แบบฟอร์มการพัฒนาปรับปรุงและบันทึกความรู้หลังการปฏิบัติงาน (AAR)

1.ชื่อองค์ความรู้	**5.3 กระบวนการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร**
2.ประเภทสินทรัพย์ทางความรู้	ด้านการพัฒนาเทคโนโลยีดิจิทัล
3.วันที่บันทึกความรู้	28 กันยายน 2566
4.ผู้เข้าร่วมบันทึกความรู้	1. นายสุเมธ เพ็ชรนิล
	2. นางสาวทรายแก้ว เกษมณี
	3.

5.วัตถุประสงค์ของการบันทึกความรู้เรื่องนี้

1. เพื่อนำข้อเสนอแนะ/ปัญหาอุปสรรคที่พบจากกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศมาพิจารณาพัฒนาปรับปรุงอย่างต่อเนื่อง และยกระดับการดำเนินงานด้านการพัฒนาเทคโนโลยีดิจิทัล
2. เพื่อสรุปองค์ความรู้ที่ได้จากการปรับปรุงกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศซึ่งสอดคล้องกับเกณฑ์ประเมินผลด้านการพัฒนาเทคโนโลยีดิจิทัล
3. เพื่อเป็นส่วนหนึ่งขององค์ความรู้ของการเคหะแห่งชาติ และใช้เป็นศูนย์กลางความรู้ให้กับหน่วยงานอื่น นำไปประยุกต์ใช้ในการปรับปรุงกระบวนการทำงานต่อไป

6. รายละเอียดเกี่ยวกับกระบวนการ (ก่อนปรับปรุง)

ชื่อกระบวนการ	**การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ**
วัตถุประสงค์ของกระบวนการ	1. เพื่อบริหารจัดการ การตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร อย่างเป็นระบบ มีประสิทธิภาพ และผ่านการตรวจรับรองมาตรฐานสากล 2. เพื่อปรับปรุงทบทวนขอบเขตการประเมินระบบบริหารความมั่นคงปลอดภัยสารสนเทศ 3. เพื่อทบทวนเกณฑ์การตรวจประเมิน และขอบเขตการประเมิน การพิจารณาเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินอย่างมีมาตรฐาน 4. เพื่อให้การดำเนินงานไม่พบความไม่สอดคล้อง (CAR) ตามข้อกำหนดในการตรวจประเมิน

7. แนวทางการปรับปรุงกระบวนการ (ใช้ในปี 2566)

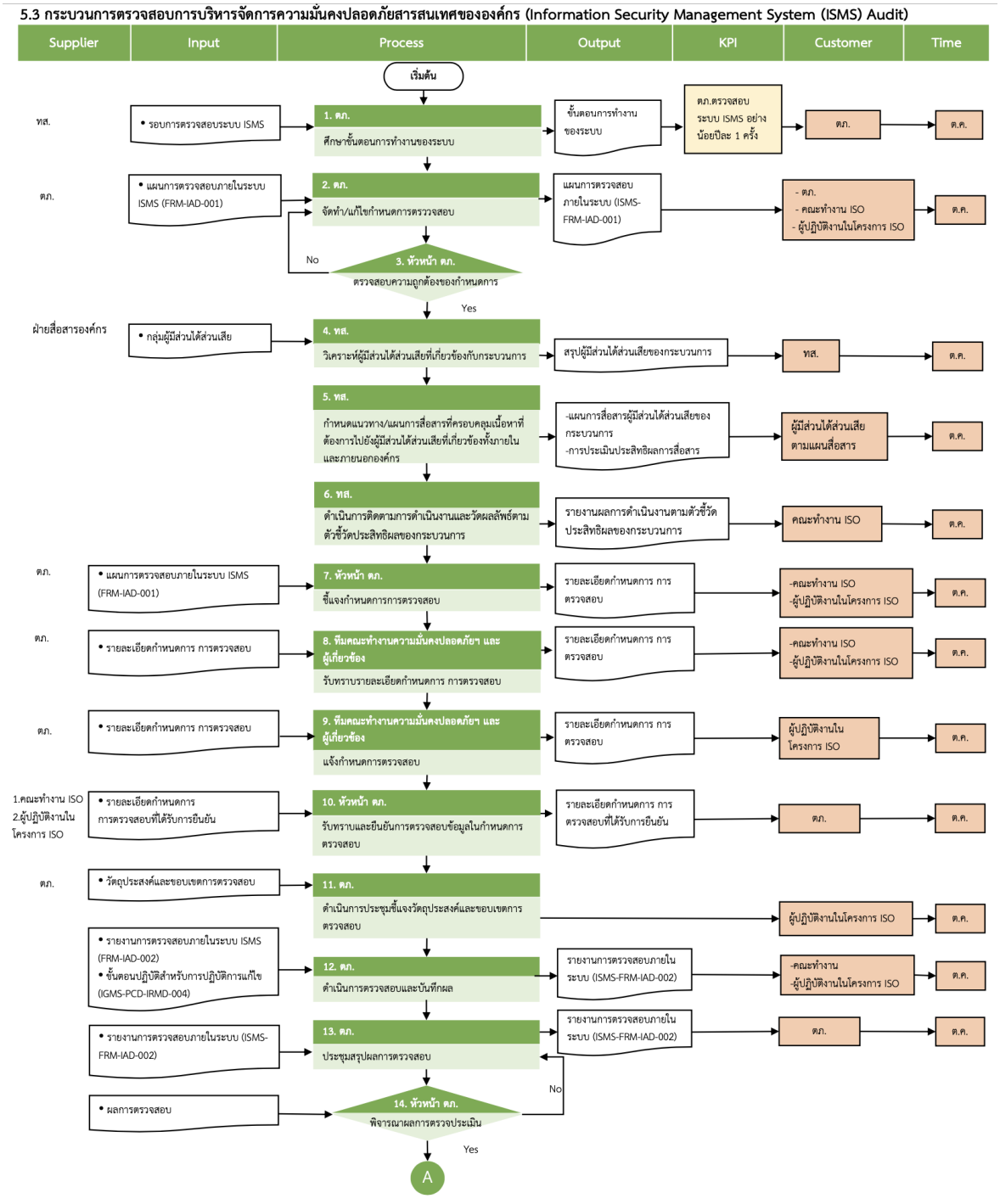
1. ปรับปรุงกระบวนการใน SIPOC เพิ่มขั้นตอนวิเคราะห์ผู้มีส่วนได้ส่วนเสีย รวมถึงการสื่อสาร และการวัดผลการสื่อสาร จากเดิมจำนวน 15 กระบวนการ ปรับเป็น 21 กระบวนการ โดยปรับเพิ่มกระบวนการ วิเคราะห์ผู้มีส่วนได้ส่วนเสีย กำหนดแนวทางการสื่อสาร ติดตามผล และรายงานผลการดำเนินงานตามตัวชี้วัดให้คณะทำงานรับทราบ (กระบวนการที่ 4-6) การตรวจประเมินโดยผู้ตรวจประเมินภายนอก และเพิ่มกระบวนการสุดท้ายคือ นำผลลัพธ์เป็นปัจจัยในการทบทวนนโยบาย แนวทางปฏิบัติและคู่มือการกำกับดูแลข้อมูล การบริหารจัดการด้านเทคโนโลยีดิจิทัล รวมถึงแผนปฏิบัติการดิจิทัลของการเคหะแห่งชาติ
2. ปรับปรุงให้สอดคล้องกับเกณฑ์ Enablers
3. ทบทวนและปรับปรุงตัวชี้วัดของกระบวนการให้มีทั้งตัวชี้วัดเชิงปริมาณ และคุณภาพ
4. ปรับปรุงการวิเคราะห์ผู้มีส่วนได้ส่วนเสียของกระบวนการ ผ่าน Value Chain ของกระบวนการ
5. จัดทำแผนการสื่อสารผู้มีส่วนได้ส่วนเสียของกระบวนการ ตามกลุ่มผู้มีส่วนได้ส่วนเสียขององค์กร
6. กำหนดให้มีการติดตามและการวัดผลลัพธ์ตามตัวชี้วัดประสิทธิผลของกระบวนการ และนำผลลัพธ์รายงานต่อคณะทำงาน
7. เพิ่มกระบวนการตรวจประเมินโดยผู้ตรวจประเมินภายนอก
8. เพิ่มขั้นตอนการนำผลลัพธ์เป็นปัจจัยในการทบทวนนโยบาย แนวทางปฏิบัติและคู่มือการกำกับดูแลข้อมูล การบริหารจัดการด้านเทคโนโลยีดิจิทัล รวมถึงแผนปฏิบัติการดิจิทัลของการเคหะแห่งชาติ

แบบฟอร์มการพัฒนาปรับปรุงและบันทึกความรู้หลังการปฏิบัติงาน (AAR)

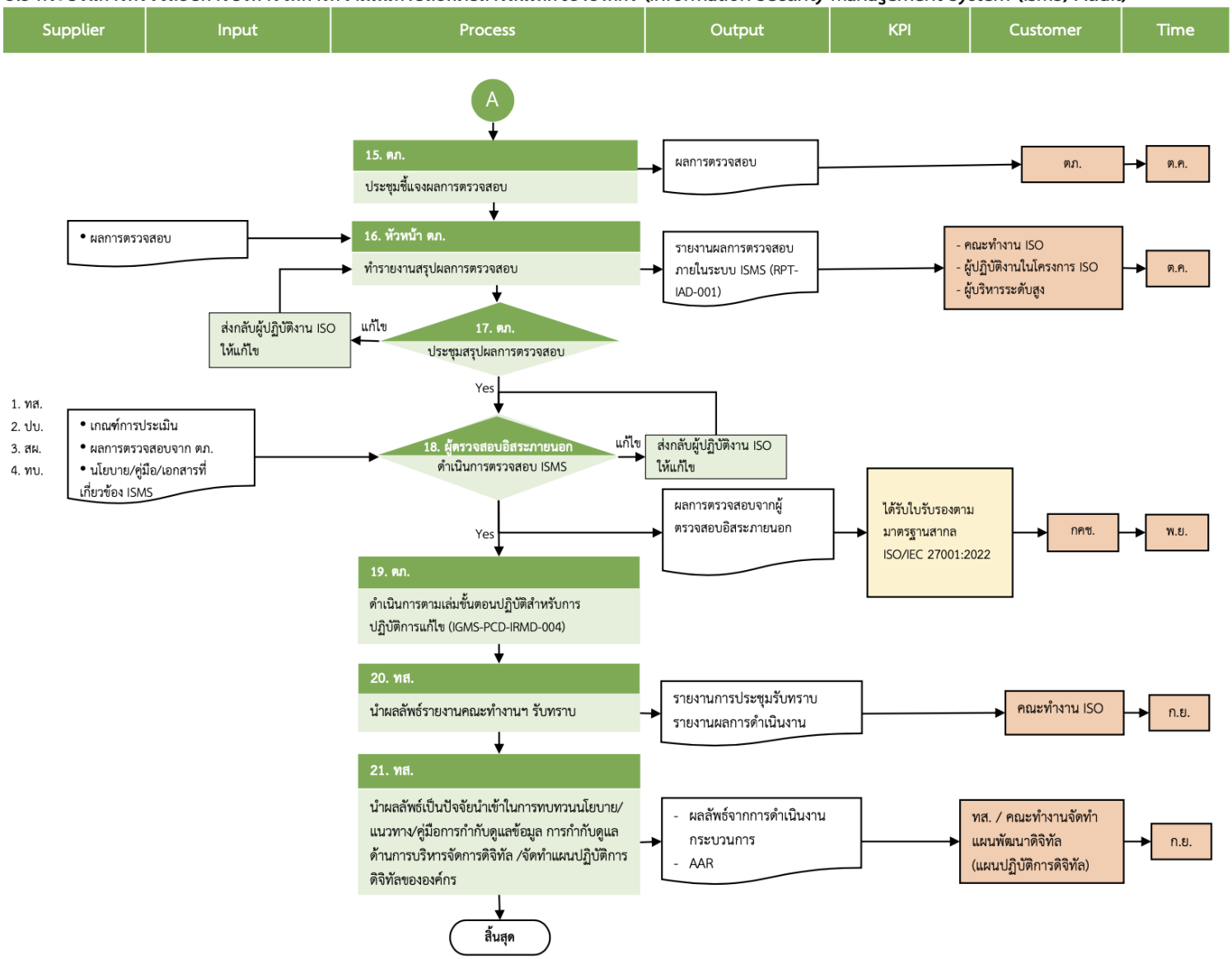
8. รายละเอียดเกี่ยวกับกระบวนการ (หลังปรับปรุง)

ตัวชี้วัดของกระบวนการ ประจำปี 2566	เป้าหมายตัวชี้วัดของกระบวนการ ประจำปี 2566	ผลการดำเนินงาน ประจำปี 2566
1. ผู้ตรวจสอบฝ่าย ตภ. (internal Audit) ตรวจสอบระบบ ISMS อย่างน้อยปีละ 1 ครั้ง	ตรวจสอบระบบ ISMS อย่างน้อยปีละ 1 ครั้ง	ดำเนินการตรวจสอบระบบ ISMS ปีละ 1 ครั้ง
2. ได้ข้อเสนอแนะเพื่อปรับปรุงความมั่นคงปลอดภัยจากการตรวจประเมิน ปีละ 2 ครั้ง	ปีละ 2 ครั้ง	ข้อเสนอแนะฯ จากการตรวจสอบปีละ 2 ครั้ง

9. Flowchart กระบวนการ ปี 2566



5.3 กระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management System (ISMS) Audit)



ตัวชี้วัดกระบวนการ :

Output:

1.ผู้ตรวจสอบภายใน (ตภ.) ตรวจสอบระบบ ISMS อย่างน้อยปีละ 1 ครั้ง

Outcome :

1. ได้ข้อเสนอแนะเพื่อปรับปรุงความมั่นคงปลอดภัยจากการตรวจสอบปีละ 2 ครั้ง

10. สิ่งที่พบจากการดำเนินงานปี 2566

ประเด็น	รายละเอียดประเด็นที่มีการพัฒนาปรับปรุง
	1. ปรับปรุงกระบวนการใน SIPOC เพิ่มขั้นตอนวิเคราะห์ผู้มีส่วนได้ส่วนเสีย รวมถึงการสื่อสาร และการวัดผลการสื่อสาร จากเดิมจำนวน 15 กระบวนการ ปรับเป็น 21 กระบวนการ - เพิ่มกระบวนการ วิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ - เพิ่มการกำหนดแนวทาง/แผนการสื่อสารที่ครอบคลุมเนื้อหาที่ต้องการไปยังผู้มีส่วนได้ส่วนเสียทั้งภายในภายนอกองค์กร - เพิ่มการติดตามผลการดำเนินงาน วัดผลตามตัวชี้วัดประสิทธิภาพของกระบวนการ และการรายงานผลลัพธ์ให้คณะทำงานรับทราบ - เพิ่มกระบวนการตรวจประเมินโดยผู้ตรวจประเมินภายนอก

	- เพิ่มขั้นตอนนำผลลัพธ์เป็นปัจจัยนำเข้าในการทบทวนนโยบาย/แนวทาง/คู่มือความมั่นคงปลอดภัยสารสนเทศ การกำกับดูแลข้อมูล การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร 2. ทบทวนเกณฑ์ การคัดเลือกผู้ตรวจประเมิน โดยกำหนดให้ผู้รับจ้างเสนอเกณฑ์ให้พิจารณาและคัดเลือกผู้ตรวจประเมินภายนอกตามหลักเกณฑ์ที่กำหนดขึ้นไว้ ดังนี้ 1) สัดส่วนการตลาด(Market Share) มีการตรวจรับรองจำนวนมาก (ตามเงื่อนไขใน องค์กรผู้ตรวจประเมินที่มีชื่อเสียง) 2) มี การตรวจประเมินของหน่วยงานภาครัฐ และรัฐวิสาหกิจ 3) มีผู้ตรวจสอบเป็นคนไทย (เรื่องการสื่อสาร) 4) เป็นบริษัทที่มีชื่อเสียง และก่อตั้งมายาวนาน (ตามเงื่อนไขใน องค์กรผู้ตรวจประเมินที่มีชื่อเสียง น่าเชื่อถือ) 5) การตรวจประเมินต่อเนื่อง ทราบบริบทของ กคช.เป็นอย่างดี ทั้งนี้ ตัวชี้วัดประสิทธิผลของกระบวนการที่ปรับปรุงได้แก่ 1) ผู้ตรวจสอบภายใน (ตภ.) ตรวจสอบระบบ ISMS อย่างน้อยปีละ 1 ครั้ง 2) ได้ข้อเสนอแนะเพื่อปรับปรุงความมั่นคงปลอดภัยจากการตรวจสอบ ปีละ 2 ครั้ง 3. ดำเนินการวิเคราะห์ผู้มีส่วนได้ส่วนเสียของกระบวนการตามกลุ่มผู้มีส่วนได้ส่วนเสียขององค์กร เพื่อนำไปจัดทำแผนการสื่อสารตามกลุ่มของผู้มีส่วนได้ส่วนเสีย 4. จัดทำแผนการสื่อสารของกระบวนการโดยแบ่งเป็นกลุ่มผู้มีส่วนได้ส่วนเสีย สิ่งที่ต้องการจะสื่อสาร ช่องทางการสื่อสาร จำนวนครั้งในการสื่อสาร ตัวชี้วัดของการสื่อสาร และการประเมินผลลัพธ์ของการสื่อสารตามตัวชี้วัด เพื่อรวบรวมข้อมูลเพื่อพัฒนาและปรับปรุงกระบวนการในปีถัดไป 5. จัดทำแบบประเมินผลกระบวนการทำงานและบันทึกความรู้ (After Action Review : AAR) ตาม SIPOC ย่อย สำหรับกระบวนการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร เพื่อเป็นฐานองค์ความรู้ด้าน CG และในระดับองค์กร (KM) พร้อมนำไปจัดเก็บในระบบการจัดการความรู้ของสำนักงานฯ เพื่อใช้แลกเปลี่ยนเรียนรู้และนำไปใช้ประโยชน์ในการปรับปรุงกระบวนการปฏิบัติงานอื่น ๆ ต่อไป
ปัญหา/อุปสรรค	- ช่วงแรกของการดำเนินงานโครงการ ผู้ตรวจประเมินภายนอกที่ได้รับการรับรองผู้ตรวจ version 2022 ยังไม่มี - ขาดผู้เชี่ยวชาญด้านกฎหมายดิจิทัล/พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และอื่น ๆ
สาเหตุของปัญหา/อุปสรรค	1. การปรับเปลี่ยน Version ของ มาตรฐานสากล ISO/IEC27001: version 2022 2. นโยบายผู้บริหาร ให้เพิ่มการดำเนินการด้านกฎหมายที่เกี่ยวข้องให้สอดคล้องกับการดำเนินการในกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทำให้เพิ่มขั้นตอนการจัดหาผู้เชี่ยวชาญด้านกฎหมายฯ ซึ่งใช้เวลาในการดำเนินการเพิ่มขึ้น 3. กระบวนการจัดหา/จัดจ้างที่ปรึกษา พ.ร.บ.จัดซื้อจัดจ้างและประกาศต่าง ๆ ทำให้กระบวนจัดหาที่ปรึกษาต้องใช้เวลามากขึ้นทำให้โครงการล่าช้ากว่าแผน

ทำ11. สาเหตุหรือที่มาในการพัฒนาปรับปรุงกระบวนการทำงานในปัจจุบัน (As-Is Process)

☒ ข้อเสนอแนะของผู้ประเมิน IRDP

☒ หลักเกณฑ์ Enablers หรือมาตรฐานหรือกรอบแนวทางที่เป็นที่ยอมรับ (เช่น มาตรฐาน ISO OECD COSO-ERM เป็นต้น)

☐ ผลลัพธ์ไม่เป็นไปตามเป้าหมายที่กำหนด

☒ เพิ่มประสิทธิภาพกระบวนการทำงาน เช่น เพิ่มกระบวนการสื่อสาร การติดตาผล การวัดดผล

☒ การเปลี่ยนแปลงของสภาพแวดล้อมที่เกี่ยวข้องกับกระบวนการ เช่น กฎหมาย ข้อบังคับ ระเบียบ คำสั่ง ประกาศ เป็นต้น

☒ นโยบายรัฐบาล กฎเกณฑ์และข้อเสนอแนะของหน่วยงานกำกับดูแล

☒ แนวทางปฏิบัติที่ดีของหน่วยงานชั้นนำหรือหน่วยงานคู่เทียบ

แบบฟอร์มการพัฒนาปรับปรุงและบันทึกความรู้หลังการปฏิบัติงาน (AAR)

☐ อื่นๆ (โปรดระบุ) เช่น ข้อเสนอแนะจากการถามตอบในกลุ่ม LINE ของ SE-EM ของ สคร. หรือคำถาม-คำตอบในวัน Feedback Day

☐ ไม่เปลี่ยนแปลง

12. แนวทางการเรียนรู้/การจัดการความรู้ เพื่อนำไปสู่การปรับปรุงกระบวนการในปีต่อไป (ปี 2567)

1. ส่งเสริมให้มีการปรับปรุงกระบวนการในแต่ละ SIPOC และจัดทำ AAR ให้เป็นองค์ความรู้ขององค์กรต่อไป
2. ปรับปรุงตามตัวอย่างการปฏิบัติที่ดีขององค์กรชั้นนำ
3. ปรับปรุงให้สอดคล้องมาตรฐานสากล กฎหมาย ระเบียบ ข้อบังคับ
4. เพิ่มการสื่อสารเชิงรุกเพื่อทำความเข้าใจให้กับหน่วยงานที่เกี่ยวข้อง เพื่อให้การตรวจสอบมีประสิทธิภาพและประสิทธิผล ความเสี่ยงลดลง ความปลอดภัยสูงสุด
5. ส่งเสริมให้บุคลากร/คณะทำงาน มีความรู้ความเข้าใจเกี่ยวกับการจัดทำ แนวทาง/กระบวนการ (SIPOC)/คู่มือปฏิบัติงาน เพราะเป็นจุดเริ่มต้นที่สำคัญที่จะทำให้ทราบขั้นตอนการปฏิบัติงานที่ชัดเจนและเป็นระบบ ซึ่งจะช่วยให้ผู้มีส่วนเกี่ยวกับแนวทาง/กระบวนการ (SIPOC) นั้น ๆ เข้าใจการปฏิบัติงานเป็นไปในทิศทางเดียวกัน

.....

นางสาวทรายแก้ว เกษมณี (ผู้จัดทำ)

พ.ระบบงาน 5 ผน.ทส.

วันที่ 29 กันยายน 2566

.....

นายสุเมธ เพ็ชรนิล (ผู้สอบทาน)

ผอก.ผน.ทส.

วันที่ 29 กันยายน 2566

.....

นายเจษฎาลักษณ์ สุวรรณโณ

รักษาการผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ (ทส.)

ผู้ประเมินและปรับปรุงกระบวนการเพื่อบันทึกทำความรู้