# บันทึกข้อความ

**ส่วนราชการ** แผนงานเทคโนโลยี กรมสนับสนุนบริการสุขภาพ โทร.๐ ๒๕๙๐๑๖๘๑
**ที่** สธ ๐๗๑๖.๐๒/๒๓ **วันที่** ๑๕ พฤษภาคม ๒๕๕๕
**เรื่อง** ขออนุมัติแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมสนับสนุนบริการสุขภาพ ประจำปีงบประมาณ พ.ศ.๒๕๕๕

**เรียน** ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ตามกรอบการประเมินผลการปฏิบัติราชการ มิติภายใน ด้านการพัฒนาองค์การ ประจำปีงบประมาณ พ.ศ. ๒๕๕๕ ของส่วนราชการ ได้กำหนดตัวชี้วัดการประเมินผลการปฏิบัติราชการ ประจำปีงบประมาณ พ.ศ. ๒๕๕๕ **ตัวชี้วัดที่ ๑๑ ระดับความสำเร็จของการพัฒนาปรับปรุงสารสนเทศ** ในรายละเอียดการประเมิน กำหนดให้หน่วยงานมีแผนบริหารความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศ และกระบวนการที่แสดงถึงการตอบสนองต่อการบุกรุกที่เสี่ยงต่อการทำงานของระบบสารสนเทศ เพื่อลดความเสียหายได้อย่างรวดเร็ว รวมถึงการป้องกันเหตุการณ์ที่อาจเกิดขึ้นและดำเนินการตามแผน นั้น (ดังรายละเอียดที่แนบ ๑)

เพื่อให้สอดคล้องกับแนวทางการตรวจประเมินตัวชี้วัดที่ ๑๑ ระดับความสำเร็จของการพัฒนาปรับปรุงสารสนเทศ สำนักเทคโนโลยีสารสนเทศและการสื่อสาร ได้มอบให้คณะทำงานจัดทำระบบบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทำการทบทวนและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมสนับสนุนบริการสุขภาพ คณะทำงานฯได้ยึดกรอบวิเคราะห์ มาตรฐานISO/IEC๒๗๐๐๑ Annex A ในการทบทวนและวิเคราะห์ และจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมสนับสนุนบริการสุขภาพ เสร็จสิ้นแล้ว(ดังรายละเอียดที่แนบ ๒)

จึงเรียนมาโปรดพิจารณา หากเห็นชอบขอได้โปรดขออนุมัติแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมสนับสนุนบริการสุขภาพ ประจำปีงบประมาณ พ.ศ.๒๕๕๕ เพื่อศูนย์สารสนเทศจะได้นำไปดำเนินการตามแผนฯต่อไป

นายสมสิทธิ์ พลนาคู
แทนหัวหน้ากลุ่มแผนงานเทคโนโลยี

เรียน หน. กลุ่มแผนงานเทคโนโลยี
- อนุมัติ และแจ้ง จนท.และหน่วยงานที่เกี่ยวข้อง
- ประชาสัมพันธ์แจ้งให้ หน่วยงานภายในกรมสนับสนุนบริการสุขภาพทราบทางเว็บไซต์

นายวิชัย จิตติกรยุทธนา
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร
แทน CIO
16/พ.ค./55

| กรมสนับสนุนบริการสุขภาพ | แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมสนับสนุนบริการสุขภาพ ประจำปีงบประมาณ พ.ศ. ๒๕๕๕ | ฉบับที่ ๑/๒๕๕๕ |
|---|---|---|

การควบคุมเอกสาร

| | |
|---|---|
| ผู้จัดทำ | สำนักเทคโนโลยีสารสนเทศและการสื่อสาร |
| ชื่อแฟ้ม | แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมสนับสนุนบริการสุขภาพ ปีงบประมาณ ๒๕๕๕ |
| สร้างเมื่อ | พฤษภาคม พ.ศ ๒๕๕ |
| แก้ไขครั้งล่าสุด | |
| จำนวน(แผ่น) | ๒๒ แผ่น |

อนุญาต

| ฉบับที่ | วัน-เดือน-ปี | ผู้อนุญาต | ตำแหน่ง | ลงชื่อ |
|---|---|---|---|---|
| | ๒๑ พฤษภาคม ๒๕๕๕ | นายวิชัย จิตติกรยุทธนา | ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร | |

# สารบัญ

หน้า

**๑. หลักการและเหตุผล**

การบริหารงานขององค์กรทุกประเภท ทั้งภาครัฐ และภาคเอกชน ต่างมีวัตถุประสงค์ของตนเอง และมุ่งหวังที่จะทำงานไปให้ถึงเป้าหมายที่วางไว้อย่างดีที่สุด สูญเสียทรัพยากรให้น้อยที่สุด แต่การดำเนินการใดๆ เพื่อบรรลุวัตถุประสงค์ที่วางไว้ มักจะต้องประสบความไม่แน่นอนที่จะประสบความสำเร็จมากน้อยแล้วแต่สภาวะที่แวดล้อมอยู่ ดังนั้นความเสี่ยงจึงเป็นภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาสที่ทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อผลเสียหายแก่องค์กร ทั้งในด้านยุทธศาสตร์ การดำเนินงาน การเงิน ทรัพยากรต่างๆ หรือแม้แต่ชื่อเสียง ภาพลักษณ์ ดังนั้นหากองค์กรสามารถเข้าไปบริหารความเสี่ยงได้อย่างถูกต้อง ภาวะคุกคาม ปัญหา อุปสรรคทั้งหลายที่คาดไว้อาจก่อให้เกิดโอกาสและนำไปสู่นวัตกรรมได้ ทั้งยังเกิดโอกาสในการพัฒนาประสิทธิภาพในการทำงาน การบริการความเสี่ยงเป็นเรื่องประกอบกันระหว่างองค์ประกอบที่สำคัญ ๒ ส่วน คือ โอกาสที่น่าจะเกิดขึ้นของสิ่งที่ไม่พึงประสงค์ กับผลกระทบที่ตามมา การบริหารความเสี่ยงอย่างเหมาะสมจะเป็นการสนับสนุน กลยุทธ์และแผนงานให้บรรลุเป้าหมายตามที่วางไว้ เข้าใจภัยคุกคามของการปฏิบัติงานในองค์กรมีประสิทธิภาพมากขึ้น สนับสนุนให้มีการปรับปรุงงานอย่างต่อเนื่อง มีการสื่อสารในองค์กรมากขึ้น ความสัมพันธ์ต่างๆก็ดีตามมา การบริหารความเสี่ยงระดับองค์กร เป็นการผสมผสานการบริหารความเสี่ยงโดยพิจารณาจากความเสี่ยงทั้งหมด เป็นกระบวนการเชิงระบบเพื่อระบุ ประเมิน ควบคุม และสื่อสารความเสี่ยง โดยให้คลอบคลุมทั้งองค์กร ให้มีกระบวนคิดในการที่จะมองไปข้างหน้า โดยได้รับการสนับสนุน และมีส่วนร่วมจากผู้บริหารในทุกระดับ และจากทุกคนในองค์กรนั้นๆ

กรมสนับสนุนบริการสุขภาพได้นำเทคโนโลยีสารสนเทศมาใช้งานเพื่อช่วยเพิ่มประสิทธิภาพการดำเนินงาน และให้บริการประชาชนได้รับความสะดวก รวดเร็ว ขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอก ส่งผลกระทบต่อการดำเนินงานของกรมสนับสนุนบริการสุขภาพ ดังนั้น เพื่อให้ระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ มีความมั่นคง ปลอดภัย กรมสนับสนุนบริการสุขภาพจึงได้มี ระบบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและจัดทำแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศขึ้น

**๒. นิยามความเสี่ยง**

**ความเสี่ยง (Risk)** คือ เหตุการณ์หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจที่กำหนด

**กระบวนการบริหารความเสี่ยง (Risk Management Process)** เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยงโดยกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งกระบวนการดัง กล่าว

นี้จะสำเร็จได้ ต้องมีการสื่อสารให้คนในองค์กรมีความรู้ ความเข้าใจในเรื่องการบริหารความเสี่ยงในทิศทางเดียวกัน

**ปัจจัยเสี่ยง** หมายถึง ต้นเหตุ หรือ สาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้

**การประเมินความเสี่ยง (Risk Assessment)** หมายถึง กระบวนการที่ใช้ในการระบุ วิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ(Impact)

- โอกาสที่จะเกิด (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดความเสี่ยง
- ผลกระทบ (Impact) หมายถึง ขนาดของความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง

**ระดับของความเสี่ยง (Degree of Risk)** หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งเป็น ๔ ระดับ คือ ระดับสูงมาก ระดับสูง ระดับปานกลาง และระดับต่ำ

## ๓. วัตถุประสงค์ของการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
๒. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ
๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศดำเนินงานได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

## ๔. ขอบเขต

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมสนับสนุนบริการสุขภาพ ฉบับนี้ครอบคลุมถึงทุกหน่วยงานภายในสังกัด กรมสนับสนุนบริการสุขภาพ

## ๕. กระบวนการบริหารความเสี่ยง

### ๕.๑ กำหนดผู้รับผิดชอบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร กรมสนับสนุนบริการสุขภาพ ได้รับมอบให้ ทำการทบทวนและวิเคราะห์ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ คณะทำงานฯ ได้ยึดกรอบวิเคราะห์ตามมาตรฐานISO/IEC๒๗๐๐๑ Annex A ในการกำหนดแนวทางในการจัดทำแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศประกอบด้วย

๑. นโยบายความมั่นคงปลอดภัย(Security policy)
๒. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

๓. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

๔. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร(Human resources security)

๕. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communications and Operating Management)

๗. การควบคุมการเข้าถึง(Access Control)

๘. การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development andMaintenance)

๙. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

๑๐. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

๑๑. การปฏิบัติตามข้อกำหนด (Compliance)

**โดยใช้ข้อมูลจาก**

๑. เหตุการณ์ที่ฝ่าฝืน ละเว้น หรือไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศในปีที่ผ่านมา

๒. เหตุการณ์จากการสังเกตุเชิงประจักษ์ในการเฝ้าระวังและติดตามภัยต่างๆ

๓. เหตุการณ์จากการวิเคราะห์จาก log file

**๕.๒ การประเมินความเสี่ยง** (Risk Assessment)

**การประเมินความเสี่ยง** (Risk Assessment) คณะทำงานฯได้ทำการวิเคราะห์ปัญหาความเสี่ยงในแง่ของโอกาสที่จะเกิดเหตุ (Likelihood) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไร และผลกระทบ (Impact) ที่ติดตามมาว่ามีความรุนแรงเสียหายมากน้อยเพียงใด โดยใช้เกณฑ์ในการประเมินระดับโอกาส(Likelihood) การเกิดแบ่งเป็น ๕ ระดับคือ ดังตารางที่๑

| ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) | | |
|---|---|---|
| ระดับ | โอกาสที่จะเกิด(ความเป็นไปได้) | คำอธิบาย |
| ๕ | สูงมาก | มีโอกาสในการเกิดเกือบทุกครั้ง |
| ๔ | สูง | มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ |
| ๓ | ปานกลาง | มีโอกาสเกิดบางครั้ง |
| ๒ | ต่ำ | อาจมีโอกาสเกิดแต่นานๆ ครั้ง |
| ๑ | ต่ำมาก | มีโอกาสเกิดในกรณียกเว้น |

ตารางที่๑

เกณฑ์ที่ใช้ในการประเมินผลกระทบ (Impact) ที่จะเกิดความเสี่ยง ดังตารางที่ ๒

| ระดับความรุนแรงของผลกระทบ(Impact) | | |
|---|---|---|
| ระดับ | ระดับผลกระทบ | คำอธิบาย |
| ๕ | สูงมาก | ระบบ IT ที่สำคัญทั้งหมดเกิดความเสียหายและทำให้การดำเนินงานหยุดชะงักนานเกินกว่า ๕ วัน |
| ๔ | สูง | ระบบ IT ที่สำคัญเกิดความเสียหายและทำให้การดำเนินงานหยุดชะงัก ๒ - ๕ วัน |
| ๓ | ปานกลาง | ระบบ IT มีปัญหาและมีความสูญเสียบางส่วนทำให้การดำเนินงานหยุดชะงักมากกว่า ๔ ชั่วโมงแต่ไม่เกิน ๒๔ ชั่วโมง |
| ๒ | ต่ำ | ระบบ IT มีปัญหาและมีความสูญเสียไม่มากทำให้การดำเนินงานหยุดชะงัก ๑ – ๔ ชั่วโมง |
| ๑ | ต่ำมาก | ระบบ IT มีปัญหาและเกิดความสูญเสียเพียงเล็กน้อย |

ตารางที่ ๒

จากนั้นจะหาค่า ระดับความเสี่ยง*(Degree of Risk)*โดยการคิดค่าของระดับความเสี่ยงจะคิดได้ดังนี้

ระดับความเสี่ยง(Risk Value)

*= ค่าคะแนนของโอกาสที่จะเกิดความเสี่ยง x ค่าคะแนนของผลกระทบจากความเสี่ยงที่เกิดขึ้น*

*= Likelihoods (L) X Impacts (I)*

ตัวเลขที่แสดงในตารางที่ ๓ เกิดจากผลคูณของ แนวตั้ง คูณ แนวนอน

| **โอกาสที่จะเกิดความเสี่ยง** | **ผลกระทบของความเสี่ยง** | | | | |
|---|---|---|---|---|---|
| | ๑ = ต่ำมาก | ๒ = ต่ำ | ๓ = ปานกลาง | ๔ = สูง | ๕ = สูงมาก |
| ๕ = สูงมาก | ๕ | ๑๐ | ๑๕ | ๒๐ | ๒๕ |
| ๔ = สูง | ๔ | ๘ | ๑๒ | ๑๖ | ๒๐ |
| ๓ = ปานกลาง | **๓** | ๖ | ๙ | ๑๒ | ๑๕ |
| ๒ = ต่ำ | **๒** | ๔ | ๖ | ๘ | ๑๐ |
| **๑ = ต่ำมาก** | ๑ | ๒ | ๓ | ๔ | ๕ |

**เขตยอมรับความเสี่ยง**

ตารางที่ ๓

นำค่าระดับคะแนนที่ได้ มาจัดระดับความเสี่ยงโดยรวม เป็น ๔ ระดับ คือ ต่ำ ปานกลาง สูง และสูงมาก เพื่อดำเนินการจัดทำแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เกณฑ์การประเมิน

ระดับความเสี่ยงโดยรวม ดังตารางที่ ๔

| ระดับความเสี่ยงโดยรวม | ระดับคะแนน | ความหมาย |
|---|---|---|
| ต่ำ (Low) | ๑-๔ | ระดับความเสี่ยงที่ยอมรับได้ โดยไม่ต้องมีการควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม |
| ปานกลาง (Medium) | ๕-๙ | ระดับความเสี่ยงที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ |
| สูง (High) | ๑๐-๑๖ | ระดับความเสี่ยงที่ไม่สามารถยอมรับได้โดยต้องมีการจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป |
| สูงมาก (Extreme) | ๑๗-๒๕ | ระดับความเสี่ยงที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที |

ตารางที่ ๔

**๕.๓ การตอบสนองความเสี่ยง (Risk Response)**

คณะทำงานฯ ได้กำหนดวิธีการการตอบสนองความเสี่ยง เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยใช้กลยุทธ์การจัดการความเสี่ยงอย่างใดอย่างหนึ่งผสมผสานกันดังต่อไปนี้

๕.๓.๑ การยอมรับความเสี่ยง (Take) เป็นการยอมรับความเสี่ยงที่เกิดขึ้นเนื่องจากไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยงหรือ หน่วยงาน มีมาตรการติดตามอย่างใกล้ชิด เพื่อรองรับผลที่จะเกิดขึ้นแล้ว หรือผลกระทบของความเสี่ยงอยู่ในระดับต่ำ ที่ หน่วยงาน ยอมรับได้ หรือเห็นว่าไม่มีวิธีจัดการความเสี่ยงที่เหมาะสม จึงตัดสินใจยอมรับความเสี่ยงที่จะเกิดขึ้น

๕.๓.๒ การลดการควบคุมความเสี่ยง (Treat) เป็นการปรับปรุงกระบวนการทำงานหรือการออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิดหรือลดผลกระทบให้อยู่ในระดับที่ยอมรับได้ เช่น การลดขนาดกิจกรรม

๕.๓.๓ การกระจายความเสี่ยงหรือถ่ายโอนความเสี่ยง (Transfer) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้ผู้อื่นช่วยแบ่งเบาความรับผิดชอบ เช่น การใช้บริการจากภายนอก (Out Source)

๕.๓.๔ การหลีกเลี่ยงความเสี่ยง (Terminate) เป็นการจัดการกับความเสี่ยงที่มีอยู่ในระดับสูงมากและหน่วยงานไม่อาจยอมรับได้จึงต้องตัดสินใจ หยุด ยกเลิก หรือเปลี่ยนแปลงกิจกรรมที่จะนำไปสู่เหตุการณ์ที่เป็นความเสี่ยง **ตามตาราง ภาคผนวก ก**

**๕.๔ กิจกรรมการตอบสนองความเสี่ยง (Control Activities)**

คณะทำงานจัดทำระบบบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กำหนดระดับความเสี่ยงโดยรวม ที่มีคะแนนประเมินความเสี่ยงที่ระดับสูงตั้งแต่ ๑๐-๑๖ ขึ้นไป นำมาดำเนินการจัดทำ

กิจกรรมการตอบสนองความเสี่ยง และจัดทำแผนบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ **ตามตารางภาคผนวก ข**

**๕.๕ ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง(Information and Communication)**

คณะทำงานฯ จัดให้มีการสื่อสารข้อมูลที่ต้องการผ่านช่องทางการสื่อสารไปยัง กลุ่มเป้าหมายที่กำหนด โดยใช้จดหมายอิเลคทรอนิกส์ หนังสือเวียน และทางเว็บไซต์ เพื่อให้บุคคลที่เกี่ยวข้องได้รับทราบการข้อมูลนำไปสู่การปฏิบัติ

**๕.๖ การติดตามผลและเฝ้าระวังความเสี่ยง (Monitoring)**

กำหนดให้มีการติดตามการประเมินผลการดำเนินงานตามระยะเวลาที่กำหนดไว้ดังนี้ เดือน มิถุนายน - กันยายน พ.ศ. ๒๕๕๕ เฝ้าระวังและติดตามผลความเสี่ยงเดือน กันยายน พ.ศ. ๒๕๕๕ จัดทำสรุปและรายงานผลการเฝ้าระวัง

**๖. บทบาท หน้าที่ของผู้ที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

**๖.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง**

ทำหน้าที่กำหนดนโยบายและแนวทางในการจัดทำทำระบบบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และทำหน้าที่กำกับดูแลให้มีการดำเนินการตามแผนบริหารความเสี่ยงเป็นไปด้วยความเรียบร้อย ถูกต้อง

**๖.๒** คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร

ทำการทบทวน วิเคราะห์ และประเมินความเสี่ยง (Risk Assessment) และจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

**๖.๓ กลุ่มพัฒนาระบบเครือข่าย**

นำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศไปสู่การปฏิบัติอย่างทั่วถึง และติดตามสรุปรายงานผลการปฏิบัติการตามแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ

**๖.๔ บุคลากรในหน่วยงาน**

ดำเนินการตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามที่กำหนดอย่างถูกต้องครบถ้วน

**๗. ตัวชี้วัด :** ระดับความสำเร็จของการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ภาคผนวก ก-1

## ตารางสรุปผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมสนับสนุนบริการสุขภาพ ประจำปีงบประมาณ ๒๕๕๕

| ความเสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| **๑.นโยบายความมั่นคงปลอดภัย(Security policy)** | | | | | |
| ๑.๑ การบริหารจัดการความมั่นคงปลอดภัยไม่สามารถทำได้อย่างมีประสิทธิภาพและประสิทธิผล ซึ่งอาจส่งผลให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยหลายๆ อย่าง | ขาดการทบทวนนโยบายด้านความมั่นคงปลอดภัย ให้ทันกับสถานการณ์ และระบบที่เปลี่ยนแปลง | ๓ | ๕ | ๑๕ (สูง) | ควบคุม/ลด (Treat) |
| **๒. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)** | | | | | |
| ๒.๑ ระบบสารสนเทศไม่มีความมั่นคงปลอดภัย | ขาดการให้การสนับสนุนต่อจัดการทางด้านความมั่นคงปลอดภัย โดยมีการ กำหนดทิศทางที่ชัดเจน | ๔ | ๕ | ๒๐ (สูงมาก) | ควบคุม/ลด (Treat) |

| ความเสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| ๒.๒ ไม่สามารถผลักดันนโยบายด้านความมั่นคงปลอดภัยให้มีผลชัดเจนและสำเร็จอย่างเป็นรูปธรรม | ขาดการกำหนดให้มีตัวแทนเจ้าหน้าที่จากฝ่ายต่างๆเพื่อประสานงาน ในการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ | ๓ | ๓ | ๙ (ปานกลาง) | . การยอมรับ (Take) |
| ๒.๓ ระบบสารสนเทศไม่มีความมั่นคงปลอดภัยเนื่องจากขาดผู้รับผิดชอบและดูแลอย่างจริงจัง | ขาดการกำหนดหน้าที่ผู้รับผิดชอบทางด้านความทั่งคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน | ๓ | ๓ | ๙ (ปานกลาง) | . การยอมรับ (Take) |
| **๓. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)** | | | | | |
| ๓.๑ การไม่สามารถบริหารจัดการความเสี่ยงด้านทรัพย์สินต่างๆ ได้ | ไม่มีการจัดทำป้ายชื่อและบัญชีทรัพย์สินสารสนเทศที่สำคัญขององค์กร | ๔ | ๔ | ๑๖ (สูง) | ควบคุม/ลด (Treat) |
| ๓.๒ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตเนื่องจากมีการป้องกันที่ไม่เหมาะสม | ไม่มีการจัดหมวดหมู่ความสำคัญของทรัพย์สินสารสนเทศ | ๔ | ๒ | ๘ (ปานกลาง) | การยอมรับ (Take) |
| ๓.๓ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต/ข้อมูลสำคัญเกิดการรั่วไหล | ขาดขั้นตอนปฏิบัติสำหรับการจัดการ กับสารสนเทศตามชั้นความลับที่กำหนดไว้ | ๓ | ๒ | ๖ (ปานกลาง) | การยอมรับ (Take) |

| ความเสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| **๔.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร(Human resources security)** | | | | | |
| ๔.๑ ข้อมูล ระบบ และเครื่องคอมพิวเตอร์ขององค์กรขาดความมั่นคงปลอดภัย | เจ้าหน้าที่ขาดการสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอซึ่งทำให้เจ้าหน้าที่สามารถป้องกันตนเองได้ในระดับหนึ่ง | ๔ | ๓ | ๑๒ (สูง) | ควบคุม/ลด (Treat) |
| ๔.๒ การเข้าถึงระบบโดยไม่ได้รับอนุญาตโดยใช้ User ID ของ**เจ้าหน้าที่**คนก่อน | ขาดการติดตามเรื่องการถอดถอนสิทธิของเจ้าหน้าที่ลาออกหรือย้ายหน่วยงาน | ๕ | ๔ | ๒๐ (สูงมาก) | ควบคุม/ลด (Treat) |
| ๔.๓ ทรัพย์สินขององค์กรเกิดการสูญหาย | ไม่มีขั้นตอนปฏิบัติสำหรับการคืนทรัพย์สินขององค์กรเมื่อเจ้าหน้าที่ลาออก | ๑ | ๓ | ๓ (ต่ำ) | การยอมรับ (Take) |
| ๔.๔ เจ้าหน้าที่ขาดความรู้ความสามารถด้านเทคโนโลยีสารสนเทศ | การเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่รวดเร็ว | ๔ | ๒ | ๘ (ปานกลาง) | การยอมรับ (Take) |
| **๕.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)** | | | | | |
| ๕.๑ กระแสไฟฟ้ากระชากซึ่งทำให้เครื่องคอมพิวเตอร์เกิดความเสียหาย | ขาดการติดตั้งเครื่องกรองกระแสไฟฟ้า | ๑ | ๕ | ๕ (ต่ำ) | การยอมรับ (Take) |

| ความเสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| ๕.๒ เครื่องเซิร์ฟเวอร์ไม่สามารถให้บริการได้ เนื่องจากอุณหภูมิไม่เหมาะสม | เครื่องปรับอากาศภายในห้องระบบคอมพิวเตอร์แม่ข่าย เป็นเครื่องเก่ามีอายุการใช้งานเกิน ๕ ปีขึ้นไป | ๔ | ๕ | ๒๐ (สูงมาก) | โอนความเสี่ยง (Transfer) |
| ๕.๓ อุปกรณ์ได้รับความเสียหายจากภัยธรรมชาติ และเข้าถึงได้โดยง่ายเนื่องจากสถานที่ตั้งไม่เหมาะสม | การออกแบบสถานที่ตั้งและบริเวณโดยรอบของห้องควบคุมระบบคอมพิวเตอร์แม่ข่ายอยู่ในที่ต่ำ | ๑ | ๕ | ๕ (ต่ำ) | การยอมรับ (Take) |
| **๖.การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communications and Operating Management)** | | | | | |
| ๖.๑ การปฏิบัติงานผิดพลาดไม่เป็นไปตามลำดับขั้นตอน | ขาดการจัดทำขั้นตอนปฏิบัติงานและปรับปรุงคู่มือปฏิบัติการ | ๒ | ๒ | ๔ (ต่ำ) | การยอมรับ (Take) |
| ๖.๒ การรับบริการจากหน่วยงานภายนอกไม่ได้ประสิทธิภาพ และมีความมั่นคงปลอดภัยพอ ตามความก้าวหน้าของเทคโนโลยี | ข้อตกลงการให้บริการระหว่างองค์กรกับผู้ให้บริการภายนอก ขาดการทบทวนตรวจสอบ อย่างสม่ำเสมอว่าได้มีแนวทางการปรับปรุงให้ดียิ่งขึ้น และมีความมั่นคงปลอดภัยสอดคล้องกับสถานการณ์ในปัจจุบันหรือไม่ | ๒ | ๓ | ๖ (ปานกลาง) | การยอมรับ (Take) |

| ความเสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| ๖.๓ การป้องกันโปรแกรมไม่ประสงค์ดีไม่สามารถป้องกันตัวใหม่ๆได้ทั่วถึง | -ขาดการตรวจสอบข่าว หรือข้อมูลที่เกี่ยวข้องกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ<br>- เจ้าหน้าที่ไม่ได้ทำการตรวจสอบโปรแกรมไม่ประสงค์ดีในเครื่องที่ตนเองใช้งานอย่างสม่ำเสมอ | ๔ | ๓ | ๑๒ (สูง) | ควบคุม/ลด (Treat) |
| ๖.๔ การไม่สามารถติดตั้งระบบกลับคืนมาได้ กรณีเกิดภัยพิบัติกับองค์กร เช่นไฟไหม้ แผ่นดินไหว เป็นต้น | ขาดขั้นตอนปฏิบัติสำหรับการทดสอบใช้งานข้อมูลที่ได้สำรองเก็บไว้ว่ายังคงสามารถเข้าถึง และใช้งานได้ตามปกติหรือไม่ | ๒ | ๓ | ๖ (ปานกลาง) | การยอมรับ (Take) |
| ๖.๕ ข้อมูลสำคัญอาจสูญหาย | ขาดการกำหนดประเภทของข้อมูลที่จะต้องมีการจัดเก็บไว้อย่างถาวรห้ามลบทิ้ง | ๒ | ๒ | ๔ (ต่ำ) | การยอมรับ (Take) |
| ๖.๖ การไม่สามารถติดตั้งระบบกลับคืน กรณีปรับปรุงแก้ไขระบบไม่สำเร็จ ทำไม่ได้ในเวลาอันสมควร | -ไม่มีการวางแผนหรือทำขั้นตอนการปฏิบัติสำหรับการถอยหลังระบบ<br>- ไม่มีการบันทึกรายละเอียดการเปลี่ยนแปลงต่อระบบเทคโนโลยีอย่างสมบูรณ์ | ๑ | ๔ | ๔ (ต่ำ) | การยอมรับ (Take) |

**ภาคผนวก ก-6**

| ความเสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| ๖.๗ เอกสารและคู่มือเกิดการสูญหาย/ข้อมูลสำคัญในเอกสารคู่มือนั้นถูกเข้าถึงโดยไม่ได้รับอนุญาต | ขาดการจัดเก็บเอกสาร และคู่มือการปฏิบัติงานไว้ในสถานที่ที่มีความปลอดภัย | ๒ | ๓ | ๖ (ปานกลาง) | การยอมรับ (Take) |
| ๖.๘ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต | ขาดขั้นตอนการปฏิบัติ การควบคุมระบบการจัดเก็บเอกสารระบบ | ๓ | ๒ | ๖ (ปานกลาง) | การยอมรับ (Take) |
| ๖.๙ ข้อมูลที่ส่งผ่านทางเครือข่ายถูกผู้ไม่ประสงค์ดีดักจับได้ | ขาดการเข้ารหัสข้อมูล ก่อนส่งผ่านไปทางเครือข่ายอินเทอร์เน็ต | ๓ | ๒ | ๖ (ปานกลาง) | การยอมรับ (Take) |
| ๖.๑๐ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต/ข้อมูลสำคัญรั่วไหล/สื่อบันทึกข้อมูลเกิดความเสียหายหรือสูญหาย | ขาดการกำหนดวิธีการที่เชื่อถือได้และมั่นคงปลอดภัยในการขนย้ายหรือส่งสื่อบันทึกข้อมูลจากสถานที่หนึ่งไปยังอีกสถานที่หนึ่ง | ๓ | ๒ | ๖ (ปานกลาง) | การยอมรับ (Take) |

| ความเสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| ๖.๑๑ ระบบได้รับความเสียหายจากการไม่ได้รับการแก้ไขปัญหาได้ทันต่อเหตุการณ์ | ขาดการตรวจสอบข้อมูลล็อกการเข้าถึงระบบสารสนเทศ (Audit Logging) อย่างสม่ำเสมอ | ๓ | ๒ | ๖ (ปานกลาง) | การยอมรับ (Take) |
| ๖.๑๒ ข้อมูลไม่ได้รับการสำรองอย่างถูกวิธี | ขาดแผนการสำรองข้อมูลที่ครบถ้วน เช่น คู่มือวิธีการสำรองข้อมูล | ๔ | ๔ | ๑๖ (สูง) | ควบคุม/ลด (Treat) |
| ๖.๑๓ ข้อมูลที่สำรองไว้ไม่สามารถใช้งานได้ | ขาดขั้นตอนปฏิบัติสำหรับการทดสอบใช้งานข้อมูลที่ได้สำรองเก็บไว้ว่ายังคงสามารถเข้าถึงและใช้งานได้หรือไม่ | ๑ | ๔ | ๔ (ต่ำ) | การยอมรับ (Take) |
| **๗. การควบคุมการเข้าถึง(Access Control)** | | | | | |
| ๗.๑ การเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาตหรือไม่เหมาะสมกับหน้าที่ความรับผิดชอบ | -ขาดนโยบายควบคุมการเข้าถึงสารสนเทศเป็นลายลักษณ์อักษร<br>-ขาดกระบวนการในการทบทวนสิทธิการเข้าถึงระบบงานของผู้ใช้งานอย่างเป็นทางการ และสม่ำเสมอ | ๔ | ๓ | ๑๒ (สูง) | ควบคุม/ลด (Treat) |
| ๗.๒ การสวมรอยปลอมเป็นผู้ใช้งานที่ล็อกอิน และใช้งานระบบค้างไว้โดยไม่ได้ล็อกเอ้าท์ | ขาดการกำหนดให้ระบบงานสำคัญ (เช่น ระบบงานการเงิน) มีการตัดและ | ๓ | ๒ | ๖ (ปานกลาง) | การยอมรับ (Take) |

| ความเสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| | หมดเวลาการใช้งาน (Session Time-Out) รวมทั้งปิดการใช้งานและล้างหน้าจอด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้ เช่น ๓๐ นาที | | | | |
| ๗.๓ การเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต ทรัพย์สินขององค์กรสูญหายหรือถูกขโมย | ขาดนโยบายด้านหน้าที่ความรับผิดชอบของผู้ใช้งาน | ๓ | ๒ | ๖ (ปานกลาง) | การยอมรับ (Take) |
| **๘.การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development andMaintenance)** | | | | | |
| ๘.๑ ข้อมูลนำเข้าเกิดความผิดพลาด | ขาดการตรวจสอบเอกสารที่จะใช้เป็นข้อมูลนำเข้าระบบงานอย่างเป็นทางการ เพื่อตรวจหาการเปลี่ยนแปลงที่เกิดขึ้นโดยไม่ได้รับอนุญาต | ๓ | ๒ | ๖ (ปานกลาง) | การยอมรับ (Take) |
| ๘.๒ ข้อมูลที่นำออกจากระบบเกิดการผิดพลาดหรือคลาดเคลื่อนไม่สมบูรณ์ | ขาดกระบวนการตรวจสอบข้อมูลที่นำออกจากระบบงานอย่างเป็นทางการเพื่อดูความถูกต้อง ความสมบูรณ์ | ๓ | ๒ | ๖ (ปานกลาง) | การยอมรับ (Take) |

| ความเสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| ๘.๓ ระบบถูกบุกรุกจากผู้ไม่ประสงค์ดี | ขาดมาตรการควบคุมบริหารจัดการช่องโหว่ทางเทคนิค อย่างเป็นทางการ | ๒ | ๓ | ๖ (ปานกลาง) | การยอมรับ (Take) |
| ๘.๔ การแก้ไขความผิดพลาดของระบบเนื่องจาก การเปลี่ยนแปลงระบบงาน หรือระบบปฏิบัติการทำได้ล่าช้า ไม่ทันต่อเหตุการณ์ | ขาดขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบอย่างเป็นลายลักษณ์อักษร | ๒ | ๓ | ๖ (ปานกลาง) | การยอมรับ (Take) |
| ๘.๕ ใช้ซอฟท์แวร์ละเมิดลิขสิทธิ์ และซอฟท์แวร์ที่ดาวโหลดมามีไวรัสทำให้ระบบเสียหาย | ขาดการควบคุมการติดตั้งซอฟท์แวร์โดยเจ้าหน้าที่สามารถติดตั้งซอฟท์แวร์ได้เอง | ๓ | ๒ | ๖ (ปานกลาง) | การยอมรับ (Take) |
| ๘.๖ ระบบเสียหาย และ แก้ไขกลับคืนได้ล่าช้า อันเนื่องมาจากการเปลี่ยนแปลงที่ไม่มีการควบคุมที่ดี | ขั้นตอนปฏิบัติสำหรับควบคุมเปลี่ยน แปลงหรือแก้ไขระบบ ทั้งHardwareและ Software เช่น การบันทึกการเปลี่ยนแปลง การทำสอบระบบก่อนเปลี่ยนแปลง | ๑ | ๕ | ๕ (ปานกลาง) | การยอมรับ (Take) |
| **๙.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)** | | | | | |
| ๙.๑ เหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุฉุกเฉินไม่ได้รับการจัดการภายในระยะเวลาที่เหมาะสมซึ่งทำให้เหตุการณ์เกิดการลุกลามหรือบานปลาย/เหตุการณ์**ความ** | ขาดขั้นตอนปฏิบัติสำหรับการรายงานเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัย | **๑** | ๔ | ๔ (ต่ำ) | การยอมรับ (Take) |

| เสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| ฉุกเฉินถูกละเลย โดยไม่มีการแจ้งเหตุเหล่านั้น | | | | | |
| ๙.๒ ระบบเสียหายกับเกิดเหตุการณ์เดิมๆที่เกิดขึ้นในด้านการละเมิดความมั่นคงปลอดภัย | ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย และต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันไว้ล่วงหน้า | ๑ | ๕ | ๕ (ปานกลาง) | การยอมรับ (Take) |
| **๑๐.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)** | | | | | |
| ๑๐.๑ การขาดความชัดเจนในกระบวนการสร้างความต่อเนื่องให้กับกระบวนการทางภารกิจขององค์กรที่สำคัญและระบบงานสนับสนุน/การขาดแผนการสร้างความต่อเนื่องทางธุรกิจสำหรับกระบวนการทางธุรกิจสำคัญบางกระบวนการ | นโยบายและวัตถุประสงค์เพื่อสร้างความต่อเนื่องให้กับกระบวนการทางภารกิจขององค์กรที่สำคัญ | ๑ | ๕ | ๕ (ปานกลาง) | การยอมรับ (Take) |
| ๑๐.๒ กระบวนการทางธุรกิจสำคัญและระบบงานสนับสนุนไม่ได้รับการกู้คืนหรือสร้างความต่อเนื่องภายในระยะเวลาที่เหมาะสมภายหลังจากที่เกิดเหตุภัยพิบัติ | - การระบุและจัดลำดับความสำคัญของกระบวนการทางธุรกิจสำคัญกล่าวคือกระบวนการทางธุรกิจใดก่อนหลังที่ต้องได้รับการกู้คืนให้สำเร็จเรียงตามลำดับความสำคัญ | ๑ | ๕ | ๕ (ปานกลาง) | การยอมรับ (Take) |

| ความเสี่ยง | ปัจจัยเสี่ยง | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยง(LxI) | การตอบสนองความเสี่ยง |
|---|---|---|---|---|---|
| ๑๐.๓ การไม่สามารถใช้แผนฯได้อย่างมีประสิทธิภาพและประสิทธิผลเนื่องจากยังไม่ได้แก้ไขจุดอ่อนต่างๆ ในแผนโดยผ่านกระบวนการทดสอบแผนอย่างสม่ำเสมอ | ขาดการทดสอบแผนสร้างความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอเช่น ปีละ ๑ ครั้ง | ๓ | ๔ | ๑๒ (สูง) | ควบคุม/ลด (Treat) |
| **๑๑. การปฏิบัติตามข้อกำหนด (Compliance)** | | | | | |
| ๑๑.๑ การละเมิดสิทธิและทรัพย์สินทางปัญญาของผู้อื่น | การใช้งานซอฟท์แวร์ละเมิดสิทธิ์ | ๑ | ๔ | ๔ (ต่ำ) | การยอมรับ (Take) |
| ๑๑.๒ การละเมิดกฎหมาย ระเบียบข้อบังคับ ข้อกำหนดในสัญญา และข้อกำหนดอื่นๆ ที่องค์กรต้องปฏิบัติตาม | การติดตามและระบุข้อมูลที่เกี่ยวข้องกับกฎหมาย ระเบียบข้อบังคับ ข้อกำหนดในสัญญา และข้อกำหนดอื่นๆ ที่องค์กรต้องปฏิบัติตาม เช่น พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นต้น | ๑ | ๕ | ๕ (ปานกลาง) | การยอมรับ (Take) |

# แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ ปีงบประมาณ ๒๕๕๕
## การตอบสนองต่อความเสี่ยง

ยุทธศาสตร์ : ส่งเสริมสนับสนุนการพัฒนาระบบเทคโนโลยีสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ
เป้าประสงค์ : เพื่อให้คุณภาพของข้อมูลสารสนเทศ มีสภาพพร้อมใช้งาน (Availability) ) ความครบถ้วนถูกต้อง (Integrity) การปฏิบัติตามกฎ(Compliance) เป็นที่ยอมรับและสร้างความมั่นใจให้ ผู้ขอรับบริการ
ตัวชี้วัด : ระดับความสำเร็จของการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
กิจกรรม/กระบวนงาน : การพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารทั่วไป

| ความเสี่ยง | ปัจจัยเสี่ยง | การตอบสนองความเสี่ยง | กิจกรรมในการตอบสนอง | ผู้รับผิดชอบ | งบประมาณ | กำหนดการ |
|---|---|---|---|---|---|---|
| **๑.นโยบายความมั่นคงปลอดภัย(Security policy)** | | | | | | |
| ๑.๑ การบริหารจัดการความมั่นคงปลอดภัยไม่สามารถทำได้อย่างมีประสิทธิภาพและประสิทธิผล ซึ่งอาจส่งผลให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยหลายๆ อย่าง | ขาดการทบทวนนโยบายด้านความมั่นคงปลอดภัย ให้ทันกับสถานะการและระบบที่เปลี่ยนแปลง | ควบคุม/ลด (Treat) | ทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ | กลุ่มพัฒนาระบบเครือข่ายฯ | - | เม.ย-พ.ค ๕๕ |

| ความเสี่ยง | ปัจจัยเสี่ยง | การตอบสนองความเสี่ยง | กิจกรรมในการตอบสนอง | ผู้รับผิดชอบ | งบประมาณ | กำหนดการ |
|---|---|---|---|---|---|---|
| **๒. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)** | | | | | | |
| ๒.๑ ระบบสารสนเทศไม่มีความมั่นคงปลอดภัย | ขาดการให้การสนับสนุน ต่อการจัดการทาง ด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน | ควบคุม/ลด (Treat | ประกาศนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ | กลุ่มพัฒนาระบบเครือข่าย | - | เม.ย-พ.ค ๕๕ |
| **๓. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)** | | | | | | |
| ๓.๑ การไม่สามารถบริหารจัดการความเสี่ยงด้านทรัพย์สินต่างๆ ได้ | ไม่มีการจัดทำป้ายชื่อและบัญชีทรัพย์สินสารสนเทศที่สำคัญขององค์กร | ควบคุม/ลด (Treat) | จัดทำทะเบียนหมวดหมู่ทรัพย์สินในห้องควบคุมคอมพิวเตอร์แม่ข่าย | กลุ่มพัฒนาระบบเครือข่ายฯ | - | **มี.ค-พ.ค ๕๕** |
| **๔.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร(Human resources security)** | | | | | | |
| ๔.๑ ข้อมูล ระบบ และเครื่องคอมพิวเตอร์ขององค์กรขาดความมั่นคงปลอดภัย | เจ้าหน้าที่ขาดการสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยอย่าง | ควบคุม/ลด (Treat | ทำการฝึกอบรมเจ้าหน้าที่ | กลุ่มพัฒนาโปรแกรมประยุกต์ฯ | - | **มี.ค-ส.ค ๕๕** |

| ความเสี่ยง | ปัจจัยเสี่ยง | การตอบสนองความเสี่ยง | กิจกรรมในการตอบสนอง | ผู้รับผิดชอบ | งบประมาณ | กำหนดการ |
|---|---|---|---|---|---|---|
| | สม่ำเสมอซึ่งทำให้เจ้าหน้าที่สามารถป้องกันตนเองได้ในระดับหนึ่ง | | | | | |
| ๔.๒ การเข้าถึงระบบโดยไม่ได้รับอนุญาตโดยใช้ User ID ของ**เจ้าหน้าที่**คนก่อน | ขาดการติดตามเรื่องการถอดถอนสิทธิของเจ้าหน้าที่ลาออกหรือย้ายหน่วยงาน | ควบคุม/ลด (Treat | ทำการทบทวน access right ผู้ใช้ในระบบต่างๆ | กลุ่มพัฒนาระบบเครือข่าย | - | มี.ค-ส.ค ๕๕ |
| **๕.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)** | | | | | | |
| ๕.๑ เครื่องเซิร์ฟเวอร์ไม่สามารถให้บริการได้เนื่องจากอุณหภูมิไม่เหมาะสม | เครื่องปรับอากาศภายในห้องระบบคอมพิวเตอร์แม่ข่ายโอนความเสี่ยง (Transfer)เป็นเครื่องเก่ามีอายุการใช้งานเกิน ๕ ปีขึ้นไป | โอนความเสี่ยง (Transfer) | - ทำการตรวจเช็คและบำรุงรักษาเครื่องปรับอากาศ<br>-หาเครื่องปรับอากาศใหม่ทดแทน | กลุ่มพัฒนาระบบเครือข่ายฯ | - | ต.ค-กย ๕๕ |

| ความเสี่ยง | ปัจจัยเสี่ยง | การตอบสนองความเสี่ยง | กิจกรรมในการตอบสนอง | ผู้รับผิดชอบ | งบประมาณ | กำหนดการ |
|---|---|---|---|---|---|---|
| **๖.การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร(Communications and Operating Management)** | | | | | | |
| ๖.๑ การป้องกันโปรแกรมไม่ประสงค์ดีไม่สามารถป้องกันตัวใหม่ๆได้ทั่วถึง | -ขาดการตรวจสอบข่าว หรือข้อมูลที่เกี่ยวข้องกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ<br>- เจ้าหน้าที่ไม่ได้ทำการตรวจสอบโปรแกรมไม่ประสงค์ดีในเครื่องที่ตนเองใช้งานอย่างสม่ำเสมอ | ควบคุม/ลด (Treat | - จัดเจ้าหน้าที่เฝ้าระวัง (monitoring) การใช้เครือข่ายของเจ้าหน้าที่<br>-ตรวจสอบ Traffic ที่วิ่งเข้าออก ระบบเครือข่ายกรมสนับสนุนบริการสุขภาพ | กลุ่มพัฒนาระบบเครือข่ายฯ | - | ต.ค-กย ๕๕ |
| ๖.๒ ข้อมูลไม่ได้รับการสำรองอย่างถูกวิธี | ขาดแผนการสำรองข้อมูลที่ครบถ้วน เช่น คู่มือวิธีการสำรองข้อมูล | ควบคุม/ลด (Treat | จัดทำคู่มือวิธีการสำรองข้อมูล | กลุ่มพัฒนาระบบเครือข่ายฯ | - | เม.ย-มิ.ย ๕๕ |

| ความเสี่ยง | ปัจจัยเสี่ยง | การตอบสนองความเสี่ยง | กิจกรรมในการตอบสนอง | ผู้รับผิดชอบ | งบประมาณ | กำหนดการ |
|---|---|---|---|---|---|---|
| **๗.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)** | | | | | | |
| ๗.๑ การไม่สามารถใช้แผนฯ ได้อย่างมีประสิทธิ ภาพและประสิทธิผลเนื่อง จากยังไม่ได้แก้ไขจุดอ่อนต่างๆ ในแผนโดยผ่านกระ บวนการทดสอบแผนอย่างสม่ำเสมอ | ขาดการทดสอบแผนสร้างความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอเช่น ปีละ ๑ ครั้ง | ควบคุม/ลด (Treat) | - ทดสอบ tape backup ข้อมูล<br>- ทดสอบระบบการป้องกันไฟไหม้ | กลุ่มพัฒนาระบบเครือข่ายฯ | - | **พ.ค-กย ๕๕** |

**รายงานผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ ปีงบประมาณ ๒๕๕๕**
**การตอบสนองต่อความเสี่ยง**

| ความเสี่ยง | ปัจจัยเสี่ยง | การตอบสนองความเสี่ยง | กิจกรรมในการตอบสนอง | ผลที่คาดว่าจะเกิดในปีงบประมาณ ๒๕๕๖ | | | | แนวทางแก้ไข |
|---|---|---|---|---|---|---|---|---|
| | | | | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยงที่ยังเหลืออยู่(LxI) | การตอบ สนองความเสี่ยง ในปีงบประมาณ ๒๕๕๖ | |
| **๑.นโยบายความมั่นคงปลอดภัย(Security policy)** | | | | | | | | |
| ๑.๑ การบริหารจัดการความมั่นคงปลอดภัยไม่สามารถทำได้อย่างมีประสิทธิภาพและประสิทธิผล ซึ่งอาจส่งผลให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยหลายๆ อย่าง | ขาดการทบทวนนโยบายด้านความมั่นคงปลอดภัย ให้ทันกับสถานะการและระบบที่เปลี่ยนแปลง | ควบคุม/ลด (Treat) | ทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ | ๑ | ๒ | ๒ | ยอมรับได้ | แจ้งนโยบายฯแจ้งให้กระทรวงICTทราบก่อนประกาศใช้ |
| **๒. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)** | | | | | | | | |
| ๒.๑ ระบบสารสนเทศไม่มีความมั่นคงปลอดภัย | ขาดการให้การสนับสนุนต่อจัดการทางด้านความมั่นคง | ควบคุม/ลด (Treat | ประกาศนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ | ๒ | ๑ | ๒ | ยอมรับได้ | ต้องแจ้งประกาศฯ ให้ กระทรวง ICTทราบ |

| ความเสี่ยง | ปัจจัยเสี่ยง | การตอบสนองความเสี่ยง | กิจกรรมในการตอบสนอง | ผลที่คาดว่าจะเกิดในปีงบประมาณ ๒๕๕๖ | | | | แนวทางแก้ไข |
|---|---|---|---|---|---|---|---|---|
| | | | | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยงที่ยังเหลืออยู่(LxI) | การตอบ สนองความเสี่ยง ในปีงบประมาณ ๒๕๕๖ | |
| | ปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน | | | | | | | ก่อนประกาศใช้ |
| **๓.การบริหารจัดการทรัพย์สินขององค์กร (Asset management)** | | | | | | | | |
| ๓.๑ การไม่สามารถบริหารจัดการความเสี่ยงด้านทรัพย์สินต่างๆ ได้ | ไม่มีการจัดทำป้ายชื่อและบัญชีทรัพย์สินสารสนเทศที่สำคัญขององค์กร | ควบคุม/ลด (Treat) | จัดทำทะเบียนหมวดหมู่ทรัพย์สินในห้องควบคุมคอมพิวเตอร์แม่ข่าย | ๒ | ๒ | ๔ | ยอมรับได้ | มีการทบทวนอุปกรณ์ในห้องควบคุมเครื่องแม่ข่ายทุกๆ ๖ เดือน |
| **๔.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร(Human resources security)** | | | | | | | | |
| ๔.๑ ข้อมูล ระบบ และเครื่องคอมพิวเตอร์ขององค์กรขาดความมั่นคงปลอดภัย | เจ้าหน้าที่ขาดความตะหนักด้านการรักษาความมั่นคงปลอดภัยอย่าง | ควบคุม/ลด (Treat | ทำการฝึกอบรมเจ้าหน้าที่ซึ่งทำให้เจ้าหน้าที่สามารถป้องกันตนเองได้ในระดับหนึ่ง | ๒ | ๒ | ๔ | ยอมรับได้ | ทำการอบรมเจ้าหน้าที่ที่ปฏิบัติงานด้านIT |

| ความเสี่ยง | ปัจจัยเสี่ยง | การตอบสนองความเสี่ยง | กิจกรรมในการตอบสนอง | ผลที่คาดว่าจะเกิดในปีงบประมาณ ๒๕๕๖ | | | | แนวทางแก้ไข |
|---|---|---|---|---|---|---|---|---|
| | | | | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยงที่ยังเหลืออยู่(LxI) | การตอบ สนองความเสี่ยง ในปีงบประมาณ ๒๕๕๖ | |
| ๔.๒ การเข้าถึงระบบโดยไม่ได้รับอนุญาตโดยใช้ User ID ของ**เจ้าหน้าที่**คนก่อน | ขาดการติดตามเรื่องการถอดถอนสิทธิของเจ้าหน้าที่ลาออกหรือย้ายหน่วยงาน | ควบคุม/ลด (Treat | ทำการทบทวน access right ผู้ใช้ในระบบต่างๆ | ๒ | ๒ | ๔ | ยอมรับได้ | หน่วยงานที่มีการปรับเปลี่ยนเจ้าหน้าที่ในการรับผิดชอบด้าน IT ของหน่วยงาน ซึ่งควรแจ้งให้สำนักเทคโนโลยีสารสนเทศและการสื่อสารทราบทุกครั้ง |
| **๕.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)** | | | | | | | | |
| ๕.๑ เครื่องเซิร์ฟเวอร์ไม่สามารถให้บริการได้เนื่องจากอุณหภูมิไม่เหมาะสม | เครื่องปรับอากาศภายในห้องระบบคอมพิวเตอร์แม่ข่ายเป็นเครื่องเก่ามีอายุการใช้งานเกิน ๕ ปีขึ้นไป | โอนความเสี่ยง (Transfer) | - ทำการตรวจเช็คและบำรุง รักษาเครื่องปรับอากาศ<br>-หาเครื่องปรับอากาศใหม่ทดแทน | ๒ | ๑ | ๒ | ถ่ายโอน | ขาดแคลนงบประมาณในการหาเครื่องเพิ่มเติมและทดแทนเครื่องเก่าที่มีอายุการใช้งานนาน |

| ความเสี่ยง | ปัจจัยเสี่ยง | การตอบสนองความเสี่ยง | กิจกรรมในการตอบสนอง | ผลที่คาดว่าจะเกิดในปีงบประมาณ ๒๕๕๖ | | | | แนวทางแก้ไข |
|---|---|---|---|---|---|---|---|---|
| | | | | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยงที่ยังเหลืออยู่(LxI) | การตอบ สนองความเสี่ยง ในปีงบประมาณ ๒๕๕๖ | |
| **๖.การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operating Management)** | | | | | | | | |
| ๖.๑ การป้องกันโปรแกรมไม่ประสงค์ดีไม่สามารถป้องกันตัวใหม่ๆได้ทั่วถึง | -ขาดการตรวจสอบข่าว หรือข้อมูลที่เกี่ยวข้องกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ<br>- เจ้าหน้าที่ไม่ได้ทำการตรวจสอบโปรแกรมไม่ประสงค์ดีในเครื่องที่ตนเองใช้งานอย่างสม่ำเสมอ | ควบคุม/ลด (Treat | - จัดเจ้าหน้าที่เฝ้าระวัง (monitoring) การใช้เครือ ข่ายของเจ้าหน้าที่<br>-ตรวจสอบ Traffic ที่วิ่งเข้า ออก ระบบเครือข่ายกรมสนับสนุนบริการสุขภาพ | ๓ | ๑ | ๓ | ยอมรับได้ | ต้องสร้างความเข้าใจกับเจ้าหน้าที่ในการเข้าใช้เว็บไซต์ที่ไม่ประสงค์ดี และเว็บไซต์ที่ไม่เหมาะสม |
| ๖.๒ ข้อมูลไม่ได้รับการสำรองอย่างถูกวิธี | ขาดแผนการสำรองข้อมูลที่ครบถ้วน เช่น คู่มือวิธีการสำรองข้อมูล | ควบคุม/ลด (Treat | จัดทำคู่มือวิธีการสำรองข้อมูล | ๑ | ๒ | ๒ | ยอมรับได้ | ควรจัดทำsiteสำรองในกรณีฉุกเฉิน |

| ความเสี่ยง | ปัจจัยเสี่ยง | การตอบสนองความเสี่ยง | กิจกรรมในการตอบสนอง | ผลที่คาดว่าจะเกิดในปีงบประมาณ ๒๕๕๖ | | | | แนวทางแก้ไข |
|---|---|---|---|---|---|---|---|---|
| | | | | โอกาส (L) | ผลกระทบ (I) | ระดับคะแนนความเสี่ยงที่ยังเหลืออยู่(LxI) | การตอบ สนองความเสี่ยง ในปีงบประมาณ ๒๕๕๖ | |
| **๗.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)** | | | | | | | | |
| ๗.๑ การไม่สามารถใช้แผนฯได้อย่างมีประสิทธิ ภาพและประสิทธิผลเนื่อง จากยังไม่ได้แก้ไขจุดอ่อนต่างๆในแผนโดยผ่านกระ บวนการทดสอบแผนอย่างสม่ำเสมอ | ขาดการทดสอบแผนสร้างความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอเช่น ปีละ ๑ ครั้ง | ควบคุม/ลด (Treat) | - ทดสอบ tape backup ข้อมูล<br>- ทดสอบระบบการป้องกันไฟไหม้ | ๑ | ๓ | ๓ | ยอมรับได้ | ควรทำการทดสอบภัยพิบัติฉุกเฉินในกรณีอื่นๆด้วย |
| | | | | | | | | |