การบริหารจัดการความเสี่ยงด้านสารสนเทศ

สถาบันราชานุกูล กรมสุขภาพจิต ปี 2565

2565

IT Risk Management

Rajanukul Institute

กระทรวงสาธารณสุข
MINISTRY OF PUBLIC HEALTH

กรมสุขภาพจิต
สถาบันราชานุกูล

www.rajanukul.go.th

การบริหารจัดการความเสี่ยงด้านสารสนเทศ

สถาบันราชานุกูล กรมสุขภาพจิต

กระทรวงสาธารณสุข

2565

สารบัญ

ความหมายของการบริหารความเสี่ยง 1

วัตถุประสงค์ 2

ขอบเขตการดำเนินการ........ 2

การประเมินความเสี่ยง

การวิเคราะห์ความเสี่ยง........ 3

ลักษณะรายละเอียดของความเสี่ยง........ 4

การประมาณความเสี่ยง

เกณฑ์การประมาณความเสี่ยง........ 7

การประมาณความเสี่ยง 8

การประเมินค่าความเสี่ยง

แผนภูมิความเสี่ยง........ 12

การประเมินค่าความเสี่ยง 13

การรายงานผลการวิเคราะห์ความเสี่ยง 16

การจัดการความเสี่ยง........ 17

ภาคผนวก

รายการเครื่องคอมพิวเตอร์และอุปกรณ์ในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย........ 21

รายการระบบสารสนเทศที่ติดตั้งในพื้นที่ความดูแลของฝ่ายสื่อสารองค์กรและเทคโนโลยี 33

การบริหารจัดการความเสี่ยงด้านสารสนเทศ
สถาบันราชานุกูล กรมสุขภาพจิต กระทรวงสาธารณสุข

เนื่องจากภารกิจของสถาบันราชานุกูลมีความหลากหลายเทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงานของสถาบัน จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของสถาบัน เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น การบริหารจัดการความเสี่ยงของสถาบัน โดยคณะกรรมการสารสนเทศนี้ มีวัตถุประสงค์เพื่อเป็นแนวทางที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของสถาบันด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงนั้นเกิดขึ้นจริงและนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในดำเนินการ

ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) **หมายถึง** เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) **หมายถึง** ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) **หมายถึง** กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) **หมายถึง** กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) **หมายถึง** นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) มีดังนี้

1. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
2. การระบุความเสี่ยงต่าง ๆ (Event Identification)
3. การประเมินความเสี่ยง (Risk Assessment)
4. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
5. กิจกรรมการบริหารความเสี่ยง (Control Activities)
6. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
7. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

วัตถุประสงค์

1. เพื่อให้การจัดการภายในสถาบันราชานุกูล มีประสิทธิภาพ และมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศ

2. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของสถาบันราชานุกูล

3. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ

4. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของคณะกรรมการสารสนเทศและกลุ่มงานเทคโนโลยีสารสนเทศ

การประเมินความเสี่ยง (Risk assessment)

การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของกรมสามารถแยกประเภทความเสี่ยงด้านเป็น 4 ประเภท ดังนี้

- **ความเสี่ยงด้านเทคนิค** เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

- **ความเสี่ยงจากผู้ปฏิบัติงาน** เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของสถาบันเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

- **ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน** เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น
- **ความเสี่ยงด้านการบริหารจัดการ** เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

ลักษณะรายละเอียดของความเสี่ยง (Description of risk) แสดงตามตาราง

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
1. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RI01	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RI02	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายของสถาบันโดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่ายของกรม ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของกรม	-การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย
3. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RI03	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
4. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RI04	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
5. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RI05	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RI06	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
7. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RI07	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ		ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ
8. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	RI08	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
9. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RI09	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ
10. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RI10	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
11. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RI11	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย

การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งสถาบันใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	5 ครั้ง/ปี
4	สูง	4 ครั้ง/ปี
3	ปานกลาง	3 ครั้ง/ ปี
2	น้อย	2 ครั้ง/ปี
1	น้อยมาก	ไม่เกิน 1 ครั้ง/ปี
ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	> 10 ล้านบาท หรือ เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความ ปลอดภัยของข้อมูลต่างๆ
4	สูง	> 5 แสนบาท – 10 ล้านบาท หรือ เกิดปัญหากับระบบ IT ที่สำคัญ และระบบ ความปลอดภัยซึ่งส่งผลต่อความถูกต้องของ ข้อมูลบางส่วน
3	ปานกลาง	> 2.5 แสนบาท – 5 แสนบาท หรือ ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	> 1 แสนบาท – 2.5 แสนบาท หรือ เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	ไม่เกิน 100,000 บาท หรือ เกิดเหตุร้ายที่ไม่มีความสำคัญ

การประมาณความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
1. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RI01	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล	5	4
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RI02	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายกรม โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของกรม ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของกรม	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย	5	3
3. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RI03	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล	5	2

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
			โดยอัตโนมัติ		ระบบสารสนเทศ		
4. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RI04	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	2	4
5. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RI05	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	5	4
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RI06	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	1	1

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
					ระบบฐานข้อมูล ระบบสารสนเทศ		
7. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RI07	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ		ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ	5	4
8. ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	RI08	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	1	5
9. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RI09	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ	1	2
10. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้	RI10	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่	3	4

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
ตามปกติ					ข่าย อุปกรณ์เครือข่าย		
11. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RI11	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	1	5

การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ x ความรุนแรงของเหตุการณ์ต่าง ๆ ซึ่งใช้เกณฑ์ในการจัดแบ่งดังนี้

ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
1 – 8	ต่ำ	ยอมรับความเสี่ยง	ขาว
9 – 16	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
17 – 24	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง

มาก

ผลกระทบ

ความเสี่ยงปานกลาง - ผลกระทบรุนแรงมาก - โอกาสเกิดน้อย	**ความเสี่ยงสูง** - ผลกระทบรุนแรงมาก - โอกาสเกิดมาก
ความเสี่ยงต่ำ - ผลกระทบน้อย - โอกาสเกิดน้อย	**ความเสี่ยงปานกลาง** - ผลกระทบน้อย - โอกาสเกิดมาก

น้อย ——— โอกาสที่จะเกิด ———→ มาก

การประเมินความเสี่ยง

ผลกระทบ					
5	**5**	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

โอกาสที่จะเกิด

สี	ระดับ
สีแดง	ความเสี่ยงสูงมาก
สีฟ้า	ความเสี่ยงสูง
สีเหลือง	ความเสี่ยงปานกลาง
สีขาว	ความเสี่ยงต่ำ (สามารถยอมรับได้)

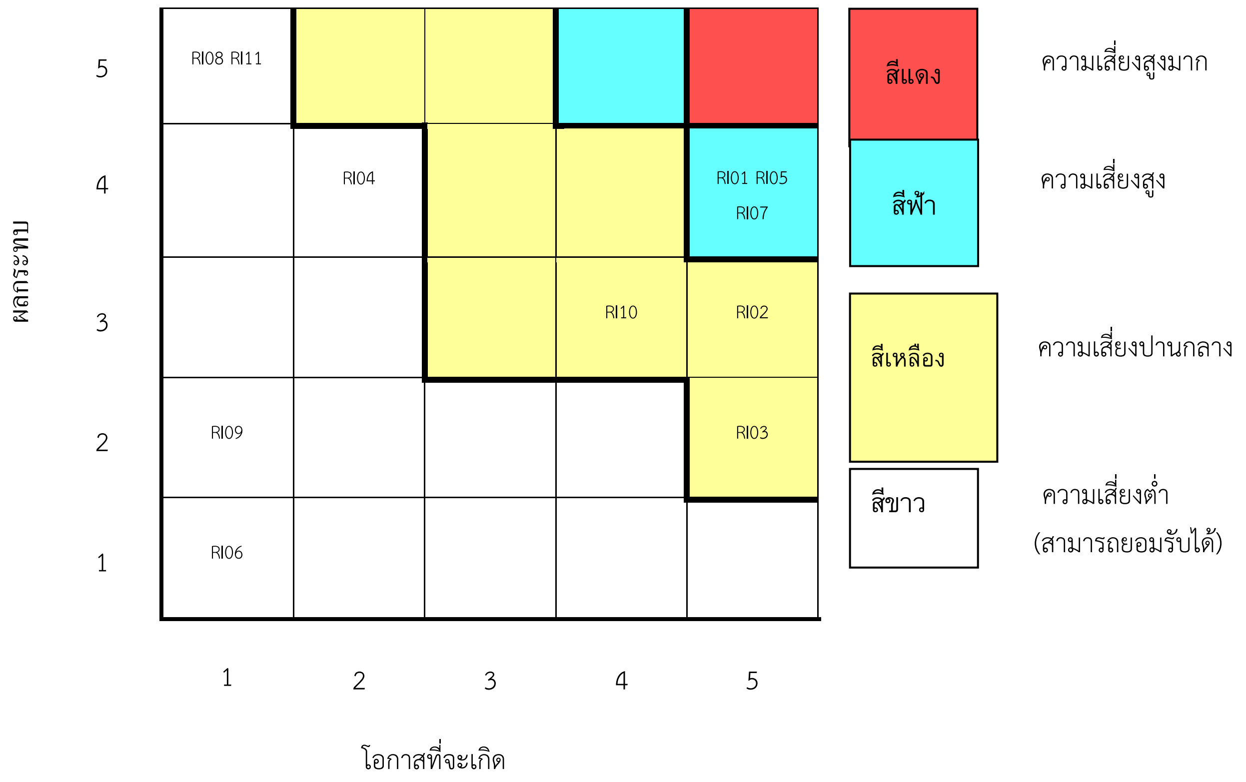
การประเมินค่าความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
1. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RI01	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	5	4	20
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RI02	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายกรมโดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของกรม ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของสถาบัน	5	3	15

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
3. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RI03	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	5	2	10
4. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RI04	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	2	4	8
5. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RI05	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	5	4	20
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RI06	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	1	1	1
7. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RI07	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	5	4	20
8. ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	RI08	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหว จนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	1	5	5
9. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RI09	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	1	2	2

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
10. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	RI10	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	3	4	12
11. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RI11	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	1	5	5

แผนภูมิความเสี่ยง



การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศ ในการบริหารจัดการได้อย่างมีประสิทธิภาพดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
1	RI01 ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	20
2	RI05 ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	20
3	RI07 ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	20
4	RI02 ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายกรม โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของกรม	15
5	RI10 ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	12
6	RI03 ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิด	10

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
			การสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	
7	RI04 ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านเทคนิค	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	8
8	RI08 ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	5
9	RI11 ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	5
10	RI09 ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อยจนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	2
11	RI06 ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	1

การจัดการความเสี่ยง

นโยบายของสถาบันราชานุกูล ระดับความเสี่ยงคงเหลือที่ยอมรับได้ ≤ 9

สำนักงาน ก.พ.ร. กำหนดให้ ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ 15 ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า 15 ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
1	RI01 ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	20	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
2	RI05 ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	20	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- สรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสม - จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้
3	RI07 ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	**20**	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ เพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ
4	RI02 ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	15	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง - ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิ์การเข้าถึงสำหรับอุปกรณ์ที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย
5	RI10 ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่	12	- ยอมรับความเสี่ยง (มี	-หาทางป้องกันสัตว์กัดแทะอุปกรณ์

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
	สามารถทำงานได้ตามปกติ		มาตรการติดตาม)	- จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว เพื่อสามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ
6	RI03 ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	10	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดหาเครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
7	RI04 ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	8	- ยอมรับความเสี่ยง	- ตรวจสอบการตั้งค่าของ firewall อย่างสม่ำเสมอ - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
8	RI08 ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	5	- ยอมรับความเสี่ยง	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด
9	RI11 ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	5	- ยอมรับความเสี่ยง	- ตรวจสอบการเข้าออกของบุคคลภายนอก - ตรวจสอบระบบการป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ - ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง
10	RI09 ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	2	- ยอมรับความเสี่ยง	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
				- จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้
11	RI06 ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	1	- ยอมรับความเสี่ยง	

ภาคผนวก

รายการเครื่องคอมพิวเตอร์และอุปกรณ์ในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง
เครื่องคอมพิวเตอร์แม่ข่าย (Server) / เครื่องจำลองแม่ข่าย (PC)/เครื่องสำรองไฟฟ้า (UPS)					
1. IBM SERVER	082051-7440-001-0001-091	20 มิ.ย. 2551	ใช้งาน	IBM รุ่น SYSTEM X3400 SN: 7973A2A-99A5771 Intel Xeon CPU 1.83 GHz RAM 1 GB OS: CentOS 7	ระบบบริการห้องสมุด (ยกเลิก) - ระบบ HIS Gateway (ติดตั้งที่ห้องสำรองข้อมูล)
2. HP ProLiant ML330 G6	082054-7440-001-0006-002	4 มี.ค. 2554	ใช้งาน	HP รุ่น ProLiant ML330 G6 SN: SGH051X106 Intel Xeon CPU 2.40 GHz RAM 4 GB ขนาด C: 458.25 GB OS: VMware ESXi 6.0	- Proxy Server - ระบบยืนยันก่อนการเข้าใช้อินเตอร์เน็ตของสถาบันฯ - เก็บ log การใช้งานในระบบอินเตอร์เน็ตของสถาบันฯ
3. DELL PowerEdge R720	082056-7440-001-0006-003	30 ต.ค. 2555	ใช้งาน	DELL รุ่น PowerEdge R720 Intel Xeon CPU 2.50 GHz RAM 8 GB ขนาด C: 552.75 GB OS: VMware ESXi 5.1.0	-ระบบบริการผู้ป่วย 2010-2 (ยกเลิก) - ระบบรายงานตัวชี้วัดและโครงการ (Scorecard. Cockpit)
4. HP ProLiant DL60 G9	082058-7440-001-0001-207	6 ส.ค.	ใช้งาน	HP รุ่น ProLiant DL60 G9	-Web Intranet

		2558		SN: SGH529YY23 Intel Xeon CPU 1.60 GHz RAM 4 GB ขนาด C: 924 GB OS: VMware ESXi 6.0	-ระบบจองห้องประชุม -ระบบบันทึกข้อมูล แฟ้ม Rehabilitation (ยกเลิก พ.ย. 63) - ระบบคิวอัตโนมัติ Q4U
5. HP ProDesk (PC) (ยกเลิกการใช้งาน)	082058-7440-001-0001-264	2558	ไม่ใช้งาน	เป็นเครื่องแม่ข่ายจำลอง CPU: Intel Core i5-4570 3.20 GHz RAM: 4 GB HDD 1 TB ระบบปฏิบัติการ CentOS	- ระบบบริการผู้ป่วย JHOS (ยกเลิก พ.ย. 63)
6. HP ProDesk (PC)	082058-7440-001-0001-264	2558	ใช้งาน	เป็นเครื่องแม่ข่ายจำลอง CPU: Intel Core i5-4570 3.20 GHz RAM: 4 GB HDD 1 TB ระบบปฏิบัติการ CentOS	- ติดตั้งโปรแกรม ESET Endpoint Antivirus สำหรับ Update เครื่องลูกข่าย (ติดตั้งที่ห้องสำรองข้อมูล)
7. DELL EMC PowerEdge	082262-7440-010-0006-004	2562	ใช้งาน	Dell รุ่น Xeon 3106 1.7 GHz RAM 32 GB HDD 1 TB x2 ระบบปฏิบัติการ CentOS 7	- ระบบบริการผู้ป่วย JHOS - Data Base ระบบบริการผู้ป่วย JHOS (ยกเลิก พ.ย. 63) - Data Base ระบบคิวอัตโนมัติ Q4U
เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง
8. DELL EMC PowerEdge	082262-7440-010-0006-005	ปี 2562	ใช้งาน	Dell รุ่น Xeon 3106 1.7 GHz RAM 16 GB HDD 1 TB x2 ระบบปฏิบัติการ CentOS 7	- ระบบบริการผู้ป่วย JHOS (ยกเลิก)
9. DELL OptiPlex 3050	082262-7440-001-0001-385	ปี 2562	ไม่ใช้	เป็นเครื่องแม่ข่ายจำลอง	- ระบบคิวอัตโนมัติ Q4U

(ยกเลิกการใช้งาน)			งาน	CPU: Intel Core i3-7100 3.90 GHz RAM: 4 GB HDD 1 TB ระบบปฏิบัติการ CentOS	(ย้ายไปอยู่บนเครื่อง server ลำดับที่ 4)
10. DELL EMC PowerEdge	082263-7440-010-0006-006	ปี 2563	ใช้งาน	Dell รุ่น EMC PowerEdge R440 2.4 GHz RAM 128 GB HDD 600 GB x 4 ระบบปฏิบัติการ CentOS 8	- เครื่อง Master สำหรับระบบบริการผู้ป่วย HOSxp v4
11. DELL EMC PowerEdge	082263-7440-010-0006-007	ปี 2563	ใช้งาน	Dell รุ่น EMC PowerEdge R440 2.4 GHz RAM 128 GB HDD 600 GB x 4 ระบบปฏิบัติการ CentOS 8	- เครื่อง Slave สำหรับระบบบริการผู้ป่วย HOSxp v4 (ติดตั้งที่ห้องสำรองข้อมูล)
12. Dell OptiPlex 3050	082262-7440-001-0001-382	ปี 2562	ใช้งาน	เป็นเครื่องแม่ข่ายจำลอง CPU: Intel Core i3-7100 3.90 GHz RAM: 4 GB HDD 1 TB ระบบปฏิบัติการ Windows 10	- Gateway เชื่อมต่อระหว่าง HOSxp กับระบบจ่ายยาอัตโนมัติ และระบบบันทึกน้ำหนัก ส่วนสูง ความดัน ของผู้มารับบริการ

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง
13. ZyXEL NAS 326	(รอตรวจสอบจากพัสดุ)	ปี 2560	ใช้งาน	อุปกรณ์จัดเก็บข้อมูลในระบบเครือข่าย (NAS-Network Attached Storage)	- ระบบไฟล์แชร์ ของสถาบันฯ - เก็บ log อินเตอร์เน็ตจาก Mikrotik
14. Synology	082263-7440-009-0005-003	ปี 2563	ใช้งาน	อุปกรณ์จัดเก็บข้อมูลในระบบเครือข่าย (NAS-Network Attached Storage)	- ระบบคลังสื่อมัลติมีเดีย
15. เครื่องสำรองไฟฟ้า (UPS)	B-082263-7440-010-0004/81	ปี 2563	ใช้งาน	เครื่องสำรองไฟฟ้า ยี่ห้อ SKD รุ่น LED-800	
16. เครื่องสำรองไฟฟ้า (UPS)	082263-7440-010-0003-041	ปี 2563	ใช้งาน	เครื่องสำรองไฟฟ้า ยี่ห้อ SKD รุ่น PS-3000	

17. เครื่องสำรองไฟฟ้า (UPS)	B-082262-7440-010-0004/83	ปี 2563	ใช้งาน	เครื่องสำรองไฟฟ้า ยี่ห้อ SKD รุ่น G-1000	
18. เครื่องสำรองไฟฟ้า (UPS)	-	ปี 2564	ใช้งาน	เครื่องสำรองไฟฟ้า ยี่ห้อ APC –SRVPM3KRIL	ติดตั้งที่ห้องสำรองข้อมูล
19.เครื่องสำรองไฟฟ้า (UPS)	-	ปี 2564	ใช้งาน	เครื่องสำรองไฟฟ้า ยี่ห้อ APC –SRVPM3KRIL	
20.เครื่องสำรองไฟฟ้า (UPS)	-	ปี 2564	ใช้งาน	เครื่องสำรองไฟฟ้า ยี่ห้อ APC –SRVPM3KRIL	

อุปกรณ์กระจายสัญญาณระบบเครือข่าย					
1. Firewall Fortinet	082056-7440-001-0008-001	30 ต.ค. 2555	ไม่ใช้งาน	Firewall Fortinet รุ่น FortiGate 100D SN: FG100D3G12805634	- ตรวจสอบป้องกันการบุกรุกเครือข่าย - บริหารจัดการระบบเครือข่ายภายใน (ยกเลิกไปใช้อุปกรณ์ ข้อ 2 แทน)
2 . Firewall Fortinet	-	ปี 2564	ใช้งาน	Firewall Fortinet รุ่น FortiGate 200F SN: FG200FT920908763	- ตรวจสอบป้องกันการบุกรุกเครือข่าย - บริหารจัดการระบบเครือข่ายภายใน
3. Switch 20-PortGigabit	082056-7440-009-0008-001	ปี 2556	ใช้งาน	Switch 20-Port Gigabit ยี่ห้อ CISCO SG300-20	(อุปกรณ์ผู้ให้บริการ leased line) กระจายสัญญาณสู่เครือข่ายภายใน
4. Switch 16 Port	082057-7440-009-0001-004	ปี 2557	ใช้งาน	Switch 16-Port /4 Port SFP	กระจายสัญญาณภายในสถาบันฯ

				ยี่ห้อ HP V1910-16G JE005A	
5. Switch 24 Port	-	ปี 2557	ใช้งาน	Switch 24-Port ยี่ห้อ SMC- GS24	กระจายสัญญาณภายในสถาบันฯ
6. Switch 24 Port	-	ปี 2558	ใช้งาน	Switch 24-Port ยี่ห้อ D-Link DGS-10240	กระจายสัญญาณภายในสถาบันฯ
7. Switch 24 Port	-	ปี 2558	ใช้งาน	Switch 24-Port ยี่ห้อ D-Link DGS-10240	กระจายสัญญาณภายในสถาบันฯ
8. Router CISCO 2800 (ยกเลิก)	-	28 พ.ย. 2560	ไม่ใช้งาน	SISCO รุ่น 2800 Series	อุปกรณ์ผู้ให้บริการ leased line (ยกเลิก ไปใช้อุปกรณ์ ข้อ 9 แทน)
9. Router Mikrotik	-	8 ต.ค. 2564	ใช้งาน	Mikrotik CCR1009-7G-1C-1S+	อุปกรณ์ผู้ให้บริการ Leased line
10. Mikrotik Route Board	082262-7440-009-0001-025	ปี 2562	ใช้งาน	Route Board รุ่น 1100AHx4	- กระจ่ายสัญญาณและควบคุมการใช้งานอินเตอร์ภายในตึกอำนวยการ
11. Zexel	082262-7440-009-0001-028	ปี 2562	ใช้งาน	Switch 24 Port รุ่น GS1920-24 SFP 4 Port	กระจายสัญญาณภายในสถาบันฯ

รายการระบบสารสนเทศที่ติดตั้งในพื้นที่ความดูแลของกลุ่มงานเทคโนโลยีสารสนเทศ

ระบบสารสนเทศ	การได้มา	วันที่ได้รับ	สถานะ	ผู้ใช้งาน/ผู้ดูแล	คุณลักษณะ
1. GFMIS ระบบบริหารการเงินการคลังภาครัฐ แบบอิเล็กทรอนิกส์	กรมบัญชีกลาง	2547	ใช้งาน	กลุ่มงานการเงินและบัญชี,กลุ่มงานพัสดุ, กลุ่มงานเภสัชกรรม/กรมบัญชีกลาง	- ใช้ Driver GF MIS Taken key ในการใช้งาน - ผ่าน http://webonlineintra.gfmis.go.th
2.ระบบตรวจสอบสิทธิการรักษา	สปสช.	2547	ใช้งาน	งานจัดเก็บรายได้/สปสช.	- ใช้ตรวจสอบสิทธิการรักษา - http:// ucsearch.nhso.go.th
3.Claim โปรแกรมเรียกเก็บเงิน	สปสช.	2547	ใช้งาน	งานจัดเก็บรายได้/สปสช.	- เป็นโปรแกรมในการจัดเก็บรายได้ - ติดตั้งโปรแกรมที่เครื่อง PC สำหรับการเรียกใช้งาน
4. ระบบบริการผู้ป่วย	จัดจ้างบุคคล	2552	ปิดระบบ	หน่วยบริการผู้ป่วย/งานจัดเก็บรายได้	- ระบบฐานข้อมูลให้บริการผู้ป่วย Client/Server ใช้ฐานข้อมูล (database) MYSQL - เรียกใช้งานผ่าน 192.168.10.2
5. ระบบ File Sharing	พัฒนาขึ้นเอง	2553	ใช้งาน	กลุ่มงานเทคโนโลยีสารสนเทศ	- ระบบเพื่อการใช้งานไฟล์งานร่วมกัน - เรียกใช้งานผ่าน 192.168.10.3
6.ฐานข้อมูลวิชาการ (อยู่ในwww.rajanukul.go.th)	พัฒนาขึ้นเอง	2553	ใช้งาน	- กลุ่มงานวิจัยและพัฒนาฯ - กลุ่มงานเทคโนโลยีสารสนเทศ	- หน้าเว็บเพจที่อยู่ในเว็บไซต์ของสถาบันราชานุกูล เป็นแหล่งรวบรวมองค์ความรู้และงานวิจัยและสำหรับเผยแพร่แก่กลุ่มนักวิชาการและประชาชนทั่วไป
7. โปรแกรม Scorecard Cockpit Enterprise	จัดซื้อ	2553	ใช้งาน	กลุ่มงานยุทธศาสตร์และแผนงานฯ	- ระบบบันทึกข้อมูลตัวชี้วัดและผลการปฏิบัติราชการตามตัวชี้วัด
8. เว็บไซต์สถาบันราชานุกูล	จัดจ้างบุคคล (นายอโนชา พันธุ์วิชัย)	2553	ใช้งาน	กลุ่มงานเทคโนโลยีสารสนเทศ	- www.rajanukul.go.th เผยแพร่ข้อมูลอันเป็นประโยชน์แก่ผู้รับบริการทั้งภายในและภายนอกประเทศตามมาตรฐานเว็บไซต์ภาครัฐ

ระบบสารสนเทศ	การได้มา	วันที่ได้รับ	สถานะ	ผู้ใช้งาน/ผู้ดูแล	คุณลักษณะ
9. ฐานข้อมูลพัสดุ	จัดจ้างบริษัท	2555	ไม่ใช้งาน	ฝ่ายพัสดุ	- ระบบบันทึกข้อมูลพัสดุ การทำงาน standalone
10. ระบบจองห้องประชุม	พัฒนาขึ้นเอง	2557 ปรับปรุง 2564	ใช้งาน	งานห้องประชุม/ กลุ่มงานเทคโนโลยีสารสนเทศ	- ระบบให้บริการจองห้องประชุม ใช้ฐานข้อมูล MySQL - เรียกใช้งานผ่าน 192.168.10.8/meeting
11. Web Intranet	พัฒนาขึ้นเอง	2558 ปรับปรุง 2561	ใช้งาน	กลุ่มงานเทคโนโลยีสารสนเทศ	- ระบบการสื่อสารภายในองค์กรที่เป็นข้อมูลเผยแพร่และสื่อสารภายในองค์กรเท่านั้น - เรียกใช้งานผ่าน 192.168.10.8
12. ฐานข้อมูลทรัพยากรเทคโนโลยี	พัฒนาขึ้นเอง	2558	ใช้งาน	กลุ่มงานเทคโนโลยีสารสนเทศ	-ระบบจัดเก็บข้อมูลครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ ใช้ฐานข้อมูล MYSQL
13. ระบบบันทึกข้อมูลผู้ขอใช้งานอินเตอร์เน็ต	พัฒนาขึ้นเอง	2559	ใช้งาน	กลุ่มงานเทคโนโลยีสารสนเทศ	- บันทึกข้อมูลผู้ใช้งานอินเตอร์เน็ตใช้ฐานข้อมูล MySQL - เรียกใช้งานผ่าน 192.168.10.6/squid user
14. ระบบบันทึกการใช้งานเครือข่าย firewall	พัฒนาขึ้นเอง	2559	ใช้งาน	กลุ่มงานเทคโนโลยีสารสนเทศ	- ระบบบันทึกการจราจรการใช้งานในเครือข่าย
15. ระบบแจ้งซ่อมผ่านเครือข่ายภายใน (helpdesk)	พัฒนาเอง	2560	ใช้งาน	หน่วยงานภายในสถาบันฯ/ กลุ่มงานเทคโนโลยีสารสนเทศ	- ใช้สำหรับแจ้งปัญหาที่เกิดขึ้นจากการใช้งานระบบคอมพิวเตอร์ผ่านทางระบบเครือข่ายภายใน
16. ฐานข้อมูลเครือข่ายด้านการพัฒนาการเด็ก	จัดจ้างบุคคล (นายอโนชา พันธุ์วิชัย)	2560	ใช้งาน	- กลุ่มงานพัฒนาศักยภาพเครือข่าย - กลุ่มงานเทคโนโลยีสารสนเทศ	- เป็นฐานข้อมูลที่ที่สามารถเข้าถึงได้ในระบบ Internet เว็บไซต์สถาบันราชานุกูล เป็นฐานข้อมูลที่รวบรวมข้อมูลด้านการให้บริการคัดกรอง ประเมิน ส่งเสริมพัฒนาการเด็ก ของสถานบริการสาธารณสุขทั่วประเทศ จำนวน 1,038 แห่ง

ระบบสารสนเทศ	การได้มา	วันที่ได้รับ	สถานะ	ผู้ใช้งาน/ผู้ดูแล	คุณลักษณะ
17.ฐานข้อมูลงานวิจัย	จัดจ้างบุคคล (นายอโนชา พันธุ์วิชัย)	2561	ใช้งาน	- กลุ่มงานวิจัยและพัฒนา	- เป็นฐานข้อมูลสำหรับนักวิชาการและบุคลากรสถาบันราชานุกูล เป็นศูนย์รวมข้อมูลทางการวิจัยด้านการพัฒนาสติปัญญาและด้านบกพร่องทางสติปัญญา
18.ฐานข้อมูลพัสดุ	จัดจ้างบุคคล (นายปิยพิภัทร)	2561	ไม่ใช้งาน	-กลุ่มงานพัสดุยกเลิกใช้งาน	-เป็นระบบฐานข้อมูลสำหรับเจ้าหน้าที่ผู้รับผิดชอบงานด้านการเบิกจ่ายพัสดุของหน่วยงาน สนับสนุนการดำเนินงานเพื่อการบริหารจัดการ และรายงานผู้บริหาร
19.ระบบงานโรงพยาบาล (JHOS)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักปลัดกระทรวงสาธารณสุข	2561	ยกเลิกการใช้งานเดือนพฤศจิกายน 2563	-กลุ่มงานเทคโนโลยีสารสนเทศ	- JHOS เป็นระบบที่พัฒนาขึ้นมาเพื่อให้การสนับสนุนโรงพยาบาลชุมชนที่ต้องการ มีระบบไอทีช่วยงาน และไม่พร้อมทางด้านงบประมาณ ช่วยลดค่าใช้จ่ายในด้านการจัดการเอกสาร รวมทั้งลดความผิดพลาดและการทำงานที่ซ้ำซ้อนได้ทั้งนี้เพื่อเพิ่มประสิทธิภาพและคุณภาพด้านการบริการและการรักษาให้ดียิ่งขึ้น Free Software โปรแกรมที่สามารถนำไปใช้งานได้โดยไม่มีค่าใช้จ่าย ออกแบบให้ทำงานได้บนหลายระบบปฏิบัติการที่รองรับ Java (อาทิ Windows, Unix, Linux) เป็น Web-Based Application ที่ทำงานผ่านเว็บเบราเซอร์ ใช้ระบบจัดการฐานข้อมูล MySQL และพัฒนาโดยภาษา Java
20.ระบบนัดผู้ป่วยใหม่ออนไลน์	จัดจ้างบุคคล (นายอโนชา พันธุ์วิชัย)	2562	ใช้งาน	-กลุ่มงานเทคโนโลยีสารสนเทศ -กลุ่มงานเวชระเบียน -งานพยาบาลผู้ป่วยนอก	-เป็นระบบที่พัฒนาด้วยฐานข้อมูล MySQL และพัฒนาโดยภาษา Java -รองรับการทำงานเครือข่ายอินเทอร์เน็ตภายใต้เว็บไซต์สถาบันราชานุกูล

ระบบสารสนเทศ	การได้มา	วันที่ได้รับ	สถานะ	ผู้ใช้งาน/ผู้ดูแล	คุณลักษณะ
					-ซึ่งเป็นระบบที่สร้างขึ้นมาเพื่อให้บริการแก่ผู้ป่วยใหม่ที่ต้องการนัดล่วงหน้า เพื่อได้ไม่พลาดการได้พบแพทย์ตั้งแต่ครั้งแรก และผู้รับบริการสามารถให้ข้อมูลในเบื้องต้น และรับทราบข้อมูลการเตรียมตัวก่อนการเข้ารับบริการ
22. ระบบบริหารคลังเวชภัณฑ์	จัดจ้างบุคคล (นายปิยพิภัทร คำหม้าว)	2563	ใช้งาน	-กลุ่มงานเภสัชกรรม	เพื่อเป็นเครื่องมืออำนวยความสะดวกในการบริหารจัดการรายการยาและเวชภัณฑ์ของสถาบันราชานุกูล อำนวยความสะดวกในการบันทึกข้อมูลรับเข้า และการเบิกจ่าย รวมถึงการตรวจสอบรายการคงเหลือในคลังยาและเวชภัณฑ์อย่างเป็นระบบ
23. ระบบฐานข้อมูลสารสนเทศทางการพยาบาล	จัดจ้างบุคคล (นายปิยพิภัทร คำหม้าว)	2563	ใช้งาน	กลุ่มภารกิจทางการพยาบาล	-เพื่อให้เกิดประโยชน์คือทำให้พยาบาลมีเวลาการปฏิบัติการพยาบาลมากขึ้น ลดเวลาในการจัดการเอกสาร โดยเฉพาะการพัฒนาระบบสารสนเทศทางการพยาบาลให้เป็นข้อมูลมาตรฐานด้วยการใช้ ภาษาสากล ในการวินิจฉัยและสะท้อนกิจกรรมการพยาบาลที่ปฏิบัติแก่ผู้ป่วย โดยระบบการบันทึกข้อมูลสามารถบันทึกข้อมูลได้อย่างถูกต้องสมบูรณ์มีระบบสัญญาณเตือนเมื่อมีสิ่งผิดปกติเกิดขึ้น และยังสามารถนำมาใช้ในการให้ข้อมูลความรู้แก่ผู้มารับบริการ -พัฒนาระบบในรูปแบบ Web Application สามารถรองรับการทำงานบนเว็บบราวเซอร์ ดังต่อไปนี้เป็นอย่างน้อย Microsoft Edge, Google Chrome และ Firefox -รองรับการทำงานเครือข่ายอินเทอร์เน็ตภายใต้เว็บไซต์สถาบันราชานุกูล (www.rajanukul.go.th)
24.ระบบ TEDA4I Online	จัดจ้างบุคคล	2563	ใช้งาน	กลุ่มงานพัฒนาศักยภาพเครือข่าย	-จัดทำระบบบริหารจัดการข้อมูลการใช้คู่มือ TEDA4I

ระบบสารสนเทศ	การได้มา	วันที่ได้รับ	สถานะ	ผู้ใช้งาน/ผู้ดูแล	คุณลักษณะ
	(นายอโนชา พันธุ์วิชัย)				รองรับการแสดงผล Responsive web design --รองรับการทำงานเครือข่ายอินเทอร์เน็ตภายใต้เว็บไซต์สถาบันราชานุกูล (www.rajanukul.go.th) - เพื่อสื่อสารข้อมูลวิธีการใช้คู่มือการประเมินเพื่อช่วยเหลือเด็กปฐมวัยที่มีปัญหาพัฒนาการ (TEDA4I) ที่ถูกต้อง สะดวก ทันสมัย เข้าถึงได้ทุกที่ ในรูปแบบออนไลน์
25.ระบบคิวอัตโนมัติ (Q4U)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักปลัดกระทรวงสาธารณสุข	2562	ใช้งาน	-กลุ่มงานเทคโนโลยีสารสนเทศ -งานพยาบาลผู้ป่วยนอก	-เพื่อให้การบริการกับผู้ป่วยหรือผู้มารับบริการมีประสิทธิภาพและลดระยะรอคอยในการให้บริการ -เพื่อให้เจ้าหน้าที่ทำงานได้คล่องตัวมากขึ้นและ ผู้รับบริการไดรับการบริการที่รวดเร็วและมีประสิทธิภาพ
26. ระบบจ่ายยาอัตโนมัติ	จัดจ้าง บริษัท ไฮทริกซ์ จำกัด	2562	ใช้งาน	-กลุ่มงานเภสัชกรรม	-เพื่อให้มีการจัดยาอย่างเป็นระบบอัตโนมัติ ง่ายต่อการให้บริการ เพิ่มความรวดเร็ว และแม่นยำในการจัดยาให้กับผู้มารับบริการ
27. ระบบงานโรงพยาบาล (BMS-HOSxP XE)	จัดจ้าง บริษัท บางกอก เมดิคอล ซอฟต์แวร์ จำกัด	2563	ใช้งาน	-กลุ่มงานเทคโนโลยีสารสนเทศ	-เป็นโปรแกรมที่พัฒนาขึ้นใช้สำหรับโรงพยาบาล เพื่อเก็บบันทึกข้อมูลผู้ป่วยและช่วยบุคลากรทางการแพทย์ในการให้บริการผู้ป่วย มีลักษณะเป็น Hospital Information System - มีระบบแจ้งเตือนข้อมูลสำคัญไปหาบุคลากรทางการแพทย์ของหน่วยงานได้ทันที

ระบบสารสนเทศ	การได้มา	วันที่ได้รับ	สถานะ	ผู้ใช้งาน/ผู้ดูแล	คุณลักษณะ
					- มีระบบรายงานที่ผู้ดูแลระบบสามารถเข้าไปแก้ไข หรือสร้างใหม่เองได้โดยไม่จำกัดจำนวน - มีระบบสำรองข้อมูลแบบ Hot Backup โดยไม่ต้องหยุดระบบ และสามารถนำข้อมูลสำรองจนถึง ณ จุดเวลาที่ทำการ Backup ครั้งสุดท้ายกลับมาใช้ใหม่ (Data Restore) ได้ - มีระบบบันทึกข้อมูลลายนิ้วมือ (Finger print) ของทั้งบุคลากร และผู้ป่วย โดยลายนิ้วมือที่บันทึกสามารถนำมาใช้ในการ Login เข้าโปรแกรมได้ (สำหรับบุคลากร) หรือนำมาใช้ระบุหาตัวผู้ป่วยในขั้นตอนการส่งตรวจได้
28. ระบบเช็คนัดฉีดวัคซีนโควิด-19 สำหรับเด็กพิเศษและครอบครัว	ณัฐชนกออกแบบระบบและจัดจ้าง (นายอโนชา พันธุ์วิชัย)	2564	ใช้งาน	-กลุ่มงานเทคโนโลยีสารสนเทศ	- เพื่อใช้ในการให้บริการตรวจสอบวันนัดหมายหลังจากครอบครัวเด็กพิเศษลงทะเบียนฉีดวัคซีนโควิด-19 มาใน Google Application โดยสามารถกดยืนยันนัดหมายและดาวน์โหลดบัตรนัดได้ ทำให้หน่วยบริการฉีดวัคซีนสามารถบริหารจัดการนัดของกลุ่มครอบครัวเด็กพิเศษได้อย่างคล่องตัว และทราบจำนวนการเข้ารับบริการในแต่ละวันได้
29. ระบบลงทะเบียนฉีดวัคซีนโควิด-19 แอสตราเซเนก้า เข็มสาม (Booster dose)	ณัฐชนก สุวรรณานนท์	2564	ใช้งาน	-กลุ่มงานเทคโนโลยีสารสนเทศ	- เพื่อใช้ในการลงทะเบียนให้บริการฉีดวัคซีนโควิด-19 แอสตราเซเนกาเข็มสาม (Booster dose) พร้อมการเข้ามาตรวจสอบวันนัดหมายวันเข้ารับบริการฉีดวัคซีนสำหรับคนทั่วไปที่ผ่านการรับวัคซีน Sinovac เข็ม 1 และ 2 แล้ว โดยสามารถกดยืนยันนัดหมายและดาวน์โหลดบัตรนัดได้

ระบบสารสนเทศ	การได้มา	วันที่ได้รับ	สถานะ	ผู้ใช้งาน/ผู้ดูแล	คุณลักษณะ
					ทำให้หน่วยบริการฉีดวัคซีนสามารถบริหารจัดการนัดของบุคคลทั่วไปได้อย่างคล่องตัว และควบคุมจำนวนการเข้ารับบริการในแต่ละวันได้
30. ระบบลงทะเบียนฉีดวัคซีนโควิด-19 ไฟเซอร์ สำหรับเด็กพิเศษที่มีอายุ 12-17 ปี	ณัฐชนก สุวรรณานนท์	2564	ใช้งาน	-กลุ่มงานเทคโนโลยีสารสนเทศ	เพื่อใช้ในการให้บริการลงทะเบียนฉีดวัคซีนโควิด-19 ไฟเซอร์ของกลุ่มเด็กพิเศษที่มีอายุ 12-17 ปี โดยสามารถเลือกวันนัดได้ตามการตรวจสอบจากระบบคำนวณระยะเวลาห่างจากเข็มสองได้โดยอัตโนมัติ และดาวน์โหลดบัตรนัดได้ ทำให้หน่วยบริการฉีดวัคซีนสามารถบริหารจัดการการเข้ารับบริการของบุคคลทั่วไปได้อย่างคล่องตัว และควบคุมจำนวนการเข้ารับบริการในแต่ละวันได้
31. ระบบลงทะเบียนฉีดวัคซีนโควิด-19 ไฟเซอร์ เข็มสาม (Booster dose)	ณัฐชนกออกแบบระบบและจัดจ้าง (นายอโนชา พันธุ์วิชัย)	2564	ใช้งาน	-กลุ่มงานเทคโนโลยีสารสนเทศ	เพื่อใช้ในการให้บริการลงทะเบียนนัดฉีดวัคซีนโควิด-19 ไฟเซอร์เข็มสาม สำหรับผู้ที่ฉีดวัคซีนเข็มที่ 2 โดยมีระยะห่าง 4 เดือนขึ้นไป โดยสามารถเลือกวันนัดได้ตามการตรวจสอบจากระบบคำนวณระยะเวลาห่างจากเข็มสองได้โดยอัตโนมัติ และดาวน์โหลดบัตรนัดได้ ทำให้หน่วยบริการฉีดวัคซีนสามารถบริหารจัดการการเข้ารับบริการของบุคคลทั่วไปได้อย่างคล่องตัว และควบคุมจำนวนการเข้ารับบริการในแต่ละวันได้
32. ระบบลงทะเบียนฉีดวัคซีนโควิด-19 ไฟเซอร์ฝาสีส้ม สำหรับเด็กอายุ 5-11 ปี	ณัฐชนกออกแบบระบบ	1 กพ.2565	ใช้งาน	-กลุ่มงานเทคโนโลยีสารสนเทศ	เพื่อใช้ในการให้บริการลงทะเบียนฉีดวัคซีนโควิด-19 ไฟเซอร์ฝาสีส้ม สำหรับเด็กอายุ 5-11 ปี โดยสามารถเลือกวันนัดได้ตามที่เปิดให้มีการลงทะเบียน โดยมีการจำกัด

ระบบสารสนเทศ	การได้มา	วันที่ได้รับ	สถานะ	ผู้ใช้งาน/ผู้ดูแล	คุณลักษณะ
					จำนวนไว้ และสามารถดาวน์โหลดบัตรนัดได้ทันที หน่วยบริการฉีดวัคซีนสามารถบริหารจัดการการเข้ารับบริการของเด็กได้อย่างมีประสิทธิภาพ และควบคุมจำนวนการเข้ารับบริการในแต่ละวันได้

การบริหารจัดการความเสี่ยงฉบับนี้ ได้ผ่านการพิจารณาและปรับปรุงในปีงบประมาณ 2565 จากคณะกรรมการสารสนเทศและกลุ่มงานเทคโนโลยีสารสนเทศ สถาบันราชานุกูล เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการเพื่อจัดการการความเสี่ยงด้านสารสนเทศต่อไป

(แพทย์หญิงจันทร์อาภา สุขทัพภ์)
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง
วันที่ ...25..../....มกราคม...../..2565