รายงานการตรวจเยี่ยมประเมินคุณภาพระบบเทคโนโลยีสารสนเทศ

รพ.บ้านฉาง จ.ระยอง

ประเมินครั้งที่ 1/2568 วันที่ 28 มีนาคม พ.ศ. 2568

คณะกรรมการผู้ประเมิน

1. **นพ.บดินทร์ ทรัพย์สมบูรณ์**
2. **นางภศิชา เธียรเชาวน์**
3. **นางสาวกุณฑลี รักษ์งาร**

สถานภาพทั่วไป

ชื่อ	โรงพยาบาล บ้านฉาง
ประเภท	โรงพยาบาลชุมชน
ขนาด	120 เตียง
สังกัด	สังกัดสำนักงานปลัดกระทรวงสาธารณสุข
ผู้อำนวยการ	นายแพทย์สุรชัย คำภักดี
Chief Information Officer (CIO)	นางสาววารีย์ ศรีบุษย์ (พยาบาลวิชาชีพชำนาญการ)
Chief Information Security Officer (CISO	-
หัวหน้าหน่วย IT	นางอรปรียา แก้วคำสอน (เจ้าพนักงานเวชสถิติชำนาญงาน) หัวหน้ากลุ่มงานสุขภาพดิจิทัล
บุคลากรหน่วย IT	นักวิชาการคอมพิวเตอร์ 3 คน เจ้าพนักงานธุรการ 1 คน
ตำแหน่งงานที่มีในหน่วย IT	Database, Network, Software developer, IT Technical Support
โปรแกรมระบบโรงพยาบาล	HOSxPXE4, IPD paperless,
โปรแกรมระบบอื่น	PACS, LIS, Moph refer
การพัฒนาโปรแกรมเอง	-
IT Outsourcing	PACS, LIS

1. แผนแม่บทการพัฒนาเทคโนโลยีสารสนเทศของโรงพยาบาล

แผนยุทธศาสตร์โรงพยาบาล	มีเล่มแผนยุทธศาสตร์โรงพยาบาลปี 2566 – 2568 ที่แสดงเพียง House model
แผนแม่บทเทคโนโลยีสารสนเทศ	มีเล่มแผนแม่บทเทคโนโลยีสารสนเทศ ปี 2566 - 2570
การจัดทำแผน	มีการจัดตั้งคณะกรรมการที่เกี่ยวข้อง จัดประชุมจากผู้มีส่วนร่วม ประกอบด้วย ผู้บริหาร หัวหน้ากลุ่มงาน หัวหน้างาน ผู้แทนจากกลุ่มวิชาชีพ และบุคลากรด้านเทคโนโลยีสารสนเทศ ร่วมในการจัดทำ และมีการให้ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศร่วมตรวจสอบ
ความสอดคล้องของแผน IT กับแผนยุทธศาสตร์ของโรงพยาบาล	มีการวิเคราะห์ปัจจัยแห่งความสำเร็จ เพื่อแสดงความเชื่อมโยงของแผน IT กับแผนยุทธศาสตร์ของโรงพยาบาล แต่ขาดความชัดเจนว่าส่วนใดๆที่เชื่อมโยงกัน
แผน IT ช่วยให้การดูแลผู้ป่วยมีคุณภาพมากขึ้น	มีแผนฯบางส่วนช่วยในการดูแลบางส่วน
การตรวจสอบ การติดตามประเมินผลการดำเนินการตามแผนแม่บท IT และนำผลการประเมินมาปรับแผนแม่บทให้ดีขึ้น	ไม่มีการตรวจสอบ การติดตามประเมินผลการดำเนินการตามแผนแม่บท IT และนำผลการประเมินมาปรับแผนแม่บทให้ดีขึ้น

จุดเด่น

ผู้บริหารมีความมุ่งมั่นและให้ความสำคัญในการนำ HAIT เป็นเครื่องมือในการขับเคลื่อนองค์กร พร้อมให้การสนับสนุนและมีส่วนร่วมในการทำแผนแม่บท IT กับผู้แทนแต่ละหน่วยงาน และหน่วยงาน IT

ความท้าทายและโอกาสพัฒนา

1. การวิเคราะห์ปัจจัยแห่งความสำเร็จที่ชัดเจน ครอบคลุมและสนับสนุนให้เป้าประสงค์ของแต่ละยุทธศาสตร์สำเร็จ เห็นผลลัพธ์ที่ต้องการผ่านการบรรลุตัวชี้วัดที่เป็นค่าเป้าหมาย นำสู่การจัดทำแผนแม่บท IT ได้อย่างสอดคล้อง เพื่อขับเคลื่อนยุทธศาสตร์โรงพยาบาลสำเร็จ
2. การกำหนดตัวชี้วัดที่มีความชัดเจนขึ้น แสดงผลลัพธ์คุณภาพที่มุ่งหวังจากโครงการ/กิจกรรม ที่ช่วยให้การดูแลผู้ป่วยมีคุณภาพมากขึ้น

2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

การประเมินความเสี่ยง	มีการประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศ แต่ไม่ระบุให้ชัดเจนว่าดำเนินการในช่วงใด ปี 2567
แผนการจัดการความเสี่ยง	มีแผนดำเนินการจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ ระบุวันที่จัดทำ 1 ตุลาคม 2567
การดำเนินการตามแผนจัดการความเสี่ยง	ขาดการแสดงผลดำเนินการตามแผนจัดการความเสี่ยงใดๆ
การประเมินผลการดำเนินการตามแผนการจัดการความเสี่ยง	ขาดการประเมินผลการดำเนินการตามแผนการจัดการความเสี่ยง และไม่มีการประเมินความเสี่ยงรอบที่ 2 และขาดการแสดงให้เห็นการค้นหาจุดอ่อน/ช่องโหว่ที่ชัดเจน ของแต่ละ IT component ใดๆ
การนำผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น	ไม่มี

จุดเด่น

การจัดให้มีคณะกรรมการบริหารความเสี่ยง และเริ่มมีพัฒนาการด้านการจัดการความเสี่ยงตามกรอบแนวทางการจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

ความท้าทายและโอกาสพัฒนา

1. การทำความเข้าใจกรอบแนวทางการจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้อย่างครอบคลุมเพื่อบรรลุตามเป้าหมาย
2. ทบทวนความเข้าใจเกี่ยวกับแต่ละกลยุทธ์การจัดการความเสี่ยงและการจัดทำแผนกลยุทธ์ฯที่ชัดเจนนำสู่การจัดทำแผนการจัดการ/ แผนปฏิบัติการการจัดการความเสี่ยงที่สอดคล้อง และมีการทบทวนในแต่ละรอบของการประเมินฯ
3. จัดทำรายงานการประเมินผลการดำเนินการตามแผนการจัดการ/ แผนปฏิบัติการจัดการความเสี่ยง และนำมาวิเคราะห์แนวโน้ม สรุปบทเรียนตามแนวทาง PDCA เพื่อปรับปรุง จัดทำแผนต่อไป เพื่อให้ความเสี่ยงลดลงได้ต่อเนื่อง

3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

นโยบายและระเบียบปฏิบัติ	มีการจัดทำประกาศนโยบายแต่ขาดความเข้าใจถึงเจตน์จำนงค์ที่ให้ผู้ที่เกี่ยวข้องกับโรงพยาบาลิ ทั้งผู้ป่วย ญาติผู้ป่วย เจ้าหน้าที่ คู่สัญญาภายนอกคือผู้ที่ต้องได้รับรู้แนวทางและจุดยืนของโรงพยาบาล มีระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ปี 2568
การป้องกันมิให้ผู้ที่ไม่ได้ทำหน้าที่ดูแลผู้ป่วยรายใดเข้าถึงข้อมูลผู้ป่วยรายนั้น	ขาดการแสดงให้เห็นว่ามี การกำหนดให้มีการป้องกันมิให้ผู้ที่ไม่ได้ทำหน้าที่ดูแลผู้ป่วยในปัจจุบันเข้าถึงข้อมูลผู้ป่วยรายนั้น
การป้องกันความลับของผู้ป่วยอย่างเคร่งครัด	มีการกำหนดไว้ในนโยบายรักษาความปลอดภัยของข้อมูล ระเบียบปฏิบัติด้านการรักษาความมั่นคงปลอดภัยฯในการห้ามเปิดเผยข้อมูลผู้ป่วย
การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติ	One page สื่อสารทางไลน์กลุ่มหน่วยงาน, ติดประกาศในแผนก, สื่อสารผ่านทางหัวหน้างานแจ้ง, หน้าข่าวประชาสัมพันธ์ในเว็บไซต์โรงพยาบาล และแจ้งผ่านในที่ประชุม
บุคลากรทุกคนของโรงพยาบาลเข้าใจ และจดจำระเบียบปฏิบัติที่สำคัญได้อย่างถูกต้อง	มีการประเมินผ่าน Google form แบบ self report สอบถามบุคลากรในหน่วยงานส่วนใหญ่รับรู้และมีความเข้าใจ
บุคลากรทุกคนของโรงพยาบาลปฏิบัติตามระเบียบอย่างเคร่งครัด	มีเพียงการประเมินผ่าน Google form แบบ self report จากการประเมินเมื่อลงพื้นที่สามารถปฏิบัติได้เป็นส่วนใหญ่
Data Center ที่ได้เกณฑ์มาตรฐาน	มีการควบคุมกำกับตามมาตรฐานห้อง Data center บางส่วน และรับรู้ในประเด็นอื่นๆที่ต้องดำเนินการต่อไป

จุดเด่น

การดำเนินการด้านการจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ที่แสดงเริ่มมีความเข้าใจและดำเนินการสอดคล้องตามแนวทางมาตรฐานได้บางส่วน

ความท้าทายและโอกาสพัฒนา

1. ทบทวนความเข้าใจและวัตถุประสงค์ของ นโยบาย แนวปฏิบัติ และระเบียบปฏิบัติด้านความมั่นคงปลอดภัยฯ ตามเจตน์จำนง เพื่อจัดทำประกาศได้อย่างถูกต้อง และทบทวนทุกปี
2. ทบทวนและให้ความสำคัญกับการประเมิน การรับรู้ ความเข้าใจ และการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของ**บุคลากรทุกคน โดยเฉพาะทบทวนแนวทางการประเมินการปฏิบัติรายบุคคล**
3. พัฒนาและดำเนินการตาม “แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอรสำหรับโรงพยาบาลของรัฐ” (HAIT Plus) นำสู่การปฏิบัติตามบริบท และนโยบาย Cyber security, PDPA และการสำรองข้อมูล ตามประกาศกระทรวงสาธารณสุข
4. ปรับปรุง Data Center และจัดทำคู่มือการปฏิบัติในสถานการณ์ฉุกเฉินที่ชัดเจน
5. ทบทวนความเข้าใจการจัดทำ ผู้ที่เกี่ยวข้อง และซ้อมแผน BCP และ DRP เพื่อ**รองรับภัยทางไซเบอร์**

4. การจัดระบบบริการเทคโนโลยีสารสนเทศโรงพยาบาล

การจัดระบบ Service Desk	จุดบริการ: อาคารผู้ป่วยนอก ชั้น 4 ห้องคอมพิวเตอร์ ติดต่อทางโทร. 4412 ในเวลาราชการ: 08.30-16.30 น., นอกเวลาราชการ: 16.30 – 20.30 น. วันหยุดราชการ ตั้งแต่ 08.30-16.30 น. จุดให้บริการข้อมูลทางสถิติ: อาคารผู้ป่วยใน ชั้น 2 กลุ่มงานสุขภาพดิจิทัล เวลา 08.30-16.30 น., ในเวลาราชการ: 08.30-16.30 น. ติดต่อทาง. 341 *ข้อสังเกต การแจ้งเลขโทร. ในเอกสาร โทร. 4412 กับ 341 ส่วนใน One page ระบุเพียง โทร. 341
การกำหนด Service Level Agreement ให้ครบทุกด้านที่สำคัญ	มีการกำหนด SLA ด้าน Hardware, การใช้งานโปรแกรม HIS, Network และ Internet ที่ยังไม่ได้เป็นหัวข้อในมุมมองผู้ใช้งานในบางข้อ
การติดตามผลการดำเนินงานตาม Service Level Agreement	มีการติดตามผลการดำเนินงานตาม SLA
การวิเคราะห์ผลการดำเนินงานตาม Service Level Agreement และนำผลมาปรับปรุงบริการให้ดีขึ้น	ขาดการวิเคราะห์ ผลการดำเนินงานตาม Service Level Agreement และนำผลมาปรับปรุงบริการให้ดีขึ้น
ระบบ Event และ Incident Report	มีการจัดเก็บข้อมูลในระบบแจ้งซ่อม (Incident report) และมีเริ่มมีการจัดทำสมุดบันทึกกิจกรรมรายวันสำหรับบุคลากร IT (IT Activity Report)

จุดเด่น

มีการกำหนดจุดบริการและช่องทางรับแจ้ง (Service Desk) ทั้งในเวลาราชการและนอกเวลาราชการ และเริ่มแสดงการกำหนด SLA ที่สำคัญสำหรับผู้ใช้บริการเป็นส่วนใหญ่

ความท้าทายและโอกาสพัฒนา

1. ทบทวนปรับข้อกำหนดและระยะเวลาประกันของ SLA เป็นมุมมองของ User
2. วิเคราะห์การดำเนินการแต่ละข้อของ SLA และนำมาปรับปรุงการดำเนินงานได้บรรลุเป้าหมาย
3. ปรับปรุงกระบวนการแจ้งปัญหา/ ความต้องการ เพื่อจัดเก็บข้อมูลใน Incident Report ให้ได้ครบถ้วน นำสู่การวิเคราะห์เพื่อการพัฒนาคุณภาพบริการของ IT
4. การจัดเก็บ IT Activity ที่ครอบคลุมกิจกรรมสำคัญที่บุคลากร IT ต้องปฏิบัติ และการวิเคราะห์ สู่การบริหารจัดการที่สอดคล้องกับบทบาทของแต่บุคคล ตามเป้าหมายของโรงพยาบาล

5. การกำกับดูแลควบคุมคุณภาพข้อมูลเวชระเบียน

การเก็บข้อมูลประวัติ ผลการตรวจร่างกาย คำวินิจฉัยโรค การทำหัตถการ การให้ยา การรักษา และรหัส ICD ของผู้ป่วยนอกและผู้ป่วยในทุกราย ในระบบเวชระเบียน	มีการเก็บข้อมูลประวัติ ผลการตรวจร่างกาย คำวินิจฉัยโรค การทำหัตถการ การให้ยา การรักษา และรหัส ICD ของผู้ป่วยนอกและผู้ป่วยในทุกรายในระบบเวชระเบียน : **ผู้ป่วยนอก:** วัน/เวลา 100 % อาการสำคัญ 85% ประวัติการเจ็บป่วย 67 % การตรวจร่างกาย 40.50% คำวินิจฉัยโรค 54.50% การรักษา 92% และคุณภาพรหัส ICD ผู้ป่วยนอก 81% **ผู้ป่วยใน:** DS1 86.07% DS2 100 % บันทึกประวัติ 75% การตรวจร่างกาย 71.43% Progress Note 75.36% Nurse's note 75% และคุณภาพรหัส ICD ผู้ป่วยใน 94.74%
ระบบตรวจสอบความครบถ้วน (สมบูรณ์) ของเวชระเบียนผู้ป่วยนอก และผู้ป่วยใน	มีระบบตรวจสอบความครบถ้วน(สมบูรณ์) ของเวชระเบียนผู้ป่วยนอกและผู้ป่วยใน โดยมีคณะผู้ตรวจสอบคุณภาพเวชระเบียน ประกอบด้วย ทีมแพทย์ พยาบาลทุกแผนก เจ้าที่เวชสถิติ และนักกายภาพ ตามคู่มือการตรวจสอบและควบคุมคุณภาพข้อมูล สำนักนโยบายและยุทธศาสตร์ 2558
ระบบตรวจสอบคุณภาพการเขียนหรือบันทึกคำวินิจฉัยโรคของแพทย์ในเวชระเบียนผู้ป่วยนอกและผู้ป่วยใน	เริ่มมีระบบตรวจสอบคุณภาพการเขียนหรือบันทึกคำวินิจฉัยโรคของแพทย์ ในเวชระเบียนผู้ป่วยนอกและผู้ป่วยใน
ระบบตรวจสอบคุณภาพรหัส ICD ผู้ป่วยนอกและผู้ป่วยใน	มีระบบตรวจสอบความครบถ้วน(สมบูรณ์) คุณภาพรหัส ICD ผู้ป่วยนอกและผู้ป่วยใน
การวิเคราะห์ประวัติ ผลการตรวจร่างกาย คำวินิจฉัยโรค การทำหัตถการ การให้ยา การรักษา และรหัส ICD ของผู้ป่วยนอกและผู้ป่วยใน เพื่อหาทางพัฒนาคุณภาพการบริการ หรือเพิ่มความปลอดภัยของผู้ป่วย	เริ่มมีการวิเคราะห์ประวัติ ผลการตรวจร่างกาย คำวินิจฉัยโรค การทำหัตถการ การให้ยา การรักษา และรหัส ICD ของผู้ป่วยนอกและผู้ป่วยใน เพื่อหาทางพัฒนาคุณภาพการบริการ หรือเพิ่มความปลอดภัยของผู้ป่วย
การนำผลการวิเคราะห์คุณภาพข้อมูลผู้ป่วยนอกและผู้ป่วยในมาดำเนินการจัดการปัญหา หรือ ปรับระบบการควบคุมคุณภาพข้อมูลให้ดีขึ้น	มีการนำผลการวิเคราะห์คุณภาพข้อมูลผู้ป่วยนอกและผู้ป่วยใน มาดำเนินการจัดการปัญหาหรือปรับระบบการควบคุมคุณภาพข้อมูลให้ดีขึ้นบางส่วน

จุดเด่น

เริ่มการให้ความสำคัญในการเก็บข้อมูลประวัติ ผลการตรวจร่างกาย คำวินิจฉัยโรค การทำหัตถการ การให้ยา การรักษา และรหัส ICD ของผู้ป่วยนอกและผู้ป่วยใน ในระบบเวชระเบียนและมีระบบตรวจสอบ

คุณภาพข้อมูลของเวชระเบียน และระบบตรวจสอบคุณภาพการให้รหัส ICD ที่เข้มแข็งรวมถึงมีการพัฒนาคุณภาพในการบันทึกเวชระเบียนทั้งในภาพรวมของโรงพยาบาล

ความท้าทายและโอกาสพัฒนา

1. ศึกษา ทำความเข้าใจดำเนินการตรวจสอบ และพัฒนาคุณภาพข้อมูลตามแนวทางของสนย. ให้คุณภาพเวชระเบียนทั้งผู้ป่วยนอกและผู้ป่วยในทุกประเด็นคุณภาพได้ไม่น้อยกว่า 80% และสามารถยกระดับสู่ 95% ในอนาคตได้
2. เพิ่มช่องทาง/ รูปแบบการสื่อสารระหว่างทีมคุณภาพ ฝ่าย IT และผู้ใช้ เกิดความร่วมมือและมีความเข้าใจตรงกันเพิ่มขึ้น
3. พัฒนาความต่อเนื่อง และความถี่ในการตรวจสอบคุณภาพข้อมูลประวัติ ผลการตรวจร่างกาย คำวินิจฉัยโรค การทำหัตถการ การให้ยา การรักษา และรหัส ICD ของผู้ป่วยนอกและผู้ป่วยใน
4. พัฒนาวิธีการใช้ประโยชน์จากข้อมูลเวชระเบียน ได้แก่ ประวิติ ผลการตรวจร่างกาย คำวินิจฉัยอื่น ๆ มาปรับปรุงคณภาพการให้บริการผู้ป่วยให้ดียิ่งขึ้น

6. การควบคุมคุณภาพการพัฒนาโปรแกรม

การวิเคราะห์และออกแบบระบบก่อนการพัฒนาโปรแกรม	NA
เอกสารผลการวิเคราะห์และออกแบบระบบขั้นพื้นฐาน	NA
การเขียน Comment ใน Source Code และการบันทึกการเปลี่ยนแปลง (version control)	NA
กระบวนการจัดการความต้องการของผู้ใช้ (Requirement Management)	NA
กระบวนการจัดการการพัฒนาโปรแกรมให้เป็นไปตามกำหนดการ (Project Management)	NA
กระบวนการทดสอบโปรแกรมที่ได้มาตรฐานก่อนส่งมอบให้ผู้ใช้ (Function Test, Usability Test)	NA
คู่มือการใช้โปรแกรม	NA

จุดเด่น

-

ความท้าทายและโอกาสพัฒนา

-

7. การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

การวิเคราะห์สถานการณ์ปัจจุบันและ การทำ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร	-มีการจัดทำทะเบียนทรัพยากร IT แต่ยังไม่ครอบคลุมทุกรายการในกลุ่มอุปกรณ์ (Hardware), Software, Network และในประเด็น Capacity สำคัญที่ควรต้องบันทึก -การทำ Gap Analysis จากการใช้งานปัจจุบัน ไม่ครอบคลุมทุกรายการ และขาดการระบุรายละเอียดการใช้ (Utilization) หรือสมรรถนะของเป้าหมายที่ชัดเจน
การจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network,	แสดงแผนพัฒนาด้าน Hardware, Software, Network และบุคลากรบางส่วนแต่ขาดความชัดเจน
การกำหนดสมรรถนะที่จำเป็น (Technical Competency) ของ บุคลากรในฝ่าย IT	มีการ**กำหนดสมรรถนะ**บางส่วน ขาดด้าน Cybersecurity และ PDPA ครอบคลุม CIO และบุคลากรกลุ่มงานสุขภาพดิจิทัล
การดำเนินการตามแผนเพิ่มศักยภาพ และการประเมินวิเคราะห์ผลการดำเนินตามแผน	มีการวางแผนพัฒนาสมรรถนะบุคลากร แต่ขาดความชัดเจนความสอดคล้องตาม Gap analysis และขาดการแสดงผลประเมินวิเคราะห์ผลการดำเนินที่ทำตามแผนไปแล้ว
มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น	ยังไม่ได้ดำเนินการ

จุดเด่น

เริ่มมีการจัดทำตามกรอบแนวทางการพัฒนา ของการจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ ตามแนวทางพัฒนาคุณภาพ

ความท้าทายและโอกาสพัฒนา

1. การจัดเก็บทะเบียนทรัพยากร IT ให้ครอบคลุม
2. การทบทวนความเข้าใจ ความสำคัญ และการวิเคราะห์ ของการจัดทำทะเบียนฯ ตามคุณค่าเพื่อการนำมาใช้ของแต่ละอุปกรณ์
3. การทบทวนจัดการเพื่อการจัดทำ competency ตามบทบาทหน้าที่ของแต่ละบุคลากร

ข้อเสนอแนะการพัฒนาคุณภาพ

กิจกรรมที่ควรดำเนินการ ☑ขอประเมินใหม่ ☑*ภายใน 180 วัน เพื่อขอโอกาสได้รับการรับรอง

ภาพรวม ศึกษาและทำความเข้าใจ TMI Hospital IT Maturity Model

1. แผนแม่บทเทคโนโลยีสารสนเทศโรงพยาบาล

1.1 จัดทำ/แสดงเอกสารเล่มแผนยุทธศาสตร์ของโรงพยาบาล และเล่มแผนแม่บท IT ที่ระบุช่วงระยะเวลา และเพิ่มเติมการแสดงสารบัญ ของแต่ละแผนให้เห็นอย่างชัดเจน

1.2 ในเล่มแผนแม่บท IT ให้เพิ่มเติมระบุค่าเป้าหมายและผลงานที่ผ่านมาของตัวชี้วัดในแต่ละยุทธศาสตร์ของโรงพยาบาล ในตารางความเชื่อมโยงระหว่างยุทธศาสตร์โรงพยาบาล กับเป้าหมาย IT ก่อนนำสู่แผนแม่บท IT

1.3 ทบทวนการวิเคราะห์ปัจจัยแห่งความสำเร็จ ที่สนับสนุนให้ตัวชี้วัดเกิดผลสำเร็จ ตอบสนองตามเป้าหมายของยุทธศาสตร์โรงพยาบาล

1.4 กำหนดตัวชี้วัดของแผนแม่บท IT ให้เน้นตัวชี้วัดเชิงกระบวนการ (Process indicator) และตัวชี้วัดเชิงผลลัพธ์ (Outcome indicator) มากขึ้น

1.5 จัดทำเล่มแผนให้มีรูปเล่มสมบูรณ์ของแผนแม่บท IT ที่แสดงให้เห็นช่วงระยะเวลาของแผนฯอย่างชัดเจน และมีแผนปฏิบัติงาน โครงการ ตัวชี้วัด ผู้รับผิดชอบ ที่มีการจัดลำดับความสำคัญและระยะเวลาดำเนินโครงการในแผนปฏิบัติการ พร้อมแสดงให้เห็นทีมงาน ผู้เกี่ยวข้อง ที่เข้าร่วมการจัดทำ รวมถึงช่องทาง/รูปแบบเพื่อการถ่ายทอดแผนฯ IT สู่ผู้ปฏิบัติ

1.6 ปรับปรุงตามคู่มือ HAIT

2. การจัดการความเสี่ยง

2.1 ทบทวนความเข้าใจระหว่างการจัดการความเสี่ยง กับ การจัดการอุบัติการณ์

2.2 ทบทวนและแสดงการค้นหาความเสี่ยงตามแบบประเมินจุดอ่อนในระบบเทคโนโลยีสารสนเทศ พัฒนาโดยสมาคมเวชสารสนเทศไทย ปี 2565, ให้เข้าใจเกณฑการให้คะแนน 0, 1 พร้อมระบุวันที่ประเมินให้ชัดเจนแต่ละรอบ

2.3 ระบุรหัสความเสี่ยงให้สอดคล้องในทุกที่ของเอกสาร

2.4 ทบทวนการให้ค่าคะแนนโอกาสที่จะเกิดความเสี่ยง ตามแบบการค้นหาจุดอ่อน/ช่องโหว่ และการกำหนดค่าผลกระทบที่ใช้ในการประเมินความเสี่ยงที่ต้องการใช้ให้ชัดเจน

2.5 เพิ่มเติมรายละเอียด ข้อ 6.3 PDPA Implementation ที่ต้องทำในแบบประเมินช่องโหว่ ต้องระบุกิจกรรมที่สอดคล้องตามนโยบายของกระทรวงสาธารณสุขที่ประกาศให้สอดคล้องตาม Policy ได้แก่ 1) Privacy Notice 2)RoPA (Record of Processing Activities) 3) DPA (Data Processing Agreement)

2.6 ทบทวนและทำความเข้าใจการวางแผนกลยุทธ์จัดการความเสี่ยง โดยนำแต่ละ IT component และข้อที่เป็นช่องโหว่ มากำหนดแผนกลยุทธ์ฯและมาตรการควบคุม

2.7 ต้องดำเนินการและจัดทำเป็น**เอกสารให้เห็นรายละเอียดเชิงประจักษ์** โดยเฉพาะหัวข้อ“ตรวจสอบและบำรุงรักษาเป็นประจำ”และ “กำกับดูแลโดยผู้บังคับบัญชา” ว่ามีการปฏิบัติ รายละเอียดรูปแบบ/ช่องการการสื่อสารให้ผู้เกี่ยวข้องรับทราบ เป็นต้น

2.8 จัดทำแผนปฏิบัติการจัดการความเสี่ยง มีรายละเอียดโครงการ ชื่อโครงการ ระยะเวลา งบประมาณ ผู้รับผิดชอบที่ชัดเจน ที่สอดคล้องมาตรการควบคุมความเสี่ยงตามกลยุทธ์ รวมทั้งแสดงจำนวนปริมาณ ประสิทธิภาพในมิติใดๆนั้น ให้มีรายละเอียดสอดคล้องกับการประเมินความเสี่ยงที่ค้นพบแล้วดำเนินการตามแผนการจัดการความเสี่ยง

2.9 จัดลำดับ Risk matrix, และเรียงลำดับจากคะแนนความเสี่ยงจากมากสุดไปน้อยสุด

2.10 จัดทำหน้าสรุปการประเมินคะแนนความเสี่ยงในแต่ละรอบและแสดงให้เห็นว่า**ความเสี่ยงลดลง**

2.11 ใช้หลักการ PDCA แสดงให้เห็นการพัฒนาการประเมินผลการจัดการความเสี่ยง เพื่อนำผลมาปรับปรุงจัดทำแผนปฏิบัติการจัดการความเสี่ยงใหม่

2.12 จัดทำเล่มแผนบริหารความเสี่ยง ที่ระบุสารบัญ ช่วงเวลาของการจัดทำ พร้อมแสดงให้เห็นทีมงานผู้เกี่ยวข้องที่เข้าร่วมการจัดทำ และมีรายละเอียดตามข้อกำหนดตามแนวทางให้ครบถ้วน

3. การจัดการด้านความมั่นคงปลอดภัย

3.1 ทบทวนการจัดทำและสื่อสาร “นโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” ของโรงพยาบาลถึงทุกฝ่ายที่เกี่ยวของกับโรงพยาบาล: ผูปวย ญาติ เจ้าหนาที่ทุกฝ่ายในโรงพยาบาล และคูสัญญาภายนอกของโรงพยาบาลไดรับรู้แนวทางและจุดยืนของโรงพยาบาล

3.2 จัดทำการกำหนดคาขั้นต่ำดานความมั่นคงปลอดภัย (Security Baseline Configuration Standards) และทบทวนช่องโหว่จากความเสี่ยง นำสู่การกำหนดหัวข้อการจัดทำระเบียบปฏิบัติ

3.3 ทบทวนหัวข้อการจัดทำระเบียบปฏิบัติและเพิ่มเติมที่ต้องมี “ห้ามการเข้าถึงข้อมูลผู้ป่วย ที่ไม่ได้อยู่ในความรับผิดชอบในช่วงเวลาปัจจุบัน” และระบุ version หรือ วันที่ประกาศใช้ให้ชัดเจน

3.4 ประชาสัมพันธ์ พร้อมสร้างความตระหนักและความรับรู้และเข้าใจของบุคลากร **ทุกคน** รวมถึง Outsource ที่ทำงานในเครือข่ายของโรงพยาบาล

3.5 ทบทวนการประเมิน และแสดงให้เห็นว่าใช้รูปแบบ และกระบวนอย่างไรในการประเมิน ทั้งการรับรู้เข้าใจ และการปฏิบัติ ตามระเบียบปฏิบัติด้านความมั่นคงรายข้อ

3.6 ปรับปรุงห้อง Datacenter ตามมาตรฐาน (โดยปรับปรุงตามคู่มือแนวทางฯ) โดยเฉพาะเพิ่มเติมคู่มือการปฏิบัติที่ครบถ้วนชัดเจน สามารถให้ผู้เกี่ยวข้องปฏิบัติงานแทนได้

การจัดการทางกายภาพ

1. จัดวางอุปกรณ์ให้สามารถเดินโดยรอบได้ และนำวัสดุที่เป็นเชื้อไฟออกจากห้อง
2. จัดทำบันทึกการเข้าออกของบุคลากรทั้งภายใน - ภายนอก

3. ทบทวนตำแหน่งการวัดที่ให้ครอบคลุมทุกตู้, ระบุช่องทางและขั้นตอนการแจ้งและมีแนวทางปฏิบัติเมื่อเกิดเหตุการณ์
4. คู่มือปฏิบัติที่เกี่ยวข้องการจัดการในห้องให้ครอบคลุม เพื่อให้ปฏิบัติงานแทนกันได้ เช่น ระบบแจ้งเตือนอัคคีภัยสำหรับงาน IT และหรือผู้รับผิดชอบ Data center และผู้ประสบเหตุที่ไม่ใช่ IT
5. จัดทำ Checklist และคู่มือการตรวจสอบในห้อง Data Center
6. ทบทวนการจัดเตรียมเครื่องดับเพลิงและมีการซ้อมการใช้
7. มีขั้นตอนการปฏิบัติที่ชัดเจน และความถี่เพื่อการกำกับดูแลความสะอาดอย่างสม่ำเสมอ

การจัดระเบียบของอุปกรณ์และสายสัญญาณ

8. จัดสายสัญญาณให้เป็นระเบียบเรียบร้อย ไม่เป็นขยุ้ม ไม่กองบนพื้น รวมถึงสายที่พาดบนอุปกรณ์
9. จัดทำ Label สายสัญญาณให้ครบทุกเส้น และจัดทำป้ายกำกับสายสัญญาณทุกเส้นให้รู้ว่าเป็นสายที่มาจากที่ใด ต่อไปที่ใด
10. จัดทำแผนผังระบุตำแหน่งของสายสัญญาณและช่องสัญญาณทุกช่อง
11. จัดทำป้ายกำกับ server ทุกเครื่อง รวมถึงอุปกรณ์เครือข่าย หรืออุปกรณ์หลักอื่นๆให้ครบถ้วน

ระบบคงทนต่อความผิดพลาดและระบบความมั่นคงพื้นฐาน

12. จัดทำการสำรองข้อมูลแบบ offline ให้ครบถ้วนสมบูรณ์ เพิ่ม HDD แบบจานแม่เหล็กเพื่อเก็บข้อมูลรายเดือน/ รายปี ของ server ที่เก็บข้อมูลทุกตัว และพิจารณาการเลือกเทคโนโลยีของอุปกรณ์การจัดเก็บไม่น้อยกว่า 2 เทคโนโลยี และมีจำนวนที่เหมาะสมที่บริหารความเสี่ยงต่อการสูญหายของข้อมูล
13. จัดเก็บ Hard disk ในตู้ที่มั่นคงปลอดภัย
14. ทบทวนระบบคงทนต่อความผิดพลาดต่างๆ ของ backbone
15. จัดทำแผนผังระบบเครือข่ายที่มีรายละเอียดครบถ้วน
16. เก็บบันทึกข้อมูลการตั้งค่า firewall (Policy) เพื่อให้มั่นคงปลอดภัยป้องกันการโจมตีจากภายนอก
17. ทบทวนการจัดเก็บ log ข้อมูลการติดต่อภายนอกและเหตุการณ์สำคัญ

การควบคุมการดำเนินงานที่เกี่ยวข้องกับ Data Center

18. จัดทำคู่มือการสำรองข้อมูล และการตรวจสอบฯ สำหรับการปฏิบัติรายวันของผู้ดูแลระบบ
19. ทำการตรวจสอบ การสำรองว่าเป็นข้อมูลที่ไม่เสียหาย นำกลับมาใช้ได้เมื่อเกิดเหตุ
20. ตรวจสอบอุปกรณ์สำคัญต่างๆ การเฝ้าติดตามการใช้ทรัพยากรระบบ เหตุการณ์ต่างๆ

3.7 ทบทวนการจัดทำ **BCP (Business Continuity Plan)**

3.7.1 มีคู่มือของแต่ละหน่วยงานที่มีการใช้งานในระบบใดๆผ่านทางระบบเครือข่าย ที่มีรายละเอียดที่ให้บุคลากรจากที่อื่นทำตามได้ และประเมินได้ว่าแต่ละประเภทการบริการใช้เวลาเท่าใดต่อคน เพื่อนำสู่การประเมินการใช้ทรัพยากร/ เวลา ต่อผู้รับบริการได้อย่างเหมาะสม

3.7.2 ทบทวนเอกสารที่ต้องใช้ในระหว่างสถานการณ์ ที่มีข้อมูลครบถ้วนครบถ้วนตามที่ต้องนำข้อมูลเข้าระบบ (เพื่อความครบถ้วนของข้อมูลคุณภาพ/ เรียกเก็บ)

3.7.3 มีการซ้อมแผนในสถานการณ์ Cyber Attack

3.7.4 จัดทำรายงานผลการซ้อมและแผนการปรับปรุงฯ

3.8 จัดทำและซ้อมแผน **DRP (Disaster Recovery Plan)**

3.8.1 ครอบคลุมทั้งในระดับแม่ข่าย และเครื่องลูกข่าย

3.8.2 แสดงขั้นตอนการปฏิบัติที่ละเอียด ตั้งแต่การจัดเตรียมเครื่อง - เครื่องกลับมาใช้งานได้ พร้อมแสดง ระยะเวลาของแต่ละขั้นตอน และเวลารวม

3.8.3 จัดทำการวิเคราะหผลกระทบทางธุรกิจ (Business Impact Analysis -BIA) เพื่อนำสู่การกำหนดกระบวน BCP และ DRP

3.8.4 มีการซ้อมแผนในสถานการณ์ Cyber Attack แสดงให้เห็นภาพของการซ้อม

3.8.5 จัดทำรายงานการซ้อมที่ครบถ้วนสมบูรณ์ และแสดงผลหลังประเมินหลังการซ้อม เพื่อปรับปรุงแผนให้ชัดเจนนำสู่การปฏิบัติได้ โดยเฉพาะหากเกิดเหตุการณ์ที่เกี่ยวข้องกับ IPD paperless

3.8.6 จัดตั้งคณะทำงาน Incident Response และจัดทำแผน Incident Response Plan (IRP)

3.9 **(HAIT) PLUS**

3.9.1 ทบทวนระเบียบปฏิบัติด้านความมั่นคงปลอดภัยจากที่ไม่สามารถควบคุมได้จากระบบใดๆ (จาก Security Baseline Configuration Standard) โดยให้มีความกระชับชัดเจน ลดการตีความ

3.9.2 ทบทวนระบบการสำรองข้อมูลแบบ Offline ในระบบงานหลัก (รวมถึงระบบ PACS และ LIS) ทั้งความครบถ้วน ถูกต้องของข้อมูล และทบทวนความถี่ที่เหมาะสมของข้อมูลที่จัดเก็บ (ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย RPO: Recovery Point Object รวมถึงระบุระยะเวลาที่ใช้ในการกู้คืน RTO: Recovery Time Object) และจัดเก็บอุปกรณ์สำรองข้อมูลในพื้นที่ปลอดภัย เพื่อรองรับความปลอดภัยระบบสารสนเทศและทาง Cyber รวมถึงมีรายงานผลการทดสอบในการกู้คืนจาก Backup offline

3.9.3 ทบทวนการดูแลระบบของ Outsource โดยเฉพาะด้านความปลอดภัยของระบบ เช่น การรักษาความลับ การ update ระบบปฏิบัติการของอุปกรณ์ เป็นต้น

4. **การจัดการระบบบริการ**

4.1 Service Desk

- ทบทวนช่องทางรับแจ้ง และหรือมีกระบวนการที่ให้สามารถทุกการรับแจ้งอยู่ในระบบการจัดเก็บการรับแจ้งได้ครบถ้วน

Service Level Agreement (SLA)

4.2 แสดงให้เห็นผู้ใช้งานเข้าร่วม ในการกำหนดหัวข้อตกลงระดับบริการ SLA และเวลา

4.3 ทบทวนกระบวนการ และผู้เข้าร่วมในการกำหนด SLA ให้เหมาะสมและชัดเจนมากขึ้น และกำหนดรายการในข้อตกลงระดับบริการและเวลาใน SLA ให้เป็นมุมมอง/ ภาษา ของ User เพื่อให้เกิดประโยชน์ต่อการบริการมากที่สุด

4.4 แสดงวันที่ประกาศใช้และจุดบริการกายภาพ ใน One page และที่ผ่านช่องทางต่างๆให้บุคลากรรับทราบ

4.5 วิเคราะห์ผลการดำเนินการตามขอตกลงระดับบริการ SLA แต่ละข้อ อัตราความสำเร็จ เวลามากสุด เวลาน้อยสุด เวลาเฉลี่ย นำมาเป็นแนวทางในการแก้ปัญหาเพื่อให้การดำเนินการตามข้อตกลงได้บรรลุเป้าหมาย

Incident Report

4.6 แสดงการวิเคราะห์และบันทึกสาเหตุของปัญหา และรายงานทางสถิติ เพื่อวิเคราะห์แนวโน้มการเปลี่ยนแปลง เกิดขึ้นที่ไหน เพิ่มขึ้น ลดลง หรือเท่าเดิม มีการนำผลมาวางแผนพัฒนาปรับปรุงการบริการในมิติ Incident management

IT Activity Report

4.7 ทบทวนการจัดทำระบบ IT Activity Report เป็น electronic และ ให้ครอบคลุมประเภทกิจกรรมที่เจ้าหน้าที่หน่วย IT **ในแต่ละบทบาทที่มีการปฏิบัติ** ตามสัดส่วนเวลาของวันทำงาน 8 ชั่วโมง โดยกำกับดูแลให้เจ้าหน้าที่ IT **ทุกคน** บันทึก**ทุกวัน** มีการจำแนกประเภทกิจกรรมตามสัดส่วนเวลาของแต่ละคน เพื่อนำผลมาวิเคราะห์และวางแผนพัฒนารายบุคคลให้สอดคล้องตามบทบาทความรับผิดชอบ

5. การพัฒนาคุณภาพข้อมูล

เวชระเบียนผู้ป่วยนอก

5.1 ผลการตรวจสอบคุณภาพ

วัน/เวลา ≥80%	CC ≥80%	ประวัติ ≥80%	ตรวจร่างกาย ≥80%	คำวินิจฉัย ≥80%	การรักษา ≥80%	คุณภาพรหัสโรค ≥80%	คะแนนภาพรวม ≥80%
100	85	67	40.50	54.50	92	81	66.29
☑	☑	☒	☒	☒	☑	☑	

โดย**ข้อที่ต้องปรับปรุงและส่งรายงานต่อคณะกรรมการ คือ** ทบทวนการบันทึกคำวินิจฉัยและการรักษา ตามหลักเกณฑ์ของสนย.

5.1.1 พัฒนาระบบบันทึกผู้ป่วยนอก

5.1.1.ก พัฒนาการบันทึกประวัติ

5.1.1.ข ในส่วนของผลการตรวจร่างกายโดยวิชาชีพ ทดแทนการใช้การตั้งโปรแกรมการตรวจร่างกายอัตโนมัติ

5.1.1.ค พัฒนาระบบบันทึกคำวินิจฉัยโรคของแพทย์ ให้ครอบคลุมทุกโรคที่เป็นในปัจจุบัน มีรายละเอียดที่ต้องระบุ ความรุนแรง เช่น Acute/Chronic, ระบุตำแหน่งของโรคโรค/อวัยวะ แทนการใช้คำอธิบายความหมายของรหัส ICD

เวชระเบียนผู้ป่วยใน

5.2 ผลการตรวจสอบคุณภาพ

DS1 ≥80%	DS2 ≥80%	HX ≥80%	PE ≥80%	Progress Note ≥80%	OP ≥80%	OB ≥80%	Nurse's Note ≥80%	คุณภาพรหัสโรค ≥80%	คะแนนภาพรวม ≥80%
86.07	100	75.00	71.43	75.36	NA	NA	75	94.74	79.63
☑	☑	☒	☒	☒	■	■	☒	☒	

โดย**ข้อที่ต้องปรับปรุงและส่งรายงานต่อคณะกรรมการ คือ**

5.2.1 ประวัติการเจ็บป่วยในส่วนที่ควรปรับปรุง Review of System ให้ยกเลิกการกำหนดค่า default เป็น normal โดยศึกษาแนวทางจากคู่มือของสนย. ดูตัวอย่างการบันทึกได้จากภาคผนวกท้ายเล่มหนังสือการตรวจสอบคุณภาพและควบคุมคุณภาพข้อมูลในระบบบริการสุขภาพด้านการบันทึกข้อมูลผู้มารับบริการและการให้รหัสICD สำนักนโยบายและยุทธศาสตร์ 2558

5.2.2 ประวัติการเจ็บป่วยในส่วนของ Review of System ยกเลิกเช็คลิสต์ระบุผลการตรวจที่เป็น Normal ให้แพทย์

5.2.3 พัฒนาการบันทึก Progress note ตามแนวทาง SOAP

5.2.4 พัฒนาระบบ Nurse's note การบันทึกข้อมูลผู้ป่วยทั้งก่อนและหลังให้การพยาบาล และนำข้อมูลมาประเมินผลการพยาบาลให้สอดคล้องกับปัญหาทางการพยาบาล

6. การพัฒนาคุณภาพโปรแกรม

-

7. การจัดการศักยภาพและสมรรถนะ

Capacity Management

7.1 จัดทำบัญชีรายการทรัพย์สินให้ครอบคลุมทบทวนทุกรายการ และแสดงให้เห็นหัวข้อรายละเอียดที่จัดเก็บของแต่ละกลุ่มรายการ **พิจารณาคุณสมบัติที่จำเป็นต้องทราบเพื่อการบริหารจัดการ/ วางแผน*

7.2 แบ่งกลุ่มทะเบียน Software: กลุ่มระบบปฏิบัติการ, กลุ่มโปรแกรมสำนักงาน, กลุ่มโปรแกรมสำเร็จรูปอื่นๆ, กลุ่มโปรแกรมป้องกันไวรัส และกลุ่มโปรแกรมที่พัฒนาเอง (หากมี) พร้อมทั้งที่มีการระบุชื่อ/ Version, มี/ไม่มีลิขสิทธิ์ เป็นอย่างน้อย

7.3 ทบทวนการประเมินสถานการณ์การใช้ Capacity และ Utilization ของทรัพยากร Hardware, Software , Network (Internet-Intranet) มีการวิเคราะห์ Gap Analysis ที่มีการเปรียบเทียบกับเป้าหมายที่ต้องการ(Capacity) เพื่อนำสู่การกำหนดแผนเพิ่มศักยภาพ วางแผนจัดการ Capacity และ Utilization Management เช่น การตรวจสอบการใช้ทรัพยากร ในส่วนของอัตราการใช้ (Growth rate) พื้นที่จัดเก็บ อัตราการใช้ CPU, RAM และ อัตราการใช้ช่องส่งสัญญานในระบบเครือข่าย เป็นต้น

7.4 ดำเนินการแผนจัดการ Software ต่างๆ ให้ถูกลิขสิทธิ์ และ Activate license ทั้งระบบปฏิบัติการสำนักงาน และ โปรแกรมป้องกันไวรัส เพื่อความมั่นคงปลอดภัย โดยมีการจัดการ Update ระบบปฏิบัติการของเครื่องแม่ข่ายและลูกข่าย

Competency

7.5 ทบทวนการจัดทำ Competency: Core Competency, Functional Competency (Common ที่ทุกคนในหน่วย IT ต้องมีร่วมกัน, Job Competency ตามบทบาทหน้าที่ ที่รับผิดชอบ)

7.6 ทบทวน Functional competency ที่สนับสนุนการขับเคลื่อนยุทธศาสตร์องค์กร และเพิ่มเติมเรื่อง Cybersecurity, PDPA ทบทวนเกณฑ์ประเมิน Competency เพื่อให้เกิดการพัฒนาศักยภาพของบุคลากรด้านสารสนเทศ

7.7 ทบทวนการทำ Competency Dictionary ที่จำแนกตาม Core Competency, Common Functional Competency, Job Functional Competency)

7.8 เพิ่มเติมการทำ Competency Mapping แสดงค่าระดับความคาดหวังต่อแต่ละ Competency ทั้งผู้ที่มีบทบาทในบริบท ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง(CIO), หัวหน้ากลุ่มงานสุขภาพดิจิทัล และบุคลากรในกลุ่มงานสุขภาพดิจิทัล ที่ระบุบทบาทให้เห็นชัดเจน

7.9 เพิ่มเติมการทำ Individual Competency Profile ที่ครอบคลุม Core Competency, Functional Competency (Common Competency, Job Competency)

7.10 ทบทวนการให้ค่าคะแนนผลการประเมินที่นำสู่การประเมิน Gap analysis ได้, จัดทำแผนพัฒนาบุคลากรรายบุคคล (Individual Development Plan) ของบุคลากรในทุก Gap ที่ประเมินได้ และจัดทำแผนปฏิบัติการ ที่มีกำหนดระยะเวลาและแนวทางการติดตามผล ให้มีความชัดเจนและสอดคล้องกับเป้าประสงค์ที่ต้องการ

ผู้จัดทำรายงาน
นางภศิชา เธียรเชาวน์
28 มีนาคม 2568

ส่งงานและถามเพิ่มเติม ที่ pasicha@tmi.or.th กรุณาลงชื่อท้ายจดหมายด้วย

Link แนวทาง Slide นำเสนอการพัฒนาคุณภาพระบบเทคโนโลยี