสารสนเทศที่สอดคล้องกับมาตรฐาน กระบวนการ ที่เกี่ยวข้อง

ฝ่ายการการเงิน และบัญชี

- บันทึกทะเบียนทรัพย์สินสารสนเทศในระบบ FixAsset เมื่อมีการจัดซื้อ
- ปรับปรุงข้อมูลทรัพย์สินเทคโนโลยีสารสนเทศเข้าสู่ระบบ FixAsset เมื่อมีการเปลี่ยนสถานะตามวงจร ทรัพย์สินเทคโนโลยีสารสนเทศ เช่น เมื่อมีการจัดซื้อ และการยกเลิกทรัพย์สิน
- ให้คำแนะนำการจัดทำงบประมาณเพื่อจัดหาทรัพย์สินเทคโนโลยีสารสนเทศ

4. การวิเคราะห์ผู้มีส่วนได้ส่วนเสีย

4.1 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ ได้แก่

1. หน่วยงานเชิงนโยบายและผู้ถือหุ้นภาครัฐ
2. คู่ค้า/ส่งมอบ
3. คู่ความร่วมมือ
4. ลูกค้า
5. พนักงานและผู้ปฏิบัติงาน
6. ชุมชน และสังคม

5. ความรับผิดชอบต่อสินทรัพย์

1.1 ทะเบียนสินทรัพย์

1) การบริหารจัดการสินทรัพย์ ต้องจัดทำและเก็บทะเบียนสินทรัพย์ ซึ่งรวมถึง สินทรัพย์ข้อมูลและเอกสาร สินทรัพย์ซอฟต์แวร์ สินทรัพย์อุปกรณ์ สินทรัพย์งานบริการ และบุคลากร เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยง และบริหารจัดการความเสี่ยงที่มีต่อสินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์ขององค์กร

2) ต้องมีการตรวจสอบสินทรัพย์ ต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ทุกประเภทตามระยะเวลาที่กำหนดไว้ เช่น ปีละ 1 ครั้ง หรือภายใน 1 เดือน เมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น เป็นต้น

3) ต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์ เมื่อมีสินทรัพย์ใหม่หรือสินทรัพย์ที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

1.2 ความเป็นเจ้าของสินทรัพย์

1) มีการกำหนดบุคคล หรือหน่วยงานผู้รับผิดชอบ ข้อมูลและสินทรัพย์ทั้งหมดด้านเทคโนโลยีสารสนเทศและการสื่อสาร อย่างชัดเจน

1.3 การอนุญาตให้ใช้สินทรัพย์

1) กำหนด แสดง บันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูลและสินทรัพย์ที่จะต้องถูกใช้

2) การอนุญาตให้ใช้งานสินทรัพย์ด้านอุปกรณ์คอมพิวเตอร์มีดังนี้

- ระบบเทคโนโลยีสารสนเทศ และอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่โรงพิมพ์ตำรวจ เป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานขององค์กร การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่

- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ขององค์กร อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน

- เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งหมดขององค์กร ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง

- ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายขององค์กร รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ขององค์กร ก่อนได้รับอนุญาตจากผู้บริหารสูงสุด

- เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในองค์กร อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ

- อุปกรณ์คอมพิวเตอร์ขององค์กร ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และเจ้าหน้าที่ ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ขององค์กร อย่างเด็ดขาด

3) การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์มีดังนี้

- ห้ามเจ้าหน้าที่ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ขององค์กร

- ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญขององค์กร ทั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนามาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศขององค์กร

- ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปขององค์กร มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้

- รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานขององค์กรเท่านั้น

4) การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้

- องค์กรจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการค้นหาข้อมูล ความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการขององค์กร

- ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้องค์กร และบุคคลผู้ที่เกี่ยวข้องกับองค์กร เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

- การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ องค์กร ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

- ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

- ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย

- องค์กรไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ด หรือบล็อก) ของเจ้าหน้าที่ ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าวถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

5) การอนุญาตให้ใช้งานอีเมล์มี ดังนี้

- ผู้ใช้งานอีเมล์ทั้งหมดขององค์กร ต้องมี E-mail Account เป็นของตนเอง

- E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมล์ไปใช้ในทางที่ผิด

- ผู้ใช้งานต้องลบอีเมล์ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล์ให้เป็นไปตามขนาดที่องค์กรกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงาน และอีเมล์ตามที่กฎหมายกำหนดไว้เท่านั้น

- ห้ามใช้ E-mail Account ขององค์กรเพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น

- ห้ามใช้ E-mail Account ขององค์กรในการประกาศข้อมูลใด ๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับองค์กร

- ห้ามผู้ใช้งานทำสาเนาข้อความหรือทำสาเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล

- ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนขององค์กร

- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นในอีเมล์ หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด

- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ e-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม

- ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้า ต่าง ๆ (Spam Mail) เป็นต้น

- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่ง อีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด

- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

- ห้ามผู้ใช้งานส่งอีเมล์ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อองค์กร

- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)

- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

6. แนวทาง/วิธีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้อง

6.1 หมวดนโยบายแผนและสารสนเทศจัดทำแบบสอบถามเพื่อประเมินการรับรู้ไปยังผู้มีส่วนได้ส่วนเสียที่สำคัญ

6.2 สรุปผลการประเมินการรับรู้ เพื่อนำมาปรับปรุงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย รวมถึงกระบวนการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

6.3 ดำเนินการปีละ 1 ครั้ง

7. การวัด ติดตาม วิเคราะห์ ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการ

การประเมินประสิทธิผลของกระบวนการกระบวนการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศประกอบไปด้วยตัววัด ดังต่อไปนี้

7.1 ทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เป็นปัจจุบัน

ตัววัดผลลัพธ์	ทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เป็นปัจจุบัน
ผู้ติดตาม วัดผล	คณะทำงานการพัฒนาเทคโนโลยีดิจิทัล, หมวดนโยบายแผนและสารสนเทศ
ผู้วิเคราะห์รายงาน	หมวดนโยบายแผนและสารสนเทศ
ข้อมูลประกอบตัววัด	ตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริง กับทะเบียนรายการทรัพย์สินเป็นประจำทุกปีโดยมี % ของความถูกต้องของรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ>= 90%
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100% ของทรัพย์สินด้านเทคโนโลยีสารสนเทศ ที่ได้รับการตรวจสอบ
หมายเหตุ	

.

7.2 ฮาร์ดแวร์ได้รับการบำรุงรักษาตามกำหนดและไม่ชำรุด เสียหายจากการขาดการบำรุงรักษา

ตัววัดผลลัพธ์	ฮาร์ดแวร์ได้รับการบำรุงรักษาตามกำหนดและไม่ชำรุด เสียหายจากการขาดการบำรุงรักษา
ผู้ติดตาม วัดผล	คณะทำงานการพัฒนาเทคโนโลยีดิจิทัล, หมวดนโยบายแผนและสารสนเทศ
ผู้วิเคราะห์รายงาน	หมวดนโยบายแผนและสารสนเทศ
ข้อมูลประกอบตัววัด	เอกสารตารางสัญญาจ้างบำรุงรักษาประจำปี และรายงานการติดตามการบำรุงรักษาฮาร์ดแวร์รายไตรมาส
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	จำนวนสัญญาที่ได้รับการบำรุงรักษาทุกสัญญาตามเอกสารตารางสัญญาจ้างบำรุงรักษาประจำปี
หมายเหตุ	

7.3 มีการระบุเพื่อเลือกใช้อุปกรณ์ กระบวนการที่เป็นมิตรต่อสิ่งแวดล้อม และปฏิบัติตามกฎหมายดิจิทัล

ตัววัดผลลัพธ์	การเลือกใช้อุปกรณ์ กระบวนการที่เป็นมิตรต่อสิ่งแวดล้อม และนโยบายความปลอดภัยสารสนเทศของโรงพิมพ์ตำรวจ
ผู้ติดตาม วัดผล	คณะทำงานการพัฒนาเทคโนโลยีดิจิทัล, หมวดนโยบายแผนและสารสนเทศ
ผู้วิเคราะห์รายงาน	หมวดนโยบายแผนและสารสนเทศ
ข้อมูลประกอบตัววัด	1. รายละเอียดในสัญญาจ้างบำรุงรักษาฮาร์ดแวร์เชิงป้องกันที่ให้ผู้รับจ้างปฏิบัติตาม นโยบายกฎ ระเบียบ ของโรงพิมพ์ตำรวจ 2. เอกสารบำรุงรักษาอุปกรณ์ดับเพลิง ที่มีการใช้สารเคมีที่เป็นมิตรต่อสิ่งแวดล้อมสอดคล้องกับนโยบายและคู่มือการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรกับสิ่งแวดล้อม
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	- จำนวนสัญญาจ้างบำรุงรักษาที่ระบุการปฏิบัติตามนโยบายความปลอดภัยสารสนเทศของโรงพิมพ์ตำรวจ - จำนวนรายการบำรุงรักษา 100 เปอร์เซ็นต์ที่มีการเลือกใช้ สารเคมี อุปกรณ์ดับเพลิง เป็นมิตรต่อสิ่งแวดล้อม
หมายเหตุ	

7.4 มีกระบวนการสอดคล้องกับกฎระเบียบการจัดซื้อจัดจ้าง

ตัววัดผลลัพธ์	มีกระบวนการสอดคล้องกับกฎระเบียบการจัดซื้อจัดจ้าง
ผู้ติดตาม วัดผล	คณะทำงานการพัฒนาเทคโนโลยีดิจิทัล, งานพัสดุ
ผู้วิเคราะห์รายงาน	หมวดนโยบายแผนและสารสนเทศ
ข้อมูลประกอบตัววัด	รายงานการทบทวนกระบวนการว่าสอดคล้องกับกฎ ระเบียบการจัดซื้อจัดจ้างของโรงพิมพ์ตำรวจ
ความถี่ในการติดตาม	ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎ และ/หรือระเบียบที่เกี่ยวข้อง
เป้าหมาย	ไม่มีกระบวนการที่ดำเนินการไม่สอดคล้องกับระเบียบการจัดซื้อจัดจ้างของโรงพิมพ์ตำรวจ
หมายเหตุ	

7.5 วางแผนด้านงบประมาณล่วงหน้าเพื่อจัดหาทรัพย์สินด้านเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจมาทดแทนทรัพย์สินฯ ที่ใกล้ครบอายุการใช้งาน และทรัพย์สินฯ ที่จะไม่ได้รับการสนับสนุนจากผู้ผลิต

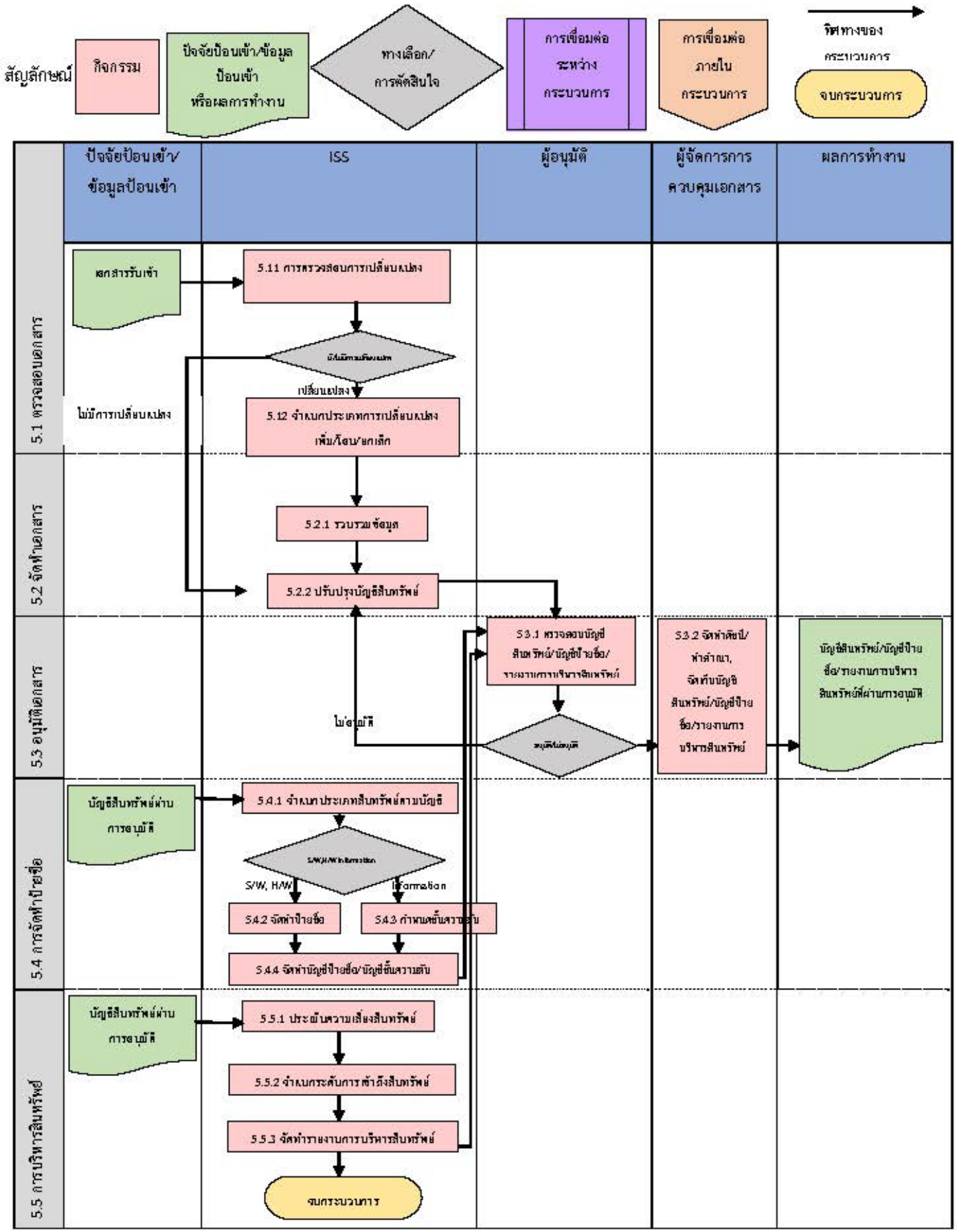
ตัววัดผลลัพธ์	เปอร์เซ็นต์ของทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีความสำคัญที่ใกล้ครบอายุการใช้งาน หรือทรัพย์สินฯ ที่จะไม่ได้รับการสนับสนุนจากผู้ผลิตที่มีการวางแผนทดแทนไว้ล่วงหน้าก่อนปีจัดหา 2 ปี
ผู้ติดตาม วัดผล	คณะทำงานการพัฒนาเทคโนโลยีดิจิทัล, งานพัสดุ, หมวดนโยบายแผนและสารสนเทศ
ผู้วิเคราะห์รายงาน	หมวดนโยบายแผนและสารสนเทศ
ข้อมูลประกอบตัววัด	มติที่ประชุมของคณะอนุกรรมการพัฒนาคุณภาพการบริหารจัดการ โรงพิมพ์ตำรวจ
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100 %
หมายเหตุ	

8. การนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน การกำกับดูแล ด้านการบริหารจัดการดิจิทัล/จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) การนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้เพื่อนำไปปรับปรุงและทำนวัตกรรม

8.1 นำตัววัดตามข้อ 7 รายงานต่อคณะอนุกรรมการบริหารงานบุคคลและสารสนเทศของโรงพิมพ์ตำรวจ ทุกไตรมาส

8.2 ผู้รับผิดชอบ นำผลที่ได้จากการประเมินไปเรียนรู้และจัดการความรู้ โดยการจัดประชุมเพื่อแลกเปลี่ยนความรู้ นำไปปรับปรุงกระบวนการ และจัดทำนวัตกรรมของกระบวนการ ปีละครั้ง

กระบวนการบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ



การบริหารจัดการคอนฟิกุเรชั่น
(Configuration Management)

การบริหารจัดการคอนฟิกุเรชั่น
(Configuration Management)

1. บทนำ

เพื่อให้การบริหารจัดการเทคโนโลยีสารสนเทศมีประสิทธิภาพสูงสุด โรงพิมพ์ตำรวจจึงนำกระบวนการบริหารจัดการคอนฟิกูเรชั่น มาใช้ โดยการบริหารจัดการคอนฟิกูเรชั่น คือการบริหารจัดการ IT Infrastructure สำหรับการให้บริการด้าน IT ทั้งที่เป็นฮาร์ดแวร์ ซอฟต์แวร์ และอุปกรณ์ต่อพ่วงต่าง ๆ ซึ่งจะต้องเก็บข้อมูลรายละเอียดของอุปกรณ์ทั้งหมดไว้เพื่อประกอบการใช้งานของระบบให้บริการด้าน IT นั้นมีความสำคัญเป็นอย่างยิ่ง เพราะมีความสัมพันธ์กับประสิทธิภาพของการให้บริการโดยตรง และองค์ประกอบอื่น ๆ ทั้งหมดที่เก็บอยู่ในฐานข้อมูลให้มีความเหมาะสม ถูกต้อง และทันสมัยอยู่เสมอ

เนื่องจาก Configuration Item ของระบบให้บริการมีอยู่เป็นจำนวนมาก ดังนั้น จึงจำเป็นต้องมีกลไกที่ใช้ในการกำหนด ควบคุม และตรวจสอบองค์ประกอบต่างๆ ของ Configuration Item โดยเฉพาะเมื่อมีการเปลี่ยนแปลงใด ๆ เกิดขึ้น ทั้งนี้ การคัดเลือกกลไกดังกล่าวจะต้องคำนึงถึงความเหมาะสม ปริมาณของConfiguration Items และความต้องการใช้งานของผู้ใช้งานด้วย

กลไกการควบคุมที่ดีจะต้องมีขั้นตอนปฏิบัติที่ชัดเจน มีระเบียบแบบแผน และสามารถตรวจสอบได้ว่า Configuration Item นั้น ได้รับการแก้ไข เพิ่มเติม ลบทิ้ง หรือเปลี่ยนแปลงอย่างไรบ้าง ดำเนินการโดยบุคคลใด เมื่อไร นอกจากนั้นยังต้องมีการบันทึกเหตุผลของการเปลี่ยนแปลงข้อมูลของ Configuration Item ทุกครั้ง และต้องจัดเก็บ Log นั้นไว้ในฐานข้อมูลที่มีการควบคุมการเข้าถึงอย่างเหมาะสม เพื่อใช้เป็นหลักฐานอ้างอิงในอนาคตอีกด้วย

2. วัตถุประสงค์

2.1 เพื่อวางแผนสำหรับการบริหารจัดการองค์ประกอบของระบบเทคโนโลยีสารสนเทศ

2.2 เพื่อจัดเก็บข้อมูลองค์ประกอบของระบบเทคโนโลยีสารสนเทศ

2.3 เพื่อควบคุมการเปลี่ยนแปลงองค์ประกอบของระบบเทคโนโลยีสารสนเทศ

2.4 เพื่อรายงานข้อมูลและสถานภาพขององค์ประกอบของระบบเทคโนโลยีสารสนเทศ

2.5 เพื่อทบทวนสถานภาพขององค์ประกอบของระบบเทคโนโลยีสารสนเทศ’

ขอบเขตและแนวทางในการบริหารจัดการคอนฟิกุเรชั่น

1. คำศัพท์และความหมาย

1.1 Configuration Management : การวางแผนสำหรบการบริหารจัดการองค์ประกอบของระบบเทคโนโลยีสารสนเทศ

1.2 Configuration Item (CI) : ข้อมูลองค์ประกอบของระบบเทคโนโลยีสารสนเทศ ตัวอย่างเช่น ซอฟท์แวร์(Software) ฮาร์ดแวร์(Hardware) เป็นต้น

1.3 Configuration Baseline : CI ที่ผ่านการทบทวนและเห็นชอบแล้ว

1.4 Configuration Management Database (CMDB) : ระบบข้อมูลสำหรับจัดเก็บข้อมูลองค์ประกอบของระบบเทคโนโลยีสารสนเทศ

1.5 Request Change : การร้องขอการเปลี่ยนแปลง

2. ขอบเขต

2.1 ต้องรองรับการเก็บข้อมูลองค์ประกอบ ซึ่งประกอบด้วยระบบการให้บริการด้านเทคโนโลยีสารสนเทศ (Service) ซอฟท์แวร์ (Software) ฮาร์ดแวร์ (Hardware) เอกสารที่เกี่ยวข้อง ระบบเครือข่ายที่เกี่ยวข้อง บุคลากรที่เกี่ยวข้อง กระบวนการทำงาน สถานที่จัดเก็บและทรัพยากรอื่นๆ ที่เกี่ยวข้องกับระบบงานด้านเทคโนโลยีสารสนเทศ

2.2 ต้องสามารถจัดเก็บและแสดงข้อมูลองค์ประกอบโดยมีรายละเอียดดังนี้ ชื่อ ประเภท รุ่น ยี่ห้อ เลขทะเบียน (Serial Number) วันที่ติดตั้งใช้งาน มูลค่า สถานที่ติดตั้ง ผู้ดูแล ข้อมูลสัญญา และการรับประกัน ใบอนุญาตการใช้งานซอฟท์แวร์ จำนวนลิขสิทธิ์ ที่อนุญาตให้ใช้งาน จำนวนลิขสิทธิ์ที่ใช้งานแล้ว จำนวนลิขสิทธิ์ที่เหลืออยู่ ความสัมพันธ์ระหว่างข้อมูลองค์ประกอบและระบบเทคโนโลยีสารสนเทศด้านต่าง ๆ การปรับปรุงเปลี่ยนแปลง การซ่อมบำรุง ข้อมูลปัญหา หรือเหตุขัดข้องที่เกี่ยวข้อง ในกรณีที่ปัญหาหรือเหตุขัดข้องมีความสัมพันธ์กับข้อมูลองค์ประกอบที่มีอยู่

3. กระบวนการบริหารจัดการคอนฟิกุเรชั่น

คือการบริหารจัดการ IT infrastructure สำหรับการให้บริการด้าน IT ทั้งที่เป็นซอฟท์แวร์ ฮาร์ดแวร์ และอุปกรณ์ต่อพ่วงต่าง ซึ่งจะต้องเก็บข้อมูลรายละเอียดของอุปกรณ์ทั้งหมดไว้เพื่อประกอบการใช้งาน และเรียกข้อมูลรายละเอียดของอุปกรณ์แต่ละตัวว่า Configuration Item

4. ขอบเขตการบริหารจัดการการตั้งค่าระบบ

เพื่อให้มีกระบวนการควบคุมการเปลี่ยนแปลงตั้งค่าระบบที่มีความรัดกุม ปลอดภัยและเป็นไปตามมาตรฐาน จึงมีขอบเขตการบริหารจัดการ การตั้งค่าระบบดังนี้

4.1 จัดทำเอกสาร minimum baseline standard เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล และระบบอุปกรณ์เครือข่ายสื่อสารต่างๆ อย่างเป็นลายลักษณ์อักษร โดยมีการทบทวน ปรับปรุงเอกสารให้เป็นปัจจุบันอย่างสม่ำเสมอ

4.2 การเปลี่ยนแปลงการตั้งค่าระบบที่ให้บริการจริงต้องผ่านกระบวนการบริหารจัดการเปลี่ยนแปลงที่กำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

4.3 มีการจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบ ของทุกอุปกรณ์และระบบงาน (system configuration version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

4.4 การสอบทานการตั้งค่าจากหน่วยงานที่มีหน้าที่ควบคุมดูแลความปลอดภัยหรือความเสี่ยงทางด้านเทคโนโลยีอย่างสม่ำเสมอเพื่อให้สอดคล้องตามมาตรฐาน

4.5 กรณีมีความจำเป็นต้องตั้งค่าที่ไม่เป็นไปตามเอกสาร minimum baseline standard ควรผ่านกระบวนการขออนุมัติ (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

การจัดทำเอกสาร Minimum Baseline Standard

1. วัตถุประสงค์

การจัดทำเอกสาร Minimum Baseline Standard เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล และระบบอุปกรณ์เครือข่ายสื่อสารต่าง ๆ อย่างเป็นลายลักษณ์อักษร โดยมีการทบทวน ปรับปรุงเอกสารให้เป็นปัจจุบันอย่างสม่ำเสมอ เพื่อให้การปฏิบัติงานของโรงพิมพ์ตำรวจเป็นไปอย่างมีระบบ รัดกุม และมีประสิทธิภาพ

2. เอกสาร Minimum Baseline Standard

เอกสาร Minimum Baseline Standard หรือคู่มือการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูลรวมถึงอุปกรณ์เครือข่ายสื่อสารต่าง ๆ อย่างเป็นลายลักษณ์อักษร ของโรงพิมพ์ตำรวจประกอบด้วยอ้างอิงตามเอกสารชื่อ คู่มือบริหารจัดการเครื่องแม่ข่าย และการสำรองข้อมูล

การสอบทานการตั้งค่า

1. วัตถุประสงค์

1.1 เพื่อให้แน่ใจว่าการบริหารจัดการกระบวนการคอนฟิกุเรชั่น เป็นไปตามระบบหรือคู่มือที่กำหนดไว้

1.2 เพื่อให้ทราบถึงผลสำเร็จของการนำระบบเทคโนโลยีสารสนเทศ ไปใช้สนับสนุนการทำงานแบบบูรณาการ

1.3 เพื่อให้เกิดกระบวนการบริหารจัดการด้านการคอนฟิกุเรชั่นที่ถูกต้องและมีประสิทธิภาพ

2. ประโยชน์ที่คาดว่าจะได้รับ

2.1 มีแนวทางในการตรวจสอบหรือการสอบทานการบริหารจัดการกระบวนการคอนฟิกุเรชั่นของระบบเทคโนโลยีสารสนเทศ ซึ่งครอบคุลมถึงมาตรฐานแนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่าง ๆ

2.2 องค์กรสามารถสร้างระบบการควบคุมสารสนเทศที่ยังขาดแคลนอยู่ เพื่อลดความเสี่ยงของระบบสารสนเทศ

2.3 การบริหารจัดการภายในองค์กรบรรลุวัตถุประสงค์ในการดำเนินงาน และปฏิบัติงานได้อย่างมีประสิทธิภาพ

3. กระบวนการสอบทาน

3.1 จัดตั้งทีมงานผู้ดูแลด้านการสอบทาน

3.2 กำหนดหัวข้อเงื่อนไขในการสอบทาน

3.3 กำหนดช่วงเวลาในการสอบทาน โดยต้องมีการสอบทานอย่างสม่ำเสมอ

3.4 จดบันทึกและทำรายงานการสอบทาน

4. หัวข้อการสอบทาน

วิธีการตรวจสอบ	ชื่อผู้ตรวจสอบ	วันที่ตรวจสอบ
1. สอบทานระบบ : เครื่องคอมพิวเตอร์แม่ข่ายระบบ ขั้นตอน - สำรวจและวิเคราะห์ปัญหา - สำรวจฟังก์ชั่นการทำงาน - เก็บความต้องการที่จำเป็นในการ Patch - Patch or Update OS - System test - Review and Confirm - การบำรุงรักษาระบบ	รชานนท์	ไตรมาส 4/64
2. สอบทานระบบ เครือข่าย ขั้นตอน - สำรวจและวิเคราะห์ปัญหา - สำรวจฟังก์ชั่นการทำงานของอุปกรณ์เครือข่าย - เก็บความต้องการที่จำเป็นในการ Patch - Patch or Update OS - System test - Review and Confirm - การบำรุงรักษาระบบ	รชานนท์	ไตรมาส 4/64

การวัดผล ติดตาม และประเมินผล การบริหารจัดการคอนฟิกูเรชั่น

1. วัตถุประสงค์

1.1 เพื่อให้การบริหารบริหารจัดการคอนฟิกุเรชั่นได้รับการดูแล และติดตาม อย่างต่อเนื่อง

1.2 เพื่อวางแผนทบทวน ผลการดำเนินการบริหารจัดการคอนฟิกุเรชั่น และหาแนวทางปรับปรุงพัฒนาให้มีประสิทธิภาพ

2. ขั้นตอนการวัดผล และติดตาม

หมวดนโยบายแผนและสารสนเทศ มีการกำหนดขั้นตอนการวัดผล ติดตาม และประเมินผล ของนโยบายทุกหมวดหมู่ที่เกี่ยวข้องกับงานการบริหารจัดการคอนฟิกูเรชั่น ดังนี้

2.1 ด้านผู้ใช้งานระบบ

2.1.2 ผู้ใช้งานระบบของโรงพิมพ์ตำรวจ ร้องขอให้หมวดนโยบายแผนและสารสนเทศดำเนินการในเรื่องต่าง ๆ โดยส่งคำร้องผ่านหมวดนโยบายแผนและสารสนเทศ

2.1.3 หมวดนโยบายแผนและสารสนเทศ รับคำร้องขอตามข้อ (1) และดำเนินการตามคำร้องขอในกรอบระยะเวลา และแนวทางการให้บริการที่วางไว้

2.1.4 หมวดนโยบายแผนและสารสนเทศ มีการทำรายงานสรุปปัญหา ส่งให้หัวหน้างานรับทราบ เพื่อวิเคราะห์ปริมาณปัญหาหรือคำรอง พร้อมวิเคราะห์ผลการประเมิน รายไตรมาส

2.2 ด้านผู้ดูแลระบบ

2.2.1 ติดตาม ตรวจสอบ ระบบฮาร์ดแวร์ ซอฟท์แวร์ รวมถึงระบบต่าง ๆ ที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ อย่างต่อเนื่องและสม่ำเสมอ หรือตามกรอบระยะเวลาที่กำหนดไว้

2.2.2 กำหนดเป้าหมาย และประเมินผลงานด้านระบบ ตามกรอบระยะเวลา

3. หลักเกณฑ์การประเมิน

3.1 จากผลคะแนนความพึงพอใจ โดยตั้งเป้าหมายสัมฤทธิ์ผลโดยรวมไม่ต่ำกว่าร้อยละ 80 ทั้งนี้แบ่งกรอบการประเมินความพึงพอใจเป็น 4 หมวดหลัก ดังนี้

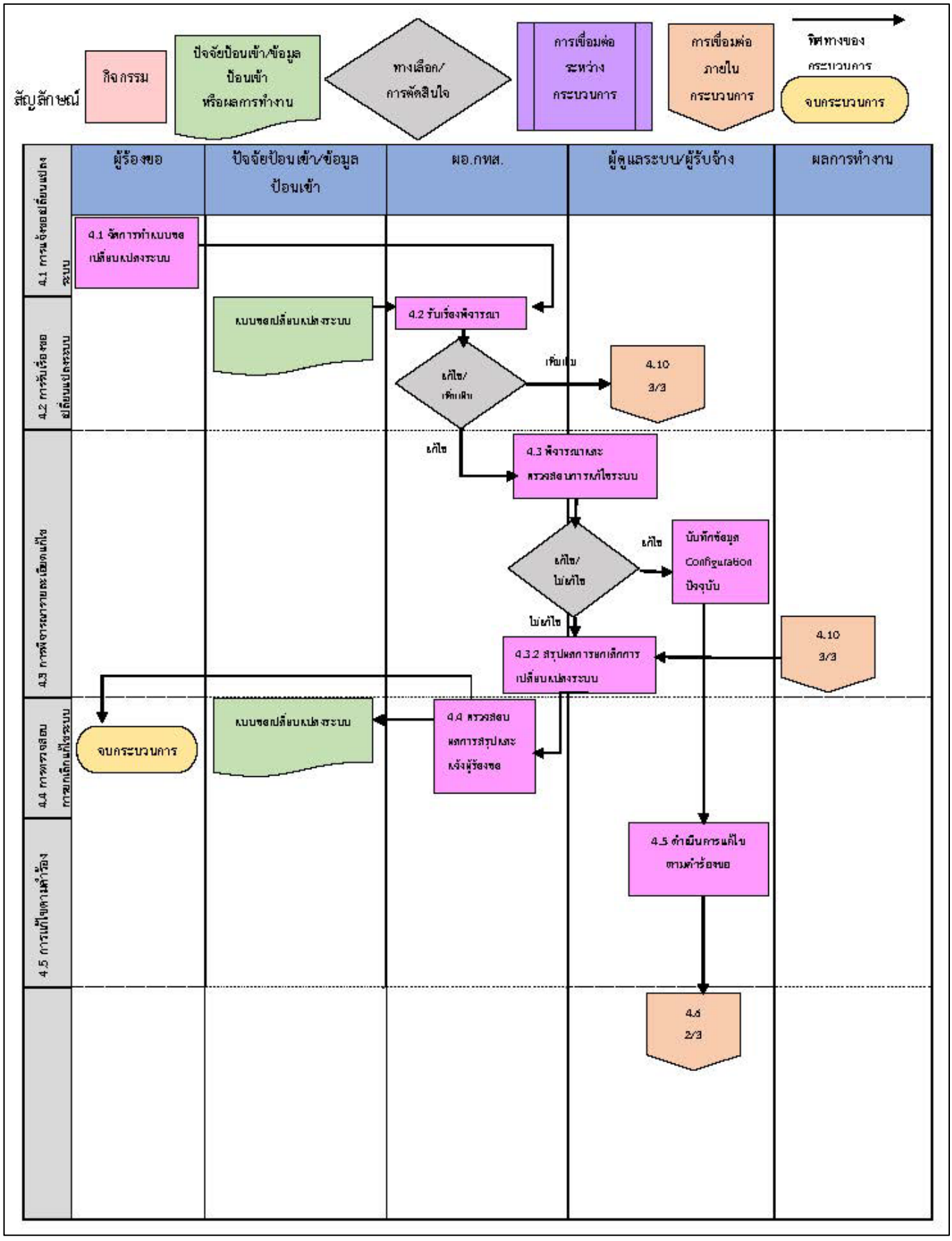
- ด้านเทคโนโลยีการให้บริการ
- ด้านขั้นตอน / กระบวนการให้บริการ
- ด้านเจ้าหน้าที่ผู้ให้บริการ
- ด้านคุณภาพ

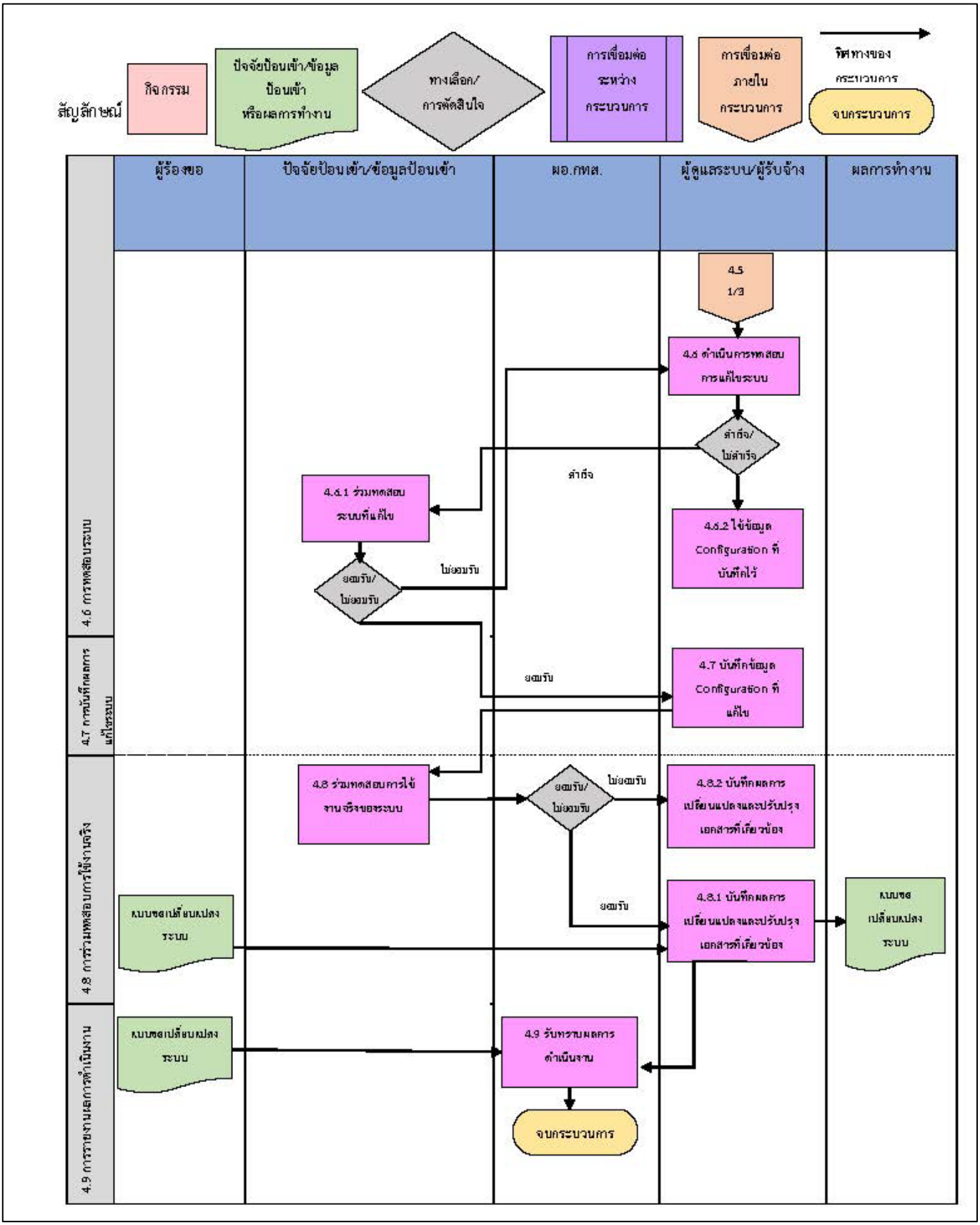
ระดับความสำคัญของข้อมูล	การประเมินมูลค่าความเสียหายหากข้อมูลมีปัญหา หรือไม่สมบูรณ์
ความสำคัญมาก	มีผลกระทบรุนแรงต่อการดำรงอยู่ของหน่วยงาน หรือปิดหน่วยงาน
ความสำคัญปานกลาง	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
ความสำคัญน้อย	ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ

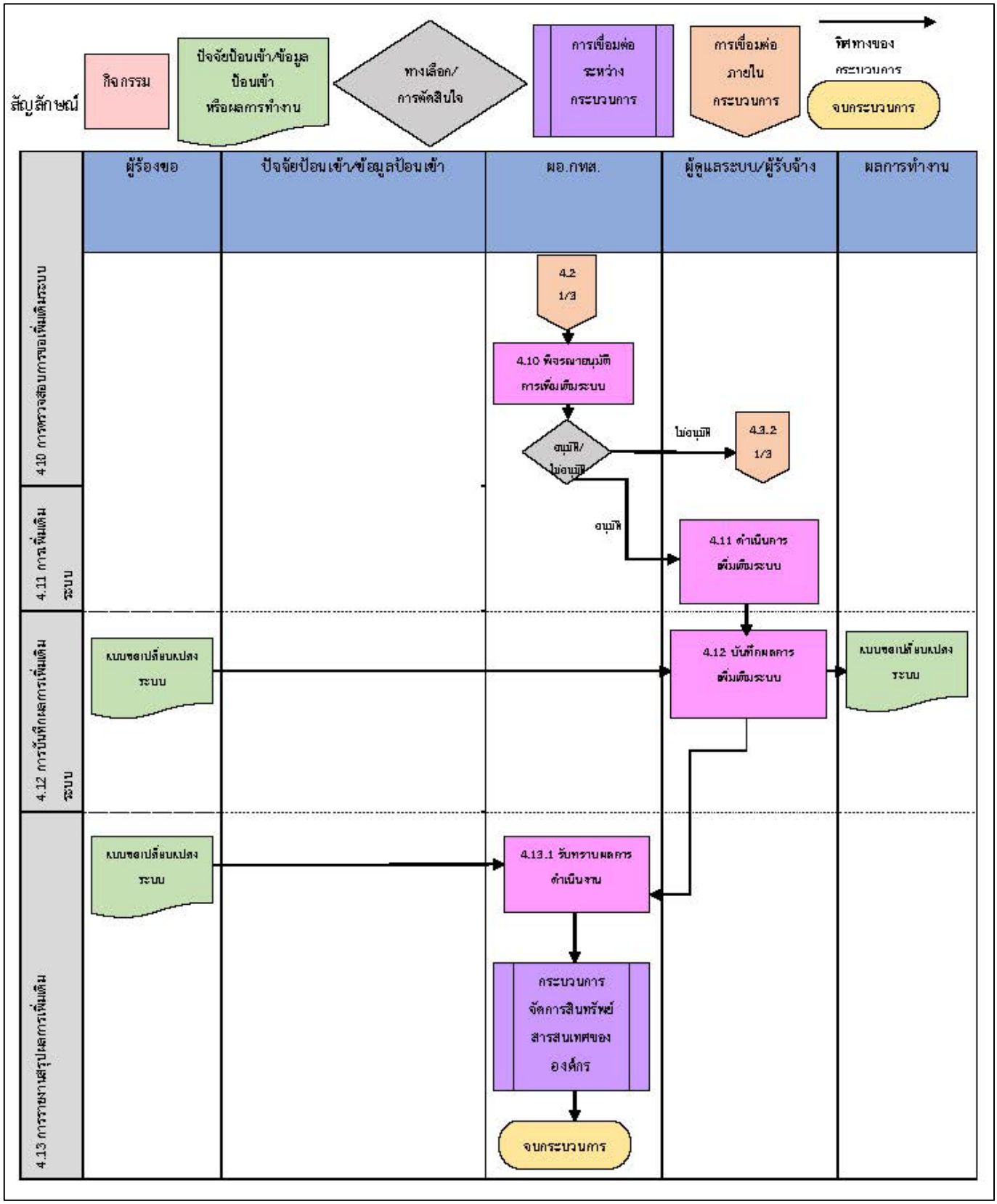
3.2 โรงพิมพ์ตำรวจนำระบบ WinSpeed มาใช้ในการดำเนินการหลาย ๆ ส่วนงาน และหลากหลาย Module ซึ่งแต่ละ Module มีการคอนฟิกค่าระบบที่แตกต่างกันออกไป ดังกล่าวจึงกำหนดตัวชี้วัดโดยตั้งเป้าหมายไปที่ระบบ WinSpeed เป็นหลัก โดยมีวัตถุประสงค์เพื่อให้การดำเนินการในหลาย ๆ ส่วนงานเป็นไปอย่างมีประสิทธิภาพ โดยตั้งเป้าหมายไว้ว่าปัญหา และการสอบถามข้อมูลทั่วไปด้านระบบ WinSpeed ต้องลดลงอย่างต่ำร้อยละ 3 ต่อไตรมาส

3.3 จากการติดตามดูแลระบบจากหมวดนโยบายแผนและสารสนเทศตั้งเป้าหมายเพื่อควบคุมการทำงานของทีมเป็นการภายใน โดยกำหนดเป้าหมายการสัมฤทธิ์ผลจากการดำเนินการ ประกอบด้วย แจ้งปัญหาการใช้งาน, ยื่นคำร้อง/คำขอ และ “[ASK] สอบถามข้อมูลทั่วไป” ซึ่งพิจารณาวัดผลในภาพรวมหัวข้อที่เกี่ยวกับระบบ WinSpeed เป็นหลัก เนื่องจากเป็นระบบที่นำมาใช้ในการปฏิบัติงานในหลาย ๆ ส่วนงาน โดยมีเป้ามายต้องดำเนินการปิดเคสที่เกี่ยวข้องกับระบบ WinSpeed ทั้งหมด ให้แล้วเสร็จภายในเวลาที่กำหนดไม่ต่ำกว่าร้อยละ 80 จากจำนวนเคสทั้งหมด

กระบวนการจัดการคอนฟิกกุเรชั่น




สัญลักษณ์
กิจกรรม
ปัจจัยป้อนเข้า/ข้อมูลป้อนเข้า หรือผลการทำงาน
ทางเลือก/การตัดสินใจ
การเชื่อมต่อระหว่างกระบวนการ
การเชื่อมต่อภายในกระบวนการ
ทิศทางของกระบวนการ
จบกระบวนการ
ผู้ร้องขอ
ปัจจัยป้อนเข้า/ข้อมูลป้อนเข้า
ผอ.กทส.
ผู้ดูแลระบบ/ผู้รับจ้าง
ผลการทำงาน
4.6 การทดสอบระบบ
4.7 การบันทึกผลการแก้ไขระบบ
4.8 การร่วมทดสอบการใช้งานจริง
4.9 การรายงานผลการดำเนินงาน
4.5 1/3
4.6 ดำเนินการทดสอบการแก้ไขระบบ
ดำเนินการสำเร็จ/ไม่สำเร็จ
ดำเนินการสำเร็จ
4.6.1 ร่วมทดสอบระบบที่แก้ไข
4.6.2 ใช้ข้อมูล Configuration ที่บันทึกไว้
ยอมรับ/ไม่ยอมรับ
ไม่ยอมรับ
ยอมรับ
4.7 บันทึกข้อมูล Configuration ที่แก้ไข
4.8 ร่วมทดสอบการใช้งานจริงของระบบ
ยอมรับ/ไม่ยอมรับ
ไม่ยอมรับ
4.8.2 บันทึกผลการเปลี่ยนแปลงและปรับปรุงเอกสารที่เกี่ยวข้อง
ยอมรับ
4.8.1 บันทึกผลการเปลี่ยนแปลงและปรับปรุงเอกสารที่เกี่ยวข้อง
แบบขอเปลี่ยนแปลงระบบ
แบบขอเปลี่ยนแปลงระบบ
แบบขอเปลี่ยนแปลงระบบ
4.9 รับทราบผลการดำเนินงาน
จบกระบวนการ


สัญลักษณ์
กิจกรรม
ปัจจัยป้อนเข้า/ข้อมูลป้อนเข้า หรือผลการทำงาน
ทางเลือก/การตัดสินใจ
การเชื่อมต่อระหว่างกระบวนการ
การเชื่อมต่อภายในกระบวนการ
ทิศทางของกระบวนการ
จบกระบวนการ
ผู้ร้องขอ
ปัจจัยป้อนเข้า/ข้อมูลป้อนเข้า
ผอ.กทส.
ผู้ดูแลระบบ/ผู้รับจ้าง
ผลการทำงาน
4.10 การตรวจสอบการขอเพิ่มเติมระบบ
4.11 การเพิ่มเติมระบบ
4.12 การบันทึกผลการเพิ่มเติมระบบ
4.13 การรายงานสรุปผลการเพิ่มเติม
4.2 1/3
4.10 พิจารณาอนุมัติการเพิ่มเติมระบบ
อนุมัติ/ไม่อนุมัติ
ไม่อนุมัติ
4.3.2 1/3
อนุมัติ
4.11 ดำเนินการเพิ่มเติมระบบ
เอกสารเปลี่ยนแปลงระบบ
4.12 บันทึกผลการเพิ่มเติมระบบ
เอกสารเปลี่ยนแปลงระบบ
เอกสารเปลี่ยนแปลงระบบ
4.13.1 รับทราบผลการดำเนินงาน
กระบวนการจัดการสินทรัพย์สารสนเทศขององค์กร
จบกระบวนการ

การบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management)

การบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management)

1. บทนำ

โรงพิมพ์ตำรวจจะมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ดีเพียงใด แต่ในทุกระบบทุกวิธีการล้วนมีจุดอ่อนหรือช่องโหว่ จึงทำให้เกิดเหตุกาณ์ไม่พึงประสงค์นอกเหนือจากความคาดหมายที่ได้ประเมินไว้ เหตุกาณ์ที่กล่าวถึงนี้เรียกว่าอุบัติการณ์ (Incident) เนื่องจากอุบัติการณ์เป็นเหตุกาณ์ที่อยู่นอกเหนือความคาดหมาย ดังนั้นโรงพิมพ์ตำรวจจึงจำเป็นต้องจัดทำกระบวนการ Incident Management ขึ้น โดยมีเป้าหมายเพื่อให้เกิดการตอบสนองต่อปัญหาอย่างเป็นระบบ มีขั้นตอนและมีแบบแผน และการจัดการกับ Incident ต่างๆ ที่เกิด เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจกลับมาทำงานได้อย่างมีประสิทธิภาพเหมือนเดิมโดยเร็วที่สุด

2. วัตถุประสงค์

2.1 เพื่อให้สามารถกู้คืนบริการให้กลับมาใช้งานได้อย่างรวดเร็ว และลดผลกระทบที่มีต่อการดำเนินงานของโรงพิมพ์ตำรวจ

2.2 เพื่อให้การดำเนินการตาม Service Request เป็นไปอย่างรวดเร็ว และสร้างความพึงพอใจแก่ผู้ใช้บริการ

2.3 เพื่อให้มีกระบวนการมาตรฐานในการทำ Service Request / Incident อย่างครบวงจร

2.4 เพื่อให้มีการบันทึกข้อมูลของ Service Request / Incident อย่างเป็นระบบ และสามารถนำข้อมูลนั้นมาวิเคราะห์ และรายงานให้กระบวนการที่เกี่ยวข้องนำไปปรับปรุงและพัฒนากระบวนการให้มีประสิทธิภาพมากยิ่งขึ้น

3. ที่มาของ Incident Management

กระบวนการของ Incident Management เป็นการจัดการเหตุการณ์การบันทึกข้อมูลการขอใช้บริการหรือเหตุการณ์ต่าง ๆ ที่เกิดขึ้นลงแล้วดำเนินการหรือส่งต่อให้กับเจ้าหน้าที่ที่รับผิดชอบไปดำเนินการต่อให้กับผู้ใช้บริการที่ร้องขอสำหรับติดตามความคืบหน้าของงาน หรือตรวจสอบผลการดำเนินงาน

4. ขอบเขตการรับบริการ

2.1 คลอบคลุมกระบวนการในการรับบริการรวมถึงการบันทึกการส่งต่อคำร้องขอไปยังหน่วยงานที่เกี่ยวข้อง รวมถึงผู้ให้บริการภายนอก Vender (กรณีที่ส่วนงานภายในไม่สามารถดำเนินการแก้ไขได้) การติดตามสถานะ การรายงานความคืบหน้าให้ผู้ใช้บริการทราบ และการปิดสถานะคำร้องขอ เมื่อได้รับคำยืนยันจากผู้ใช้บริการว่าการร้องขอนั้นได้ดำเนินการเสร็จเรียบร้อยแล้ว

2.2 คลอบคุลมกระบวนการในการรับแจ้งการเกิด incident ทุกประเภทที่เกิดขึ้นกับการให้บริการรวมถึงการบันทึก การจัดลำดับความสำคัญ การตรวจสอบ และแก้ไขปัญหาเบื้องต้น การติดตามสถานะ การรายงานความคืบหน้าให้ผู้ใช้บริการทราบ

2.3 คลอบคลุมทุกบริการเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ ที่ให้บริการกับผู้ใช้บริการ

2.4 คลอบคลุมบุคคลทั้งหมดที่มีส่วนเกี่ยวข้องกับกระบวนการจัดการเทคโนโลยีสารสนเทศ ของหมวดนโยบายแผนและสารสนเทศ ซึ่งได้แก่ผู้บริหาร ลูกจ้างประจำ ลูกจ้างชั่วคราว บุคคลภายนอกที่ถูกว่าจ้างโดยหมวดนโยบายแผนและสารสนเทศ บริษัทคู่ค้า บริษัทหรือบุคคลที่เป็นคู่สัญญา และผู้ให้บริการ

5. บทบาทและหน้าที่ผู้รับผิดชอบกระบวนการ

ตำแหน่ง	หน้าที่ความรับผิดชอบ
1. หัวหน้าหมวดนโยบายแผนและสารสนเทศ	1. กำหนดตัวชี้วัดประสิทธิภาพการปฏิบัติงาน 2. กำหนดตัวชี้วัดความพึงพอใจผู้รับบริการ 3. วิเคราะห์แนวโน้มของ Incident เพื่อหา แนวทางในการแก้ไขหรือป้องกัน 4. ควบคุมและดูแลการทำงานให้ตรงตามวัตถุประสงค์ 5. สรุปรายงาน เพื่อนำไปเป็นข้อมูลในการพัฒนาระบบ
2. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง	1.ส่งต่องานไปยังหน่วยงานอื่นที่เกี่ยวข้องในกรณีที่ต้องการความช่วยเหลือในการแก้ปัญหา
3. พนักงานนโยบายแผนและสารสนเทศ	1. รับแจ้งและบันทึกจัดเก็บ Incident จากผู้ใช้ 2. จัดทำรายงานสรุปการดำเนินการจัดการ Incident ที่ได้รับแจ้งเข้ามา พร้อมแยกหมวดหมู่ตามชนิดของ Incident ที่ได้รับแจ้ง 3. ตรวจสอบติดตามการแก้ปัญหา Incident ของผู้ใช้ที่แจ้งเข้ามาและบันทึกผลการแก้ปัญหา 4. แบ่งกลุ่มระดับของ Incident ที่ได้รับแจ้ง เพื่อวิเคราะห์และประเมิน Incident ที่ เกิดขึ้นและการแก้ปัญหา
4. ผู้ขอรับบริการ	1. แจ้ง Incident ที่เกิดขึ้นในการใช้งานระบบ ให้กับพนักงานนโยบายแผนและสารสนเทศ 2 ประเมินผลความพึงพอใจหลังจบการใช้บริการ หรือปัญหาได้รับการแก้ไขแล้วเสร็จ

6. หลักการบันทึกการจัดเก็บ Incident ส่วนสารสนเทศและพัฒนาระบบ

การได้รับการแจ้งเหตุขัดข้องในการใช้งานบริการ แบ่งออก ดังนี้

6.1 Software เป็นการแจ้งเหตุระบบปฏิบัติการหรือโปรแกรมต่าง ๆ ขัดข้อง

6.2 Hardware เป็นการแจ้งเหตุอุปกรณ์ขัดข้อง เช่น คอมพิวเตอร์ไม่ทำงาน เครื่องพิมพ์ไม่ทำงาน เป็นต้น

6.3 User เป็นการแจ้งเหตุการณ์ใช้งาน เมื่อไม่สามารถงานระบบงานได้เต็มประสิทธิภาพ เช่น อินเตอร์เน็ตช้า เครื่องคอมพิวเตอร์มีอาการดับเองบ่อย เป็นต้น

6.4 Electric เป็นการแจ้งเหตุการณ์เกิดไฟฟ้าขัดข้องไฟดับ

7. ตารางแสดงการประกาศหรือแจ้งเตือนไปยังผู้ใช้บริการ

ประเภท	วัตถุประสงค์	เนื้อหาของการประกาศแจ้งเตือน
การแจ้งขั้นต้น	แจ้งให้ฝ่ายต่าง ๆ ทราบว่าหมวดนโยบายแผนและสารสนเทศได้รับทราบถึง เหตุการณ์ที่เกิดขึ้นเรียบร้อยแล้ว ระยะเวลาที่คาดว่าต้องใช้ในการแก้ไข - น้อยกว่า 4 ชั่วโมง : แจ้งปัญหาที่เกิดขึ้นและระบุว่าแก้ปัญหาได้แล้ว - มากกว่า 4 ชั่วโมง : แจ้งปัญหาที่เกิดขึ้น	- รายละเอียดของปัญหา - ระบบอื่น ๆ ที่ได้รับผลกระทบ - ระยะเวลาที่คาดว่าจะใช้ในการแก้ไข - แนวทางหรือทางออกในการใช้งานแบบอื่น ๆ
การแจ้งสถานะปัจจุบันของเหตุการณ์	แจ้งให้ฝ่ายต่าง ๆ ทราบถึง สถานะปัจจุบันของการแก้ไขปัญหา – ระยะเวลา เมื่อมีการเปลี่ยนแปลงหรือความก้าวหน้าในการแก้ปัญหาที่สำคัญ เกิดขึ้น	- แจ้งให้ทราบว่าได้มีการ แก้ปัญหาอย่างไรบ้าง - ระยะเวลาที่คาดว่าจะใช้ในการ แก้ไข
การแจ้งความพร้อมใช้งาน	แจ้งให้ผู้ใช้งานทราบถึงความพร้อมใช้งานของระบบ ระยะเวลา - ภายใน 1 ชั่ว โมงเมื่อระบบสามารถใช้งานได้	- รายละเอียดของปัญหาที่เกิดขึ้น - สาเหตุของปัญหา - ผลกระทบของปัญหา

8. การส่งต่อปัญหาไปยังผู้ให้บริการภายนอก

เป็นการเรียกใช้บริการจากผู้ให้บริการภายนอกทีที่มีความชำนาญมาแก้ไขปัญหา ทั้งที่อยู่ภายใต้เงื่อนไขสัญญาที่ว่าจ้างไว้ (Supplier / Vendor) หรือว่าจ้างเป็นกรณีพิเศษ

การบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ

กระบวนการของการบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศเป็นการตรวจสอบรายงานจาก Incident ที่เกิดขึ้น เพื่อทำการวิเคราะห์ว่ามี Incident ใดที่เกิดขึ้นซ้ำ ๆ เป็นประจำ เพื่อนำมาตรวจสอบวิเคราะห์ หาสาเหตุที่แท้จริงของปัญหา และทำการแก้ไขได้ถูกต้อง กระบวนการนี้เป็นการนำข้อมูลจาก Incident รายเดือน มาทำการจัดกลุ่มเพื่อแยกแยะ Incident จากนั้นทำการวิเคราะห์ว่าเรื่องใดน่าจะเป็นปัญหา ที่ควรยกระดับปัญหาเป็น Problem เพื่อทำการแก้ไขต่อไป

1.วัตถุประสงค์

1.1 เพื่อลดผลกระทบที่เกิดจากความผิดพลาด

1.2 เพื่อป้องกันการเกิดเหตุการณ์ซ้ำ ๆ

1.3 เพื่อวิเคราะห์หาสาเหตุของปัญหาที่แท้จริง

1.4 เพื่อกำหนดแนวทางการแก้ไขปัญหาให้ถูกต้อง

1.5 เพื่อกำหนดวิธีการตรวจสอบการแก้ไขปัญหาอย่างถูกต้อง

1.6 เพื่อทำการบันทึกสาเหตุของปัญหาที่เกิดขึ้น วิธีการแก้ไขปัญหา และการ ติดตามปัญหา

2. ขอบเขต

2.1 เพื่อวิเคราะห์หาสาเหตุที่แท้จริงของปัญหา

2.2 เพื่อแยกปัญหาออกเป็นตามลำดับความสำคัญของปัญหา

2.3 เพื่อหาแนวทางแก้ไขปัญหาที่เกิดขึ้น โดยมุ่งเน้นที่การแก้ไขที่ต้นเหตุ

2.4 เพื่อวางแผนการป้องกันการเกิดปัญหาเดิมซ้ำ ๆ

3.ตัวชี้วัด

3.1 จำนวนปัญหาที่เกิดขึ้นและข้อผิดพลาดที่ตรวจพบ

3.2 ระยะเวลาในการปิดปัญหา

3.3 เวลาเฉลี่ยและเวลาสูงสุดในการปิดปัญหา

3.4 การแก้ปัญหาชั่วคราวหรือระยะสั้น

4. ผู้รับผิดชอบกระบวนการ

4.1 หัวหน้าหมวดนโยบายแผนและสารสนเทศ

4.2 พนักงานนโยบายแผนและสารสนเทศ

5. ตารางแสดงหน้าที่รับผิดชอบ

ตำแหน่ง	หน้าที่รับผิดชอบ
หัวหน้าหมวดนโยบายแผนและสารสนเทศ	พิจารณารายงานของปัญหาทีเกิดขึ้น - สนับสนุนทรัพยากรสำหรับการแก้ไขปัญหา - กระบวนการในการบำรุงรักษาระบบ - ทบทวนมาตราฐานและประสิทธิภาพของกระบวนการ - รายงานการจัดการ - การจัดการพนักงานสนับสนุน
พนักงานนโยบายแผนและสารสนเทศ	- ระบุปัญหาโดยวิเคราะห์จากข้อมูลเหตุการณ์ - ค้นหาสาเหตุของปัญหา - ติดตามความคืบหน้าของการแก้ไขปัญหา - ให้คำแนะนาในการแก้ปัญหาเบื้องต้น - การให้ความช่วยเหลือเหตุการณ์สำคัญ - วิเคราะห์แนวโน้มของปัญหา

และมีการประเมินผลการรับรู้จากผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับการบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบของโรงพิมพ์ตำรวจ โดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการวิเคราะห์และจัดทำกรอบทิศทางฯ จัดทำการกำกับการบริหารความต่อเนื่องทางธุรกิจและความ

พร้อมใช้ของระบบที่ได้จัดทำขึ้นนั้น ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ และเข้าใจถึงกระบวนการทำงานในด้านต่าง ๆ ตามที่กำหนด โดยเฉพาะอย่างยิ่งในกิจกรรมที่ตนเองนั้นมีความเกี่ยวข้องโดยตรง เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับนั้นมาปรับปรุง แก้ไข และพัฒนากระบวนการวิเคราะห์และการบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ ให้มีประสิทธิภาพยิ่งขึ้นต่อไป

การวัดผล ติดตาม และประเมินผลการบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศขององค์กร

1. วัตถุประสงค์

1.1 เพื่อให้การบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศขององค์กรได้รับการดูแล และติดตาม อย่างต่อเนื่อง

1.2 เพื่อวางแผนทบทวน การบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศขององค์กร และหาแนวทางปรับปรุงพัฒนาให้มีประสิทธิภาพ

2. ขั้นตอนการวัดผล ติดตาม และประเมินผล

หมวดนโยบายแผนและสารสนเทศ มีการกำหนดขั้นตอนการวัดผล ติดตาม และประเมินผล การบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศขององค์กร ดังนี้

2.1 ด้านผู้ใช้งานระบบ

2.1.1 ผู้ใช้งานระบบของโรงพิมพ์ตำรวจ ร้องขอให้หมวดนโยบายแผนและสารสนเทศดำเนินการในเรื่องต่าง ๆ

2.1.2 หมวดนโยบายแผนและสารสนเทศ รับคำร้องขอตามข้อ (2.1.1) และดำเนินการตามคำร้องขอในกรอบระยะเวลา และแนวทางการให้บริการที่วางไว้

2.1.3 ผู้ใช้งานระบบ ต้องทำการประเมินผลความพึงพอใจในการใช้บริการ หลังคำร้องขอได้รับการดำเนินการแล้วเสร็จ

2.1.4 พนักงานนโยบายแผนและสารสนเทศ ทำรายงานสรุปปัญหาประจำเดือน ส่งให้หัวหน้างานรับทราบ เพื่อวิเคราะห์ปริมาณปัญหาหรือคำรอง พร้อมวิเคราะห์ผลการประเมิน

2.2 ด้านผู้ดูแลระบบ

2.2.1 ติดตาม ตรวจสอบ ระบบฮาร์ดแวร์ ซอฟท์แวร์ รวมถึงระบบต่าง ๆ ที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ อย่างต่อเนื่องและสม่ำเสมอ หรือตามกรอบระยะเวลาที่กำหนดไว้

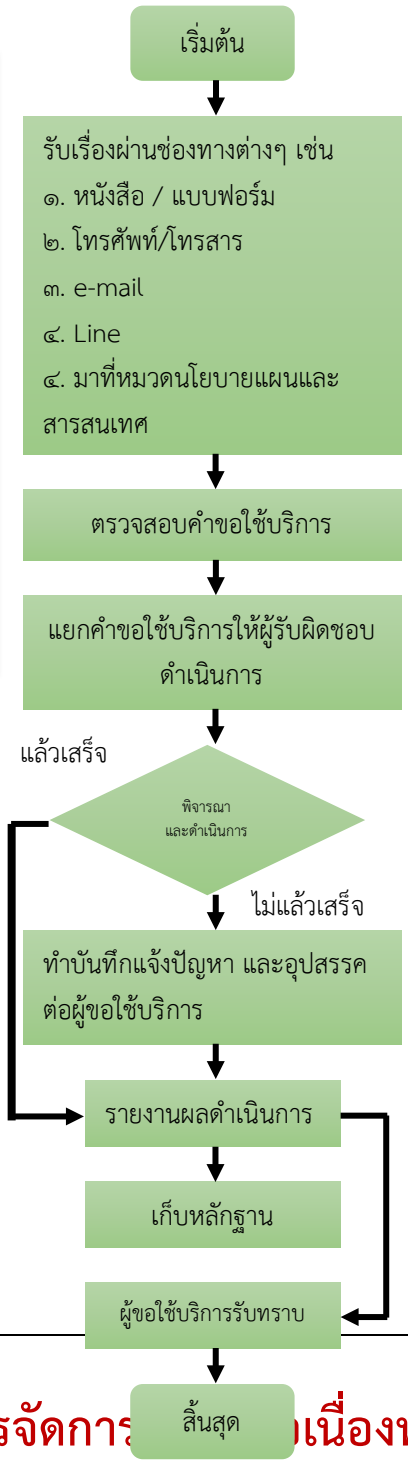
2.2.2 กำหนดเป้าหมาย และประเมินผลงานด้านระบบ ตามกรอบระยะเวลา

3. หลักเกณฑ์การประเมิน

3.1 จากผลคะแนนความพึงพอใจ โดยแบ่งกรอบการประเมินความพึงพอใจเป็น 4 หมวดหลัก ดังนี้

- ด้านเทคโนโลยีการให้บริการ
- ด้านขั้นตอน / กระบวนการให้บริการ
- ด้านเจ้าหน้าที่ผู้ให้บริการ
- ด้านคุณภาพ

กระบวนการบริหารจัดการเหตุการณ์ผิดปกติ (IT Incident)
การร้องขอ การบริการ (Service Requests)
และปัญหาด้านเทคโนโลยีสารสนเทศ (Problem Management)

ผู้ส่งมอบหรือ ผู้ที่เกี่ยวข้อง	ปัจจัยนำเข้า	กระบวนการ/ ขั้นตอนในการดำเนินงาน	Output	ผู้รับบริการ
-หน่วยงานภายในโรงพิมพ์ตำรวจที่แจ้งปัญหา - หมวดนโยบายแผนและสารสนเทศ - บุคลากรหมวดนโยบายแผนและสารสนเทศที่ดำเนินการแก้ไขปัญหา	-เรื่องปัญหาที่ได้รับแจ้ง - ระบบต่างๆ ๑. บริการ user account ๒. บริการ e-mail ๓. บริการ work flow ๔. ระบบ Internet ๕. ระบบ WinSpeed ๖. บริการ antivirus ๗. บริการ VPN ๘. บริการ Wireless หรือ Wi-Fi		- รายงานผลการดำเนินการแก้ไข - หลักฐานในการแก้ไข - พบช่องโหว่ของปัญหาที่เกิดขึ้น - ปัญหาแก้ไขแล้วเสร็จ - ประวัติการเกิดปัญหา - แนวทางการแก้ไขปัญหา	- ผู้แจ้งปัญหา/ผู้ใช้บริการ - หน่วยงานของผู้แจ้งปัญหา/ผู้ที่ใช้บริการ

การบริหารจัดการ[illegible]เนื่องทางธุรกิจ

(Business Continuity Management)

การบริหารจัดการความต่อเนื่องทางธุรกิจ
(Business Continuity Management)

บทนำ

แผนความต่อเนื่อง หรือเรียกว่า “Business Continuity Plan (BCP) จัดทำขึ้น เพื่อให้หมวดนโยบายแผนและสารสนเทศ สามารถนำไปใช้ในการตอบสนองและปฏิบัติงานในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ ไม่ว่าจะเกิดจากภัยธรรมชาติ อุบัติเหตุ หรือการมุ่งร้ายต่อองค์กร เช่น อัคคีภัย ไฟฟ้าดับ ชุมนุมประท้วง/การจลาจล/ผู้ก่อการร้าย เป็นต้น โดยสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินดังกล่าว ส่งผลให้หมวดนโยบายแผนและสารสนเทศ ต้องหยุดการดำเนินงาน หรือไม่สามารถให้บริการได้อย่างต่อเนื่อง

หากหมวดนโยบายแผนและสารสนเทศไม่มีกระบวนการรองรับการดำเนินงานอย่างต่อเนื่อง อาจส่งผลกระทบที่อาจเกิดขึ้นต่อหมวดนโยบายแผนและสารสนเทศ ในด้านต่าง ๆ เช่น ไม่ว่าจะเป็นผลกระทบด้านการให้บริการ สังคม ชุมชน และสิ่งแวดล้อม แผนความต่อเนื่องจึงเป็นสิ่งสำคัญที่จะช่วยให้หมวดนโยบายแผนและสารสนเทศ สามารถรับมือกับเหตุการณ์ฉุกเฉินที่ไม่คาดคิด และทำให้กระบวนการที่สำคัญ สามารถกลับมาดำเนินการได้อย่างปกติ หรือตามระดับการให้บริการที่กำหนดได้ในระยะเวลาที่เหมาะสม ซึ่งจะช่วยให้สามารถลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อหมวดนโยบายแผนและสารสนเทศ

การจัดทำแผนการบริหารความต่อเนื่องทางธุรกิจ ของหมวดนโยบายแผนและสารสนเทศ นั้นได้ประยุกต์ข้อกำหนดระบบ Business Continuity Management (BCM) เป็นกรอบแนวทางการปฏิบัติการในกรณีเกิดเหตุฉุกเฉินหรือภัยพิบัติ โดยมีสาระสำคัญเกี่ยวกับกระบวนการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planing : BCP)

วัตถุประสงค์

2.1 เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่อง

2.2 เพื่อให้หน่วยงานมีการเตรียมความพร้อมล่วงหน้าในการรับมือกับสภาวะวิกฤติ หรือเหตุการณ์ฉุกเฉินที่เกิดขึ้น

2.3 เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินธุรกิจ และบรรเทาความเสียหายให้อยู่ในระดับที่ยอมรับได้

2.4 เพื่อให้ประชาชน เจ้าหน้าที่ หน่วยงานรัฐวิสาหกิจ หน่วยงานภาครัฐ และผู้มีส่วนได้ส่วนเสียมีความเชื่อมั่นในศักยภาพของหน่วยงาน แม้หน่วยงานต้องเผชิญกับเหตุการณ์ร้อยแรง และส่งผลกระทบจนทำให้การดำเนินธุรกิจต้องหยุดชะงัก

แผนบริหารความต่อเนื่องทางธุรกิจ

1. สมมุติฐานของแผนความต่อเนื่อง (BCP Assumption)

1.1 เหตุการณ์ฉุกเฉินที่เกิดขึ้นในช่วงเวลาในการดำเนินงานต่าง ๆ ที่ส่งผลต่อการดำเนินงานทางด้านเทคโนโลยีสารสนเทศ ของโรงพิมพ์ตำรวจ แต่มิได้ส่งผลกระทบต่อระบบสารสนเทศสำรองที่ได้มีการจัดเตรียมไว้

1.2 หมวดนโยบายแผนและสารสนเทศ รับผิดชอบในการสำรองระบบสารสนเทศต่าง ๆ โดยระบบสารสนเทศสำรองนั้น มิได้รับผลกระทบจากเหตุการณ์ฉุกเฉินเดียวกันกับระบบสารสนเทศหลัก

1.3 “บุคลากร” ที่ถูกระบุในเอกสารนี้ หมายถึง พนักงานทั้งหมดของโรงพิมพ์ตำรวจ

2. ขอบเขตแผนความต่อเนื่อง (Scope of BCP)

แผนความต่อเนื่อง (BCP) ฉบับนี้ ใช้รับรองกรณีเกิดสภาวะวิกฤติ หรือเหตุการณ์ฉุกเฉิน บริเวณโรงพิมพ์ตำรวจหรือภายในโรงพิมพ์ตำรวจประกอบด้วยเหตุการณ์ต่อไปนี้

2.1 เหตุการณ์อันเนื่องมาจาก เหตุอุทกภัย

2.2 เหตุการณ์อันเนื่องมาจาก เหตุอัคคีภัย

2.3 เหตุการณ์อันเนื่องมาจาก เหตุชุมนุมประท้วง/จลาจล และความไม่สงบทางเหตุการเมืองต่าง ๆ

2.4 เหตุการณ์โรคระบาด

3. การวิเคราะห์ทรัพยากรที่สำคัญ

แผนความต่อเนื่องฉบับนี้ได้จัดทำขึ้น เพื่อให้รองรับกับความเสี่ยงที่เกิดขึ้น ซึ่งเป็นความเสี่ยงที่จะส่งผลให้การดำเนินงานทางด้านเทคโนโลยีสารสนเทศ หยุดชะงักได้ โดยพิจารณาถึงผลกระทบต่อทรัพยากรที่สำคัญ ซึ่งแบ่งออกเป็น 5 ประเภท คือ

3.1 ผลกระทบด้านอาคาร/สถานปฏิบัติงานหลัก หมายถึง เหตุการณ์ที่เกิดขึ้น ซึ่งส่งผลให้ไม่สามารถปฏิบัติงานที่สถานที่ปฏิบัติงานหลักของโรงพิมพ์ตำรวจได้รับความเสียหาย และส่งผลให้บุคลากรไม่สามารถเข้าปฏิบัติงานหลักได้เป็นระยะเวลาชั่วคราวหรือระยะยาว

3.2 ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญ หรือไม่สามารถจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญได้หรือมีวัสดุอุปกรณ์ให้สามารถใช้งานในการปฏิบัติงานได้ตามปกติ

3.3 ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้ระบบงานเทคโนโลยี หรือระบบสารสนเทศ หรือข้อมูลที่สำคัญได้

3.4 ผลกระทบด้านบุคลากรหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ

3.5 ผลกระทบด้านคู่ค้า/ผู้ให้บริการที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย ไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้

เหตุการณ์สภาวะวิกฤต		ผลกระทบ				
		ด้านอาคาร/สถานที่ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ	ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	ด้านบุคลากรหลัก	คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้เสีย
1	เหตุอุทกภัย	√	√	√	√	√
2	เหตุอัคคีภัย	√	√	√	√	√
3	เหตุชุมนุมประท้วง/จลาจล	√	√	√	√	√
4	โรคระบาด	√	-	-	√	-

4. การบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ของโรงพิมพ์ตำรวจ

4.1 กลยุทธ์ความต่อเนื่องทางธุรกิจ (Business Continuity Strategy)

ทรัพยากร	กลยุทธความต่อเนื่องทางธุรกิจ
อาคาร/สถานปฏิบัติงานหลัก	- กรณีอาคาร สถานที่ ไม่ได้รับความเสียหายและสามารถปฏิบัติงานได้หลังจากเกิดเหตุ จะปฏิบัติงานตามปกติ - กรณีอาคาร สถานที่ ได้รับความเสียหายส่งผลให้ไม่สามารถปฏิบัติงานได้ เกินกว่า 10 วัน และความเสียหายขยายเป็นวงกว้าง กำหนดให้ใช้พื้นที่ตาม BCM ของโรงพิมพ์ตำรวจ - กำหนดให้เจ้าหน้าที่สามารถปฏิบัติงานที่บ้านได้
วัสดุอุปกรณ์ที่สำคัญ / การจัดหาวัสดุอุปกรณ์ที่สำคัญ	- กำหนดให้มีการจัดหาคอมพิวเตอร์สำรองที่มีคุณลักษณะเหมาะสมกับการใช้งาน พร้อมอุปกรณ์ที่สามารถเชื่อมโยงต่อผ่านอินเตอร์เน็ต - กรณีปฏิบัติงานที่บ้านให้ใช้อุปกรณ์ส่วนตัวแต่ละบุคคล โดยให้อยู่ภายใต้เงื่อนไขนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ
เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	- กำหนดให้มี DR Site ที่มีคอมพิวเตอร์แม่ข่าย คอมพิวเตอร์ลูกข่าย และอุปกรณ์เครือข่ายสื่อสาร - กำหนดให้มีเจ้าหน้าที่จัดเก็บข้อมูล ในส่วนที่เกี่ยวข้องกับการปฏิบัติงานไว้ในรูปแบบอิเล็กทรอนิกส์ พร้อมจัดเก็บสื่อสำรองข้อมูลไว้ที่ระบบ Cloud
บุคลากรหลัก	- กำหนดให้ใช้อุปกรณ์สำรอง ทดแทนภายในสำนักงานหรือกลุ่มงานเดียวกัน
คู่ค้า / ผู้ให้บริการสำคัญ	- กำหนดให้จัดหาอุปกรณ์เชื่อมโยงระบบเครือข่ายผ่านอินเตอร์เน็ตพกพาเพื่อเชื่อมต่อกับข้อมูลระบบส่วนกลาง

4.2 ผลกระทบทางธุรกิจ (Business Impact Analysis)

จากการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) พบว่า กระบวนการหลักส่วนใหญ่มีความสำคัญ และจำเป็นต้องดำเนินงานให้บริการได้ ภายในระยะเวลาอันสั้น อันประกอบด้วย

ผลการวิเคราะห์ BIA ของระบบสารสนเทศ			
ระบบงาน	**RTO***	**RPO****	**MTPoD*****
ระบบ WinSpeed	1 ชม.	3 ชม.	5 ชม.
ระบบ FiXAsset	1 ชม.	3 ชม.	5 ชม.
ระบบ Payroll	1 ชม.	3 ชม.	5 ชม.
ระบบอินเตอร์เน็ต	1 ชม.	3 ชม.	5 ชม.

RTO* - Recovery Time Objective หมายถึง ระยะเวลาที่องค์กรยอมรับได้ในการกู้คืนระบบให้กลับสู่สภาวะปกติ ในกรณีเกิดเหตุฉุกเฉิน

RPO** - Recovery Point Objective หมายถึง ปริมาณข้อมูลสูญหายที่องค์กรยอมรับได้ในช่วงเวลาหนึ่ง

MTPoD*** - Maximum Time Period of Disruption หมายถึง ระยะเวลาสูงสุดที่องค์กรยอมรับได้ในการกู้คืนระบบ เมื่อเกิดเหตุขัดข้อง หากพ้นจากระยะนี้แล้ว มีผลต่อการดำเนินงานในระดับสูงสุด

4.3 ขั้นตอนการบริหารความต่อเนื่องและกอบกู้กระบวนการ

ขั้นตอนและกิจกรรม	ผู้รับผิดชอบ
1. แจ้งเหตุฉุกเฉิน วิกฤติ ให้กับผู้อำนวยการ	หัวหน้าหมวดนโยบายแผนและสารสนเทศ
2. จัดประชุมคณะทำงานการพัฒนาเทคโนโลยีดิจิทัล เพื่อประเมินสถานะการณ์ ความเสียหาย ผลกระทบต่อการดำเนินงาน การให้บริการ และทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง	คณะทำงานการพัฒนาเทคโนโลยีดิจิทัล
3. ทบทวนกระบวนการที่มีโดยเร่งด่วน หรือส่งผลกระทบอย่างสูง (หากไม่ดำเนินการ) ดังนั้น จำเป็นต้องดำเนินงานหรือปฏิบัติด้วยมือ (Manual Processing)	คณะทำงานการพัฒนาเทคโนโลยีดิจิทัล
4. รายงานผลการประชุม ต่อรองผู้อำนวยการ โรงพิมพ์ตำรวจเพื่อทราบ โดยครอบคลุมประเด็นดังนี้ - จำนวนรายชื่อ เจ้าหน้าที่ที่ได้รับผลกระทบจากสถานการณ์ฉุกเฉิน - ความเสียหายและผลกระทบต่อการดำเนินงาน - ทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง - กระบวนการเร่งด่วนและส่งผลกระทบอย่างสูง หากไม่ดำเนินการและจำเป็นต้องดำเนินงานหรือปฏิบัติด้วยมือ	หัวหน้าหมวดนโยบายแผนและสารสนเทศ
5. ประเมินและระบุกระบวนการหลัก และงานเร่งด่วนที่จำเป็นต้องดำเนินการแก้ไข	คณะทำงานการพัฒนาเทคโนโลยีดิจิทัล

ขั้นตอนและกิจกรรม	ผู้รับผิดชอบ
6. ติดต่อและประสานงานกับหน่วยงานที่เกี่ยวข้องในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง ได้แก่ - สถานที่ปฏิบัติงานสำรอง - วัสดุอุปกรณ์ที่สำคัญ - เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ - บุคลากร - คู่ค้า/ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย	คณะทำงานการพัฒนาเทคโนโลยีดิจิทัล
7. รายงานผลความคืบหน้าให้แก่ ผู้อำนวยการ	หัวหน้าหมวดนโยบายแผนและสารสนเทศ

การสื่อสารแนวทางการบริหารจัดการความต่อเนื่องทางธุรกิจ

1. วัตถุประสงค์

1.1 เพื่อให้ผู้เกี่ยวข้องและผู้มีส่วนได้เสีย ทั้งภายในและภายนอกองค์กร ยึดถือเป็นกรอบแนวทางปฏิบัติอย่างสอดคล้องกัน

1.2 เพื่อให้นโยบายการบริหารจัดการความต่อเนื่องทางธุรกิจ ถูกนำไปใช้ในทุกภาคส่วนอย่างมีระบบ

1.3 เพื่อให้ผู้บริหาร พนักงาน และลูกจ้างของโรงพิมพ์ตำรวจตระหนักถึงการมีส่วนร่วมเพื่อให้การดำเนินการบริหารความต่อเนื่องทางธุรกิจของโรงพิมพ์ตำรวจ บรรลุตามวัตถุประสงค์

1.4 เพื่อให้การบริหารจัดการความต่อเนื่องทางธุรกิจ มีประสิทธิภาพสูงสุด

2. ช่องทางการสื่อสาร

หมวดนโยบายแผนและสารสนเทศ ถ่ายทอดกระบวนการวิเคราะห์และจัดทำกรอบทิศทางฯ การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ ประกอบด้วย ผู้ส่งสาร ข้อมูลข่าวสาร ช่องทางการสื่อสาร และผู้รับสาร

1) ผู้ส่งสาร

ผู้ส่งสาร คือ หัวหน้าหมวดนโยบายแผนและสารสนเทศ ซึ่งเป็นผู้ที่มีบทบาทหน้าที่ในการจัดทำกระบวนการวิเคราะห์และจัดทำการบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ โดยภายหลังจากที่ได้ดำเนินการจัดทำข้อมูลเป็นที่เรียบร้อยแล้ว จะต้องจัดส่งให้ผู้อำนวยการพิจารณาเห็นชอบในหลักการและความถูกต้องของเนื้อหาและรายละเอียด ก่อนทำการส่งต่อข้อมูลข่าวสารไปยังบุคลากรในส่วนต่าง ๆ ต่อไป

2) ข้อมูลข่าวสาร

ข้อมูลข่าวสาร ได้แก่ การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ ที่ผ่านการพิจารณาจากผู้อำนวยการ โดยได้รับการรับรองความถูกต้องเป็นที่เรียบร้อยแล้ว

3) ช่องทางการสื่อสาร

ช่องทางการสื่อสารข้อมูลของโรงพิมพ์ตำรวจ ใช้ทั้งสื่อดั้งเดิม และสื่อสมัยใหม่ ดังนี้ สื่อดังเดิม ได้แก่ สื่อสิ่งพิมพ์ โดยทำการสื่อสารผ่าน 2 ช่องทาง ได้แก่

(1) ติดประกาศที่ป้ายประกาศประจำจุดต่าง ๆ ของโรงพิมพ์ตำรวจ

(2) สื่อสารผ่านเว็บไซต์ จดหมายอิเล็กทรอนิกส์ ระบบเครื่อข่ายภายในโรงพิมพ์ตำรวจ

และมีการประเมินผลการรับรู้จากผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้องกับการบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบของโรงพิมพ์ตำรวจ โดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการวิเคราะห์และจัดทำกรอบทิศทางฯ จัดทำการกำกับการบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบที่ได้จัดทำขึ้นนั้น ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้รับทราบ และเข้าใจถึงกระบวนการทำงานในด้านต่าง ๆ ตามที่กำหนด โดยเฉพาะอย่างยิ่งในกิจกรรมที่ตนเองนั้นมีความเกี่ยวข้องโดยตรง เพื่อที่จะได้นำข้อมูลต่าง ๆ ที่ได้รับนั้นมาปรับปรุง แก้ไข และพัฒนากระบวนการวิเคราะห์และการบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ ให้มีประสิทธิภาพยิ่งขึ้นต่อไป

การวัดผล ติดตาม และประเมินผล การบริหารจัดการความต่อเนื่องทางธุรกิจ

1. วัตถุประสงค์

1.1 เพื่อให้การบริหารจัดการความต่อเนื่องทางธุรกิจได้รับการดูแล และติดตาม อย่างต่อเนื่อง

1.1 เพื่อวางแผนทบทวน ผลการดำเนินการบริหารความมั่นคงปลอดภัยของสารสนเทศ และหาแนวทางปรับปรุงพัฒนาให้ มีประสิทธิภาพ

2. ขั้นตอนการวัดผล ติดตาม และประเมินผล

หมวดนโยบายแผนและสารสนเทศ มีการกำหนดขั้นตอนการวัดผล ติดตาม และประเมินผล ของนโยบายทุกหมวดหมู่ที่เกี่ยวข้องกับงานด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ ดังนี้

2.1 ด้านผู้ใช้งานระบบ

2.1.1 ผู้ใช้งานระบบของโรงพิมพ์ตำรวจ ร้องขอให้หมวดนโยบายแผนและสารสนเทศดำเนินการในเรื่องต่าง ๆ

2.1.2 หมวดนโยบายแผนและสารสนเทศ รับคำร้องขอตามข้อ (2.1.1) และดำเนินการตามคำร้องขอในกรอบระยะเวลา และแนวทางการให้บริการที่วางไว้

2.1.3 ผู้ใช้งานระบบ ต้องทำการประเมินผลความพึงพอใจในการใช้บริการ หลังคำร้องขอได้รับการดำเนินการแล้วเสร็จ

2.1.4 พนักงานนโยบายแผนและสารสนเทศ ทำรายงานสรุปปัญหาประจำเดือน ส่งให้หัวหน้างานรับทราบ เพื่อวิเคราะห์ปริมาณปัญหาหรือคำร้อง พร้อมวิเคราะห์ผลการประเมิน

2.2 ด้านผู้ดูแลระบบ

2.2.1 ติดตาม ตรวจสอบ ระบบฮาร์ดแวร์ ซอฟท์แวร์ รวมถึงระบบต่างๆ ที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ อย่างต่อเนื่องและสม่ำเสมอ หรือตามกรอบระยะเวลาที่กำหนดไว้

2.2.2 กำหนดเป้าหมาย และประเมินผลงานด้านระบบ ตามกรอบระยะเวลา

กระบวนการการบริหารจัดการความต่อเนื่องทางธุรกิจ