แผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ
หน่วยบัญชาการนาวิกโยธิน

<u>อ้างถึง</u> ระเบียบและนโยบายด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

ก. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐
ข. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐
ค. ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ.๒๕๔๔
ง. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒
จ. ระเบียบกองทัพเรือว่าด้วยการรักษาความปลอดภัย พ.ศ.๒๕๓๑
ฉ. ระเบียบกองทัพเรือว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔
ช. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม
ซ. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ
ฌ. แนวทางการใช้งานระบบสารสนเทศของกองทัพเรือ
ญ. ระเบียบหน่วยบัญชาการนาวิกโยธินว่าด้วยการใช้งานระบบเครือข่ายคอมพิวเตอร์ของหน่วยบัญชาการนาวิกโยธิน พ.ศ.๒๕๔๙

๑. หลักการและเหตุผล

การบริหารจัดการความเสี่ยง มีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ ที่เป็นสินทรัพย์ของหน่วยบัญชาการนาวิกโยธิน และยังรวมถึงการปกป้อง “ภารกิจ” ของหน่วยบัญชาการนาวิกโยธิน ให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับระบบสารสนเทศอีกด้วย ขั้นตอนในการบริหารจัดการความเสี่ยงควรจัดให้อยู่ในความรับผิดชอบหลักของฝ่ายกรรมวิธีข้อมูลกองบัญชาการ หน่วยบัญชาการนาวิกโยธิน ซึ่งมีเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศเป็นผู้ดูแลระบบสารสนเทศของหน่วยบัญชาการนาวิกโยธิน

หน่วยบัญชาการนาวิกโยธินจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงด้านระบบสารสนเทศที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยง และเพื่อความสามารถในการดำเนินภารกิจของหน่วยบัญชาการนาวิกโยธินให้บรรลุผลสำเร็จ ไม่ใช่แค่เพียงการปกป้องสินทรัพย์ระบบสารสนเทศของหน่วยบัญชาการนาวิกโยธินเพียงเท่านั้น

การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ตามพระราชกฤษฎีกาว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ.๒๕๔๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวน การบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุเป้าประสงค์และภารกิจที่ตั้งไว้และเป็น การพัฒนาผลการปฏิบัติงานของหน่วยงาน ที่จะนำไปสู่การใช้ทรัพยากรอย่างมีประสิทธิภาพและคุ้มค่า

๒. วัตถุประสงค์

๒.๑ เพื่อให้การบริหารจัดการของหน่วยบัญชาการนาวิกโยธิน มีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศ

๒.๒ เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบสารสนเทศของหน่วยบัญชาการนาวิกโยธิน

๒.๓ เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านระบบสารสนเทศ

๒.๔ เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านระบบสารสนเทศ

๒.๕ เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

๓. ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงระบบสารสนเทศ ที่อยู่ในความรับผิดชอบของหน่วยบัญชาการนาวิกโยธิน

๔. ทีมงานบริหารแผนเตรียมพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศของ นย.

เพื่อให้แผนเตรียมพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ นย. สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล จะต้องจัดตั้งคณะทำงานบริหารความเสี่ยง ประกอบด้วยโครงสร้างดังนี้

๑. ผู้บริหารเทคโนโลยีสารสนเทศ นย. มีหน้าที่บริหารงานด้านระบบสารสนเทศภายใน นย. ให้สามารถบริการระบบสารสนเทศหลักของ นย. ได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

๒. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย. มีหน้าที่ดำเนินการรักษาความมั่นคงปลอดภัย วิเคราะห์และประเมินความเสี่ยงของระบบที่ให้บริการใน นย.

๓. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ควบคุมระบบสารสนเทศ นย. มีหน้าที่ให้บริการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย ตรวจสอบ ควบคุมการทำงาน สำรองและกู้คืนข้อมูลระบบสารสนเทศในระดับระบบปฏิบัติการ

๔. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ด้านซอฟท์แวร์ ฮาร์ดแวร์ เครือข่าย ระบบสารสนเทศที่ให้บริการใน นย. มีหน้าที่บำรุงรักษา วิเคราะห์ ปรับปรุง แก้ไขปัญหาด้านซอฟท์แวร์ ฮาร์ดแวร์ เครือข่าย ระบบสารสนเทศที่ติดตั้งภายใน นย.

๕. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ตรวจสอบและวิเคราะห์ความเสียหายที่เกิดขึ้นภายใน นย. มีหน้าที่กำหนดแนวทางและมาตรการการรักษาความมั่นคงปลอดภัย ตรวจสอบและวิเคราะห์สาเหตุของความเสียหายที่เกิดขึ้นจากการโจมตีทางไซเบอร์ พร้อมทั้งให้คำแนะนำในการแก้ไขปัญหาของระบบที่เกิดการโจมตีทางไซเบอร์

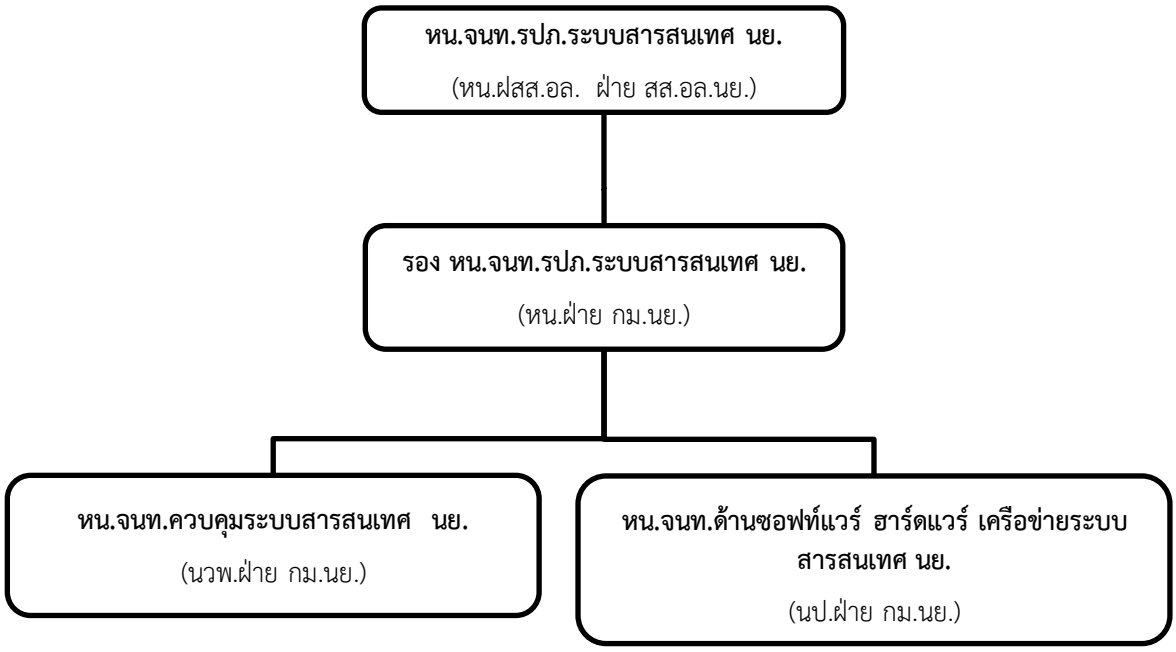
๖. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ประสานงานกับผู้ดูแลระบบสารสนเทศ นขต.นย. มีหน้าที่ บริหารระบบผู้ใช้งานระบบสารสนเทศ ทร. ประสานงานการให้บริการ เผยแพร่และควบคุมการให้บริการต่างๆ ของ นย.

โดยทุกตำแหน่งจะต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงาน และกู้คืนเหตุการณ์ฉุกเฉินในส่วนที่รับผิดชอบให้สามารถบริหารแผนฯ และกลับสู่สภาวะปกติได้โดยเร็ว ตามบทบาทหน้าที่ที่กำหนดไว้ของทีมบริหารความเสี่ยง (CP Team) และในกรณีที่บุคลากรไม่สามารถปฏิบัติหน้าที่ได้ ให้บุคลากรสำรองรับผิดชอบทำหน้าที่ในหน้าที่ของบุคลากรหลัก ปรากฏดังในตาราง ทีมงานบริหารแผนเตรียมพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศของ นย.

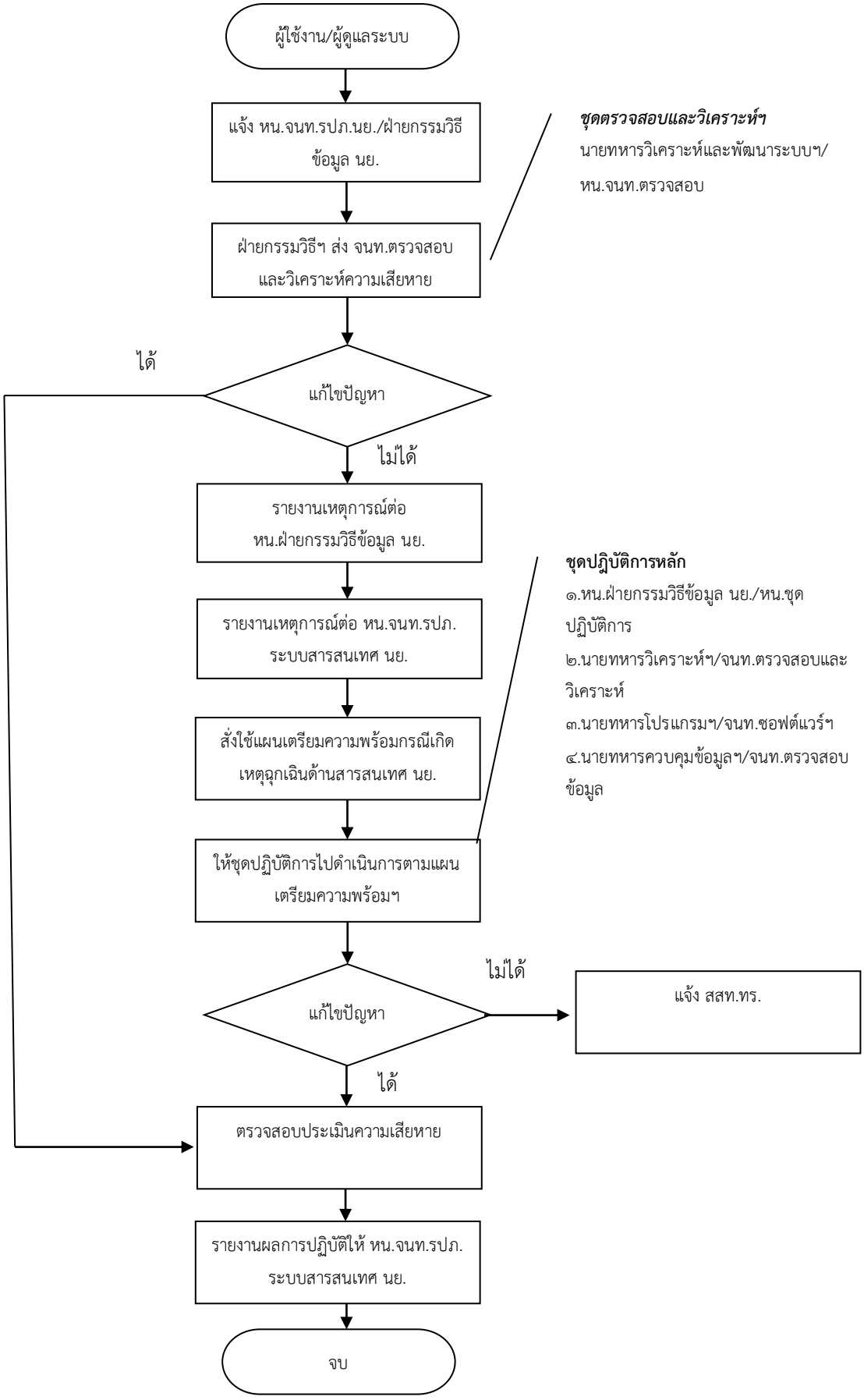
ทีมงานบริหารแผนเตรียมพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศของ นย.

บุคคลากรหลัก		บทบาท	บุคคลากรสำรอง		บทบาท
ชื่อ/ตำแหน่ง	โทรศัพท์		ชื่อ/ตำแหน่ง	โทรศัพท์	
หน.ฝสส.อล. ฝ่าย สส.อล.นย.	๐๘๙ ๙๙๔๑๑๗๗	ผู้บริหารเทคโนโลยีสารสนเทศ นย.	-หน.ฝ่าย กม.นย. -นวพ.ฝ่าย กม.นย. -นป.ฝ่าย กม.นย.	๐๘๕ ๔๓๖๔๕๑๖ ๐๘๗ ๙๔๒๙๗๖๙ ๐๘๙ ๘๙๐๗๐๒๙	ผู้ช่วยผู้บริหารฯ ผู้ช่วยผู้บริหารฯ ผู้ช่วยผู้บริหารฯ
หน.ฝสส.อล. ฝ่าย สส.อล.นย.	๐๘๙ ๙๙๔๑๑๗๗	หน.จนท.รปภ.ระบบสารสนเทศ นย.	หน.ฝ่าย กม.นย.	๐๘๕ ๔๓๖๔๕๑๖	รอง หน.จนท.รปภ.ระบบสารสนเทศ นย.
หน.ฝ่าย กม.นย.	๐๘๕ ๔๓๖๔๕๑๖	หน.จนท.ควบคุมระบบสารสนเทศ นย.	นวพ.ฝ่าย กม.นย.	๐๘๗ ๙๔๒๙๗๖๙	รอง หน.จนท.ควบคุมระบบสารสนเทศ นย.
นวพ.ฝ่าย กม.นย.	๐๘๗ ๙๔๒๙๗๖๙	หน.จนท.ตรวจสอบและวิเคราะห์ความเสียหาย	นวพ.ฝ่าย กม.นย. (ร.อ.)	๐๘๔ ๖๔๙๔๙๕๒	รอง หน.จนท.ตรวจสอบและวิเคราะห์ความเสียหาย
นป.ฝ่าย กม.นย.	๐๘๙ ๘๙๐๗๐๒๙	หน.จนท.ด้านซอฟท์แวร์ ฮาร์ดแวร์ เครือข่ายระบบสารสนเทศ นย.	นป.ฝ่าย กม.นย. (ร.อ.)	๐๘๓ ๙๒๙๔๔๗๔	รอง หน.จนท.ด้านซอฟท์แวร์ ฮาร์ดแวร์ เครือข่ายระบบสารสนเทศ นย.
นวพ.ฝ่าย กม.นย. (ร.อ.)	๐๘๔ ๖๔๙๔๙๕๒	หน.จนท.ประสานงานกับผู้ดูแลระบบสารสนเทศ นขต.นย.	นายทหารควบคุมข้อมูลฯ		รอง หน.จนท.ประสานงานกับผู้ดูแลระบบสารสนเทศ นขต.นย.

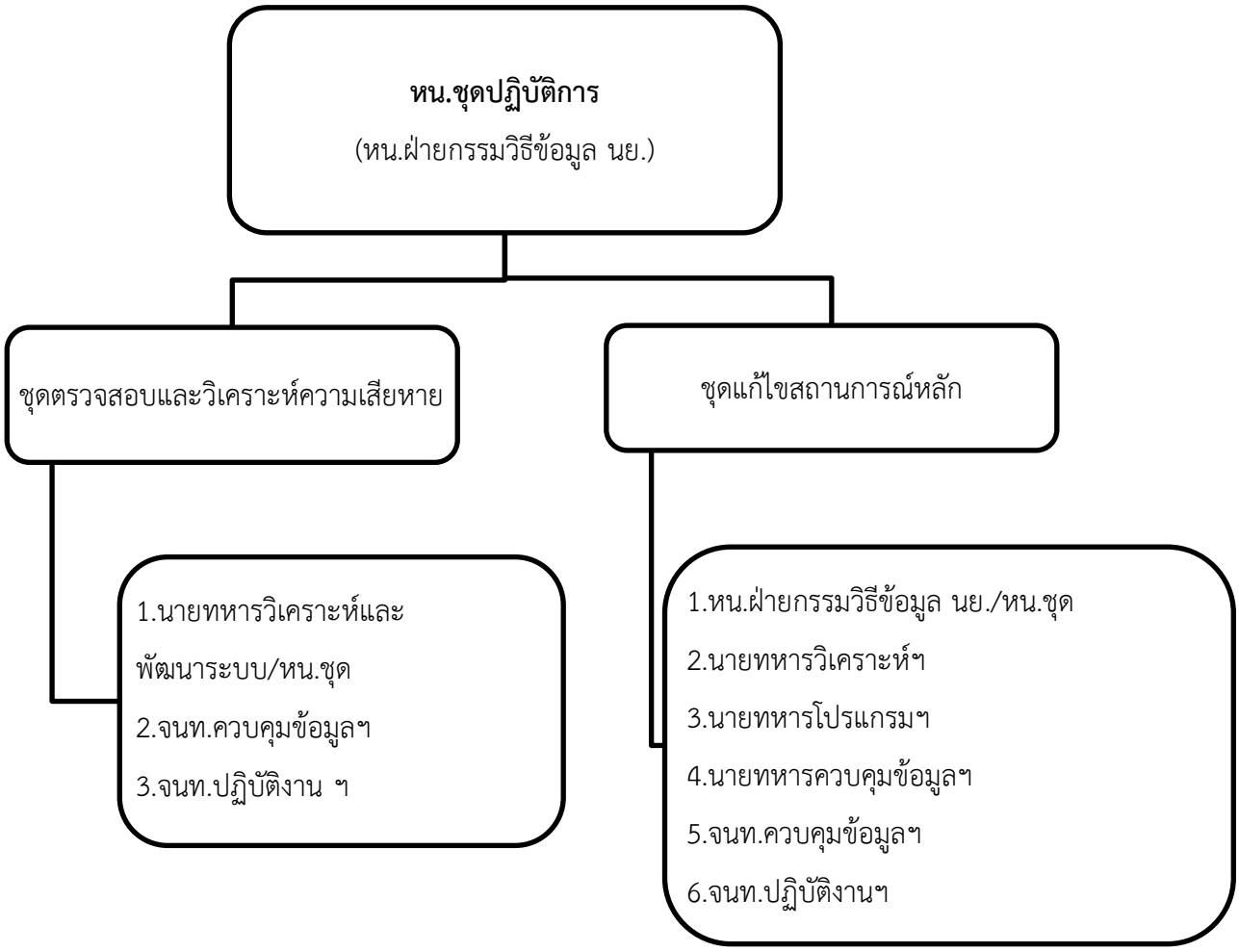
โครงสร้าง/สายการบังคับบัญชาด้านการรักษาความปลอดภัยระบบสารสนเทศ นย.



ผังการปฏิบัติเมื่อเกิดเหตุฉุกเฉินด้านสารสนเทศของ นย.



การจัดชุดปฏิบัติการในกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศของ นย.



๕. การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านระบบสารสนเทศของหน่วยงานสามารถแยกประเภทความเสี่ยงเป็น ๔ ประเภท ดังนี้

๕.๑ ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นกับระบบเชื่อมโยงเครือข่ายระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์รวมถึงข้อมูลสารสนเทศได้แก่

๕.๑.๑ การถูกมัลแวร์ (Malware) ทำลายฐานข้อมูล โปรแกรมใช้งานหรือระบบปฏิบัติการต่าง ๆ

๕.๑.๒ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคล (Hacker) โดยไม่ได้รับอนุญาต

๕.๑.๓ ระบบเชื่อมโยงเครือข่ายคอมพิวเตอร์หลัก (Backbone) เสียหาย/ขัดข้อง

๕.๑.๔ การชำรุดเสียหายของเครื่องคอมพิวเตอร์แม่ข่าย จากการเคลื่อนย้ายหรืออื่นๆเช่น Hard Disk คอมพิวเตอร์แม่ข่ายเสียหายไม่สามารถให้บริการได้เป็นต้น

๕.๒ ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้ได้แก่

๕.๒.๑ การอำพรางหรือสวมรอยผู้ใช้การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๕.๒.๒ ระบบฐานข้อมูลเสียหายข้อมูลถูกทำลาย ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต

๕.๒.๓ การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ

๕.๓ ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ ได้แก่

๕.๓.๑ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๕.๓.๒ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องคอมพิวเตอร์แม่ข่าย (Server) เช่น อัคคีภัยวาตภัย อุทกภัย แผ่นดินไหว อาคารถล่ม สึนามิเป็นต้น

๕.๓.๓ การโจรกรรมเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ประกอบ ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๕.๓.๔ การเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องคอมพิวเตอร์แม่ข่าย ของระบบฐานข้อมูล เช่นการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๕.๔ ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศรวมถึงการขาดแคลนงบประมาณ หรือบุคลากรด้านเทคโนโลยีสารสนเทศ

๖.การบรรเทาความเสี่ยง (Risk mitigation)

การบรรเทาความเสี่ยงเกี่ยวข้องกับการจัดลำดับ การคำนวณความเสี่ยง และการลงมือควบคุมการลดความเสี่ยงอย่างเหมาะสมตามแนวทางที่มาจากการประเมินความเสี่ยง เนื่องจากการที่จะกำจัดความเสี่ยงในระบบทั้งหมดนั้นเป็นเรื่องที่ทำได้ยาก ด้วยเงื่อนไขในการใช้งบประมาณที่สมดุล เพื่อให้เกิดประสิทธิภาพสูงสุด และใช้วิธีการควบคุมที่เหมาะสมที่สุดเพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยส่งผลกระทบต่อภารกิจและทรัพยากรของหน่วยให้น้อยที่สุดทางเลือกเพื่อการบรรเทาความเสี่ยง สามารถแบ่งออกเป็น ๕ ประเภทดังนี้

๖.๑ การยอมรับความเสี่ยง (Risk Acceptance) คือการยอมรับความเสี่ยงในระดับที่เป็นอยู่และให้ระบบสารสนเทศดำเนินงานไปตามปกติ ซึ่งเป็นการยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวตน เพียงใช้ชื่อผู้ใช้งานและรหัสผ่าน มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้ การใช้ Biometrics เช่น การตรวจ ลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่า หน่วยงานอาจยอมรับความเสี่ยงของระบบปัจจุบันและ ทำงานต่อไปและปรับปรุงเมื่อมีโอกาส

๖.๒ การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือการหลีกเลี่ยงความเสี่ยงด้วยการกำจัดสาเหตุของความเสี่ยง เช่น เมื่อพบว่าปัจจุบันหน่วยงานมีการสำรองข้อมูลเพียง ๑ ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล ๒ ชุด และแยกเก็บในสถานที่ต่างกันหรือ ระบบด้านยุทธการที่มีชั้นความลับ ลับมาก ต้องห้ามมีการเชื่อมต่อกับอินเทอร์เน็ต เพื่อหลีกเลี่ยงภัยจาก Hacker เป็นต้น

๖.๓ การจำกัดความเสี่ยง (Risk Limitation) คือ การทำระบบควบคุมเพื่อให้เกิดผลกระทบจากการถูกคุกคามระบบหรือจากความไม่มั่นคงของระบบให้น้อยที่สุด เช่น การใช้ Firewall ป้องกันระบบจากภัยคุกคามในอินเทอร์เน็ต

๖.๔ การวิจัยและการรับรู้ความเสี่ยง (Research and Acknowledgement) คือการลดความสูญเสียที่เกิดจากความเสี่ยงโดยการตรวจสอบเพื่อรับทราบความอ่อนแอของระบบและค้นคว้าวิจัยให้ได้วิธีการควบคุมเพื่อเสริมความมั่นคงให้แก่ระบบ

๖.๕ การถ่ายโอนความเสี่ยง (Risk Transfer) คือ การถ่ายโอนความเสี่ยงด้วยการหาทางเลือกอื่นเพื่อชดเชยความสูญเสีย เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน หน่วยงานอาจเลือกซื้อประกัน หรือสัญญาการซ่อมบำรุง เป็นต้น

๗. ลักษณะรายละเอียดของความเสี่ยง (Description of risk) แสดงตามตารางดังนี้

ชื่อความเสี่ยง	รหัส	ประเภท ความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/ สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับ ผลกระทบ
๑.ความเสี่ยงจากการถูกมัลแวร์ (Malware) ทำลายฐานข้อมูล โปรแกรมใช้งานหรือระบบปฏิบัติการต่าง	RIT01	ความเสี่ยงด้านเทคนิค	การบุกรุกโจมตีโดยโปรแกรมไม่ประสงค์ดีเช่นการติด Malware เป็นต้น	- Malware	- ระบบสารสนเทศ - เครื่องคอมพิวเตอร์แม่ข่าย
๒.ความเสี่ยงจากการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคล (Hacker) โดยไม่ได้รับอนุญาต	RIT02	ความเสี่ยงด้านเทคนิค	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดีเช่นhackerเป็นต้นการดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย	- ผู้ไม่ประสงค์ดี	- ระบบสารสนเทศ - เครื่องคอมพิวเตอร์แม่ข่าย
๓.ความเสี่ยงจากระบบเชื่อมโยงเครือข่ายคอมพิวเตอร์หลัก (Backbone) เสียหาย/ขัดข้อง	RIT03	ความเสี่ยงด้านเทคนิค	ระบบเชื่อมโยงเครือข่ายคอมพิวเตอร์หลัก (Backbone) เสียหาย/ขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์ กัดแทะ เช่นหนูหรือแมลงเป็นต้น	- อุปกรณ์ชำรุดหรือขัดข้อง	- ระบบเครือข่าย
๔.ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ ขัดข้องไม่ สามารถทำงานได้ตามปกติ	RIT04	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิคหรือจากสัตว์ กัดแทะเช่นหนูหรือแมลงเป็นต้น	- อุปกรณ์ชำรุดหรือขัดข้อง	- ระบบสารสนเทศ - ระบบเครือข่าย
๕.ความเสี่ยงจากการอำพรางหรือสวมรอยผู้ใช้การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	RIT05	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้	- ระบบสารสนเทศ - ผู้ใช้งาน

ชื่อความเสี่ยง	รหัส	ประเภท ความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/ สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับ ผลกระทบ
๖.ความเสี่ยงจาก ระบบฐานข้อมูล เสียหาย ข้อมูลถูก ทำลาย ข้อมูลถูก แก้ไขโดยไม่ได้รับ อนุญาต	RIT06	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ระบบฐานข้อมูลเสียหาย ข้อมูลถูกทำลาย ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต	- ฐานข้อมูลเสียหาย - ข้อมูลถูกทำลาย - ข้อมูลถูกแก้ไข	- ระบบสารสนเทศ
๗.ความเสี่ยงจาก การนำเอา อุปกรณ์อื่นที่ ไม่ได้รับอนุญาต มาเชื่อมต่อ	RIT07	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่ายเช่นการนำ wirelessrouterหรือ switch/hubมาเชื่อมต่อกับระบบเครือข่ายหน่วยงานโดยไม่ได้รับอนุญาตและไม่ได้มีการตั้งค่าเครื่องที่ถูกต้องทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่าย ไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัยทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆ ที่รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่ายของหน่วยงานทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของหน่วยงาน	-การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ -ความล้มเหลวทางเทคนิค	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - เครื่องคอมพิวเตอร์แม่ข่าย
๘.ความเสี่ยงจาก กระแสไฟฟ้า ขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT08	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้องหรือเกิดแรงดันไฟฟ้าไม่คงที่ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องคอมพิวเตอร์แม่ข่าย ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหายและการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- กระแสไฟฟ้าขัดข้องไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	- ระบบสารสนเทศ - เครื่องคอมพิวเตอร์แม่ข่าย
๙.ความเสี่ยงจาก การเกิดไฟไหม้ แผ่นดินไหวอาคาร ถล่ม	RIT09	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคารแผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่อง คอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ทำให้ ได้รับความเสียหายทั้งหมด	- การเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	- ระบบสารสนเทศ - ห้องเก็บเครื่องคอมพิวเตอร์แม่ข่าย

ชื่อความเสี่ยง	รหัส	ประเภท ความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/ สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับ ผลกระทบ
๑๐.ความเสี่ยงจาก การโจรกรรมเครื่อง คอมพิวเตอร์แม่ข่าย และอุปกรณ์	RIT10	ความเสี่ยงจากภัยหรือ สถานการณ์ฉุกเฉิน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์หรือชิ้นส่วน ภายในเครื่องเช่น CPUและRAM ทำให้ไม่สามารถปฏิบัติงาน หรือ เกิดการสูญหายของข้อมูลบน เครื่อง คอมพิวเตอร์นั้นได้	- การโจรกรรม	- ระบบ สารสนเทศ - ห้องเก็บ เครื่อง คอมพิวเตอร์ แม่ข่าย
๑๑.ความเสี่ยงจาก สถานการณ์ความไม่ สงบเรียบร้อย ใน บ้านเมือง	RIT11	ความเสี่ยงจากภัยหรือ สถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อยจนทำ ให้บุคลากรไม่สามารถปฏิบัติงาน ได้ตามปกติ	- สถานการณ์ ความไม่สงบ เรียบร้อย	- ระบบ สารสนเทศ - ห้องเก็บ เครื่อง คอมพิวเตอร์ แม่ข่าย
๑๒.ความเสี่ยงจาก การขาดแคลน บุคลากร ผู้ปฏิบัติงาน	RIT12	ความเสี่ยงด้านการ บริหารจัดการ	การขาดแคลนบุคลากรด้าน สารสนเทศทำให้การทำงานอาจ หยุดชะงัก หากบุคลากร ผู้รับผิดชอบไม่สามารถมา ปฏิบัติงานได้และ จำนวน บุคลากรที่มีไม่เพียงพอต่อระบบ เทคโนโลยีสารสนเทศที่เพิ่มขึ้น ตามความ ต้องการของผู้ใช้งาน ส่งผลกระทบต่อการ พัฒนาและ ควบคุมดูแลระบบ	- การขาด แคลนบุคลากร	- ผู้ดูแลระบบ - ระบบ สารสนเทศ
๑๓.ความเสี่ยงจาก การเปลี่ยนแปลง นโยบาย ผู้บังคับบัญชา	RIT13	ความเสี่ยงด้านการ บริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้นโยบายการบริหาร จัดการสารสนเทศเปลี่ยนแปลง ด้วยทำให้การดำเนินการ โครงการต่างๆ ได้รับผลกระทบ	- นโยบายการ บริหารจัดการ สารสนเทศ	- ระบบ สารสนเทศ
๑๔.ความเสี่ยงจาก การได้รับการ สนับสนุน งบประมาณไม่ เพียงพอ	RIT14	ความเสี่ยงด้านการ บริหารจัดการ	การขาดแคลนงบประมาณในการ ดำเนินการให้ระบบสารสนเทศ สามารถดำเนินการได้ต่อเนื่อง อย่างมีประสิทธิภาพ	- งบประมาณ	- ระบบ สารสนเทศ

๘. การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณเป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยงได้แก่ระดับโอกาสที่จะเกิดความเสี่ยงระดับความรุนแรงของผลกระทบและระดับความเสี่ยงซึ่งใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
๕	สูงมาก	ตั้งแต่ ๕ ครั้ง/ปี
๔	สูง	๔ ครั้ง/ปี
๓	ปานกลาง	๓ ครั้ง/ ปี
๒	น้อย	๒ ครั้ง/ปี
๑	น้อยมาก	ไม่เกิน ๑ ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง

ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	>๑๐ล้านบาทหรือ เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	>๕แสนบาท – ๑๐ล้านบาทหรือ เกิดปัญหากับระบบ IT ที่สำคัญและระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	>๒.๕แสนบาท – ๕แสนบาทหรือ ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	>๑แสนบาท – ๑.๕แสนบาทหรือ เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	ไม่เกิน๑๐๐,๐๐๐บาทหรือ เกิดเหตุร้ายที่ไม่มีความสำคัญ

การประมาณความเสี่ยง (Risk estimation) แสดงดังตารางดังนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่ (ครั้ง/ปี)	ความรุนแรง	ระดับความเสี่ยง
๑.ความเสี่ยงจากการถูกมัลแวร์ (Malware) ทำลายฐานข้อมูล โปรแกรมใช้งานหรือระบบปฏิบัติการต่าง	RIT01	ความเสี่ยงด้านเทคนิค	การบุกรุกโจมตีโดยโปรแกรมไม่ประสงค์ดีเช่นการติด Malware เป็นต้น	๕	๔	๒๐
๒.ความเสี่ยงจากการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคล (Hacker) โดยไม่ได้รับอนุญาต	RIT02	ความเสี่ยงด้านเทคนิค	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดีเช่นhackerเป็นต้นการดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย	๔	๕	๒๐

ชื่อความเสี่ยง	รหัส	ประเภท ความเสี่ยง	ลักษณะความเสี่ยง	ความถี่ (ครั้ง/ปี)	ความ รุนแรง	ระดับ ความเสี่ยง
๓.ความเสี่ยงจาก ระบบเชื่อมโยง เครือข่าย คอมพิวเตอร์หลัก (Backbone) เสียหาย/ขัดข้อง	RIT03	ความเสี่ยงด้านเทคนิค	ระบบเชื่อมโยงเครือข่าย คอมพิวเตอร์หลัก (Backbone) เสียหาย/ขัดข้องด้วยสาเหตุทาง เทคนิค หรือจากสัตว์ กัดแทะ เช่นหนูหรือแมลงเป็นต้น	๕	๔	๒๐
๔.ความเสี่ยงจาก เครื่องคอมพิวเตอร์ หรืออุปกรณ์ ขัดข้อง ไม่ สามารถทำงาน ได้ตามปกติ	RIT04	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ ชำรุดหรือขัดข้องด้วยสาเหตุทาง เทคนิคหรือจากสัตว์ กัดแทะ เช่น หนูหรือแมลงเป็นต้น	๕	๔	๒๐
๕.ความเสี่ยงจาก การอำพรางหรือสวม รอยผู้ใช้การเข้าถึง ข้อมูลโดยไม่ได้รับ อนุญาต	RIT05	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการ เข้าใช้ระบบสารสนเทศ เช่น การ มอบหมายให้ผู้อื่นใช้รหัสผ่านของ ตนเองเข้าใช้ระบบหรือใช้งานแทน	๔	๔	๑๖
๖.ความเสี่ยงจาก ระบบฐานข้อมูล เสียหาย ข้อมูลถูก ทำลาย ข้อมูลถูก แก้ไขโดยไม่ได้รับ อนุญาต	RIT06	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ระบบฐานข้อมูลเสียหาย ข้อมูล ถูกทำลาย ข้อมูลถูกแก้ไขโดย ไม่ได้รับอนุญาต	๓	๔	๑๒
๗.ความเสี่ยงจาก การนำเอา อุปกรณ์ อื่นที่ ไม่ได้รับอนุญาต มาเชื่อมต่อ	RIT07	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการ ใช้ระบบเครือข่ายเช่นการนำ wirelessrouterหรือ switch/hubมาเชื่อมต่อกับระบบ เครือข่ายหน่วยงานโดยไม่ได้รับ อนุญาตและไม่ได้มีการตั้งค่า เครื่องที่ถูกต้องทำให้เครื่อง คอมพิวเตอร์อื่นในระบบ เครือข่าย ไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษา ความปลอดภัยทำให้เครื่อง คอมพิวเตอร์ของบุคคลภายนอก อื่นๆ ที่รับสัญญาณได้เชื่อมต่อเข้า กับระบบเครือข่ายของหน่วยงาน ทำให้เกิดช่องโหว่กับระบบรักษา ความปลอดภัยของหน่วยงาน	๓	๓	๙

ชื่อความเสี่ยง	รหัส	ประเภท ความเสี่ยง	ลักษณะความเสี่ยง	ความถี่ (ครั้ง/ปี)	ความ รุนแรง	ระดับ ความเสี่ยง
๘.ความเสี่ยงจาก กระแสไฟฟ้า ขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT08	ความเสี่ยงจากภัยหรือ สถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้องหรือ เกิดแรงดันไฟฟ้าไม่คงที่ทำให้ เครื่องคอมพิวเตอร์และอุปกรณ์ อาจได้รับความเสียหายจาก แรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อ กระแสไฟฟ้าขัดข้องทำให้เครื่อง คอมพิวเตอร์แม่ข่าย ถูกปิดไปโดย ไม่สมบูรณ์ อาจทำให้ข้อมูล สารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่ สามารถเปิดใช้งานได้โดยอัตโนมัติ	๕	๔	๒๐
๙.ความเสี่ยงจาก การเกิดไฟไหม้ แผ่นดินไหวอาคาร ถล่ม	RIT09	ความเสี่ยงจากภัยหรือ สถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคารแผ่นดินไหว จนอาคารถล่ม ไม่สามารถ เคลื่อนย้ายเครื่อง คอมพิวเตอร์ และอุปกรณ์ต่างๆ ได้ทำให้ ได้รับ ความเสียหายทั้งหมด	๑	๕	๕
๑๐.ความเสี่ยงจาก การโจรกรรมเครื่อง คอมพิวเตอร์แม่ข่าย และอุปกรณ์	RIT10	ความเสี่ยงจากภัยหรือ สถานการณ์ฉุกเฉิน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์หรือชิ้นส่วน ภายในเครื่องเช่น CPUและRAM ทำให้ไม่สามารถปฏิบัติงาน หรือ เกิดการสูญหายของข้อมูลบน เครื่อง คอมพิวเตอร์นั้นได้	๑	๕	๕
๑๑.ความเสี่ยงจาก สถานการณ์ความไม่ สงบเรียบร้อย ใน บ้านเมือง	RIT11	ความเสี่ยงจากภัยหรือ สถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อยจนทำ ให้บุคลากรไม่สามารถปฏิบัติงาน ได้ตามปกติ	๔	๔	๑๖
๑๒.ความเสี่ยงจาก การขาดแคลน บุคลากร ผู้ปฏิบัติงาน	RIT12	ความเสี่ยงด้านการ บริหารจัดการ	การขาดแคลนบุคลากรด้าน สารสนเทศทำให้การทำงานอาจ หยุดชะงัก หากบุคลากร ผู้รับผิดชอบไม่สามารถมา ปฏิบัติงานได้และ จำนวน บุคลากรที่มีไม่เพียงพอต่อระบบ เทคโนโลยีสารสนเทศที่เพิ่มขึ้น ตามความ ต้องการของผู้ใช้งาน ส่งผลกระทบต่อการ พัฒนาและ ควบคุมดูแลระบบ	๓	๔	๑๒

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่ (ครั้ง/ปี)	ความรุนแรง	ระดับความเสี่ยง
๑๓.ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บังคับบัญชา	RIT13	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชาอาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วยทำให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ	๑	๒	๒
๑๔.ความเสี่ยงจากการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT14	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๓	๓	๙

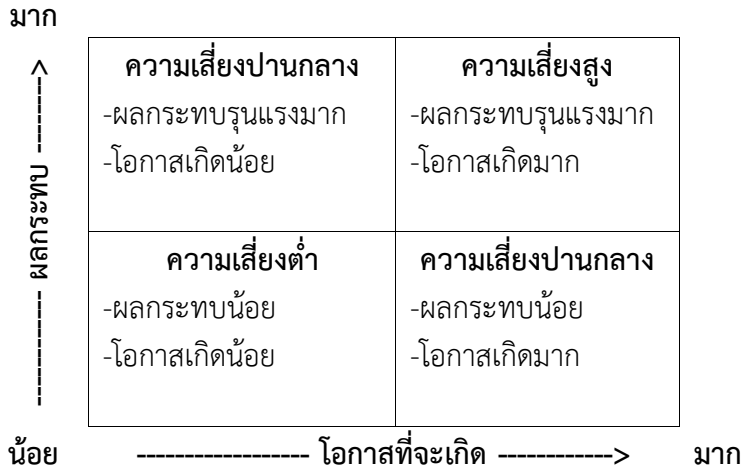
๙.การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยของขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และ ประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และ ผลกระทบที่เกิดขึ้นและขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

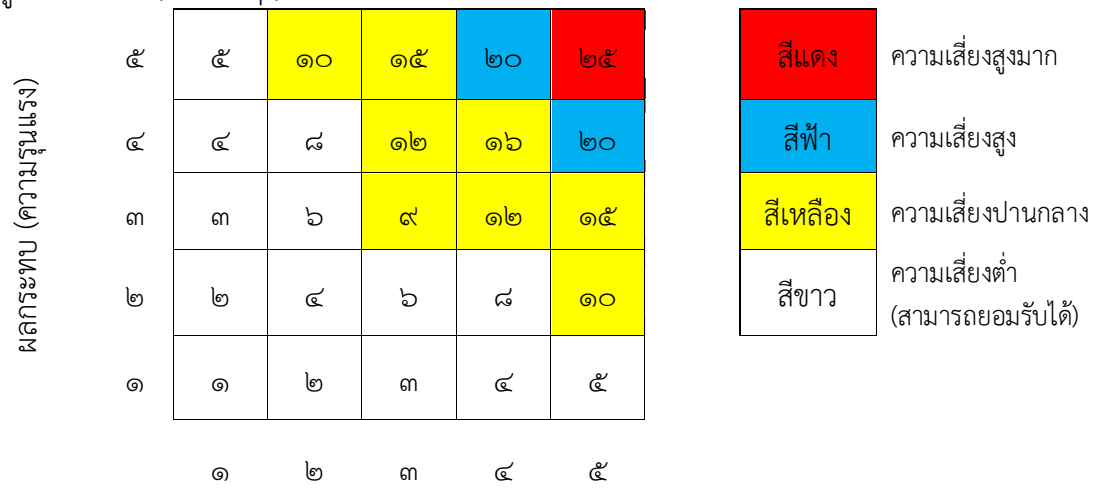
ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่างๆ x ความรุนแรงของเหตุการณ์ต่างๆ ซึ่งใช้เกณฑ์ในการจัดแบ่งดังนี้

ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑– ๘	ต่ำ	ยอมรับความเสี่ยง	ขาว
๙– ๑๖	ปานกลาง	ยอมรับความเสี่ยง(มีมาตรการติดตาม)	เหลือง
๑๗– ๒๔	สูง	จำกัดความเสี่ยง(มีแผนควบคุมความเสี่ยง)	ฟ้า
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

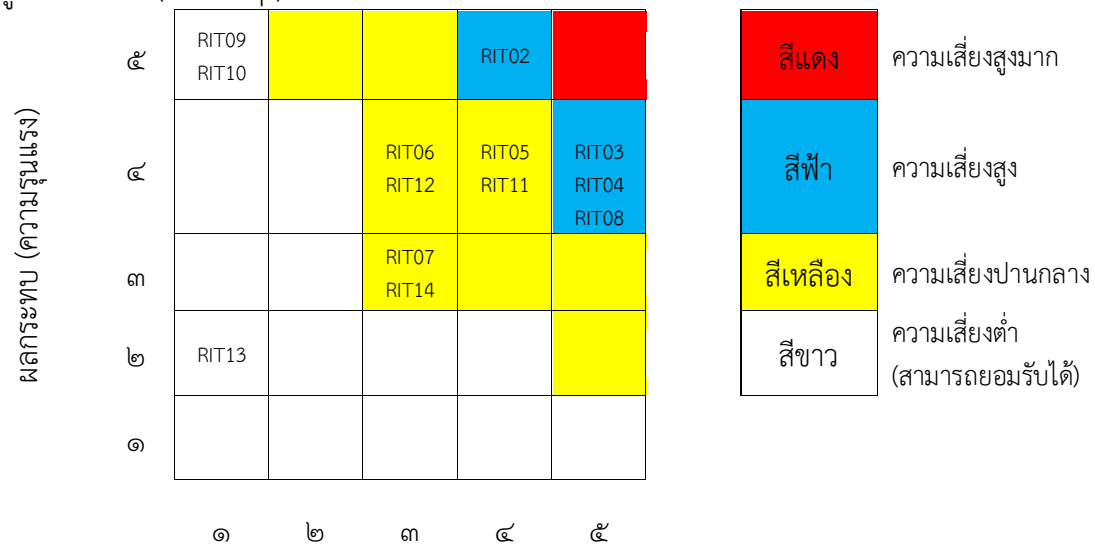
แผนภูมิความเสี่ยง (Risk Map) เป็นการวัดระดับความเสี่ยงโดยจัดลำดับจากผลกระทบและความเป็นไปได้ที่จะเกิดขึ้น



แผนภูมิความเสี่ยง (Risk Map)



แผนภูมิความเสี่ยง (Risk Map)



๑๐. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

แสดงดังตารางจากผลการประเมินค่าความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงของระบบสารสนเทศ ในการบริหารจัดการได้อย่างมีประสิทธิภาพดังนี้

ลำดับ	ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ระดับความเสี่ยง
๑.	ความเสี่ยงจากการถูกมัลแวร์ (Malware) ทำลายฐานข้อมูล โปรแกรมใช้งานหรือระบบปฏิบัติการต่าง ๆ	RIT01	ความเสี่ยงด้านเทคนิค	การบุกรุกโจมตีโดยโปรแกรมไม่ประสงค์ดีเช่นการติด Malware เป็นต้น	๒๐
๒.	ความเสี่ยงจากการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคล (Hacker) โดยไม่ได้รับอนุญาต	RIT02	ความเสี่ยงด้านเทคนิค	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดีเช่นhackerเป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย	๒๐

ลำดับ	ชื่อความเสี่ยง	รหัส	ประเภท ความเสี่ยง	ลักษณะความเสี่ยง	ระดับ ความเสี่ยง
๓.	ความเสี่ยงจากระบบเชื่อมโยงเครือข่ายคอมพิวเตอร์หลัก (Backbone) เสียหาย/ขัดข้อง	RIT03	ความเสี่ยงด้านเทคนิค	ระบบเชื่อมโยงเครือข่ายคอมพิวเตอร์หลัก (Backbone) เสียหาย/ขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์ กัดแทะ เช่นหนูหรือแมลงเป็นต้น	๒๐
๔.	ความเสี่ยงจากเครื่องคอมพิวเตอร์ หรืออุปกรณ์ขัดข้องไม่ สามารถทำงาน ได้ตามปกติ	RIT04	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิคหรือจากสัตว์ กัดแทะ เช่นหนูหรือแมลงเป็นต้น	๒๐
๕.	ความเสี่ยงจากกระแสไฟฟ้าขัดข้องไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT08	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้องหรือเกิดแรงดันไฟฟ้าไม่คงที่ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องคอมพิวเตอร์แม่ข่าย ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหายและการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๒๐
๖.	ความเสี่ยงจากการอำพรางหรือสวมรอยผู้ใช้การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	RIT05	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของ ตนเองเข้าใช้ระบบหรือใช้งานแทน	๑๖
๗.	ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อย ในบ้านเมือง	RIT11	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อยจนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๑๖
๘.	ความเสี่ยงจากระบบฐานข้อมูลเสียหาย ข้อมูลถูกทำลาย ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต	RIT06	ความเสี่ยงจากผู้ปฏิบัติงาน	ระบบฐานข้อมูลเสียหาย ข้อมูลถูกทำลาย ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต	๑๒

ลำดับ	ชื่อความเสี่ยง	รหัส	ประเภท ความเสี่ยง	ลักษณะความเสี่ยง	ระดับ ความเสี่ยง
๙.	ความเสี่ยงจากการขาดแคลนบุคลากร ผู้ปฏิบัติงาน	RIT12	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้และ จำนวนบุคลากรที่มีไม่เพียงพอต่อระบบ เทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความ ต้องการของผู้ใช้งานส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๑๒
๑๐.	ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ ไม่ได้รับอนุญาต มาเชื่อมต่อ	RIT07	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่ายเช่นการนำ wirelessrouterหรือ switch/hubมาเชื่อมต่อกับระบบเครือข่ายหน่วยงานโดยไม่ได้รับอนุญาตและไม่ได้มีการตั้งค่าเครื่องที่ถูกต้องทำให้เครื่อง คอมพิวเตอร์อื่นในระบบเครือข่าย ไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัยทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอก อื่นๆ ที่รับสัญญาณได้เชื่อมต่อเข้า กับระบบเครือข่ายของหน่วยงาน ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของหน่วยงาน	๙
๑๑.	ความเสี่ยงจากการได้รับการสนับสนุน งบประมาณไม่เพียงพอ	RIT14	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๙
๑๒.	ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหวอาคารถล่ม	RIT09	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ทำให้ ได้รับความเสียหายทั้งหมด	๕

ลำดับ	ชื่อความเสี่ยง	รหัส	ประเภท ความเสี่ยง	ลักษณะความเสี่ยง	ระดับ ความเสี่ยง
๑๓.	ความเสี่ยงจากการโจรกรรม เครื่อง คอมพิวเตอร์แม่ข่าย และ อุปกรณ์	RIT10	ความเสี่ยงจากภัยหรือ สถานการณ์ฉุกเฉิน	การโจรกรรมเครื่อง คอมพิวเตอร์อุปกรณ์ คอมพิวเตอร์หรือชิ้นส่วนภายใน เครื่องเช่น CPUและRAMทำให้ ไม่สามารถปฏิบัติงาน หรือเกิด การสูญหายของข้อมูลบนเครื่อง คอมพิวเตอร์นั้นได้	๕
๑๔.	ความเสี่ยงจากการเปลี่ยนแปลง นโยบาย ผู้บังคับบัญชา	RIT13	ความเสี่ยงด้านการ บริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้นโยบายการบริหาร จัดการสารสนเทศเปลี่ยนแปลง ด้วยทำให้การดำเนินการ โครงการต่างๆ ได้รับผลกระทบ	๒

๑๑. การจัดการความเสี่ยง(Risk management)

ระดับความเสี่ยงคงเหลือที่ยอมรับได้<๙หน่วยงานกำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยงคือความเสี่ยงที่มีระดับความเสี่ยงสูงตั้งแต่๑๗ขึ้นไปส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๗ ถือว่ามีความเสี่ยงค่อนข้าง ต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ลำดับ	ชื่อความเสี่ยง	รหัส	ระดับ ความเสี่ยง	กลยุทธ์การจัดการ ความเสี่ยง	แนวทางการดำเนินการ จัดการความเสี่ยง
๑.	ความเสี่ยงจาก การถูกมัลแวร์ (Malware) ทำลาย ฐานข้อมูล โปรแกรมใช้งานหรือ ระบบปฏิบัติการต่าง ๆ	RIT01	๒๐	-จำกัดความเสี่ยง	-ติดตั้งโปรแกรมป้องกันมัลแวร์และ update patchอย่างสม่ำเสมอ
๒.	ความเสี่ยงจาก การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบ ฐานข้อมูลจากบุคคล (Hacker) โดยไม่ได้รับ อนุญาต	RIT02	๒๐	-จำกัดความเสี่ยง	-ตรวจสอบการตั้งค่าของfirewallอย่าง สม่ำเสมอ - ติดตั้งระบบตรวจสอบการบุกรุก เครือข่ายและติดตาม เพื่อปรับปรุง อย่างสม่ำเสมอ - ติดตั้งpatch ของ ระบบปฏิบัติการ อย่าง สม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนว ทางการใช้งานระบบสารสนเทศที่กำหนด

ลำดับ	ชื่อความเสี่ยง	รหัส	ระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๓.	ความเสี่ยงจากระบบเชื่อมโยงเครือข่ายคอมพิวเตอร์หลัก (Backbone) เสียหาย/ขัดข้อง	RIT03	๒๐	- จำกัดความเสี่ยง	- ตรวจสอบระบบเชื่อมโยงเครือข่ายอย่างสม่ำเสมอ - ใช้ระบบเครือข่ายสำรอง
๔.	ความเสี่ยงจากเครื่องคอมพิวเตอร์ หรืออุปกรณ์ ขัดข้องไม่สามารถทำงาน ได้ตามปกติ	RIT04	๒๐	- จำกัดความเสี่ยง	-จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ ทดแทนชั่วคราวเพื่อสามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบ - จัดจ้างบำรุงรักษา เครื่องและอุปกรณ์อย่างสม่ำเสมอ
๕.	ความเสี่ยงจากกระแสไฟฟ้า ขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT08	๒๐	- จำกัดความเสี่ยง	- จัดหาเครื่องเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่
๖.	ความเสี่ยงจากการอำพรางหรือสวมรอยผู้ใช้การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	RIT05	๑๖	-ยอมรับความเสี่ยง	-สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนว ทางการใช้งานระบบสารสนเทศที่กำหนด
๗.	ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อย ในบ้านเมือง	RIT11	๑๖	-ยอมรับความเสี่ยง	- จัดหาระบบสำรองข้อมูลเพื่อให้ระบบสารสนเทศสามารถทำงานได้
๘.	ความเสี่ยงจากระบบฐานข้อมูลเสียหาย ข้อมูลถูกทำลาย ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต	RIT06	๑๒	-ยอมรับความเสี่ยง	- จัดหาระบบสำรองข้อมูลเพื่อให้ระบบสารสนเทศสามารถทำงานได้
๙.	ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT12	๑๒	-ยอมรับความเสี่ยง	-จัดอบรมเจ้าหน้าที่ให้มีความรู้เพิ่มเติม -จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่น สามารถปฏิบัติตามคู่มือได้

ลำดับ	ชื่อความเสี่ยง	รหัส	ระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๑๐.	ความเสี่ยงจากการนำเอา อุปกรณ์อื่นที่ไม่ได้รับอนุญาต มาเชื่อมต่อ	RIT07	๙	-ยอมรับความเสี่ยง	-จัดอบรมเพื่อสร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบสารสนเทศ -กระตุ้นให้เกิดการปฏิบัติ ตามแนวนโยบายหรือ ระเบียบด้านสารสนเทศ อย่างจริงจัง -ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิการเข้าถึง สำหรับอุปกรณ์ที่ไม่ได้รับ อนุญาตให้เชื่อมต่อเข้า เครือข่าย
๑๑.	ความเสี่ยงจากการได้รับการ สนับสนุนงบประมาณไม่ เพียงพอ	RIT14	๙	-ยอมรับความเสี่ยง	-จัดทำโครงการเพื่อขอรับการสนับสนุน - ใช้งบประมาณของหน่วย
๑๒.	ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหวอาคารถล่ม	RIT09	๕	-ยอมรับความเสี่ยง	-จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ -สำรองข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด
๑๓.	ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์	RIT10	๕	-ยอมรับความเสี่ยง	-ตรวจสอบการเข้าออกของบุคคลภายนอก -กำหนดพื้นที่หวงห้ามใน การเข้าถึงพื้นที่ปฏิบัติงาน -ตรวจสอบระบบการป้องกันรักษาความปลอดภัย ของสถานที่ให้อยู่ในสภาพ ปกติ -ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง
๑๔.	ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บังคับบัญชา	RIT13	๒	-ยอมรับความเสี่ยง	- ปฏิบัติตามนโยบายผู้บังคับบัญชา

การบริหารจัดการความเสี่ยงฉบับนี้ ให้ใช้เป็นแนวทางในการดำเนินการเพื่อการบริหารจัดการความเสี่ยงระบบสารสนเทศของหน่วยบัญชาการนาวิกโยธิน ต่อไป

๑๒. แนวทางการปฏิบัติรองรับสถานการณ์ฉุกเฉินด้านสารสนเทศ

๑๒.๑ การถูกมัลแวร์ (Malware) ทำลายฐานข้อมูล โปรแกรมใช้งานหรือระบบปฏิบัติการต่าง ๆ รายละเอียดตาม ผนวก ก

๑๒.๒ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคล (Hacker) โดยไม่ได้รับอนุญาต รายละเอียดตาม ผนวก ข

๑๒.๓ กระแสไฟฟ้าขัดข้อง ไฟดับ แรงดันไฟฟ้าไม่คงที่ รายละเอียดตาม ผนวก ค

๑๒.๔ ระบบเชื่อมโยงเครือข่ายคอมพิวเตอร์หลัก (Backbone) เสียหาย/ขัดข้อง รายละเอียดตาม ผนวก ง

๑๒.๕ เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถใช้งานได้ตามปกติ รายละเอียดตาม ผนวก จ

๑๒.๖ ระบบฐานข้อมูลเสียหายข้อมูลถูกทำลายข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต รายละเอียดตาม ผนวก ฉ

๑๒.๗ การเกิดแผ่นดินไหว ภัยธรรมชาติ รายละเอียดตาม ผนวก ช

๑๒.๘ การโจรกรรมเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ รายละเอียดตาม ผนวก ซ

๑๒.๙ สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง รายละเอียดตาม ผนวก ฌ

๑๒.๑๐ การเกิดเพลิงไหม้อาคาร รายละเอียดตาม ผนวก ญ

๑๒.๑๑ มาตรการหรือแนวทางการปฏิบัติ รายละเอียดตาม ผนวก ฎ

๑๓. แนวทางการปฏิบัติรองรับสถานการณ์ฉุกเฉิน

สำหรับแนวทางการปฏิบัติรองรับสถานการณ์ฉุกเฉินอื่นๆ นอกเหนือจากที่กล่าวไว้ในข้อ ๑๒ ให้คณะผู้บริหารเทคโนโลยีสารสนเทศ นย. พร้อมกับคณะเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย. และฝ่ายกรรมวิธีข้อมูล นย. เป็นผู้กำหนดแนวทางการปฏิบัติ

๑๔. การทบทวน ตรวจสอบและปรับปรุงแผน

คณะผู้บริหารเทคโนโลยีสารสนเทศ นย. พร้อมกับคณะเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย. และฝ่ายกรรมวิธีข้อมูล นย. จะดำเนินการทบทวนตรวจสอบและปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ปีละ ๑ ครั้ง ภายในไตรมาสแรกของปีงบประมาณหรือเมื่อเวลาที่เหมาะสม

(ลงชื่อ) น.อ.

(ปรัชญา หาญเทียม)
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล. ฝ่าย สส.อล.นย.
๓๐ เม.ย.๖๑

ผนวก ก

การถูกมัลแวร์ (Malware) ทำลายฐานข้อมูล โปรแกรมใช้งานหรือระบบปฏิบัติการต่าง ๆ

๑. ผู้สั่งการในที่เกิดเหตุ : หน.ฝ่ายกรรมวิธีข้อมูล นย./หน.ชุดปฏิบัติการ

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

๒.๑ เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ เช่น Log in เข้าระบบได้

๒.๒ ไฟล์งานในเครื่องคอมพิวเตอร์หายไป โดยการสังเกตจากข้อความที่แจ้งเตือน

๒.๓ โปรแกรมไม่สามารถทำงานได้ (Run ไม่ขึ้น)

๒.๔ มี System Message ที่แสดงให้เห็นว่าคอมพิวเตอร์ไม่สามารถทำงานได้

๓. การรายงานเหตุ

๓.๑ รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ผู้บังคับบัญชาและผู้เกี่ยวข้องรับทราบ

๓.๒ วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา

๓.๓ รายงานการปฏิบัติทั้งหมดในการแก้ไขปัญหา

๔. ขั้นตอนการปฏิบัติ

๔.๑ ดำเนินการจดบันทึก/สรุป และทำการ Print Screen ข้อความที่ผิดปกติ

๔.๒ แจ้งผู้รับผิดชอบหรือเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย. หรือฝ่ายกรรมวิธีข้อมูล นย.

๔.๓ ติดตั้งโปรแกรมระบบปฏิบัติการใหม่

๔.๔ ติดตั้งระบบการให้บริการของเครื่องคอมพิวเตอร์แม่ข่าย

๔.๕ กู้คืนข้อมูลจากระบบสำรองข้อมูลเข้ามาในระบบฐานข้อมูลเดิม

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑

ผนวก ข

การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ฐานข้อมูลจากบุคคล (Hacker) โดยไม่ได้รับอนุญาต

๑. ผู้สั่งการในที่เกิดเหตุ : หน.ฝ่ายกรรมวิธีข้อมูล นย./หน.ชุดปฏิบัติการ

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

๒.๑ เกิดความผิดปกติทางกายภาพ เช่น ดิสก์สูญหาย หรือเสียหาย

๒.๒ เกิดจากการทำงานของระบบ เช่น ไม่สามารถเข้าถึงข้อมูลได้

๒.๓ มี System Message ที่แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้

๓. การรายงานเหตุ

๓.๑ รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ผู้บังคับบัญชาและผู้เกี่ยวข้องรับทราบ

๓.๒ วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา

๓.๓ รายงานการปฏิบัติทั้งหมดในการแก้ไขปัญหา

๔. ขั้นตอนการปฏิบัติ

๔.๑ ตรวจสอบภัยคุกคาม เพื่อแก้ปัญหา

๔.๒ ตัดการเชื่อมต่อของเครื่องคอมพิวเตอร์แม่ข่ายหรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย

๔.๓ เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก

๔.๔ วิเคราะห์การถูกโจมตี โดยตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการและไฟล์อื่น

๔.๕ วิเคราะห์ Log file ตรวจสอบโปรแกรมหรือข้อมูลที่ผู้บุกรุกทิ้งไว้

๔.๖ ตรวจสอบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

๔.๗ ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ

๔.๘ กู้คืนระบบคอมพิวเตอร์ ระบบฐานข้อมูลหรือระบบสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการใหม่ทั้งหมด

๔.๙ งดใช้ Service ที่ไม่จำเป็น

๔.๑๐ ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

๔.๑๑ อุดช่องโหว่ในระบบเครือข่าย

๔.๑๒ เปลี่ยนแปลง Password ใหม่ หลังจากแก้ไขช่องโหว่ของระบบแล้ว

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑

ผนวก ค

กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่

๑. ผู้สั่งการในที่เกิดเหตุ : หน.ฝ่ายกรรมวิธีข้อมูล นย./หน.ชุดปฏิบัติการ

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

๒.๑ ไฟฟ้าขัดข้อง (ไฟตก)

๒.๒ ไฟฟ้าดับ

๓. การรายงานเหตุ

๓.๑ รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ผู้บังคับบัญชาและผู้เกี่ยวข้องทราบ

๓.๒ วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ปัญหา

๓.๓ รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

๔.๑ ตรวจสอบว่าไฟฟ้าขัดข้อง/ไฟดับ เกิน ๑๕ นาทีหรือไม่

๔.๒ ปิดอุปกรณ์เครือข่าย

๔.๓ ปิดเครื่องคอมพิวเตอร์แม่ข่ายและระบบสารสนเทศ

๔.๔ เปิดอุปกรณ์เครือข่าย

๔.๕ ตรวจสอบความเสียหายระบบสารสนเทศ

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑

ผนวก ง

ระบบเชื่อมโยงเครือข่ายคอมพิวเตอร์หลัก (Backbone) เสียหาย/ขัดข้อง

๑. ผู้สั่งการในที่เกิดเหตุ : หน.ฝ่ายกรรมวิธีข้อมูล นย./หน.ชุดปฏิบัติการ

๒. การตรวจสอบและสรุปปัญหาสาเหตุเบื้องต้น

๒.๑ เครื่องคอมพิวเตอร์ เรียกดูข้อมูลจากระบบ Intranet ทร. ไม่ได้

๒.๒ เครื่องคอมพิวเตอร์ เรียกดูข้อมูลจากระบบ Internet ไม่ได้

๓. การรายงานเหตุ

๓.๑ รายงานการตรวจสอบและสรุปหาสาเหตุเบื่องต้นให้ผู้บังคับบัญชาและผู้เกี่ยวข้องทราบ

๓.๒ วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ปัญหา

๓.๓ รายงานการปฏิบัติทั้งหมดในการแก้ไขปัญหา

๔. ขั้นตอนการปฏิบัติ

๔.๑ แจ้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย. และฝ่ายกรรมวิธีข้อมูล นย.

๔.๒ ตรวจสอบระบบเครือข่ายภายใน (LAN) และระบบเชื่อมโยง

๔.๓ แก้ไขโดยใช้อุปกรณ์ Hardware สับเปลี่ยน กรณีอุปกรณ์เครือข่ายชำรุด หากเกินขีดความสามารถของหน่วยให้แจ้ง สสท.ทร. ดำเนินการต่อไป

๔.๔ หลังการตรวจสอบแก้ไขเสร็จเรียบร้อยแล้ว ให้ทำการทดลองระบบและตรวจสอบผลการใช้งาน

๔.๕ บันทึกผลการตรวจสอบแก้ไข

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑

ผนวก จ

เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถใช้งานได้ตามปกติ

๑. ผู้สั่งการในที่เกิดเหตุ : หน.ฝ่ายกรรมวิธีข้อมูล นย./หน.ชุดปฏิบัติการ

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

๒.๑ เกิดเสียงดังผิดปกติ หรือเสียงการหมุน Hard Disk ดังผิดปกติ

๒.๒ อุปกรณ์มีอาการสั่น

๒.๓ ไฟฟ้าดับ/กระพริบ

๒.๔ มี System Message ที่แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้

๓. การรายงานเหตุ

๓.๑ รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ผู้บังคับบัญชาและผู้เกี่ยวข้องทราบ

๓.๒ วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา

๓.๓ รายงานการปฏิบัติทั้งหมดในการแก้ไขปัญหา

๔. ขั้นตอนการปฏิบัติ

๔.๑ การจดบันทึก/สรุป และทำการ Print Screen ข้อความที่ผิดปกติ

๔.๒ แจ้งผู้รับผิดชอบหรือเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย.หรือ ฝ่ายกรรมวิธีข้อมูล นย.

๔.๓ ทำการสำรองข้อมูล (Back Up) จัดเก็บไว้ในสื่อบันทึกข้อมูลแบบภายนอก

๔.๔ ติดตั้งโปรแกรมระบบปฏิบัติการใหม่

๔.๕ ตั้งค่าระบบการให้บริการของเครื่องคอมพิวเตอร์แม่ข่าย

๔.๖ ดึงข้อมูลจากระบบสำรองข้อมูลเข้ามาในระบบฐานข้อมูลเดิม

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑

ผนวก ฉ

ระบบฐานข้อมูลเสียหาย ข้อมูลถูกทำลาย ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต

๑. ผู้สั่งการในที่เกิดเหตุ : หน.ฝ่ายกรรมวิธีข้อมูล นย./หน.ชุดปฏิบัติการ

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

๒.๑ เกิดความผิดปกติทางกายภาพ เช่น ดิสก์สูญหาย หรือเสียหาย

๒.๒ เกิดจากการทำงานของระบบ เช่น ไม่สามารถเข้าถึงข้อมูลได้

๒.๓ ที System Message ที่แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้

๓. การรายงานเหตุ

๓.๑ รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ผู้บังคับบัญชาและผู้เกี่ยวข้องทราบ

๓.๒ วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา

๓.๓ รายงานการปฏิบัติทั้งหมดในการแก้ไขปัญหา

๔. ขั้นตอนการปฏิบัติ

๔.๑ ดำเนินการจดบันทึก / สรุป และทำการ Print Screen ข้อความที่ผิดปกติ

๔.๒ แจ้งผู้รับผิดชอบ หรือเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย.

๔.๓ นำข้อมูลสำรอง (Backup) ในช่วงที่ต้องการมากู้คืนข้อมูล

๔.๔ ทำการตรวจสอบความถูกต้องของข้อมูล ว่าข้อมูลมีความสมบูรณ์ ครบถ้วน มีความน่าเชื่อถือ

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑

ผนวก ช

การเกิดแผ่นดินไหว ภัยธรรมชาติ

๑. ผู้สั่งการในที่เกิดเหตุ : หน.ฝ่ายกรรมวิธีข้อมูล นย./หน.ชุดปฏิบัติการ

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

๒.๑ รับแจ้งจากผู้เห็นเหตุการณ์ แผ่นดินไหว ภัยธรรมชาติ ที่เกิดความเสียหายต่อระบบเครือข่ายสารสนเทศ

๒.๒ นย. ตรวจสอบความเสียหายทางกายภาพที่เกิดภายใน นย.

๓. การรายงานเหตุ

๓.๑ รายงานสรุปการตรวจสอบความเสียหายให้ผู้บังคับบัญชาทราบ

๓.๒ เสนอหนทางการแก้ไขปัญหา

๓.๓ รายงานการปฏิบัติทั้งหมดในการแก้ไขปัญหา

๔. ขั้นตอนการปฏิบัติ

๔.๑ ประเมินและตรวจสอบความเสียหายเมื่อเหตุการณ์กลับสู่สภาวะปกติ

๔.๒ นำเครื่องคอมพิวเตอร์แม่ข่ายสำรองมาติดตั้งให้บริการทดแทนโดยเร็วที่สุด

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑

ผนวก ซ

การโจรกรรมเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์

๑. ผู้สั่งการในที่เกิดเหตุ : หน.ฝ่ายกรรมวิธีข้อมูล นย./หน.ชุดปฏิบัติการ

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

๒.๑ การสรุปเหตุเบื้องต้น โดยสังเกตจากเหตุผิดปกติ เช่น มีการงัดแงะ หรือร่องรอยการทำลายเพื่อการโจรกรรม

๓. การรายงานเหตุ

๓.๑ รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ผู้บังคับบัญชาและผู้เกี่ยวข้องทราบ

๓.๒ วิเคราะห์หาสาเหตุและเสนอแนะการแก้ไขปัญหา

๓.๓ รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

๔.๑ แจ้งนายทหารเวรประจำวัน

๔.๒ แจ้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย.

๔.๓ ประเมินและตรวจสอบความเสียหาย รายงานให้ผู้บังคับบัญชาทราบ

๔.๔ นำเครื่องคอมพิวเตอร์แม่ข่ายสำรองมาติดตั้งให้บริการแทนโดยเร็วที่สุด

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑

ผนวก ฌ

สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

๑. ผู้สั่งการในที่เกิดเหตุ : หน.ฝ่ายกรรมวิธีข้อมูล นย./หน.ชุดปฏิบัติการ.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

๒.๑ เกิดการชุมนุมประท้วงบริเวณ นย.หรือบริเวณใกล้เคียง

๒.๒ ไม่สามารถควบคุมกลุ่มผู้ชุมนุมประท้วงได้

๓. การรายงานเหตุ

๓.๑ รายงานสรุปการตรวจสอบเหตุเบื้องต้นให้ผู้บังคับบัญชาและผู้เกี่ยวข้องทราบ

๓.๒ เสนอแนะหนทางการแก้ไขปัญหา

๓.๓ รายงานการปฏิบัติทั้งหมดในการแก้ไขปัญหา

๔. ขั้นตอนการปฏิบัติ

๔.๑ แจ้งนายทหารเวรประจำวัน

๔.๒ แจ้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย.

๔.๓ ปิดระบบสารสนเทศ เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ประกอบ

๔.๔ ขนย้ายเครื่องคอมพิวเตอร์แม่ข่ายไว้ที่ปลอดภัย

๔.๕ ประเมินและตรวจสอบความเสียหาย เมื่อเหตุการณ์กลับสู่สภาวะปกติ

๔.๖ นำเครื่องคอมพิวเตอร์แม่ข่ายมาติดตั้งให้บริการโดยเร็วที่สุด

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑

ผนวก ญ
มาตรการรองรับ กรณีไฟไหม้อาคาร

๑. ผู้สั่งการในที่เกิดเหตุ : หน.ฝ่ายกรรมวิธีข้อมูล นย./หน.ชุดปฏิบัติการ

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

๒.๑ สัญญาณเตือนอัคคีภัยทำงาน

๒.๒ รับแจ้งว่าไฟไหม้อาคาร

๓. การรายงานเหตุ

๓.๑ รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ หน.จนท.รปภ.ระบบสารสนเทศ นย./ผู้บริหารเทคโนโลยีสารสนเทศ หรือผู้บังคับบัญชาของ นย. ทราบในโอกาสแรก

๓.๒ วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา

๓.๓ รายงานการปฏิบัติทั้งหมดในการแก้ปัญหาให้ผู้บังคับบัญชาทราบ

๔. ขั้นตอนการปฏิบัติ

๔.๑ แจ้งนายทหารเวรประจำวัน นย.

๔.๒ ขณะเกิดเหตุให้ปฏิบัติตามแผนเผชิญเหตุของ นย. (การป้องกันและระงับอัคคีภัย)

๔.๓ หลังเกิดเหตุให้ตรวจสอบและประเมินความเสียหาย ที่เกิดระบบสารสนเทศ

๔.๔ เข้าตรวจสอบอุปกรณ์ทั้งหมด ถ้าไม่เสียหาย ดำเนินการกู้ระบบทั้งหมดกลับมาใช้งาน

๔.๕ ในกรณีที่เกิดความเสียหายจนไม่สามารถให้บริการได้ ทำการสำรองข้อมูล ปิดระบบทั้งหมด

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑

ผนวก ฎ

มาตรการหรือแนวทางการปฏิบัติ

จากการวิเคราะห์ปัจจัยความเสี่ยงในรูปแบบต่าง ๆ ที่อาจเกิดขึ้น เพื่อให้การป้องกันและแก้ไขตลอดจนการจัดการกับระบบสารสนเทศและระบบเครือข่ายเป็นไปอย่างมีประสิทธิภาพในกรณีที่เกิดเหตุการณ์ที่ไม่ปลอดภัยหรือภัยพิบัติฉุกเฉินขึ้น จึงกำหนดการหรือแนวทางการปฏิบัติ ดังนี้

๑. การตรวจสอบและสรุปสาเหตุเบื้องต้น โดยการสังเกตอาการหรือเหตุผิดปกติ มี ๒ องค์ประกอบ คือ

๑.๑ ทางกายภาพ สภาพอันผิดปกติ เช่น กลิ่น อุณหภูมิ ไฟฟ้าดับ เสียง อาการสั่น

๑.๒ การทำงานของระบบ เช่น ไม่สามารถเข้าระบบงานได้ ระบบทำงานผิดพลาดมีข้อความแจ้งเหตุอันผิดปกติ

๒. การแจ้งเหตุ

๒.๑ แจ้งเหตุกรณีเร่งด่วน ให้ประสานแจ้งผู้ที่เกี่ยวข้องโดยตรง เช่น เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย. หรือนายทหารเวรประจำวัน บก.นย.

๒.๒ แจ้งเหตุกรณีปกติ ให้สรุปสาเหตุและจัดทำรายงานแจ้งไปยังผู้ที่เกี่ยวข้อง หรือแจ้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย. เพื่อรายงานผู้บังคับบัญชาทราบตามลำดับต่อไป

๓. การประเมินการปฏิบัติ

ให้เจ้าหน้าที่ ณ ที่เกิดเหตุ ประเมินสถานการณ์ที่เกิดขึ้น แล้วแจ้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย. เพื่อทำการป้องกันและแก้ไขปัญหาจากภัยพิบัติฉุกเฉินต่อไป

๔. แนวทางการปฏิบัติ

๔.๑ เป้าหมายการปฏิบัติ

๔.๑.๑ หน่วยงานที่เกี่ยวข้องสามารถสนับสนุนและประสานการปฏิบัติด้านระบบสารสนเทศอย่างเป็นระบบและรวดเร็ว

๔.๑.๒ สามารถป้องกันและลดความเสียหายที่อาจเกิดขึ้น ทั้งที่เป็นผลที่เกิดจากเหตุการณ์ภัยพิบัติฉุกเฉินโดยตรงและผลกระทบที่ตามมาได้อย่างทันท่วงที

๔.๒ หลักการปฏิบัติ

๔.๒.๑ ความรวดเร็วในการแก้ปัญหา การประเมินสถานการณ์ในกรณีที่เกิดเหตุภัยพิบัติฉุกเฉินในเขตพื้นที่รับผิดชอบ ให้พิจารณาเหตุการณ์ว่าเป็นภัยฉุกเฉินประเภทใดและรายงานให้ นย. ทราบทันที

๔.๒.๒ การสั่งการ เพื่อแก้ปัญหาให้หน่วยงานและบุคคลที่เกี่ยวข้องกับการปฏิบัติดำเนินการภายใต้คำสั่งของ นย. หรือ ผู้บริหารเทคโนโลยีสารสนเทศ นย.(CIO) หรือผู้ที่ได้รับมอบหมาย (แล้วแต่กรณี)

๔.๒.๓ ในกรณี นย. พิจารณาเห็นว่าเหตุการณ์ที่เกิดขึ้นเกินขีดความสามารถในการดำเนินการให้ประสานขอรับการสนับสนุนจากหน่วยงานอื่นที่เกี่ยวข้องหรือขอรับการสนับสนุนจากหน่วยงานอื่นที่เกี่ยวข้องหรือขอรับการสนับสนุนจากศูนย์เทคโนโลยีสารสนเทศ สสท.ทร. เข้าร่วมปฏิบัติการตามความจำเป็นและเหมาะสม

๔.๒.๔ ในกรณีที่ปรากฏว่าภัยที่เกิดขึ้นจากระบบเทคโนโลยี ให้ถือว่าการรักษาข้อมูลสารสนเทศเพื่อการบริหารเป็นสิ่งที่สำคัญที่สุด หากจำเป็นให้ทำการขนย้ายวัสดุอุปกรณ์และระบบฐานข้อมูลสารสนเทศออกจากบริเวณเกิดภัยทันที

๔.๒.๕ ความสม่ำเสมอในการตรวจสอบระบบ โดยใช้โปรแกรมป้องกันมัลแวร์ และ Firewall

๔.๒.๖ ต้องใช้วัสดุอุปกรณ์ที่ได้มาตรฐานและกำหนดมาตรฐานในการควบคุมดูแล ในกรณีที่มีการเก็บรักษาข้อมูลสารสนเทศที่อาจก่อให้เกิดผลกระทบต่อการดำเนินงานด้านระบบสารสนเทศ

๕. ขั้นตอนการปฏิบัติ (ก่อนเกิดภัย ขณะเกิดภัย และฟื้นฟูบูรณะ)

๕.๑ การเตรียมการก่อนเกิดภัย

๕.๑.๑ จัดทำให้มีการฝึกอบรมให้ความรู้แก่เจ้าหน้าที่ ให้ทราบถึงพิบัติภัยและวิธีป้องกันในการเก็บรักษาข้อมูลสารสนเทศ หากเกิดภัยพิบัติฉุกเฉินขึ้นในพื้นที่

๕.๑.๒ จัดให้มีการฝึกอบรมเพื่อเตรียมการดูแลรักษาเครื่องมืออุปกรณ์และข้อมูลที่มีการจัดเก็บโดยชี้แจงให้ทราบขั้นตอนและวิธีการปฏิบัติในขณะที่เกิดเหตุภัยพิบัติฉุกเฉิน

๕.๑.๓ จัดทำบัญชี E-mail หรือเว็บไซต์ของหน่วยงานเพื่อแจ้งเตือนในกรณีเกิดเหตุภัยพิบัติฉุกเฉินเกิดขึ้นในพื้นที่

๕.๑.๔ จัดให้มีวัสดุ อุปกรณ์ และคอมพิวเตอร์ ที่เหมาะสมและเตรียมสถานที่รองรับในการติดตั้ง หากมีปัญหาภัยพิบัติฉุกเฉินเกิดขึ้น

๕.๑.๕ ให้ตรวจสอบวัสดุ / อุปกรณ์ที่ใช้ในการเก็บรักษาข้อมูลสารสนเทศอยู่เป็นประจำ

๕.๒ การปฏิบัติเมื่อเกิดอัคคีภัย

๕.๒.๑ ภายในเขต บก.นย. ให้แจ้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย. ออกปฏิบัติงานตามแผนทันที

๕.๒.๒ นอกเขต บก.นย. ให้แจ้งเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ นย.หรือหน่วยงานด้านสารสนเทศที่สามารถขอรับการสนับสนุนความช่วยเหลือภายในเขตพื้นที่ช่วยแก้ไขปัญหาในเบื้องต้นและรายงานให้ นย. ทราบ

๕.๓ การฟื้นฟู

๕.๓.๑ หน่วยงานที่ประสบภัยพิบัติฉุกเฉิน ประเมินค่าความเสียหาย

๕.๓.๒ ปรับปรุงแก้ไขให้สถานการณ์คืนสู่สภาพปกติ กู้ข้อมูลคืนในกรณีที่เห็นว่าสามารถดำเนินการได้เอง

๕.๓.๓ กรณีที่ไม่สามารถดำเนินการได้ ให้รายงานความเสียหาย ประมาณการค่าความเสียหายให้ นย. ทราบ เพื่อขอสนับสนุนงบประมาณต่อไป

๖. แนวทางปฏิบัติเพื่อป้องกันภัยพิบัติฉุกเฉินด้านสารสนเทศ

๖.๑ การบำรุงรักษาทั่วไป

๖.๑.๑ มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้ โดยผู้ดูแลเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ รวมถึงการมีการรับประกันความเสียหายจากผู้ขายและมีการดูแลอย่างถูกต้องและต่อเนื่อง

๖.๑.๒ ปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

๖.๑.๓ ทำความสะอาดเครื่องคอมพิวเตอร์อยู่เสมอ และมีการตรวจสอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ

๖.๑.๔ ใช้คำสั่งของระบบปฏิบัติการในการบำรุงรักษาเครื่องเป็นประจำ

๖.๑.๕ การฝึกอบรมผู้ดูแลระบบและผู้ใช้งานให้มีความรู้ความเข้าใจในระบบงาน รวมถึงการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ

๖.๑.๖ การจัดเตรียมอุปกรณ์ที่จำเป็นในการเตรียมความพร้อมรับภัยพิบัติฉุกเฉินที่จะเกิดขึ้นต่อระบบสารสนเทศ ดังนี้

๖.๑.๖.๑ แผ่น Startup ระบบปฏิบัติการ

๖.๑.๖.๒ แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/ระบบงานต่าง ๆ

๖.๑.๖.๓ แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

๖.๑.๖.๔ แผ่นโปรแกรมป้องกันโปรแกรมประสงค์ร้าย

๖.๑.๖.๕ แผ่น Driver อุปกรณ์ต่าง ๆ

๖.๑.๖.๖ ระบบสำรองไฟฉุกเฉิน

๖.๑.๖.๗ อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๖.๒ มาตรการรักษาความปลอดภัยระบบสารสนเทศ

๖.๒.๑ กำหนดเจ้าหน้าที่ที่รับผิดชอบในการดำเนินการไว้อย่างชัดเจน

๖.๒.๒ ป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ โดยการติดตั้ง Firewall เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย ป้องกันการบุกรุกจากผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตเข้าสู่ระบบเครือข่ายของ นย. และกำหนดให้ Firewall มีการทำงานตลอดเวลา

๖.๒.๓ กำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์และในกรณีที่พบว่ามีการใช้งานหรือมีการเปลี่ยนแปลงในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที

๖.๒.๔ ทำการทดสอบโปรแกรมรักษาความปลอดภัยและประสิทธิภาพการใช้งานอย่างสม่ำเสมอ

๖.๒.๕ การจัดเก็บข้อมูลที่มีชั้นความลับจะต้องมีมาตรการควบคุมการเข้าถึงข้อมูล เช่น การใส่รหัสผ่าน การเข้ารหัสเป็นต้น

๖.๓ มาตรการในการป้องกันมัลแวร์

๖.๓.๑ ติดตั้งซอฟแวร์ป้องกันมัลแวร์ สำหรับคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย ซึ่งผู้ใช้งานจำเป็นต้องระมัดระวังการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะการเชื่อมต่อกับระบบอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบ โดยวิธีการดังนี้

๑) ติดตั้งโปรแกรมป้องกันมัลแวร์ที่เหมาะสมและอัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ

๒) เปิดใช้งาน Auto Protect

๓) ตรวจสอบหามัลแวร์ทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกต่าง ๆ

๔) ใช้โปรแกรมเพื่อทำการตรวจหามัลแวร์อย่างน้อยสัปดาห์ละ ๑ ครั้ง

๖.๓.๒ การป้องกันภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลข้อมูลต่าง ๆ

๑) ระวังภัยจากการเปิดไฟล์สื่อบันทึกข้อมูลต่าง ๆ เช่น External Harddisk USB Flash Drive ควรมีการสแกนก่อนเปิดใช้งานทุกครั้ง

๒) ระมัดระวังในการปิด E-mail เช่น อย่าเปิดไฟล์ที่ไม่ทราบแหล่งที่มาหรือถ้าไม่ทราบแหล่งที่มาควรลบทิ้งทันที

๓) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น หากมีการแชร์ไฟล์ต้องมีมาตรการควบคุมการเข้าถึงข้อมูล เช่น การใส่รหัสผ่าน การเข้ารหัส

๔) ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จากอินเทอร์เน็ต เช่น ไม่ดาวน์โหลดจากเว็บไซต์ที่ไม่น่าเชื่อถือ

๕) ไม่ควรเปิดไฟล์นามสกุลแปลก ๆ ที่น่าสงสัย เช่น *.pif

๖) หลีกเลี่ยงการใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๖.๔ การจัดการด้านกายภาพและสิ่งแวดล้อม

๖.๔.๑ พิจารณาตำแหน่งของห้องเก็บเครื่องคอมพิวเตอร์แม่ข่าย รวมถึงกำหนดที่ตั้งของเครื่องคอมพิวเตอร์ การเดินสายไฟฟ้า สายสัญญาณ โดยหลีกเลี่ยงการติดตั้งระบุไว้ในจุดที่มีความเสี่ยง รวมทั้งมีอุปกรณ์ป้องกันภัยพิบัติฉุกเฉินเบื้องต้น เช่น เครื่องปรับอากาศ ตู้ Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย ถังดับเพลิง เป็นต้น

๖.๔.๒ การควบคุมการเข้าออกห้องเก็บเครื่องคอมพิวเตอร์แม่ข่าย และการป้องกันความเสียหายโดยมีกุญแจล็อก และห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องเก็บเครื่องคอมพิวเตอร์แม่ข่ายหากไม่มีความจำเป็น

๖.๔.๓ กำหนดให้ห้องเก็บเครื่องคอมพิวเตอร์แม่ข่าย เป็นพื้นที่หวงห้ามและกำหนดสิทธิการเข้าออกโดยเฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น

๖.๔.๔ จัดเก็บเครื่องคอมพิวเตอร์แม่ข่ายให้เป็นสัดส่วนเฉพาะ เพื่อความสะดวกในการปฏิบัติงานและยังทำให้การควบคุมและการเข้าถึงอุปกรณ์คอมพิวเตอร์ต่าง ๆ มีประสิทธิภาพมากขึ้น โดยจัดแยกส่วนอุปกรณ์ที่จำเป็นในการเข้าถึงข้อมูล เช่น การสำรองข้อมูลไว้กรณีฉุกเฉินเมื่อข้อมูลเกิดการเสียหาย

๖.๔.๕ วางระบบป้องกันภัยที่เหมาะสม โดยให้มีอุปกรณ์ดับเพลิงที่พร้อมใช้งานตลอดเวลา

๖.๔.๖ จัดให้มีระบบป้องกันไฟกระชาก เพื่อไม่ให้เครื่องคอมพิวเตอร์ได้รับความเสียหาย รวมทั้งติดตั้งระบบสายดินที่ได้มาตรฐานหรือจัดให้มีระบบไฟสำรอง

๖.๔.๗ มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยการตั้งอุณหภูมิเครื่องปรับอากาศและค่าความชื้นให้มีระดับเหมาะสมกับระบบคอมพิวเตอร์

๖.๕ การสำรองข้อมูลและการกู้คืนข้อมูล

๖.๕.๑ การสำรองข้อมูล (Back Up) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น ให้ทำการสำรองข้อมูลไว้ใน External Hard disk USB Flash Drive DVD CD หรือติดตั้งระบบ Backup อื่น ๆ เพื่อให้มีความพร้อมในการใช้งานและป้องกันข้อมูลสูญหายของข้อมูลในระบบสารสนเทศ โดยให้ทำการสำรองข้อมูลไว้ดังนี้

๑) การ Backup ข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายให้ Backup ไว้ที่เครื่องคอมพิวเตอร์แม่ข่ายสำรองข้อมูล (Backup Server) ที่เวลา ๑๖๐๐ ของทุกวัน

๒) การ Backup ข้อมูลของหน่วยงาน ให้เจ้าหน้าที่ประจำเครื่องนั้น ๆ ทำการ Backup ข้อมูลลงใน External Harddisk หรือสื่อบันทึกข้อมูลทุกสัปดาห์ และหากเป็นการสำรองข้อมูลที่มีชั้นความลับ จะต้องมีมาตรการควบคุมการเข้าถึงข้อมูล เช่น การใส่รหัสผ่าน การเข้ารหัส

๖.๕.๒ ลงคำสั่งแต่งตั้งเจ้าหน้าที่รับผิดชอบงานรักษาความปลอดภัยระบบสารสนเทศไว้อย่างชัดเจน

๖.๕.๓ กำหนดให้มีการทดสอบข้อมูลสำรองอย่างน้อยเดือนละ ๑ ครั้ง เพื่อตรวจสอบว่าข้อมูลและโปรแกรมต่าง ๆ ที่สำรองไว้มีความครบถ้วนและสามารถใช้งานได้จริง

๖.๕.๔ จัดเก็บข้อมูลสำรองไว้ในสถานที่ที่ปลอดภัยและติดป้ายแสดงไว้อย่างชัดเจน

๖.๖ การตรวจสอบการเข้าสู่ระบบ

๖.๖.๑ กำหนดสิทธิให้แก่ผู้ใช้งาน

๑) กำหนดสิทธิการเข้าถึงระบบสารสนเทศ เช่น กำหนดสิทธิในการเข้าใช้ระบบให้แก่ผู้ใช้งานให้เหมาะกับหน้าที่และความรับผิดชอบ

๒) กำหนดระยะเวลาการใช้งานของ User และ Password และต้องระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓) กำหนดให้มีการเปลี่ยนแปลงรหัสผ่านอย่างรอบคอบและมีชั้นความลับ

๔) ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น จะต้องขออนุญาตจากผู้มีอำนาจหน้าที่เพื่อให้การอนุมัติทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นในการเข้าใช้งาน

๖.๖.๒ ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน

๑) กำหนดให้รหัสผ่านมีความยาวตามมาตรฐานสากล

๒) ควรใช้อักขระพิเศษประกอบเช่น @ ; < > เป็นต้น

๓) สำหรับผู้ใช้งานทั่วไปควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุก ๖ เดือน ส่วนผู้ดูแลระบบควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๓ เดือน

๔) ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรจะกำหนดรหัสผ่านใหม่ซ้ำรหัสเดิม

๕) ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ไม่เปิดเผยรหัสผ่านให้แก่ผู้อื่น หรือยินยอมให้ผู้อื่นใช้รหัสผ่านของตนเองหรือไม่ใช้รหัสผ่านร่วมกับผู้อื่น ทั้งในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

๖.๗ มาตรการป้องกันปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

๖.๗.๑ ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายซึ่งมีระยะเวลาสำรองไฟได้ประมาณ ๑๕ – ๓๐ นาที

๖.๗.๒ เปิดเครื่องสำรองไฟตลอดเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา

๖.๖.๓ เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้งานรีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

๖.๘ การบริหารจัดการบุคลากร

๖.๘.๑ การบริหารจัดการบุคลากรด้านเทคโนโลยีสารสนเทศในลักษณะกระจายภารกิจและความรับผิดชอบ รวมทั้งการแต่งตั้งเจ้าหน้าที่ที่มีความรู้ความสามารถและมีประสบการณ์ด้านระบบสารสนเทศซึ่งสามารถถ่ายทอดความรู้แก่ผู้ใช้งานได้อย่างมีประสิทธิภาพ

๖.๘.๒ หากมีการเปลี่ยนแปลงผู้ดูแลระบบหรือเจ้าหน้าที่รับผิดชอบจะต้องแจ้งให้ผู้บังคับบัญชาทราบเพื่อประโยชน์ในการบริหารงาน

๖.๘.๓ ในกรณีที่มีความจำเป็น ควรจัดบุคลากรภายนอก (Outsourcings) เพื่อดำเนินการและควบคุมกำกับดูแลหรือเป็นที่ปรึกษาจากบริษัทที่มีความชำนาญเฉพาะทาง มีเครื่องมือและเทคโนโลยีทันสมัยซึ่งเอื้อต่อการพัฒนาระบบฐานข้อมูลสารสนเทศ

๖.๘.๔ จัดส่งเจ้าหน้าที่เข้ารับการฝึกอบรมความรู้ทางเทคโนโลยีสารสนเทศตามช่วงระยะเวลาที่เหมาะสม

ตรวจถูกต้อง

น.อ.

(ปรัชญา หาญเทียม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ นย./หน.ฝสส.อล.ฝ่าย สส.อล.นย.

๓๐ เม.ย.๖๑