การบริหารจัดการ

"ความเสี่ยง"

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

ประจำปีงบประมาณ พ.ศ. 2567

R

S

K

บทนำ

การบริหารจัดการความเสี่ยงมีความสำคัญและจำเป็นอย่างยิ่งในการป้องกันและควบคุมในด้านต่างๆ ที่อาจจะเกิดขึ้นจากสถานการณ์ที่ไม่แน่นอน ซึ่งมีผลกระทบต่อความสำเร็จขององค์กรโดยรวม ดังนั้น “การบริหารความเสี่ยงที่ดี” คือการที่คนในองค์กรมีหน้าที่เกี่ยวข้องทุกฝ่ายได้มีส่วนร่วมในการวิเคราะห์ ตรวจสอบ ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับองค์กรอยู่เสมอ อีกทั้งมีการร่วมกันวางแผนป้องกันและควบคุมให้เหมาะสมกับภารกิจ เพื่อลดสภาพปัญหาหรือหลีกเลี่ยงความเสี่ยงที่อาจจะสร้างความเสียหายหรือความสูญเสียให้กับองค์กร

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ จัดทำขึ้นเพื่อเป็นกรอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยหวังเป็นอย่างยิ่งว่าจะใช้เป็นแนวทางในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้เกิดประโยชน์ และช่วยให้การปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพและเกิดประสิทธิผลสูงสุดต่อไป

คณะทำงานบริหารจัดการความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
มีนาคม ๒๕๖๗

สารบัญ

บทที่ ๑
บทนำ

๑.๑ ความเป็นมา

เนื่องจากภารกิจของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช มีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงานของกรม จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรม เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น การบริหารจัดการความเสี่ยงของกรม โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารนี้ มีวัตถุประสงค์เพื่อเป็นแนวทางที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ซึ่งดำเนินการโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงนั้นเกิดขึ้นจริงและนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในดำเนินการ

๑.๒ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) คือ ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำเทคโนโลยีสารสนเทศมาใช้หรือมีการเปลี่ยนแปลงเทคโนโลยีหรือนวัตกรรมต่าง ๆ อย่างเฉียบพลัน (Disruptive Technology / Disruptive Innovation) ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน ทั้งนี้ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จะมีองค์ประกอบที่สำคัญ ๓ ประการ ได้แก่ แผนงานการใช้เทคโนโลยีสารสนเทศ การตัดสินใจในการนำเทคโนโลยีสารสนเทศมาใช้และการวัดผลและติดตามความเสี่ยงที่อาจเกิดขึ้น โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายในระบบงาน เหตุการณ์ภายนอก หรือคน (เจ้าหน้าที่ บุคคลภายนอก) ซึ่งส่งผลกระทบต่อการดำเนินงานของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑.๓ ความหมายและคำจำกัดความ

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือ ลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)

เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยงและทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

๑.๔ กรอบการบริหารจัดการความเสี่ยง (Framework)

การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ให้ความสำคัญต่อการดำเนินงานในกระบวนการที่บุคลากรทั่วทั้งองค์กรได้มีส่วนร่วม ในการคิดวิเคราะห์ และคาดการณ์ถึงเหตุการณ์ หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการกับความเสี่ยงดังกล่าว ให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ เพื่อให้องค์กรบรรลุในวัตถุประสงค์ที่ต้องการตามกรอบวิสัยทัศน์ และพันธกิจขององค์กร กรอบการบริหารความเสี่ยงสะท้อนถึงนโยบายการบริหารจัดการและการกำกับดูแลกิจกรรม ซึ่งสามารถบรรลุวัตถุประสงค์องค์กรทั้งในเชิงประสิทธิภาพและประสิทธิผลของงาน กรอบการบริหารความเสี่ยง ดำเนินการบริหารความเสี่ยงตามหลักการ Enterprise Risk Management-Integrated Framework ของ The Committee of Sponsoring Organizations of the Tread way Commission หรือ COSO ตามกรอบการบริหารความเสี่ยง ดังนี้

๑) สภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมขององค์กรเป็นองค์ประกอบที่สำคัญ ในการกำหนดกรอบบริหารความเสี่ยง ประกอบด้วยปัจจัยหลายประการ เช่น วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงาน บุคลากร กระบวนการทำงาน ระบบสารสนเทศ ระเบียบ เป็นต้น สภาพแวดล้อมภายในองค์กรประกอบเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงขององค์กร

๒) การกำหนดวัตถุประสงค์ (Objective Setting)

องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยง ให้มีความสอดคล้องกับกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจนและเหมาะสม

๓) การบ่งชี้เหตุการณ์ (Event Identification)

เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งในส่วนของปัจจัยเสี่ยงที่เกิดจากภายในและภายนอกองค์กร เช่น นโยบายบริหารงาน บุคลากร การปฏิบัติงาน การเงิน ระบบสารสนเทศ ระเบียบกฎหมาย ระบบบัญชี ภาษีอากร ทั้งนี้เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้น เพื่อให้ผู้บริหารสามารถพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจจะเกิดขึ้นได้เป็นอย่างดี

๔) การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงเป็นการจำแนกและพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โดยสามารถประเมินความเสี่ยงได้ทั้งจากปัจจัยความเสี่ยงภายนอกและปัจจัยความเสี่ยงภายในองค์กร

๕) การตอบสนองความเสี่ยง (Risk Response)

เป็นการดำเนินการหลังจากที่องค์กรสามารถบ่งชี้ความเสี่ยงขององค์กร และประเมินความสำคัญของความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงไปดำเนินการตอบสนองด้วยวิธีการที่เหมาะสม เพื่อลดความสูญเสียหรือโอกาสที่จะเกิดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้

๖) กิจกรรมการควบคุม (Control Activities)

การกำหนดกิจกรรมและการปฏิบัติต่างๆ ที่กระทำเพื่อลดความเสี่ยง และทำให้การดำเนินงานบรรลุตามวัตถุประสงค์และเป้าหมายขององค์กร เช่น การกำหนดกระบวนการปฏิบัติงานที่เกี่ยวข้องกับการจัดการความเสี่ยงให้กับบุคลากรภายในองค์กร เพื่อเป็นการสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้องและเป็นไปตามเป้าหมายที่กำหนด

๗) สารสนเทศและการสื่อสาร (Information and Communication)

องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยงให้เป็นไปตามกรอบ และขั้นตอนการปฏิบัติที่องค์กรกำหนด

๘) การติดตามประเมินผล (Monitoring)

องค์กรจะต้องมีการติดตามผล เพื่อให้ทราบถึงผลการดำเนินการว่ามีความเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

๑.๕ วัตถุประสงค์

๑) เพื่อให้การจัดการภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกรมอุทยานแห่งชาติ สัตว์ป่าและพันธุ์พืช มีประสิทธิภาพ และมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศ

๒) เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

๓) เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๔) เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๕) เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

๑.๖ ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

บทที่ ๒
การวิเคราะห์ความเสี่ยง

๒.๑ ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Type of Risk)

๑) ความเสี่ยงด้านข้อมูล (Information Risk) หมายถึง ความเสี่ยงที่เกิดจากข้อมูลต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ ไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาดโดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access risk) ทำให้ข้อมูลที่จัดเก็บรั่วไหล อาจทำให้เกิดการฟ้องร้องได้หรือมีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้โดยความเสี่ยงนี้อาจเกิดจากไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ ยังรวมไปถึงความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back Up) ที่สำคัญคือเพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูลสำรอง (Information Back-Up) การกู้คืนข้อมูล (Information Recovery) ซึ่งเป็นส่วนหนึ่งของแผนบริหารความต่อเนื่อง (Business Continuity Plan) และแผนกู้คืนข้อมูล (Disaster Recovery Plan)

๒) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม ความเสี่ยงในเรื่องของการจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่เหมาะสมกับลักษณะของงาน และขององค์กรที่ต้องมีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการและเหมาะสมกับงบประมาณ หรือความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงจากการที่อุปกรณ์เทคโนโลยีสารสนเทศหมดอายุไปเอง ความเสี่ยงจากการไม่ได้กำหนดหรือกำหนดกระบวนการอนุมัติใช้อุปกรณ์เทคโนโลยีสารสนเทศไม่ชัดเจน

๓) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึงความเสี่ยงที่เกิดจากการเลือกใช้หรือความเสี่ยงจากการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง การถูกผู้ไม่หวังดีทำลายระบบ (Hacker) การควบคุมการไม่เพียงพอ การที่ซอฟต์แวร์ที่ใช้อยู่ Out of date ความเสี่ยงที่เกิดจากการเลือกใช้ Software platforms ความเสี่ยงที่เกิดจากควบคุมการเปลี่ยนแปลงไม่เหมาะสมเพียงพอ ความเสี่ยงที่ไม่ได้กำหนดขั้นตอนการอนุมัติการใช้งานซอฟต์แวร์ การไม่ได้จัดทำขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Document operating procedures) ความเสี่ยงจากการไม่แยกระบบสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน (Separation of development, test and operation facilities) เป็นต้น

๔) ความเสี่ยงด้านบุคลากร (People Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ในเรื่องของการกำหนดโครงสร้าง การมอบหมายงานในหน้าที่ให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศที่มีความเหมาะสม คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีสารสนเทศ และสามารถถ่ายทอดความรู้นั้นให้แก่ผู้ใช้งานด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ทั้งนี้ ยังรวมถึงการที่ขาดแผนการฝึกอบรมด้านเทคโนโลยีสารสนเทศให้กับเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารอย่างทั่วถึง ทั้งในส่วนของผู้ดูแลระบบ (Administration) ผู้พัฒนาระบบ (Developer/Programmer) และผู้ใช้งานทั่วไป (User) อย่างสม่ำเสมอ

๕) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การไม่มีระบบรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย และการก่อการร้าย เป็นต้น

๖) ความเสี่ยงด้านเครือข่ายสื่อสาร (Network Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบเครือข่ายสื่อสารขัดข้อง ไม่มีระบบเครือข่ายสื่อสารสำรอง ความเสี่ยงที่เกิดจากไม่ได้กำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดในการบริหารจัดการสำหรับบริหารเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่ายโดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก การบำรุงรักษาอุปกรณ์เครือข่ายสื่อสารไม่สม่ำเสมอ ความเสี่ยงที่ผู้ดูแลระบบไม่มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และดูแล รักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่าง ๆ ที่ส่งผ่านทาง เครือข่าย เป็นต้น

๗) ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing) หมายถึง ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำโครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ เช่น ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่กำหนดไว้ เป็นต้น

๘) ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk) หมายถึง ความเสี่ยงที่เกิดจากกระบวนการทำงานด้านเทคโนโลยีสารสนเทศที่ไม่เป็นไปตามมาตรฐานสากล ขาดการนำ Best Practice ที่ดีมาใช้งานตามกำหนดกระบวนการที่เป็นมาตรฐานที่ดี ซึ่งอาจส่งผลทำให้องค์กรไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่มาตรฐานดังกล่าวได้กำหนดไว้

๒.๒ ลักษณะรายละเอียดของความเสี่ยง (Description of risk) แสดงตามตาราง

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	๑. ความเสี่ยงด้านข้อมูล	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๘. ความเสี่ยงด้านกระบวนการทำงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายกรม โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่ายของกรม ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของกรม	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	๕. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๔. ความเสี่ยงจากการถูกบุกรุกทางไซเบอร์ และการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๐๔	๒.ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๓. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	- การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม - การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ อุปกรณ์เครือข่าย
๕. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT๐๕	๔. ความเสี่ยงด้านบุคลากร	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	๔. ความเสี่ยงด้านบุคลากร	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ รวมถึงการดูแลรักษาห้องปฏิบัติการคอมพิวเตอร์และอุปกรณ์ให้มีความพร้อมใช้อย่างสม่ำเสมอ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ
๘. ความเสี่ยงจาก ภัยพิบัติ ภัยธรรมชาติ และภัยจากการทำงานของมนุษย์ รวมถึงสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๘	๕. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด - การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ - การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๙. ความเสี่ยงจาก เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT๐๙	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
๑๐. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	RIT๑๐	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๖. ความเสี่ยงด้านเครือข่ายสื่อสาร	-เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล -ไม่สามารถใช้งานระบบสารสนเทศที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน	- ความล้มเหลวทางเทคนิค	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑๑. ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	RIT๑๑	๗. ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก	หากมีทำงานผิดพลาดของโปรแกรม จะไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่และแก้ไขการทำงานที่ผิดพลาดได้ทันกับเหตุการณ์	ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ

๒.๓ การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งกรมใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	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	> ๑๐ ล้านบาท หรือ เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	> ๕ แสนบาท – ๑๐ ล้านบาท หรือ เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	> ๒.๕ แสนบาท – ๕ แสนบาท หรือ ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	> ๑ แสนบาท – ๒.๕ แสนบาท หรือ เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	ไม่เกิน ๑๐๐,๐๐๐ บาท หรือ เกิดเหตุร้ายที่ไม่มีความสำคัญ

ผลการประมาณความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	๑. ความเสี่ยงด้านข้อมูล	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล	๔	๔
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๘. ความเสี่ยงด้านกระบวนการทำงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายกรม โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของกรม ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของกรม	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย	๒	๒

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	๕. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ	๒	๔
๔. ความเสี่ยงจากการถูกบุกรุกทางไซเบอร์ และการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๐๔	๒.ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๓. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	- การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม - การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงานหรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ อุปกรณ์เครือข่าย	๕	๒

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๕. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT๐๕	๔. ความเสี่ยงด้านบุคลากร	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๒	๒
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	๔. ความเสี่ยงด้านบุคลากร	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๔
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ รวมถึงการดูแลรักษาห้องปฏิบัติการคอมพิวเตอร์และอุปกรณ์ให้มีความพร้อมใช้อย่างสม่ำเสมอ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ	๕	๔

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๘. ความเสี่ยงจาก ภัยพิบัติ ภัยธรรมชาติ และภัยจากการทำงานของมนุษย์ รวมถึงสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๘	๕. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด - การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ - การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๕
๙. ความเสี่ยงจาก เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT๐๙	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค สัตว์กัดแทะประเภทหนูหรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	๒	๒
๑๐. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	RIT๑๐	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๖. ความเสี่ยงด้านเครือข่ายสื่อสาร	-เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล -ไม่สามารถใช้งานระบบสารสนเทศที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน	- ความล้มเหลวทางเทคนิค	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	๑	๕

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๑๑. ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	RIT๑๑	๗. ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก	หากมีทำงานผิดพลาดของโปรแกรม จะไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่และแก้ไขการทำงานที่ผิดพลาดได้ทันกับเหตุการณ์	ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๒	๔

บทที่ ๓
การประเมินค่าความเสี่ยง

๓.๑ การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่าง ๆ x ความรุนแรงของเหตุการณ์ต่าง ๆ ซึ่งใช้เกณฑ์ในการจัดแบ่งดังนี้

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

๓.๒ แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง

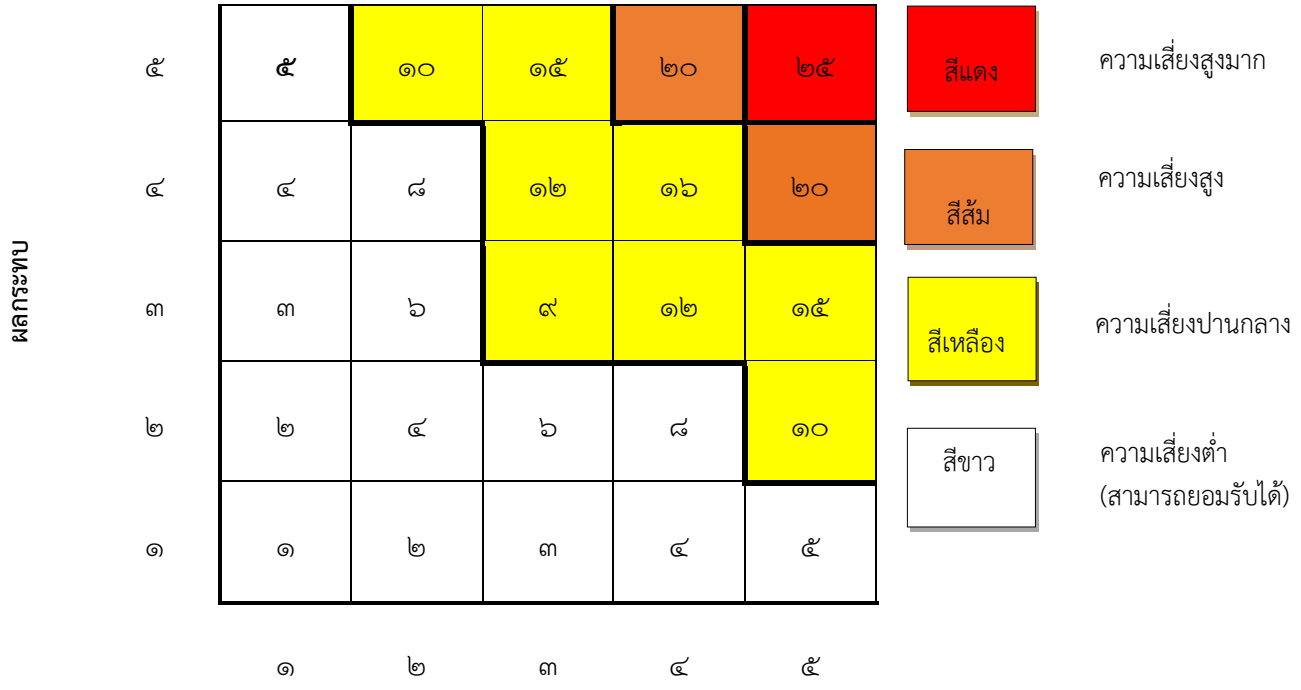
มาก

ผลกระทบ

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

น้อย ——— **โอกาสที่จะเกิด** ———→ มาก

๓.๓ การประเมินความเสี่ยง



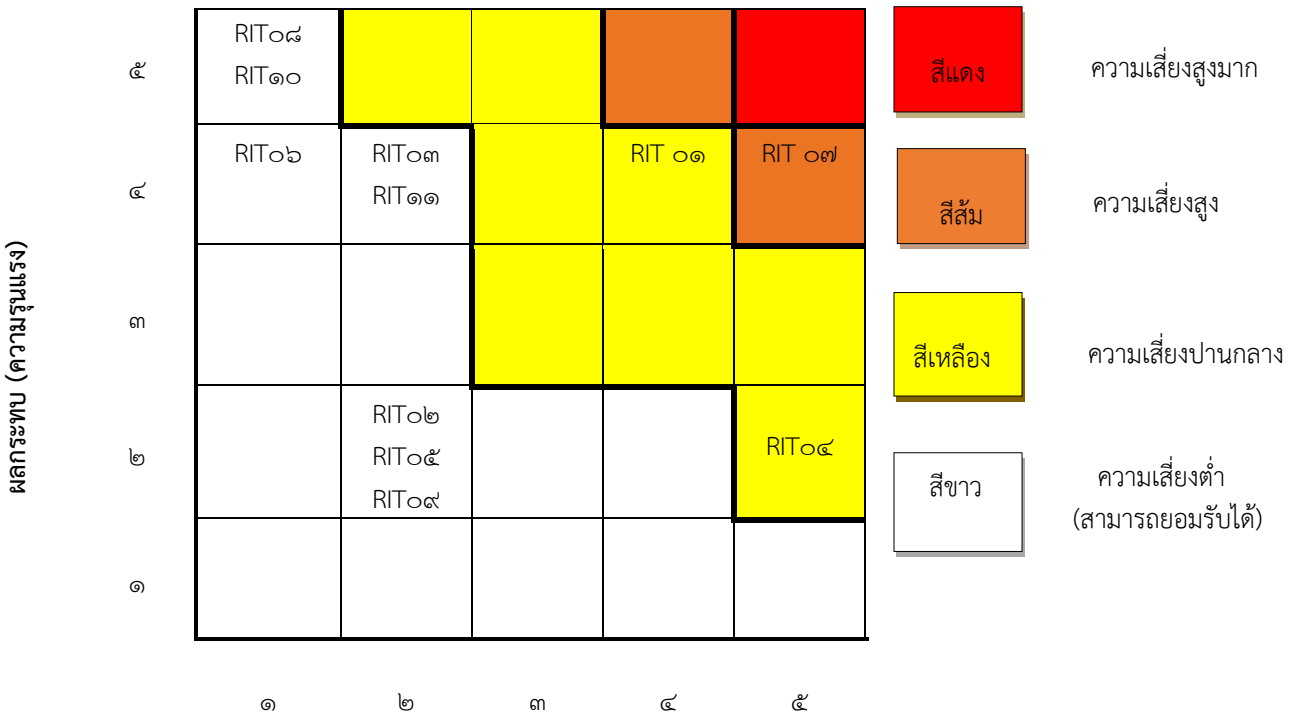
การประเมินค่าความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	๑. ความเสี่ยงด้านข้อมูล	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๔	๔	๑๖
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๘. ความเสี่ยงด้านกระบวนการทำงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายกรม โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือการไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของกรม ทำให้	๒	๒	๔

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
			เกิดช่องโหว่กับระบบรักษาความปลอดภัยของกรม			
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	๕. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๒	๔	๘
๔. ความเสี่ยงจากการถูกบุกรุกทางไซเบอร์และการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๐๔	๒.ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๓. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	- การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม - การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงานหรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๕	๒	๑๐
๕. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT๐๕	๔. ความเสี่ยงด้านบุคลากร	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๒	๒	๔
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	๔. ความเสี่ยงด้านบุคลากร	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำ	๑	๔	๔

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
			ให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ			
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ รวมถึงการดูแลรักษาห้องปฏิบัติการคอมพิวเตอร์และอุปกรณ์ให้มีความพร้อมใช้อย่างสม่ำเสมอ	๕	๔	๒๐
๘. ความเสี่ยงจาก ภัยพิบัติ ภัยธรรมชาติ และภัยจากการทำงานของมนุษย์ รวมถึงสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๘	๕. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด - การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	๑	๕	๕
๙. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT๐๙	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	๒	๒	๔
๑๐. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	RIT๑๐	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๖. ความเสี่ยงด้านเครือข่ายสื่อสาร	-เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล -ไม่สามารถใช้งานระบบสารสนเทศที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน	๑	๕	๕
๑๑. ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	RIT๑๑	๗. ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก	หากมีทำงานผิดพลาดของโปรแกรม จะไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่และแก้ไขการทำงานที่ผิดพลาดได้ทันกับเหตุการณ์	๒	๔	๘

แผนภูมิความเสี่ยง



๓.๔ การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีการจัดทำรายงานการประเมินการควบคุมความเสี่ยงด้วยตนเอง (Risk and Control Self-Assessment หรือ RCSA) อย่างน้อยปีละ ๑ ครั้ง โดยจุดที่มีความเสี่ยงอยู่ในระดับที่มีนัยสำคัญและระดับสูง จะต้องมีการจัดทำ Action Plan เพื่อปิดความเสี่ยงที่เกิดขึ้นกับหน่วยงานต่อไป และควรมีการติดตามและประเมินผล (Monitoring) กระบวนการในการติดตามความเสี่ยงที่มีอยู่ตามช่วงเวลาที่เหมาะสม ทั้งนี้ เพื่อให้ผู้บริหาร หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สามารถติดตามสถานะของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีอยู่ และสามารถวางแผนในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นได้อย่างเหมาะสมและมีประสิทธิภาพ อีกทั้งยังช่วยให้หน่วยงานสามารถป้องกันและควบคุมเหตุการณ์ความเสียหายที่อาจเกิดขึ้นได้อย่างทันท่วงที

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศในการบริหารจัดการได้อย่างมีประสิทธิภาพดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ รวมถึงการดูแลรักษาห้องปฏิบัติการคอมพิวเตอร์และอุปกรณ์ให้มีความพร้อมใช้อย่างสม่ำเสมอ	๒๐
๒	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	๑. ความเสี่ยงด้านข้อมูล	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๑๖
๓	RIT๐๔ ความเสี่ยงจากการถูกบุกรุกทางไซเบอร์และการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๒.ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๓. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม - การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๑๐
๔	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๕. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูล	๘

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
			สารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	
๕	RIT๑๑ ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	๗. ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก	หากมีทำงานผิดพลาดของโปรแกรม จะไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่และแก้ไขการทำงานที่ผิดพลาดได้ทันกับเหตุการณ์	๘
๖	RIT๐๘ ความเสี่ยงจากภัยพิบัติ ภัยธรรมชาติ และภัยจากการทำงานของมนุษย์ รวมถึงสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๕. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด - การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	๕
๗	RIT๑๐ ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๖. ความเสี่ยงด้านเครือข่ายสื่อสาร	-เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล -ไม่สามารถใช้งานระบบสารสนเทศที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน	๕
๘	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๘. ความเสี่ยงด้านกระบวนการทำงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายกรม โดยไม่ได้รับอนุญาตและไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่ายของกรม ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของกรม	๔
๙	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๔. ความเสี่ยงด้านบุคลากร	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๔

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑๐	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๔. ความเสี่ยงด้านบุคลากร	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	๔
๑๑	RIT๐๙ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	๔

บทที่ ๔
การจัดการความเสี่ยง

๔.๑ การจัดการความเสี่ยง

ในการควบคุมและบรรเทาความเสี่ยง จะขึ้นอยู่กับค่าระดับความเสี่ยงที่ประเมินและได้ค่ามานั้น ทางเลือกในการควบคุมหรือบรรเทาความเสี่ยงจะมีด้วยกัน ๔ ทางเลือก ดังนี้

๑) การยอมรับความเสี่ยง (Acceptance) กรณีที่ค่าระดับความเสี่ยงอยู่ในบริเวณสีขาว ผู้ประเมินความเสี่ยงสามารถยอมรับความเสี่ยงได้ กรณีการยอมรับความเสี่ยงยังหมายรวมถึง

- กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเหลือง สีส้ม หรือ สีแดง ก็ตาม แต่หน่วยงานหรือยังไม่สามารถระบุมาตรการที่เหมาะสมได้ จึงอาจต้องยอมรับความเสี่ยงไว้ก่อน ในภายหลังเมื่อได้มาตรการที่เหมาะสมแล้ว จึงเสนอมาตรการเพื่อหาทางลดความเสี่ยงให้ลดลง มาอยู่ในระดับสีขาว เป็นต้น
- กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเหลือง สีส้ม หรือ สีแดง แต่หน่วยงาน พบว่าการจะจัดการกับความเสี่ยงนี้จะมีค่าใช้จ่ายที่ค่อนข้างสูงและไม่คุ้มค่าที่จะลงทุน จึงเห็นสมควรให้ยอมรับความเสี่ยงและไม่ดำเนินการใด ๆ

๒) การเลี่ยงความเสี่ยง (Avoidance) คือ การหาหนทางที่เหมาะสมเพื่อหลีกเลี่ยงความเสี่ยงที่พบนั้น เช่น หากพบว่าการนำทรัพย์สินไปตั้งไว้ในบริเวณที่มีความเสี่ยงต่อการสูญหาย ก็ควรจะหลีกเลี่ยงโดยการนำไปจัดเก็บไว้ในสถานที่ที่ปลอดภัย

การตัดสินใจที่จะแลกเปลี่ยนข้อมูลสำคัญกับองค์กรหนึ่งผ่านทางระบบออนไลน์ เมื่อพบว่าองค์กรนั้นยังไม่มีมาตรการความมั่นคงปลอดภัยที่ดีเพียงพอ ก็อาจยับยั้งการตัดสินใจนั้น โดยหลีกเลี่ยงความเสี่ยงไปใช้วิธีการแลกเปลี่ยนแบบ Manual แทน การหาหนทางที่เหมาะสมกว่าควรพิจารณาว่าความเสี่ยงลดลงมาอยู่ในระดับที่ยอมรับได้หรือไม่

๓) การโอนย้ายความเสี่ยง (Transfer) คือ การให้หน่วยงานอื่นเป็นผู้รับความเสี่ยงหรือดำเนินการแทนศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เช่น การใช้ Outsource เรื่องการพัฒนาระบบให้หน่วยงานภายนอกโดยการทำสัญญาดูแลรักษาฮาร์ดแวร์ อุปกรณ์เครือข่าย หรือการซื้อประกันภัยจากหน่วยงานภายนอก เป็นต้น

การโอนย้ายความเสี่ยง ควรพิจารณาว่า ผู้ดำเนินการสามารถจัดการความเสี่ยงนั้นได้เป็นอย่างดีหรือไม่ ระดับความเสี่ยงที่เกิดจากผู้ดำเนินการแทน ควรจะอยู่ในระดับที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารยอมรับได้ หากผู้ดำเนินการแทนไม่สามารถทำได้ดี ความเสี่ยงจะตกกลับมาที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเอง

๔) การลดความเสี่ยง (Reduction) คือ การหาทางลดค่าความเสี่ยงที่อาจตกอยู่ในบริเวณสีเหลือง สีส้ม หรือ สีแดงก็ตาม ให้ลงมาอยู่ในระดับที่น้อยลง

กรณีที่หน่วยงานสามารถลดความเสี่ยงลงมาอยู่ในบริเวณสีขาวได้ หน่วยงานสามารถยอมรับความเสี่ยงได้ และไม่ต้องทำอะไรเพิ่มเติม แต่หากอยู่ในบริเวณสีเหลือง หน่วยงานยังต้องคอยคุมความเสี่ยงไว้ (เพื่อป้องกันการเลื่อนระดับไปสู่ระดับที่สูงขึ้น)

เมื่อมีการประเมินระดับความเสี่ยงในแต่ละประเด็นแล้ว หน่วยงาน หรือคณะทำงานต้องพิจารณาค่าระดับความเสี่ยงนั้นและตัดสินใจว่าจะใช้ทางเลือกใด (จาก ๑ ใน ๔ ทางเลือก) เพื่อจัดการกับความเสี่ยงที่ประเมินนั้นซึ่งได้อธิบายวิธีการใช้ทางเลือกแต่ละทางเลือกไปแล้วในข้างต้น

๔.๒ กลยุทธ์การจัดการความเสี่ยง

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นหน่วยงานที่เกี่ยวข้องหรือเป็นเจ้าของความเสี่ยง มีหน้าที่ติดตามและควบคุมดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจะควบคุมความเสี่ยงให้สอดคล้องกับระดับความเสี่ยง และดำเนินการควบคุมป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงมีการติดตามและรายงานต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ประจำกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

นโยบายของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ระดับความเสี่ยงคงเหลือที่ยอมรับได้ ≤ ๙ สำนักงาน ก.พ.ร. กำหนดให้ ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๕ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๕ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้

การดำเนินการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารแสดงดังตารางต่อไปนี้

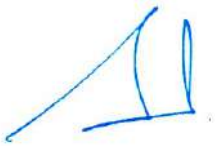
ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๑	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๒๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนปฏิบัติการดิจิทัลฯ เพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ
๒	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	๑๖	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๕

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๓	RIT๐๔ ความเสี่ยงจากการถูกบุกรุกทางไซเบอร์ และการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๑๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - ดำเนินการตามแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ - ตรวจสอบการตั้งค่าของ firewall เป็นประจำทุกวัน - ตรวจสอบการทำงานของอุปกรณ์รักษาความปลอดภัย monitor หน้า Dashboard ความถี่ ๑ ครั้ง ต่อ วัน - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส และ patch ให้เป็นตัวใหม่ล่าสุด ความถี่การอัปเดต ๑ ครั้ง ต่อ สัปดาห์ - ติดตั้ง patch ของระบบปฏิบัติการให้เป็นตัวใหม่ล่าสุด - เปลี่ยนรหัสผ่านตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๕ - ตรวจสอบการเข้าออกของบุคคลภายนอก - จัดเวรอัคคีภัย เพื่อตรวจสอบความเรียบร้อยของสถานที่ - ตรวจสอบระบบการป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ - ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง
๔	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๘	ยอมรับความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนการจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์เครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - ตรวจสอบ และทดสอบการทำงานเครื่องและอุปกรณ์เครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ให้ทำงานได้อย่างปกติ อาทิตย์ละครั้ง - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๕	RIT๑๑ ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	๘	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ปรับปรุงร่างขอบเขตของงาน (TOR) ให้สอดคล้องกับภารกิจของงานและรายงานผลการจัดซื้อจัดจ้างอย่างต่อเนื่องเพื่อให้ครอบคลุมกับสถานการณ์ปัจจุบัน
๖	RIT๐๘ ความเสี่ยงจาก ภัยพิบัติ ภัยธรรมชาติ และภัยจากการทำงานของมนุษย์ รวมถึงสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๕	ยอมรับความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - จัดเวรอัคคีภัย - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด
๗	RIT๑๐ ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๕	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว เพื่อสามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ
๘	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๔	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง - กำหนดสิทธิ์ การใช้อุปกรณ์ บนเครือข่าย LAN แก่ user ละ ๑ สิทธิ์ - กำหนดสิทธิ์การใช้อุปกรณ์แบบพกพาบนเครือข่าย WIFI แก่ user ละ ๑ สิทธิ์ - ตรวจเช็คการขอสิทธิ์ใช้เครือข่ายใหม่ทุกครั้ง เพื่อเลี่ยงกรณีขอซ้ำซ้อนเกินกว่าข้อกำหนด
๙	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๔	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- เสนอผู้บริหารให้พิจารณาให้มีโครงสร้างศูนย์เทคโนโลยีสารสนเทศและการสื่อสารในกฎกระทรวง และสรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสม - จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๑๐	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๔	ยอมรับความเสี่ยง	- สร้างความเข้าใจนโยบายที่เกี่ยวข้องดังนี้ ๑) นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ๒๕๖๑ - ๒๕๘๐ ๒) แผนปฏิบัติการดิจิทัล พ.ศ. ๒๕๖๕-๒๕๖๙ ๓) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๕
๑๑	RIT๐๙ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	๒	ยอมรับความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารฉบับนี้ ได้ผ่านการพิจารณาจากคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการเพื่อจัดการการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารต่อไป



(นายวิชิต จิรมงคลการ)
หัวหน้าคณะทำงานบริหารจัดการความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
มีนาคม ๒๕๖๗

ภาคผนวก

หนังสือที่เกี่ยวข้อง

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โทร. ๐ ๒๕๖๑ ๐๗๗๗ ต่อ ๑๒๔๕
ที่ ทส ๐๙๖๔.๓/ ๒๐๕ **วันที่** ๒๙ กุมภาพันธ์ ๒๕๖๗
เรื่อง แต่งตั้งคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

เรียน ผู้อำนวยการส่วนทุกส่วน
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (สุราษฎร์ธานี)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (สงขลา)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (ขอนแก่น)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (อุบลราชธานี)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (พิษณุโลก)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (แพร่)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงราย)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงใหม่)
หัวหน้าศูนย์ราชการสะดวก กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ขอส่งสำเนาคำสั่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่ ๕ /๒๕๖๗ ลงวันที่ ๒๙ กุมภาพันธ์ พ.ศ. ๒๕๖๗ เรื่อง แต่งตั้งคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นไปอย่างต่อเนื่อง และสอดคล้องตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช พ.ศ. ๒๕๖๕ และแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช พ.ศ. ๒๕๖๖

จึงเรียนมาเพื่อโปรดทราบ

(นายวิชิต จิรมงคลการ)
ผู้เชี่ยวชาญเฉพาะด้านระบบการฟื้นฟูและพัฒนาพื้นที่อนุรักษ์
ทำหน้าที่ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สำเนา

คำสั่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ที่ ๔ / ๒๕๖๗
เรื่อง แต่งตั้งคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ตามคำสั่งคณะกรรมการบริหารจัดการความเสี่ยง กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช ที่ ๒๑๙๗/๒๕๖๖ ลงวันที่ ๑๕ พฤษภาคม พ.ศ. ๒๕๖๖ เรื่อง แต่งตั้งคณะทำงานบริหารจัดการความเสี่ยง กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช มีหน้าที่และอำนาจ ในการระบุ วิเคราะห์เหตุการณ์และความเสี่ยงต่าง ๆ ที่มีผลกระทบต่อการดำเนินงานโดยครอบคลุมทุกพันธกิจของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช เพื่อเสนอแนะกลไกและวิธีการในการบริหารความเสี่ยง ให้อยู่ในระดับที่ยอมรับได้ เพื่อให้กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช มีความพร้อมในการพัฒนาอย่างยั่งยืน และมีภูมิคุ้มกันเพื่อเผชิญต่อการเปลี่ยนแปลงของสภาพแวดล้อมทั้งภายในและภายนอกได้ นั้น

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พิจารณาแล้ว เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เป็นไปอย่างถูกต้อง มีประสิทธิภาพ ครอบคลุม และสอดคล้องตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช พ.ศ. ๒๕๖๕ และแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช พ.ศ. ๒๕๖๖ จึงแต่งตั้งคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ โดยมีองค์ประกอบ หน้าที่และอำนาจ ดังนี้

<u>องค์ประกอบ</u>

๑. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	ประธานคณะทำงาน
๒. ผู้อำนวยการส่วนอำนวยการ	คณะทำงาน
๓. ผู้อำนวยการส่วนพัฒนาระบบสารสนเทศ	คณะทำงาน
๔. ผู้อำนวยการส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย	คณะทำงาน
๕. ผู้อำนวยการส่วนภูมิสารสนเทศ	คณะทำงาน
๖. ผู้อำนวยการส่วนฐานข้อมูลและสถิติ	คณะทำงาน
๗. ผู้อำนวยการส่วนการสื่อสาร	คณะทำงาน
๘. หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (สุราษฎร์ธานี)	คณะทำงาน
๙. หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (สงขลา)	คณะทำงาน
๑๐. หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (ขอนแก่น)	คณะทำงาน
๑๑. หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (อุบลราชธานี)	คณะทำงาน

๑๒. หัวหน้า...

๑๒. หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (พิษณุโลก) คณะทำงาน
๑๓. หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (แพร่) คณะทำงาน
๑๔. หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก) คณะทำงาน
๑๕. หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงราย) คณะทำงาน
๑๖. หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงใหม่) คณะทำงาน
๑๗. หัวหน้าศูนย์ราชการสะดวก กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช
คณะทำงาน
๑๘. นายวรวุฒิ วีระกุล คณะทำงาน
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ส่วนพัฒนาระบบสารสนเทศ
๑๙. นายกานต์ บุญทองเสน คณะทำงาน
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ส่วนพัฒนาระบบสารสนเทศ
๒๐. นายธนาคม คำวัฒนา คณะทำงาน
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย
๒๑. นางสาวณัฐชานันท์ ลายเงินมณี คณะทำงาน
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ส่วนภูมิสารสนเทศ
๒๒. นายยุทธนา แสงทอง คณะทำงาน
นักวิชาการป่าไม้ชำนาญการ
ส่วนภูมิสารสนเทศ
๒๓. นางสาวกาญจนา โพนภาค คณะทำงาน
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ส่วนฐานข้อมูลและสถิติ
๒๔. นายธวัชชัย ขันธจิตร คณะทำงาน
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ส่วนฐานข้อมูลและสถิติ
๒๕. นายณัฐพล นันใจนา คณะทำงาน
เจ้าพนักงานธุรการชำนาญงาน
ส่วนการสื่อสาร
๒๖. นายชลนที ทองศรีนุ่น คณะทำงานและ
นักวิชาการคอมพิวเตอร์ปฏิบัติการ เลขานุการ
ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย

๒๗. นางสาว...

๒๗. นางสาวประภัสสร ถิตย์ประไพ	คณะทำงานและ
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ผู้ช่วยเลขานุการ
ส่วนพัฒนาระบบสารสนเทศ	
๒๘. นายปารเมศ จันทมาศ	คณะทำงานและ
นักวิชาการคอมพิวเตอร์	ผู้ช่วยเลขานุการ
ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย	
๒๙. นางสาวบัสตี สารี	คณะทำงานและ
เจ้าหน้าที่บริหารงานทั่วไป	ผู้ช่วยเลขานุการ
ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย	

<u>หน้าที่และอำนาจ</u>

๑. จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒. ทบทวน ระบุ วิเคราะห์เหตุการณ์และความเสี่ยงต่างๆ เพื่อปรับปรุงแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีความเหมาะสมและเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๓. จัดทำแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อกำหนดกลไก และวิธีการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔. จัดทำรายงาน และติดตามประเมินผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเสนอต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ประจำกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช

๕. ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๙ กุมภาพันธ์ พ.ศ. ๒๕๖๗

(ลงนาม) วิชิต จิรมงคลการ

(นายวิชิต จิรมงคลการ)
ผู้เชี่ยวชาญเฉพาะด้านระบบการฟื้นฟูและพัฒนาพื้นที่อนุรักษ์
ทำหน้าที่ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สำเนาถูกต้อง

(นางสาวอระนุช โกศล)
นักวิเคราะห์นโยบายและแผนชำนาญการ

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย
โทร. ๐ ๒๕๖๑ ๐๗๗๗ ต่อ ๑๒๔๕

ที่ ทส ๐๙๖๔.๓/ ๒๕๗ **วันที่** ๑๔ มีนาคม ๒๕๖๗

เรื่อง ขอเชิญประชุมคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ครั้งที่ ๑/๒๕๖๗

เรียน ผู้อำนวยการส่วนทุกส่วน
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (สุราษฎร์ธานี)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (สงขลา)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (ขอนแก่น)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (อุบลราชธานี)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (พิษณุโลก)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (แพร่)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงราย)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงใหม่)

ตามคำสั่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่ ๔/๒๕๖๗ ลงวันที่ ๒๙ กุมภาพันธ์ พ.ศ. ๒๕๖๗ เรื่อง แต่งตั้งคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อกำหนดแนวทางและหลักเกณฑ์การบริหารความเสี่ยง พิจารณาทบทวนแผน และติดตามผลการดำเนินงานการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร นั้น

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พิจารณาแล้ว เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เป็นไปอย่างถูกต้อง มีประสิทธิภาพ ครอบคลุม และสอดคล้องตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช พ.ศ. ๒๕๖๕ จึงขอเชิญคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เข้าร่วมประชุมครั้งที่ ๑/๒๕๖๗ **ในวันจันทร์ที่ ๑๘ มีนาคม ๒๕๖๗ เวลา ๑๓.๐๐ - ๑๕.๓๐ น. ณ ห้องประชุมศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๒ อาคารอเนกประสงค์** ตามระเบียบวาระการประชุมที่แนบมาพร้อมนี้ ทั้งนี้ หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศให้เข้าร่วมการประชุมทางไกลผ่านระบบ Video Conference (Meeting ID: ๙๙๓ ๘๓๙๐ ๓๗๙๖ Passcode: ๖๖๓๒๕๕)

จึงเรียนมาเพื่อโปรดทราบ และเข้าร่วมประชุม ตามวัน เวลา และสถานที่ดังกล่าว

(นายวิชิต จิรมงคลการ)
ผู้เชี่ยวชาญเฉพาะด้านระบบการฟื้นฟูและพัฒนาพื้นที่อนุรักษ์
ทำหน้าที่ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

เอกสารประกอบการประชุม

ระเบียบวาระการประชุม
คณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ครั้งที่ ๑/๒๕๖๗
วันจันทร์ที่ ๑๘ มีนาคม ๒๕๖๗ เวลา ๑๓.๐๐ - ๑๕.๓๐ น.
ณ ห้องประชุมศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๒ อาคารอเนกประสงค์

.....

ระเบียบวาระที่ ๑ เรื่องที่ประธานแจ้งให้ทราบ

.....

.....

ระเบียบวาระที่ ๒ เรื่องเพื่อทราบ

๒.๑ คำสั่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่ ๔/๒๕๖๗ ลงวันที่ ๒๙ กุมภาพันธ์ พ.ศ. ๒๕๖๗ เรื่อง แต่งตั้งคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

.....

.....

ระเบียบวาระที่ ๓ เรื่องเพื่อพิจารณา

๓.๑ ร่างการวิเคราะห์และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

๓.๒ ร่างแผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency plan) ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

.....

.....

ระเบียบวาระที่ ๔ เรื่องอื่น ๆ (ถ้ามี)

.....

.....

.....

ด่วนที่สุด **บันทึกข้อความ**

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย
โทร. ๐ ๒๕๖๑ ๐๗๗๗ ต่อ ๑๒๔๕

ที่ ทส ๐๙๖๔.๓/ ๒๕๐ **วันที่** ๒๖ มีนาคม ๒๕๖๗

เรื่อง ขอส่งรายงานการประชุมคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ครั้งที่ ๑/๒๕๖๗

เรียน ผู้อำนวยการส่วนทุกส่วน
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (สุราษฎร์ธานี)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (สงขลา)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (ขอนแก่น)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (อุบลราชธานี)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (พิษณุโลก)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (แพร่)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงราย)
หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงใหม่)

ตามหนังสือศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่ ทส ๐๙๖๔.๓/๒๕๗ ลงวันที่ ๑๔ มีนาคม ๒๕๖๗ เรื่อง ขอเชิญประชุมคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ครั้งที่ ๑/๒๕๖๗ ในวันจันทร์ที่ ๑๘ มีนาคม ๒๕๖๗ เวลา ๑๓.๐๐ ถึง ๑๕.๓๐ น. ณ ห้องประชุมศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๒ อาคารอเนกประสงค์ และผ่านระบบ Video Conference เพื่อกำหนดแนวทางและหลักเกณฑ์การบริหารความเสี่ยง พิจารณาทบทวนแผน และติดตามผลการดำเนินงานการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ นั้น

บัดนี้ ฝ่ายเลขานุการฯ ได้จัดทำรายงานการประชุมเสร็จเรียบร้อยแล้ว จึงขอส่งรายงานการประชุมตามเอกสารที่แนบมาพร้อมนี้ ทั้งนี้ หากมีข้อแก้ไขประการใด โปรดแจ้งให้ฝ่ายเลขานุการฯทราบ **ภายในวันพฤหัสบดีที่ ๒๘ มีนาคม ๒๕๖๗ เวลา ๑๖.๓๐ น.** หากพ้นระยะเวลากำหนดดังกล่าวแล้ว ให้ถือว่ารับรองรายงานการประชุม

จึงเรียนมาเพื่อโปรดทราบและพิจารณา

(นายวิชิต จิรมงคลการ)
ผู้เชี่ยวชาญเฉพาะด้านระบบการฟื้นฟูและพัฒนาพื้นที่อนุรักษ์
ทำหน้าที่ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

รายงานการประชุม
คณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ครั้งที่ ๑/๒๕๖๗
เมื่อวันจันทร์ที่ ๑๘ มีนาคม ๒๕๖๗ เวลา ๑๓.๐๐ - ๑๕.๓๐ น.
ณ ห้องประชุมศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๒ อาคารอเนกประสงค์

ผู้มาประชุม (On-site)

๑. นายวิชิต จิรมงคลการ	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๒. นางสาวอระนุช โกศล	ผู้อำนวยการส่วนอำนวยการ
๓. นางศศิธร กฤติยาภิชาตกุล	ผู้อำนวยการส่วนพัฒนาระบบสารสนเทศ
๔. นายพิชิต ศึกษากิจ	ผู้อำนวยการส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย
๕. นางสาวธนารัตน์ สุภาพ	ผู้อำนวยการส่วนฐานข้อมูลและสถิติ
๖. นายนพคุณ แก้วสิงห์	ผู้อำนวยการส่วนภูมิสารสนเทศ
๗. นายสมศักดิ์ แย้มเยื้อน	ผู้อำนวยการส่วนการสื่อสาร
๘. นายยุทธนา แสงทอง	นักวิชาการป่าไม้ชำนาญการ
๙. นายปารเมศ จันทมาศ	นักวิชาการคอมพิวเตอร์
๑๐. นางสาวบัสตี สารี	เจ้าหน้าที่บริหารงานทั่วไป

ผู้มาประชุม (Online)

๑. นางสาวกิติยา นิลพัฒน์	หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (สุราษฎร์ธานี)
๒. นายอธิป ศรีสุวรรณ์	หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (สงขลา)
๓. นายศุภมิตร จารุธัญลักษณ์	หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (ขอนแก่น)
๔. นางนพมาศ แก้วพรมชัย	หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (อุบลราชธานี)
๕. นายไพรัช มณีงาม	หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (พิษณุโลก)
๖. นางสาววิภาภรณ์ ใบยา	หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (แพร่)
๗. นายบัลลังก์ บินลอย	หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
๘. นางสาวผกา อวรรณา	แทน หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงราย)
๙. นายบัณฑิต เงินสม	แทน หัวหน้าศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงใหม่)
๑๐. นายวรวุฒิ วีระกุล	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๑๑. นายกานต์ บุญทองเสน	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๑๒. นายธนาคม คำวัฒนา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๑๓. นางสาวณัฐชานันท์ ลายเงินมณี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๑๔. นางสาวกาญจนา โพนภาค	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๑๕. นายธวัชชัย ขันธจิตร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ผู้ไม่มาประชุม

๑. นายณัฐพล นันใจนา	เจ้าพนักงานธุรการชำนาญงาน	ติดราชการ
๒. นางสาวประภัสสร ถิตย์ประไพ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ติดราชการ
๓. นายชลนที ทองศรีนุ่น	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ลาพักผ่อน

ผู้เข้าร่วมประชุม (On-site)

๑. นายกิตติพิฎญ์ ทองคำ	เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๒. นางสาวชลธิชา จันทร์นภาลัย	นักวิชาการป่าไม้

ผู้เข้าร่วมประชุม (Online)

๑. นางสาวลลิตา แสงสุริยันต์	นักวิชาการป่าไม้ปฏิบัติการ ศูนย์ปฏิบัติการภูมิสารสนเทศ (สุราษฎร์ธานี)
๒. นางสาวสิรีมาตร จิตปาโล	นักวิชาการป่าไม้ปฏิบัติการ ศูนย์ปฏิบัติการภูมิสารสนเทศ (สงขลา)
๓. นายระเด่น ยืนยง	เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ศูนย์ปฏิบัติการภูมิสารสนเทศ (พิษณุโลก)
๔. นายณัฐกิตต์ เจ็กอยู่	นักวิชาการภูมิสารสนเทศ ศูนย์ปฏิบัติการภูมิสารสนเทศ (พิษณุโลก)
๕. นายวรนน โคกพระปราง	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (พิษณุโลก)
๖. นายธนพสิษฐ์ ชาบางโชตินันทน์	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (พิษณุโลก)
๗. นางสาวรักษ์สิตา กองเพชร	พนักงานราชการ ศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
๘. นางสาวณัฐกฤตา ม่วงมิตร	พนักงานราชการ ศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
๙. นางสาวพรพรรณ เดชพันธ์	พนักงานราชการ ศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
๑๐. นายธีรวัฒน์ ธังดิน	พนักงานราชการ ศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
๑๑. นางสาวขนิษฐา โฉมงาม	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
๑๒. นางสาวธนพร พรพชรบำรุง	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
๑๓. นางสาวปริยาภัทร พรมมา	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
๑๔. นางสาวกีรติกัณฐ์ เสือเดช	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)
๑๕. นายภาณุวัฒน์ สาลี	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (ตาก)

๑๖. นายสุทธิพงษ์ ยี่นา	นักวิชาการภูมิสารสนเทศ ศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงใหม่)
๑๗. นางสาวกรรณิกา วงศ์ทิพย์	เจ้าหน้าที่บริหารงานทั่วไป ศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงใหม่)
๑๘. นายศราวุธ ฝาเรือนดี	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (แพร่)
๑๙. นายจตุพร พันสนิท	นักวิชาการป่าไม้ปฏิบัติการ ศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงราย)
๒๐. นายปองพล ชนะภัย	เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงราย)
๒๑. นางสาวชัญญานุช เสาร์จันทร์	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงราย)
๒๒. นางสาวนวลลออ วัณโณ	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงราย)
๒๓. นายนราศักดิ์ สมแก้ว	พนักงานจ้างเหมา ศูนย์ปฏิบัติการภูมิสารสนเทศ (เชียงราย)
๒๔. นางสาวสุปราณี จันทร์เพ็ญ	นักวิชาการป่าไม้ ศูนย์ปฏิบัติการภูมิสารสนเทศ (อุบลราชธานี)
๒๕. นายวัชรินทร์ วงษ์ทอง	เจ้าหน้าที่ระบบคอมพิวเตอร์ ศูนย์ปฏิบัติการภูมิสารสนเทศ (อุบลราชธานี)
๒๖. นางสาวปิยากร พรบุตร	เจ้าหน้าที่ภูมิสารสนเทศ ศูนย์ปฏิบัติการภูมิสารสนเทศ (อุบลราชธานี)
๒๗. นายพงษ์ศิริ จันทร์ลุน	เจ้าหน้าที่ภูมิสารสนเทศ ศูนย์ปฏิบัติการภูมิสารสนเทศ (อุบลราชธานี)
๒๘. นายณัฐกมล ซ่อมโมง	เจ้าหน้าที่ภูมิสารสนเทศ ศูนย์ปฏิบัติการภูมิสารสนเทศ (อุบลราชธานี)

เริ่มประชุมเวลา ๑๓.๐๐ น.

<u>ระเบียบวาระที่ ๑</u> เรื่องที่ประธานแจ้งให้ทราบ

นายวิชิต จิรมงคลการ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ประธานในที่ประชุมได้กล่าวเปิดประชุม

<u>มติที่ประชุม</u> รับทราบ

<u>ระเบียบวาระที่ ๒</u> เรื่องเพื่อทราบ

ประธานฯ แจ้งคำสั่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่ ๔/๒๕๖๗ ลงวันที่ ๒๙ กุมภาพันธ์ พ.ศ. ๒๕๖๗ เรื่อง แต่งตั้งคณะทำงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้ที่ประชุมทราบ

<u>มติที่ประชุม</u> รับทราบ

<u>ระเบียบวาระที่ ๓</u> เรื่องพิจารณา

๓.๑ คณะทำงานฯ พิจารณาร่างการวิเคราะห์และบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ดังนี้

ประเมินค่าความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	๑. ความเสี่ยงด้านข้อมูล	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล	๔	๔
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๘. ความเสี่ยงด้านกระบวนการทำงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายกรม โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่อง	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย	๒	๒

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
			คอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของกรม ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของกรมฯ				
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้องไฟฟ้าดับแรงดันไฟฟ้าไม่คงที่	RIT๐๓	๕. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ	๒	๔
๔. ความเสี่ยงจากการถูกบุกรุกทางไซเบอร์ และการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๐๔	๒.ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๓. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	- การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม - การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ อุปกรณ์เครือข่าย	๕	๒
๕. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT๐๕	๔. ความเสี่ยงด้านบุคลากร	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ	๒	๒

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
			สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ		เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ		
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	๔. ความเสี่ยงด้านบุคลากร	การเปลี่ยนแปลงผู้บริหารอาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๔
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ รวมถึงการดูแลรักษาห้องปฏิบัติการคอมพิวเตอร์และอุปกรณ์ให้มีความพร้อมใช้อย่างสม่ำเสมอ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ	๕	๔
๘. ความเสี่ยงจากภัยพิบัติ ภัยธรรมชาติ และภัยจากการทำงานของมนุษย์ รวมถึงสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๘	๕. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด - การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ - การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์ แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล	๑	๕

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
			บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ		ระบบสารสนเทศ		
๙. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	RIT๐๙	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิคหรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	๒	๒
๑๐. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	RIT๑๐	๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ๖. ความเสี่ยงด้านเครือข่ายสื่อสาร	-เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล -ไม่สามารถใช้งานระบบสารสนเทศที่มีความสำคัญและต้องใช้งานอย่างเร่งด่วน	- ความล้มเหลวทางเทคนิค	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	๑	๕
๑๑. ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	RIT๑๑	๗. ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก	หากมีทำงานผิดพลาดของโปรแกรม จะไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่และแก้ไขการทำงานที่ผิดพลาดได้ทันกับเหตุการณ์	ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๒	๔

ฝ่ายเลขาฯ ปรับปรุงการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามมติคณะทำงานฯ และสรุปการประเมินค่าระดับความเสี่ยงแล้ว จึงจัดทำกลยุทธ์การจัดการความเสี่ยง และแนวทางการดำเนินการจัดการความเสี่ยง ดังนี้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๑	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๒๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนปฏิบัติการดิจิทัลฯ เพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๒	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	๑๖	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๕
๓	RIT๐๔ ความเสี่ยงจากการถูกบุกรุกทางไซเบอร์ และการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๑๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - ดำเนินการตามแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ - ตรวจสอบการตั้งค่าของ firewall เป็นประจำทุกวัน - ตรวจสอบการทำงานของอุปกรณ์รักษาความปลอดภัย monitor หน้า Dashboard ความถี่ ๑ ครั้ง ต่อ วัน - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส และ patch ให้เป็นตัวใหม่ล่าสุด ความถี่การอัปเดต ๑ ครั้ง ต่อ สัปดาห์ - ติดตั้ง patch ของระบบปฏิบัติการให้เป็นตัวใหม่ล่าสุด เปลี่ยนรหัสผ่านตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๕ - ตรวจสอบการเข้าออกของบุคคลภายนอก - จัดเวรอัคคีภัย เพื่อตรวจสอบความเรียบร้อยของสถานที่ - ตรวจสอบระบบการป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ - ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง
๔	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๘	ยอมรับความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนการจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์เครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - ตรวจสอบ และทดสอบการทำงานเครื่องและอุปกรณ์เครื่องกำเนิดไฟฟ้า และเครื่อง

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
				สำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ให้ทำงานได้อย่างปกติ อาทิตย์ละครั้ง - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
๕	RIT๑๑ ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	๘	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ปรับปรุงร่างขอบเขตของงาน (TOR) ให้สอดคล้องกับภารกิจของงานและรายงานผลการจัดซื้อจัดจ้างอย่างต่อเนื่อง เพื่อให้ครอบคลุมกับสถานการณ์ปัจจุบัน
๖	RIT๐๘ ความเสี่ยงจาก ภัยพิบัติ ภัยธรรมชาติ และภัยจากการทำงานของมนุษย์ รวมถึงสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๕	ยอมรับความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - จัดเวรอัคคีภัย - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด
๗	RIT๑๐ ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๕	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว เพื่อสามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ
๘	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๔	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง - กำหนดสิทธิ์ การใช้อุปกรณ์ บนเครือข่าย LAN แก่ user ละ ๑ สิทธิ์ - กำหนดสิทธิ์การใช้อุปกรณ์แบบพกพาบนเครือข่าย WIFI แก่ user ละ ๑ สิทธิ์ - ตรวจเช็คการขอสิทธิ์ใช้เครือข่ายใหม่ทุกครั้ง เพื่อเลี่ยงกรณีขอซ้ำซ้อนเกินกว่าข้อกำหนด
๙	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๔	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- เสนอผู้บริหารให้พิจารณาให้มีโครงสร้างศูนย์เทคโนโลยีสารสนเทศและการสื่อสารในกฎกระทรวง และสรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสม

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
				- จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้
๑๐	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๔	ยอมรับความเสี่ยง	- สร้างความเข้าใจนโยบายที่เกี่ยวข้องดังนี้ ๑) นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ๒๕๖๑ - ๒๕๘๐ ๒) แผนปฏิบัติการดิจิทัล พ.ศ. ๒๕๖๕-๒๕๖๙ ๓) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๕
๑๑	RIT๐๙ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	๒	ยอมรับความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้

มติที่ประชุม เห็นชอบแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

๓.๒ คณะทำงานฯ พิจารณาร่างแผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency plan) ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

ประธานในที่ประชุม กล่าวถึงการนำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ และมอบฝ่ายเลขาฯ ปรับปรุงแผนรองรับสถานการณ์ฉุกเฉิน ให้สอดคล้องกับการวิเคราะห์และบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร และปรับปรุงรายชื่อบุคลากร กำหนดผู้รับผิดชอบให้มีความเหมาะสม และเป็นปัจจุบัน

มติที่ประชุม เห็นชอบ มอบฝ่ายเลขาฯ ปรับปรุงแผนรองรับสถานการณ์ฉุกเฉิน ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

ระเบียบวาระที่ ๔ เรื่องอื่นๆ

-

เลิกประชุมเวลา ๑๕.๓๐ น.

..... ผู้จดรายงานการประชุม
(นางสาวบัสตี สารี)
เจ้าหน้าที่บริหารงานทั่วไป

..... ผู้ตรวจรายงานการประชุม
(นางสาวอระนุช โกศล)
นักวิเคราะห์นโยบายและแผนชำนาญการ

รายการสินทรัพย์ในห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย พ.ศ. 2567

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
Rack ตู้ที่ 1						
1. CISCO Catalyst 9800 WLC 1	อส 63-64-02020-0001/1	3 ก.ย. 2563	ใช้งาน	อุปกรณ์ Wireless LAN Controller S/N: FCL235100CF	Wireless LAN	*ประจำห้อง Data Center
2. CISCO Catalyst 9800 WLC 2	อส 63-64-02020-0001/2	3 ก.ย. 2563	ใช้งาน	อุปกรณ์ Wireless LAN Controller S/N: FCL241200ES	Wireless LAN	*ประจำห้อง Data Center
3. CISCO Catalyst 9606R Switch (Core SW DNP1)	อส 65-64-02035-0100	8 พ.ย. 2565	ใช้งาน	อุปกรณ์ Core Switch S/N: FOX2614PC47	LAN	*ประจำห้อง Data Center
4. CISCO Catalyst 9606R Switch (Core SW DNP2)	อส 65-64-02035-0101	8 พ.ย. 2565	ใช้งาน	อุปกรณ์ Core Switch S/N: FOX2614PV6W	LAN	*ประจำห้อง Data Center
Rack ตู้ที่ 2						
5. HP v1910-24g Switch	อส 55-05-02035-0002	30 ก.ย. 2561	ใช้งาน	อุปกรณ์ Switch S/N: CN26BX22LF	LAN	*ประจำห้อง Data Center
6. HUAWEI S5700 Switch (8 Ports)	UIH	30 ก.ย. 2561	ใช้งาน	อุปกรณ์ UIH Switch	LAN	*ประจำห้อง Data Center
7. HUAWEI AR2200 Series Router	UIH	30 ก.ย. 2561	ใช้งาน	อุปกรณ์ UIH Router	Internet UIH	*ประจำห้อง Data Center
8. HUAWEI S5700 Switch (8 Ports)	UIH	30 ก.ย. 2561	ใช้งาน	อุปกรณ์ UIH Switch	LAN	*ประจำห้อง Data Center
9. HUAWEI AR1220E Router (8 Ports)	UIH	30 ก.ย. 2561	ใช้งาน	อุปกรณ์ UIH Router	Internet UIH	*ประจำห้อง Data Center
10. HUAWEI AR2200 Series Router	UIH	30 ก.ย. 2561	ใช้งาน	อุปกรณ์ UIH Router	Internet UIH	*ประจำห้อง Data Center
11. CISCO 1841 Series Router	UIH	30 ก.ย. 2561	ใช้งาน	อุปกรณ์ UIH Router	Internet UIH	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
12. Fortinet Fortigate 2200E		6 พ.ค. 2565	ใช้งาน	อุปกรณ์ Firewall S/N: FG2K2ET920900986	-Security -Internet	*ประจำห้อง Data Center
13. Dell Server (Voice Conference System)			ใช้งาน	อุปกรณ์ Voice Conference	-Server -Voice Conference System	*ประจำห้อง Data Center
14. Dell EMC Server (Log Server)	INET		ใช้งาน	อุปกรณ์ Log Server INET	Log Server INET	*ประจำห้อง Data Center
15. CISCO SG200 (VPN9002)	INET	28 ก.ย. 2561	ใช้งาน	อุปกรณ์ Switch Internet INET DR Site	Internet INET DR Site 100M	*ประจำห้อง Data Center
16. ForeScout CounterACT 5100	อส 66-64-02101-0001	4 ก.ย. 2566	ใช้งาน	อุปกรณ์ Network Access Control NAC S/N: D23B841MA00101CM	-Security -Internet	*ประจำห้อง Data Center
17. CISCO 1841 Integrated Service Router	INET	28 ก.ย. 2561	ใช้งาน	อุปกรณ์ Router Internet INET DR Site	Internet INET DR Site 100M	*ประจำห้อง Data Center
18. CISCO 1921 Integrated Service Router (INET)	INET	28 ก.ย. 2561	ใช้งาน	อุปกรณ์ Router Internet INET DR Site	Internet INET DR Site 100M	*ประจำห้อง Data Center
19. CISCO 2800 Series (GIN TOT)	TOT DGA		ใช้งาน	อุปกรณ์ Router Internet TOT	DGA	*ประจำห้อง Data Center
20. LINKSYS SRW224G4 Switch	TOT DGA		ใช้งาน	อุปกรณ์ Switch Internet TOT	DGA	*ประจำห้อง Data Center
21. HP Proliant DL360 G10 (DNS Internal)	อส 63-64-02038-0002		ใช้งาน	อุปกรณ์ DNS Internal S/N: SGH026YVB2 OS: MS-Windows Server 2019 IP: 192.168.10.XXX	-DNS Server -DHCP Server	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
22. EMC VNX 3200 Storage System	อส 59-05-02043-0001	3 พ.ค. 2559	ใช้งาน	อุปกรณ์ Storage Headdisk : 7.8Tb S/N: FL100160900003	File Share Server	*ประจำห้อง Data Center
23. HP Proliant DL380 G5	อส 52-05-02038-0001	7 เม.ย. 2552	ใช้งาน	อุปกรณ์ DNS S/N: SGH848XFP	DNS Server Old	*ประจำห้อง Data Center
Rack ตู้ที่ 3						
24. CISCO Catalyst 9200L (VLAN 172)	อส 65-64-02035-0088	8 พ.ย. 2565	ใช้งาน	อุปกรณ์ Switch S/N: JAE26300QAN	LAN	*ประจำห้อง Data Center
25. CISCO Catalyst 9200L (VLAN 1)	อส 65-64-02035-0089	8 พ.ย. 2565	ใช้งาน	อุปกรณ์ Switch S/N: JAE26300QB6	LAN	*ประจำห้อง Data Center
26. ZABBIX			ใช้งาน	อุปกรณ์ตรวจสอบและเฝ้าระวังสำหรับเครื่องแม่ข่าย S/N: 672042000041 IP : 192.168.1.XXX	Network Monitor	*ประจำห้อง Data Center
27. IBM SYSTEM X 3250 M4	อส 54-06-02038-0001		ใช้งาน	อุปกรณ์ NAT Database S/N: 99B9600 IP : 172.25.25.XXX	NAT Database สำนักฟื้นฟูและพัฒนาพื้นที่อนุรักษ์	*ประจำห้อง Data Center
28. HP Proliant DL380 G4	อส 48-05-02033-0009	19 พ.ย. 2548	ใช้งาน	อุปกรณ์ DNS Server S/N: GH511X0V0 IP : 192.168.1.XXX	DNS Server	*ประจำห้อง Data Center
29. IBM SYSTEM X 3250 M4 BUSARIN (งาช้าง)	อส 54-06-02038-0002		ใช้งาน	อุปกรณ์ Ivory Server S/N: 99B9601 IP : 172.25.25.XXX	Ivory Server	*ประจำห้อง Data Center
30. AVTECH Room Alert 32E			ใช้งาน	อุปกรณ์ Room Alert	-Security -Alert Device	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
31. HP StorageWorks P2000 SAN Storage Disk Systems	อส 54-05-02043-0001	19 ส.ค. 2554	ไม่ได้ใช้งาน	อุปกรณ์ Storage S/N: CZC112VXLT	SAN Storage	*ประจำห้อง Data Center
32. HP Blade Enclosure C7000	อส 57-02046-0001		ไม่ได้ใช้งาน	อุปกรณ์ตู้ Enclosure/Chassis สำหรับติดตั้งแผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย S/N: SGH117X95J	Server	*ประจำห้อง Data Center
32.1 HP Proliant BL460c G7	อส 54-05-02040-0001		ไม่ได้ใช้งาน	อุปกรณ์แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/ Chassis แบบที่ 2 S/N: SSGH117X95K	Web Portal Server	*ประจำห้อง Data Center
32.2 HP Proliant BL460c G7	อส 54-05-02040-0002		ไม่ได้ใช้งาน	อุปกรณ์แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/ Chassis แบบที่ 2 S/N: SSGH117X95P IP : 192.168.1.XXX	Web Server	*ประจำห้อง Data Center
32.3 HP Proliant BL460c G8	อส 54-05-02040-0003		ไม่ได้ใช้งาน	อุปกรณ์แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/ Chassis แบบที่ 2 S/N: SGH34890TK IP : 192.168.1.XXX	NSW1	*ประจำห้อง Data Center
32.4 HP Proliant BL460c G8			ไม่ได้ใช้งาน	อุปกรณ์แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/ Chassis แบบที่ 2 S/N: SGH34890TB IP : 192.168.1.XXX	NSW2	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
32.5 HP Proliant BL660c G8	อส 57-05-02040-0001	20 มิ.ย. 2557	ไม่ได้ใช้งาน	อุปกรณ์แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/ Chassis แบบที่ 2 S/N: SGH416F80F IP : 192.168.1.XXX	จองบ้านพัก	*ประจำห้อง Data Center
32.6 HP Proliant BL460c G7	อส 54-05-02040-0001		ไม่ได้ใช้งาน	อุปกรณ์แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/ Chassis แบบที่ 2 S/N: SSGH117X95K IP : 192.168.1.XXX	NSW3	*ประจำห้อง Data Center
32.7 HP Proliant BL680c G7			ไม่ได้ใช้งาน	อุปกรณ์แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/ Chassis แบบที่ 2 S/N: SGS242E5KF IP : 192.168.1.XXX	Database	*ประจำห้อง Data Center
32.8 HP Proliant BL460c G7	อส 54-05-02040-0003		ไม่ได้ใช้งาน	อุปกรณ์แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/ Chassis แบบที่ 2 S/N: SSGH117X95M	Cites Server	*ประจำห้อง Data Center
32.9 HP Proliant BL460c G7	อส 54-05-02040-0004		ไม่ได้ใช้งาน	อุปกรณ์แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/ Chassis แบบที่ 2	Server	*ประจำห้อง Data Center
32.10 HP Proliant BL460c G8	อส 58-05-02019-0001		ไม่ได้ใช้งาน	อุปกรณ์แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/ Chassis แบบที่ 2 IP : 192.168.1.XXX	Web Portal	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
Rack ตู้ที่ 4						
33. CISCO Catalyst 9200L (VLAN 2,5)	อส 65-64-02035-0090	8 พ.ย. 2565	ใช้งาน	อุปกรณ์ Switch S/N: JAE26300QBX	LAN	*ประจำห้อง Data Center
34. HP Proliant DL320 G5P (NET WEB APP)			ไม่ได้ใช้งาน	อุปกรณ์ NET WEB APP S/N: CN68290HPE IP: 192.168.1.XXX	-Server -Park DNP	*ประจำห้อง Data Center
35. VIDYO Portal			ไม่ได้ใช้งาน	อุปกรณ์ Server S/N: 6341020614A715 IP: 192.168.5.XXX	Vidyo Server	*ประจำห้อง Data Center
36. VIDYO Replay			ไม่ได้ใช้งาน	อุปกรณ์ Server S/N: 9321010314A190 IP: 192.168.5.XXX	Vidyo Server	*ประจำห้อง Data Center
37. HP Proliant DL360 G10 (Database Server)	อส 63-64-02038-0001	5 พ.ย. 2563	ใช้งาน	อุปกรณ์ Database Server S/N: SGH026YVB1	Database Sever	*ประจำห้อง Data Center
38. HPE SN3600B Fiber Chanel Switch (NPS)	อส 64-10-02035-0001		ใช้งาน	อุปกรณ์ Switch NPS S/N: **CZC111WACR**	NPS Server	*ประจำห้อง Data Center
39. HPE Proliant DL380 G10 NPS Server 1	อส 64-10-02038-0001		ใช้งาน	VMware System (VMWare vCenter 7.0.2) S/N: **SGH115SK86** IP: 192.168.2.XXX IP vCenter: 192.168.2.XXX	-NPS Server -Park-DNP Server -ParkDB Server -Veeam Backup NPS -Waste 2.77 -Water Meter Server -WEB Server200	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
40. HPE Proliant DL380 G10 NPS Server 2	อส 64-10-02038-0002		ใช้งาน	VMware System (VMWare vCenter 7.0.2) S/N: **SGH115SK88** IP: 192.168.2.XXX IP vCenter: 192.168.2.XXX	-NSW221 Server -NSW222 Server -CKAN STAT Server -WEB2DNP -Zabbix Server -Test Waste 2.78	*ประจำห้อง Data Center
41. HPE MSA 2050 Storage (NPS)	อส 64-10-02043-0001		ใช้งาน	SAN Storage S/N: **ACM036T2WV**	SAN Storage System NPS	*ประจำห้อง Data Center
42. Network Critical SmartNA			ไม่ได้ใช้งาน	อุปกรณ์ Network Monitor S/N: 72790069194	Network Monitor	*ประจำห้อง Data Center
43. SUPERMICRO VMware System			ใช้งาน	VMware System (VMWare vSpere 6.Standard) IP: 192.168.5.XXX, 192.168.2.XXX	-Webreg Server (21สำนัก) -Database webreg Server -Dpis Server -DNP app Server -GDX_Vitaul Sever -Ivory Server -KTBBankNSW Server -Link-Park Server -NPD-APP209 -WaterShed Server -WEB2-206 -Requestformnew Server	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
					-Smart patrol Server -ReadCard Server	
44. Cyberroam CR2500ING-XP	อส 58-05-02034-0001	3 ก.ค. 2558	ไม่ได้ใช้งาน	อุปกรณ์ Firewall S/N: FC47314180102	-Security -Internet	*ประจำห้อง Data Center
45. Dell Poweredge 2900 (File Server)	อส 49-01-02003-0001		ใช้งาน	อุปกรณ์ File Server S/N: G5KVL1S IP: 172.25.25.XXX	File Server	*ประจำห้อง Data Center
Rack ตู้ที่ 5						
46. CISCO SG350 (VLAN 1)	อส 63-64-02035-0004	8 พ.ย. 2565	ใช้งาน	อุปกรณ์ Switch	LAN	*ประจำห้อง Data Center
47. HP Proliant DL380 G5 (NPD APP/ORACLE APP)			ไม่ได้ใช้งาน	อุปกรณ์ NPD APP/Oracle APP S/N: SGH847Y1BB IP: 192.168.1.XXX	NPD App Server	*ประจำห้อง Data Center
48. HP Proliant DL180 G6 (DNP WEB 2) (สบอ.9 อุบล)	อส 55-06-02062-0001	29 เม.ย. 2554	ไม่ได้ใช้งาน	Intel Xeon Processor E5620 2.4 GHz L3 Cache: 12MB Ram : 8GB (2 x 4GB) (RDIMM) Graphic : 32MB RAID Onboard : (RAID 0/1/1+0/5) IP : 192.168.1.XXX S/N: SGH116X17U	Web Server : www2.dnp.go.th	*ประจำห้อง Data Center
49. HP Proliant DL380 G4 (EQSO)	อส 48-05-02033-0008		ใช้งาน	อุปกรณ์ EQSO S/N: SGH511H0UY IP: 192.168.1.XXX	EQSE Server	*ประจำห้อง Data Center
50. IBM SYSTEM X 3650M2 (BACK UP)	อส 52-01-02038-0010 (สบก.)		ไม่ได้ใช้งาน	Application Server IBM System X3650 M2	Backup Server	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
				S/N: 99H6112 IP:192.168.1.XXX		
Rack ตู้ที่ 6						
51. CISCO Catalyst 9200L	อส 65-64-02035-0061	8 พ.ย. 2565	ใช้งาน	อุปกรณ์ Switch S/N: JAE26300P9S	LAN	*ประจำห้อง Data Center
52. HP Proliant DL360 G10 (CKAN Sever)	อส 63-64-02038-0003	5 พ.ย. 2563	ใช้งาน	CKAN S/N: SGH026YVB3 OS: Ubuntu 20.4 IP: 192.168.2.XXX	CKAN SERVER	*ประจำห้อง Data Center
53. HP Proliant DL360 G10 (Stat Share File)	อส 63-64-02038-0004	5 พ.ย. 2563	ใช้งาน	STAT Files Share S/N: SGH026YVB4 OS: MS-Windows Server 2019 IP: 192.168.1.XXX	STAT Files Share SERVER	*ประจำห้อง Data Center
54. HP Proliant DL360 G10 (DNS External)	อส 63-64-02038-0005	5 พ.ย. 2563	ใช้งาน	DNS External S/N: SGH026YVB5 OS: MS-Windows Server 2019 IP: 192.168.1.XXX	DNS SERVER	*ประจำห้อง Data Center
55. HP Proliant DL360 G10	อส 63-64-02038-0006		ใช้งาน	อุปกรณ์ ICT1 Server S/N: SGH026YVB6	ICT1 Server	*ประจำห้อง Data Center
56. HP Proliant DL360 G10	อส 63-64-02038-0007		ใช้งาน	อุปกรณ์ ICT2 Server S/N: SGH026YVB7	ICT2 Server	*ประจำห้อง Data Center
57. HPE SN3600B Fiber Chanel Switch			ใช้งาน	Fiber Chanet Switch	San Switch NSW	*ประจำห้อง Data Center
58. HP Proliant DL380 G10 (NSW Server)	อส 64-64-02038-0002	9 ธ.ค. 2564	ใช้งาน	VMware System (VMWare vCenter 7.0.2) IP: 192.168.2.XXX	-NSW210 Cites Server	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
				IP vCenter: 192.168.2.XXX S/N: SGH123TV5Q	-DNP APP218 Server -Files NSW server -Web portal Server -Database Server -Veeam Backup NSW	
59. HPE MSA 2060 SAN Storage (NSW Storage System)	อส 64-64-02099-0001	9 ธ.ค. 2564	ใช้งาน	อุปกรณ์ NSW Storage System S/N: ACM110S46P	NSW Storage System	*ประจำห้อง Data Center
60. HPE MSA 2050 Storage (CKAN)	อส 63-64-02043-0001	5 พ.ย. 2563	ใช้งาน	อุปกรณ์ CKAN S/N: ACM020T3R6	CKAN Storage	*ประจำห้อง Data Center
61. HPE MSA 2050 Storage (Stat)	อส 63-64-02043-0002	5 พ.ย. 2563	ใช้งาน	อุปกรณ์ Stat S/N: ACM020T3R8	Stat Storage	*ประจำห้อง Data Center
62. HPE MSA 2050 Storage	อส 63-64-02043-0003	5 พ.ย. 2563	ใช้งาน	อุปกรณ์ S/N: ACM020T3R9	Storage	*ประจำห้อง Data Center
Rack ตู้ที่ 7						
63. CISCO SG350 (VLAN 1)	อส 63-64-02035-0006	5 พ.ย. 2563	ใช้งาน	อุปกรณ์ Switch S/N: DN1242004PS	LAN	*ประจำห้อง Data Center
64. EDGE-Core ECS4620-28T (VLAN 6) (Cites)		26 มิ.ย. 2566	ใช้งาน	อุปกรณ์ Switch S/N: EC2001001224	LAN	*ประจำห้อง Data Center
65. HPE Proliant DL380 G10 PLUS (1) (Cites)		26 มิ.ย. 2566	ใช้งาน	อุปกรณ์ Cites Server S/N: SGH319MMGF IP: 192.168.6.XXX	e-Service Server กองคุ้มครอง	*ประจำห้อง Data Center
66. HPE Proliant DL380 G10 PLUS (2) (Cites)		26 มิ.ย. 2566	ใช้งาน	อุปกรณ์ Cites Server IP: 192.168.6.XXX	e-Service Server	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
					กองคุ้มครอง	
67. HPE Proliant DL380 G10 PLUS (3) (Cites)		26 มิ.ย. 2566	ใช้งาน	อุปกรณ์ Cites Server IP: 192.168.6.XXX	e-Service Server กองคุ้มครอง	*ประจำห้อง Data Center
68. HPE MSA 2060 Storage (Cites)		26 มิ.ย. 2566	ใช้งาน	อุปกรณ์ Cites Storage S/N: ACM237S22V IP: 192.168.6.XXX	e-Service Storage กองคุ้มครอง	*ประจำห้อง Data Center
69. Dell EMC PowerEdge R750xs (Wildlife Crime)		6 พ.ย. 2566	ใช้งาน	อุปกรณ์ Wildlife Crime Server S/N: D1KVXW3 IP: 192.168.6.XXX	ศูนย์ข่าวกรองอาชญากรรมสัตว์ป่า Server	*ประจำห้อง Data Center
70. SYNOLOGY 8 BAY Rackstation RS1221+ (Wildlife Crime)		6 พ.ย. 2566	ใช้งาน	อุปกรณ์ Wildlife Crime NAS IP: 192.168.6.XXX	ศูนย์ข่าวกรองอาชญากรรมสัตว์ป่า NAS	*ประจำห้อง Data Center
71. ARUBA Switch Instant On 1430 8G (Wildlife Crime)		6 พ.ย. 2566	ใช้งาน	อุปกรณ์ Wildlife Crime Switch IP: 192.168.6.XXX	ศูนย์ข่าวกรองอาชญากรรมสัตว์ป่า LAN	*ประจำห้อง Data Center
72. Dell EMC PowerEdge R450 (1) (NPS)		1 มี.ค. 2567	ใช้งาน	อุปกรณ์ NPS Server S/N: 78VZ6Y3 IP: 192.168.2.XXX	สำนักอุทยานแห่งชาติ Server	*ประจำห้อง Data Center
73. Dell EMC PowerEdge R450 (2) (NPS)		1 มี.ค. 2567	ใช้งาน	อุปกรณ์ NPS Server S/N: 88VZ6Y3 IP: 192.168.2.XXX	สำนักอุทยานแห่งชาติ Server	*ประจำห้อง Data Center
74. Dell EMC PowerEdge R450 (3) (NPS)		1 มี.ค. 2567	ใช้งาน	อุปกรณ์ NPS Server S/N: 98VZ6Y3 IP: 192.168.2.XXX	สำนักอุทยานแห่งชาติ Server	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
75. Dell EMC PowerVault ME5024 Storage (NPS)		1 มี.ค. 2567	ใช้งาน	อุปกรณ์ NPS Storage S/N: J9VZ6Y3 IP: 192.168.2.XXX	สำนักอุทยานแห่งชาติ Storage	*ประจำห้อง Data Center
Rack ตู้ที่ 8						
76. CISCO Catalyst 9200L (VLAN 1)	อส 65-64-02035-0091	8 พ.ย. 2565	ใช้งาน	อุปกรณ์ Switch S/N: JAE26300QCP	LAN	*ประจำห้อง Data Center
77. CISCO SG350 (VLAN 1)	อส 65-64-02035-0001		ใช้งาน	อุปกรณ์ Switch	LAN	*ประจำห้อง Data Center
78. CISCO Nexus 3548-X			ใช้งาน	อุปกรณ์ Switch	iForms LAN	*ประจำห้อง Data Center
79. HP Proliant DL380 G10 (iForms Server)			ใช้งาน	อุปกรณ์ iForms Server S/N: SGH220Y6DQ	iForms Server	*ประจำห้อง Data Center
80. HP Proliant DL380 G10 (iForms Server)			ใช้งาน	อุปกรณ์ iForms Server	iForms Server	*ประจำห้อง Data Center
81. HP Proliant DL380 G10 (iForms Server)			ใช้งาน	อุปกรณ์ iForms Server	iForms Server	*ประจำห้อง Data Center
82. HP Proliant DL380 G10 (iForms Server)			ใช้งาน	อุปกรณ์ iForms Server S/N: SGH220Y6F3	iForms Server	*ประจำห้อง Data Center
83. HP Proliant DL380 G10 (iForms Server)			ใช้งาน	อุปกรณ์ iForms Server	iForms Server	*ประจำห้อง Data Center
84. DELL Poweredge R210 II (Ivory)		22 ก.ค. 2558	ใช้งาน	อุปกรณ์ Ivory S/N: 3NCF862 IP : 192.168.1.XXX	Ivory Server	*ประจำห้อง Data Center
85. DELL Poweredge R210 II (Geo Server)			ไม่ได้ใช้งาน	อุปกรณ์ Geo Server IP : 58.181.150.XXX	GEO Server	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
86. DELL Poweredge R420 (ไฟป่า)			ใช้งาน	อุปกรณ์ Server ไฟป่า S/N: 78RDNW1 IP : 192.168.1.XXX	สำนักอนุรักษ์สัตว์ป่า	*ประจำห้อง Data Center
87. DELL Poweredge R620 (สำนักสนองฯ)			ใช้งาน	อุปกรณ์ Server สำนักสนองฯ S/N: 45DNQ02 IP : 192.168.1.XXX	สำนักสนองฯ	*ประจำห้อง Data Center
88. HP Proliant DL360p G8	อส 56-05-02038-0001	6 ม.ค. 2557	ไม่ได้ใช้งาน	อุปกรณ์ EGO Server S/N: SGH324XDEF	EGO Server สำนักแผน	*ประจำห้อง Data Center
89. HUAWEI RH1288V3 (สัตว์ป่า)			ใช้งาน	อุปกรณ์ Server สัตว์ป่า IP : 58.181.150.XXX	สัตว์ป่า	*ประจำห้อง Data Center
90. HP Proliant DL380 G8 (สัตว์ป่า)	อส 57-09-02038-0001		ใช้งาน	อุปกรณ์ Server สัตว์ป่า S/N: SGH410D7EV IP : 192.168.1.XXX	สำนักอนุรักษ์สัตว์ป่า	*ประจำห้อง Data Center
91. HPE MSA 2050 Storage	อส 63-64-02043-0004		ใช้งาน	อุปกรณ์ Storage S/N: ACM020T3RB	Storage	*ประจำห้อง Data Center
92. HPE MSA 2050 Storage			ใช้งาน	อุปกรณ์ Storage	Storage	*ประจำห้อง Data Center
93. HP Proliant DL180 G6			ไม่ได้ใช้งาน	อุปกรณ์ Server S/N: SGH116X17X	Server	*ประจำห้อง Data Center
Tower						
94. CISCO SG350 (VLAN 1)	อส 63-64-02035-0007		ใช้งาน	อุปกรณ์ Switch	LAN	*ประจำห้อง Data Center
95. DELL Poweredge T440			ใช้งาน	อุปกรณ์ Server IP : 10.100.40.XXX	Server	*ประจำห้อง Data Center
96. HP d220m			ไม่ได้ใช้งาน	อุปกรณ์ Server S/N: SGH33304HZ	ส่วนวิจัย	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
				IP : 192.168.1.XXX		
97. HP Proliant ML310e Gen8			ใช้งาน	อุปกรณ์ Server S/N: SGH3373W0E IP : 192.168.1.XXX	Server	*ประจำห้อง Data Center
98. LENOVO Thinkcentre (Back Up)	อส 56-05-02059-0010		ใช้งาน	อุปกรณ์ Backup Server S/N: PB9LE72 IP : 192.168.1.XXX	Server	*ประจำห้อง Data Center
99. IBM System X3100 M4 (Back Up)	อส 57-09-02038-0001		ใช้งาน	อุปกรณ์ Backup Server S/N: D6BLEKM IP : 192.168.1.XXX	ส่วนคุ้มครองสัตว์ป่า	*ประจำห้อง Data Center
100. HP Prodesk 400 G4 MT			ไม่ได้ใช้งาน	อุปกรณ์ Server Backup	Server Backup	*ประจำห้อง Data Center
101. HP Pavilion p62831	สพภ 7010-02-03/001		ไม่ได้ใช้งาน	Biodiversity IP: 58.181.150.XXX / 192.168.1.XXX	สำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ(องค์การมหาชน)	*ประจำห้อง Data Center
102. Hikvision DVR		7 ก.พ.56	ใช้งาน	อุปกรณ์บันทึกภาพกล้องวงจรปิด	กล้องวงจรปิด	*ประจำห้อง Data Center
103. Hikvision DVR		7 ก.พ.56	ใช้งาน	อุปกรณ์บันทึกภาพกล้องวงจรปิด	กล้องวงจรปิด	*ประจำห้อง Data Center
104. Hikvision DVR		7 ก.พ.56	ใช้งาน	อุปกรณ์บันทึกภาพกล้องวงจรปิด	กล้องวงจรปิด	*ประจำห้อง Data Center
105. QNAP NAS			ใช้งาน	อุปกรณ์ NAS	NAS Backup	*ประจำห้อง Data Center
106. Synology		9 พ.ย. 2566	ใช้งาน	อุปกรณ์ NAS	NAS File Share Server	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
					กองคุ้มครอง	
DR-Site (INET)						
107. Fortinet FortiGate 200B			ไม่ได้ใช้งาน	อุปกรณ์ Firewall IP : 192.168.20.XXX	Security	*ประจำห้อง Data Center
108. Fortinet FortiGate 5050			ไม่ได้ใช้งาน	อุปกรณ์ Firewall IP : 192.168.20.XXX	Security	*ประจำห้อง Data Center
109. Fortinet FortiAnalyzer 2000A	อส 51-05-02037-0001	7 พ.ย. 2551	ใช้งาน	อุปกรณ์จัดเก็บข้อมูลจราจรทางอิเลคทรอนิกส์ยี่ห้อ Fortinet รุ่น/แบบ fortiAnalyzer-2000A S/N: 2K3F08000237 IP : 192.168.20.XXX	Log Server	*ประจำห้อง Data Center
110. HP v1910-24g Switch			ใช้งาน	อุปกรณ์ Switch IP : 192.168.20.XXX	LAN	*ประจำห้อง Data Center
111. Cisco UCS C220 M4	อส 59-05-02038-0001	4 พ.ค. 2559	ใช้งาน	อุปกรณ์ Server RAM : 32Gb Headdisk : 1.8Tb S/N: SFCH2004V09T IP : 192.168.20.XXX	VMware Server	*ประจำห้อง Data Center
112. Cisco UCS C220 M4	อส 59-05-02038-0002	4 พ.ค. 2559	ใช้งาน	อุปกรณ์ Server RAM : 32Gb Headdisk : 1.8Tb S/N: SFCH2004V0GN IP : 192.168.20.XXX	VMware Server	*ประจำห้อง Data Center
113. Cisco UCS C220 M4	อส 59-05-02038-0003	4 พ.ค. 2559	ใช้งาน	อุปกรณ์ Server RAM : 32Gb Headdisk : 1.8Tb	VMware Server	*ประจำห้อง Data Center

เครื่อง/อุปกรณ์	เลขครุภัณฑ์	วันที่ได้รับ	สถานะ	คุณลักษณะ	ระบบสารสนเทศที่เกี่ยวข้อง	หมายเหตุ
				S/N: SFCH2004V0OU IP : 192.168.20.XXX		
114. NetApp FAS2552 SAS	อส.59-05-02043-0002	4 พ.ค. 2559	ใช้งาน	Ext-Vmware IP : 192.168.20.XXX	VMware Server	*ประจำห้อง Data Center
115. HP Proliant DL380p G8			ใช้งาน	อุปกรณ์ Server IP : 192.168.20.XXX	VMware Server	*ประจำห้อง Data Center
116. QNAP TVS-882			ใช้งาน	อุปกรณ์ NAS IP : 192.168.20.XXX	NAS Backup	*ประจำห้อง Data Center

ระบบสารสนเทศภายใต้การดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับที่	ระบบสารสนเทศ	จำนวน	หน่วย	หน่วยงาน
ระบบสารสนเทศที่ทำสัญญาจ้างกับบริษัท				
๑	ระบบบริหารงานบุคคล และระบบต่อเนื่องบน DPIS	๑	ระบบ	สำนักบริหารงานกลาง
๒	ระบบบริหารงานบุคคล พนักงานราชการ	๑	ระบบ	สำนักบริหารงานกลาง
๓	ระบบงานเงินเดือน ค่าจ้าง และค่าตอบแทน	๑	ระบบ	สำนักบริหารงานกลาง
๔	ระบบบริหารงานคลัง	๑	ระบบ	สำนักบริหารงานกลาง
๕	ระบบจ่ายตรงเงินเดือนข้าราชการและลูกจ้างประจำ	๑	ระบบ	สำนักบริหารงานกลาง
๖	ระบบบริหารการจ่ายค่าตอบแทนพนักงานราชการและพนักงานจ้างเหมา	๑	ระบบ	สำนักบริหารงานกลาง
๗	ระบบใบเสร็จรับเงินกลาง	๑	ระบบ	สำนักบริหารงานกลาง
๘	ระบบบริหารพัสดุกลาง	๑	ระบบ	สำนักบริหารงานกลาง
๙	ระบบเชื่อมโยงคำขอกลางและระบบสนับสนุนใบอนุญาตและใบรับรองผ่านอินเทอร์เน็ต	๑	ระบบ	กองคุ้มครองพันธุ์สัตว์ป่าและพืชป่าตามอนุสัญญา
๑๐	ระบบแลกเปลี่ยนข้อมูลคำขออนุญาตอิเล็กทรอนิกส์และระบบการชำระเงินทางอิเล็กทรอนิกส์ (e-Payment) ผ่านระบบ NSW	๑	ระบบ	กองคุ้มครองพันธุ์สัตว์ป่าและพืชป่าตามอนุสัญญา
๑๑	ระบบอนุญาตนำเข้า ส่งออก และนำผ่าน สัตว์ป่าตามอนุสัญญาไซเตส	๑	ระบบ	กองคุ้มครองพันธุ์สัตว์ป่าและพืชป่าตามอนุสัญญา
๑๒	ระบบบริหารจัดการงาช้างภายในประเทศ	๑	ระบบ	กองคุ้มครองพันธุ์สัตว์ป่าและพืชป่าตามอนุสัญญา
๑๓	ระบบ ebxml Server สำหรับเชื่อมต่อกับโครงการ NSW	๑	ระบบ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๑๔	ระบบบริหารจัดการบน Application Server	๑	ระบบ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๑๕	ระบบจัดการฐานข้อมูล Oracle RDBMS	๑	ระบบ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๑๖	ระบบสารสนเทศเพื่อการบริหาร	๑	ระบบ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
๑๗	ระบบบริการอินเทอร์เน็ต (Internet)	๑	ระบบ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับที่	ระบบสารสนเทศ	หน่วยงาน
ระบบสารสนเทศของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร		
๑	ระบบสารสนเทศกลาง (Web Portal)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)
๒	ระบบสนับสนุนการตัดสินใจ (Business Intelligence)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนฐานข้อมูลและสถิติ)
๓	ระบบบัญชีข้อมูล (Data Catalog) กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนฐานข้อมูลและสถิติ)
๔	โครงการปลูกต้นรวงผึ้งเฉลิมพระเกียรติฯ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)
๕	ระบบสืบค้นข้อมูลบุคลากรกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช "นามสงเคราะห์"	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนการสื่อสาร/ส่วนพัฒนาระบบสารสนเทศ)
๖	โปรแกรมอ่านบัตรประจำตัวประชาชน (ICT DNP Smart Card)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)
๗	ระบบบริการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย/ ส่วนพัฒนาระบบสารสนเทศ)
๘	ระบบจัดการความรู้กลางกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ/ ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย)
๙	ระบบจัดการบัญชีผู้ใช้งานระบบเครือข่ายกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช (Authentication)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย/ ส่วนพัฒนาระบบสารสนเทศ)
๑๐	โปรแกรมรับสมัครอาสาสมัครพิทักษ์อุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช (อส.อส.)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)
๑๑	ระบบบริหารจัดการฐานข้อมูลไฟป่า กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช (DNP : Forest Fire Database Management System)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)
๑๒	ระบบการสื่อสารแบบรวมศูนย์ (workD Platform)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย/สพร.)
๑๓	ระบบบริหารจัดการเรื่องร้องเรียน	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร, ศูนย์ราชการสะดวกฯ
๑๔	ระบบติดตามการเปลี่ยนแปลงพื้นที่ป่าไม้อัจฉริยะ iForMS	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนภูมิสารสนเทศ)
๑๕	ระบบการตรวจสอบการเปลี่ยนแปลงพื้นที่ป่าไม้ด้วยการประมวลผลข้อมูลจากดาวเทียมสำรวจทรัพยากรธรรมชาติ (ForMS)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)
๑๖	ระบบฐานข้อมูลเพื่อการบริหารจัดการพื้นที่อนุรักษ์ ๒๑ สำนัก	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร, สำนักบริหารพื้นที่อนุรักษ์ ๒๑ สำนัก
๑๗	ระบบถาม - ตอบ กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)

ลำดับที่	ระบบสารสนเทศ	หน่วยงาน
๑๘	ระบบสารสนเทศกลาง (DNP-APP)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)
๑๙	ระบบจดหมายอิเล็กทรอนิกส์ กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช (DNP Mail)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนปฏิบัติการคอมพิวเตอร์และเครือข่าย)
๒๐	ระบบการจ้างบุคคลภายนอก/การจ้างเอกชนดำเนินงาน กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)
๒๑	การประเมินคุณธรรมและความโปร่งใสในการดำเนินงานของหน่วยงานภาครัฐ (ITA)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)
๒๒	ระบบคำขออนุญาตเพื่อการถ่ายทำภาพยนตร์ วีดิทัศน์ หรือสารคดี หรือการถ่ายภาพ ในอุทยานแห่งชาติและวนอุทยาน	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)
๒๓	ระบบฐานข้อมูลเพื่อใช้ในการปฏิบัติงานของส่วนเสริมสร้างวินัย	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ส่วนพัฒนาระบบสารสนเทศ)

ปรับปรุงล่าสุด
๒๗ มีนาคม ๒๕๖๗