



แผนการบริหารความเสี่ยงของระบบสารสนเทศ จังหวัดอ่างทอง
ประจำปี พ.ศ.๒๕๕๖

สำนักงานจังหวัดอ่างทอง
กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร
โทร ๐-๓๕๖๑-๔๙๑๒

แผนการบริหารความเสี่ยงของระบบสารสนเทศ จังหวัดอ่างทอง
ประจำปี พ.ศ. ๒๕๕๖

นิยาม ความเสี่ยงของระบบสารสนเทศ

คือ เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหายหรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบริหารงานของระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการบริหาร

นิยาม ระบบสารสนเทศ

คือ ระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การของไหลข้อมูลทั้งภายในและภายนอกองค์กร และการนำเสนอสารสนเทศ

องค์ประกอบของระบบคอมพิวเตอร์

๑. **Hardware** หมายถึง อุปกรณ์ต่าง ๆ ที่กระทำกับข้อมูล เอกสาร ทั้งที่เป็นอุปกรณ์คอมพิวเตอร์และไม่ใช้คอมพิวเตอร์
๒. **Software** หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน
๓. **บุคลากร** หมายถึง กลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศ คือ เป็นผู้นำจัดการข้อมูล และนำผลลัพธ์ออกจากระบบคอมพิวเตอร์
๔. **ข้อมูลและแฟ้มข้อมูล** หมายถึง ข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง
๕. **หน้าที่การปฏิบัติงาน** หมายถึง คำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

องค์ประกอบของระบบสารสนเทศ

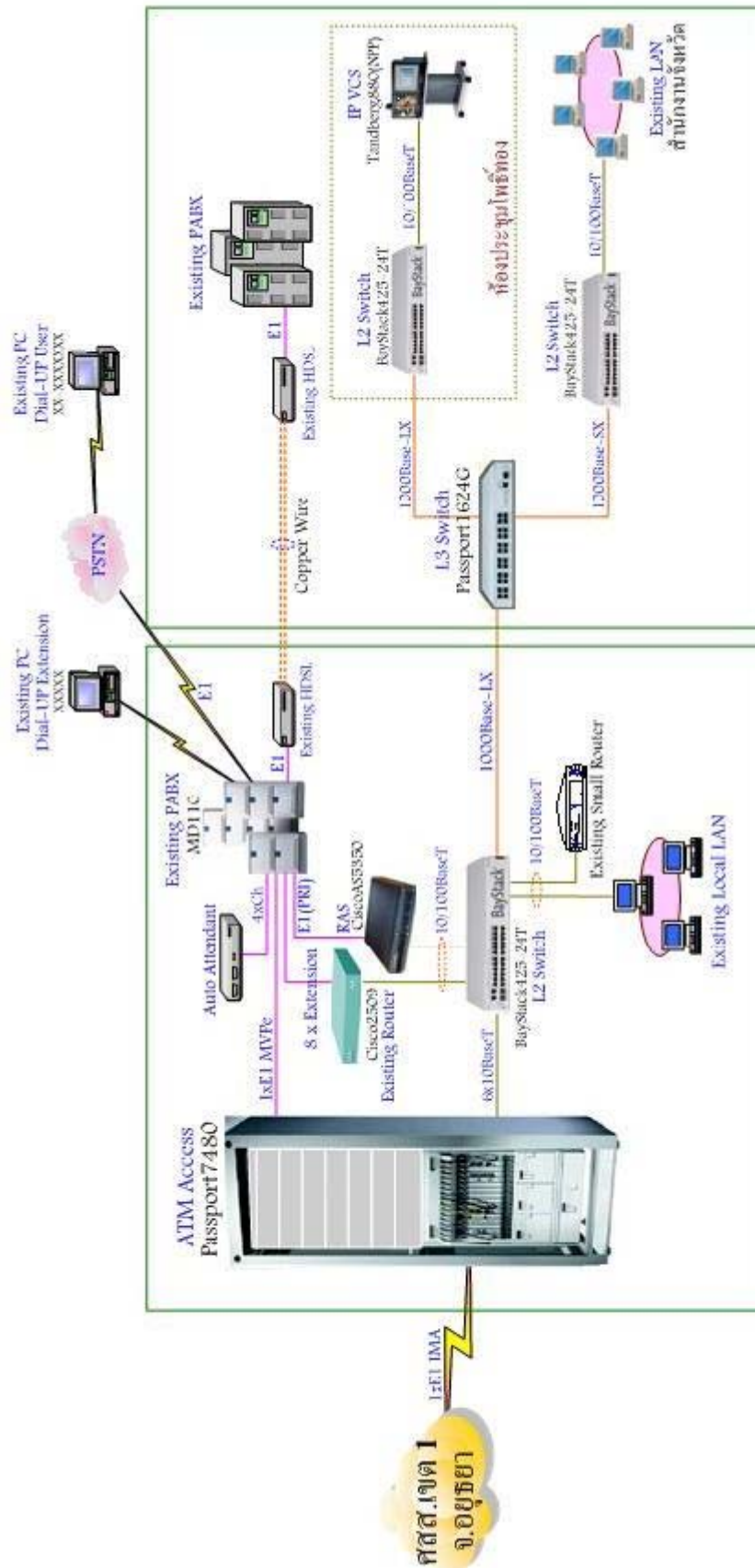
องค์กร โครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานขององค์กรโดยรวม ไม่ว่าจะเป็นฝ่ายต่าง ๆ ขององค์กร

บุคลากร บุคลากรที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน บุคลากรที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งต่อไปยังคอมพิวเตอร์

เทคโนโลยี อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศ เพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ

หมายเหตุ องค์ประกอบของระบบสารสนเทศที่ใช้ระบบคอมพิวเตอร์ในการบริหาร จึงประกอบด้วยองค์ประกอบของทั้งสองระบบรวมกัน

องค์ประกอบของระบบเครือข่าย



สถานีสื่อสารจังหวัดอ่างทอง

สถานีสื่อสารจังหวัดอ่างทอง

การบริหารความเสี่ยง (Risk Management)

เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วยการวางแผนความเสี่ยง การประเมินความเสี่ยงด้านต่างๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความเสี่ยงเพื่อหาว่าความเสี่ยงได้เปลี่ยนแปลงไปอย่างไร

การประเมินความเสี่ยง

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
๑	ความเสี่ยงด้าน Hardware		
	๑.๑ อุปกรณ์คอมพิวเตอร์เสียหาย	- หหมดอายุการใช้งาน - มีการใช้งานเกินประสิทธิภาพ - สภาวะแวดล้อมไม่ดี	ไม่สามารถทำงานต่อไปได้
	๑.๒ ระบบเครือข่ายไม่สามารถใช้งานได้	- อุปกรณ์เครือข่ายเสียหาย - ผู้ให้บริการเครือข่ายขัดข้อง	ไม่สามารถใช้บริการผ่านเครือข่ายได้
๒	ความเสี่ยงด้าน Software		
	๒.๑ Software ไม่สามารถทำงานได้	- ระบบปฏิบัติการเสียหาย - Software มีการทำงานผิดพลาด - Virus /Hacker /Spyware	- ไม่สามารถปฏิบัติงานได้ - ข้อมูลที่มีอยู่อาจเสียหายได้
๓	ความเสี่ยงด้านข้อมูล		
	๓.๑ ข้อมูลถูกทำลาย / สูญหาย	- Hardware เสีย - การปฏิบัติงานผิดพลาด - ผู้ไม่หวังดี - ไวรัสคอมพิวเตอร์	ไม่มีข้อมูลเพื่อนำไปใช้ในการบริหารงาน
	๓.๒ ข้อมูลผิดพลาด / ไม่ถูกต้อง	- เนื่องจากการปฏิบัติงานผิดพลาด - โปรแกรมทำงานผิดพลาด	- ไม่สามารถนำข้อมูลไปใช้เพื่อการตัดสินใจได้ - ข้อมูลไม่มีความน่าเชื่อถือ
	๓.๓ ข้อมูลไม่ครบ	- ผู้มีหน้าที่ไม่ทำตามขั้นตอนอย่างครบถ้วน	ข้อมูลไม่เพียงพอต่อการตัดสินใจบางอย่าง
	๓.๔ ความปลอดภัยของข้อมูล	- ขาดอุปกรณ์ป้องกันข้อมูลที่ดี - ขาดการตรวจสอบ - ขาดบุคลากรที่มีความรู้อย่างแท้จริง	- อาจทำให้ข้อมูลเสียหาย - ข้อมูลรั่วไหล

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
๔	ความเสี่ยงด้านบุคลากร		
	๔.๑ ขาดทักษะในการทำงาน	- ไม่เข้าใจระบบงานนั้น ๆ อย่างถึถ้วน	งานที่ได้ไม่มีประสิทธิภาพ เท่าที่ควร
	๔.๒ ทำงานในตำแหน่งที่ไม่เคยทำมาก่อน	- ทำงานที่ไม่ใช่หน้าที่หลักที่ รับผิดชอบของตน - ปรับเปลี่ยนตำแหน่ง	- งานอาจเกิดการผิดพลาด ได้
๕	ความเสี่ยงด้านหน้าที่การปฏิบัติ		
	๕.๑ ปฏิบัติหน้าที่ไม่ถูกต้อง	ไม่เข้าใจในขั้นตอนปฏิบัติงาน	- งานอาจผิดพลาดได้ - ขาดความน่าเชื่อถือ
	๕.๒ ละเลยการปฏิบัติ	ไม่เอาใจใส่ในงาน	งานไม่มีประสิทธิภาพ

แผนปฏิบัติที่ ๑

คำอธิบายความเสี่ยง อุปกรณ์คอมพิวเตอร์เสียหาย
เจ้าของความเสี่ยง เจ้าหน้าที่ดูแลระบบคอมพิวเตอร์
สาเหตุความเสี่ยง - เสื่อมสภาพหมดอายุการใช้งาน - มีการใช้งานนาน หรือเกินประสิทธิภาพ - สภาพแวดล้อมไม่ดี (กระแสไฟฟ้าไม่นิ่ง , อากาศร้อน , ฝุ่นละอองมาก)
ผลกระทบของความเสี่ยง - ทำให้การทำงานหยุดชะงัก ไม่สามารถทำงานต่อไปได้
แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง - เลือกอุปกรณ์ที่ดีและมีมาตรฐาน (มีประกันทุกชิ้นอย่างน้อย ๑ ปี) - เลือกบริการของผู้ขายที่มีเครื่องสำรองให้ใช้งาน - ทำการตรวจสอบและบำรุงอุปกรณ์อย่างสม่ำเสมอ - ทำตารางการตรวจสอบสถานะการมีตัวตน , ความสามารถในการใช้งานได้ , การทำความสะอาดอย่างน้อยสัปดาห์ละครั้ง - ทำการอบรมเจ้าหน้าที่ของแต่ละกลุ่ม / ฝ่าย ให้สามารถแก้ไขปัญหาเบื้องต้นได้ - ปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเลิกใช้งาน - ปิดเครื่องคอมพิวเตอร์ในช่วงพักกลางวัน และช่วงที่ออกไปทำธุระข้างนอก - ปิดหน้าจอทุกครั้งเมื่อหยุดการใช้งานชั่วคราว
ผู้รับผิดชอบ เจ้าหน้าที่คอมพิวเตอร์ / ผู้ใช้งาน / เจ้าหน้าที่ดูแลประจำเครื่องคอมพิวเตอร์

แผนปฏิบัติที่ ๒

คำอธิบายความเสี่ยง ระบบเครือข่ายคอมพิวเตอร์ไม่สามารถใช้งานได้
เจ้าของความเสี่ยง เจ้าหน้าที่ดูแลระบบเครือข่ายคอมพิวเตอร์
สาเหตุความเสี่ยง - อุปกรณ์เครือข่ายคอมพิวเตอร์ชำรุดเสียหาย - ระบบเครือข่ายของกระทรวงมหาดไทย หรือผู้ให้บริการเครือข่ายขัดข้อง - ปิดเพื่อปรับปรุงระบบชั่วคราว
ผลกระทบของความเสี่ยง - ทำให้การทำงานหยุดชะงัก - ไม่สามารถใช้บริการผ่านเครือข่ายได้
การบริหารจัดการความเสี่ยง - เลือกอุปกรณ์ที่ดีและมีมาตรฐาน (มีประกันทุกชิ้นอย่างน้อย ๑ ปี) - เลือกบริการของผู้ขายที่มีเครื่องสำรองให้ใช้งาน - ทำการตรวจสอบและบำรุงอุปกรณ์อย่างสม่ำเสมอ - ทำตารางการตรวจสอบสถานะการมีตัวตน , ความสามารถการใช้งานได้ , การทำความสะอาดอย่างน้อยสัปดาห์ละครั้ง - ทำการอบรมเจ้าหน้าที่ของแต่ละกลุ่ม / ฝ่าย ให้สามารถแก้ไขปัญหาเบื้องต้นได้
ผู้รับผิดชอบ เจ้าหน้าที่ดูแลระบบคอมพิวเตอร์

แผนปฏิบัติที่ ๓

คำอธิบายความเสี่ยง Software ไม่สามารถทำงานได้ (ทั้งระบบปฏิบัติการหรือโปรแกรมประยุกต์)
เจ้าของความเสี่ยง ผู้ใช้งานระบบสารสนเทศ , เจ้าของโปรแกรมประยุกต์ , เจ้าหน้าที่คอมพิวเตอร์
สาเหตุความเสี่ยง - ระบบปฏิบัติการเสียหาย - Software มีการทำงานผิดพลาด - Virus /Hacker / Spyware
ผลกระทบของความเสี่ยง - ทำให้การทำงานหยุดชะงัก - ไม่สามารถปฏิบัติงานได้ - ข้อมูลที่มีอยู่อาจเสียหายได้
การจัดการควบคุมความเสี่ยงในปัจจุบัน - มีระบบป้องกันไวรัสคอมพิวเตอร์ประจำเครื่อง - แต่ละหน่วยงานจะมีหน้าที่ดูแลคอมพิวเตอร์
การบริหารจัดการความเสี่ยง - ตรวจสอบการทำงานของระบบปฏิบัติการ /โปรแกรมประยุกต์อยู่เสมอว่าสามารถทำงานได้ปกติหรือไม่ - ติดตั้งและปรับปรุงระบบป้องกันไวรัสให้ทันสมัยอยู่เสมอ - ผู้ใช้งานทุกคนต้องสามารถตรวจสอบการทำงานของระบบป้องกันไวรัสได้ - ติดตั้งระบบไฟล်วอล เพื่อป้องกันไวรัสและสปายแวร์
ผู้รับผิดชอบ เจ้าหน้าที่ดูแลระบบคอมพิวเตอร์ /เจ้าของเครื่อง

แผนปฏิบัติที่ ๔

คำอธิบายความเสี่ยง ข้อมูลถูกทำลาย / สูญหาย
เจ้าของความเสี่ยง เจ้าของงานนั้น ๆ / เจ้าหน้าที่คอมพิวเตอร์
สาเหตุความเสี่ยง - Hardware เสีย - เนื่องจากการปฏิบัติงานผิดพลาด - ผู้ไม่หวังดี - ไวรัสคอมพิวเตอร์
ผลกระทบของความเสี่ยง - ทำให้การทำงานหยุดชะงัก - ต้องมีการทำงานซ้ำ ๆ เพื่อทำการกรอกข้อมูลซ้ำ ๆ เดิม - ไม่มีข้อมูลสารสนเทศเพื่อใช้ในการบริหารงาน
การจัดการควบคุมความเสี่ยงในปัจจุบัน - มีระบบป้องกันไวรัสของแต่ละเครื่อง
การบริหารจัดการความเสี่ยง - มีระบบการสำรองข้อมูลเป็นประจำทุกวัน - กำหนดรหัสผ่านของเครื่องคอมพิวเตอร์ โปรแกรมต่าง ๆ เพื่อไม่ให้ผู้ไม่หวังดีเข้าถึงข้อมูลนั้น ๆ พร้อมกับทำการเปลี่ยนรหัสอย่างน้อยทุกเดือน
ผู้รับผิดชอบ - เจ้าหน้าที่คอมพิวเตอร์ / เจ้าของข้อมูลนั้น ๆ - เจ้าหน้าที่คอมพิวเตอร์

แผนปฏิบัติที่ ๕

คำอธิบายความเสี่ยง ข้อมูลผิดพลาด / ไม่ถูกต้อง
เจ้าของความเสี่ยง เจ้าของงานนั้น ๆ / เจ้าหน้าที่คอมพิวเตอร์
สาเหตุความเสี่ยง - เนื่องจากการปฏิบัติงานผิดพลาด - โปรแกรมทำงานผิดพลาด
ผลกระทบของความเสี่ยง - ทำให้การทำงานหยุดชะงัก - ทำให้การทำงานอื่นเนื่องมาจากการใช้ข้อมูลนั้น ๆ ผิดพลาดในกรณีที่ไม่ทราบว่าข้อมูลนั้นไม่ถูกต้อง - ไม่มีข้อมูลสารสนเทศเพื่อใช้ในการบริหารงาน - ข้อมูลไม่มีความน่าเชื่อถือ - ไม่สามารถนำข้อมูลไปใช้เพื่อการตัดสินใจได้
การจัดการควบคุมความเสี่ยงในปัจจุบัน - มีการตรวจเช็คข้อมูลเป็นระยะ - มีการสำรองข้อมูลที่สำคัญเป็นประจำ
การบริหารจัดการความเสี่ยง - มีระบบการสำรองข้อมูลเป็นประจำทุกวัน และจัดทำแบบบันทึกการสำรองข้อมูล - กำหนดรหัสผ่านของเครื่องคอมพิวเตอร์ โปรแกรมต่าง ๆ เพื่อไม่ให้ผู้ไม่หวังดีเข้าถึงข้อมูลนั้น ๆ พร้อมกับทำการเปลี่ยนรหัสอย่างน้อยทุกเดือน - ตรวจสอบความถูกต้องของข้อมูลเสมออย่างน้อยอาทิตย์ละครั้ง
ผู้รับผิดชอบ - เจ้าหน้าที่คอมพิวเตอร์ / เจ้าของข้อมูลนั้น ๆ

แผนปฏิบัติที่ ๖

คำอธิบายความเสี่ยง ข้อมูลไม่ครบ
เจ้าของความเสี่ยง เจ้าของงานนั้น ๆ / เจ้าหน้าที่คอมพิวเตอร์
สาเหตุความเสี่ยง - ผู้มีหน้าที่ไม่ทำตามขั้นตอนอย่างครบถ้วน
ผลกระทบของความเสี่ยง - ทำให้การทำงานที่เป็นงานต่อเนื่องต้องหยุดชะงัก - ไม่มีข้อมูลสารสนเทศเพื่อใช้ในการบริหารงาน - ข้อมูลไม่เพียงพอต่อการตัดสินใจบางอย่าง
การจัดการควบคุมความเสี่ยงในปัจจุบัน - มีการกระตุ้นให้กรอกข้อมูลเป็นระยะ
การบริหารจัดการความเสี่ยง - หัวหน้างานต้องทำการตรวจสอบข้อมูลจากรายงานทุกอาทิตย์ - หัวหน้างานต้องคอยกระตุ้นให้มีการกรอกข้อมูลให้ครบ - ในแต่ละงานต้องมีผู้รับผิดชอบอย่างน้อย ๒ คน เพื่อตรวจสอบงานของกันและกันด้วย
ผู้รับผิดชอบ - หัวหน้างานนั้น ๆ / เจ้าของข้อมูลนั้น ๆ

แผนปฏิบัติที่ ๗

คำอธิบายความเสี่ยง ความปลอดภัยของข้อมูล
เจ้าของความเสี่ยง เจ้าของงานนั้น ๆ / เจ้าหน้าที่คอมพิวเตอร์
สาเหตุความเสี่ยง - ขาดอุปกรณ์ป้องกันที่ดีพอ - ขาดการตรวจสอบ - ขาดบุคลากรที่มีความรู้อย่างแท้จริง
ผลกระทบของความเสี่ยง - ทำให้การทำงานที่เป็นงานต่อเนื่องต้องหยุดชะงัก - ไม่มีข้อมูลสารสนเทศเพื่อใช้ในการบริหารงาน - อาจทำให้ข้อมูลเสียหาย - ข้อมูลรั่วไหล
การจัดการควบคุมความเสี่ยงในปัจจุบัน - มีการใช้รหัสผ่านกับข้อมูลที่มีความสำคัญ
การบริหารจัดการความเสี่ยง - ทำการอบรมและชี้แจงให้ทุกคนตระหนักถึงความปลอดภัยในการเข้าถึงข้อมูล - เมื่อไม่อยู่หน้าเครื่องต้องทำการล็อกการใช้งานเครื่องหรือปิดเครื่องทุกครั้ง - ต้องทำการเปลี่ยนรหัสผ่านทุกเดือน
ผู้รับผิดชอบ - เจ้าของข้อมูลนั้น ๆ / เจ้าหน้าที่คอมพิวเตอร์

แผนปฏิบัติที่ ๘

คำอธิบายความเสี่ยง ขาดทักษะในการทำงาน
เจ้าของความเสี่ยง เจ้าของเครื่อง , เจ้าของโปรแกรมประยุกต์ , เจ้าหน้าที่คอมพิวเตอร์
สาเหตุความเสี่ยง - ไม่เข้าใจระบบงานนั้น ๆ อย่างถ่องแท้ - พื้นฐานทางด้านคอมพิวเตอร์ยังไม่ดีพอ - โปรแกรมระบบสารสนเทศบางโปรแกรมมีรายละเอียดมากต้องใช้เวลาในการศึกษา - มีการโยกย้าย ปรับเปลี่ยนตำแหน่ง
ผลกระทบของความเสี่ยง - ทำให้การทำงานหยุดชะงัก - ข้อมูลสารสนเทศอาจผิดพลาดไปจากความเป็นจริงทำให้เสียหายต่อการตัดสินใจต่าง ๆ - งานที่ได้ไม่มีประสิทธิภาพเท่าที่ควร
การจัดการควบคุมความเสี่ยงในปัจจุบัน - ทำการอบรมการใช้งานโปรแกรมระบบสารสนเทศที่ปรับปรุง / จัดหาใหม่
การบริหารจัดการความเสี่ยง - ทำการอบรมเพื่อเพิ่มทักษะ ความรู้ ความสามารถ การทำงานของเจ้าหน้าที่ - ทำการติดตามประเมินผลความสามารถในการทำงานทุกปี - มีแนวทางปฏิบัติสำรองเมื่อมีความเสียหายเกิดขึ้น
ผู้รับผิดชอบ บุคลากรที่ได้รับมอบหมาย / หัวหน้างาน

แผนปฏิบัติที่ ๙

คำอธิบายความเสี่ยง ทำงานในตำแหน่งที่ไม่เคยทำมาก่อน
เจ้าของความเสี่ยง เจ้าของงานนั้น ๆ / เจ้าหน้าที่คอมพิวเตอร์
สาเหตุความเสี่ยง - เป็นเจ้าหน้าที่ใหม่ - ปรับเปลี่ยนตำแหน่ง - ทำงานที่ไม่ใช่หน้าที่หลักรับผิดชอบของตน
ผลกระทบของความเสี่ยง - ทำให้การทำงานหยุดชะงัก - ข้อมูลสารสนเทศต่างอาจผิดไปจากความเป็นจริงทำให้เสียหายต่อการตัดสินใจต่าง ๆ - งานอาจผิดพลาดได้
การจัดการควบคุมความเสี่ยงในปัจจุบัน - ทำการแนะนำก่อนเข้าทำงาน
การบริหารจัดการความเสี่ยง - ทำการอบรมทักษะการทำงานของพนักงานเพิ่มเติม - ทำการอบรมก่อนมีการเปลี่ยนตำแหน่งงานทุกครั้งอย่างน้อยต้องมีการปฐมนิเทศ - ทำการประเมินความสามารถในการทำงานทุกปี - มีแนวทางปฏิบัติสำรองเมื่อมีความเสียหายเกิดขึ้น - ห้ามมีการทำงานแทนกันเด็ดขาด และมีบทกำหนดลงโทษอย่างชัดเจนเมื่อมีเหตุการณ์เกิดขึ้น
ผู้รับผิดชอบ บุคลากรที่ได้รับมอบหมาย / หัวหน้างาน

แผนปฏิบัติที่ ๑๐

คำอธิบายความเสี่ยง ปฏิบัติหน้าที่ไม่ถูกต้อง
เจ้าของความเสี่ยง เจ้าของงานนั้น ๆ / เจ้าหน้าที่คอมพิวเตอร์
สาเหตุความเสี่ยง - ไม่เข้าใจในขั้นตอนปฏิบัติ
ผลกระทบของความเสี่ยง - งานอาจผิดพลาดได้ - ข้อมูลสารสนเทศขาดความน่าเชื่อถือ
การบริหารจัดการความเสี่ยง - จัดทำกรอบขั้นตอนการปฏิบัติงาน - จัดทำคู่มือการปฏิบัติงาน - ทำการตรวจสอบอย่างน้อยสัปดาห์ละครั้ง
ผู้รับผิดชอบ - เจ้าของงานนั้น ๆ

แผนปฏิบัติที่ ๑๑

คำอธิบายความเสี่ยง ละเลยการปฏิบัติหน้าที่
เจ้าของความเสี่ยง เจ้าของงานนั้น ๆ
สาเหตุความเสี่ยง - ไม่เอาใจใส่ในงาน - มีงานมากจนทำไม่ทัน
ผลกระทบของความเสี่ยง - งานไม่มีประสิทธิภาพ - ข้อมูลสารสนเทศไม่ครบถ้วน
การจัดการควบคุมความเสี่ยงในปัจจุบัน - ทำการตักเตือน
การบริหารจัดการความเสี่ยง - ออกมาตรการ ปฏิบัติต่อผู้กระทำผิดให้ชัดเจน
ผู้รับผิดชอบ หัวหน้างานนั้น ๆ

สรุปแนวทางการปฏิบัติเพื่อป้องกันความเสี่ยง

การบริหารความเสี่ยงของระบบสารสนเทศ เป็นหน้าที่ความรับผิดชอบของทุกคน และการปฏิบัติเพื่อป้องกันความเสี่ยงทุกคนต้องช่วยกันปฏิบัติ เพราะเมื่อคนใดคนหนึ่งละเลยการปฏิบัติหน้าที่นั้น อาจทำให้มีความเสี่ยงเกิดขึ้นกับระบบ ตนเองและผู้อื่น และอาจทำให้ผู้อื่นไม่สามารถป้องกันความเสี่ยงได้ เพราะฉะนั้นจำเป็นต้องสรุปภาพรวมของการปฏิบัติงานเพื่อป้องกันความเสี่ยง ดังนี้

๑. ด้าน Hardware

๑.๑ ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server)

- ไม่อนุญาตให้บุคคลภายนอกเข้า
- เลือกสถานที่ที่ยากต่อการเข้าถึง

๑.๒ ห้องปฏิบัติการ ไม่อนุญาตให้ผู้อื่นใช้เครื่องของตนเอง

๒. ด้าน Software

๒.๑ ซอฟต์แวร์ที่จัดซื้อต้องมีการรับประกันการใช้งาน หรือการบริการหลังการขายจากผู้ขายเป็นระยะเวลาอย่างน้อย ๑ ปี

๒.๒ ซอฟต์แวร์ที่จัดซื้อจะต้องมีการอบรมก่อนการใช้งานจริง

๒.๓ ติดตั้งระบบป้องกันไวรัสไว้ที่เครื่องคอมพิวเตอร์ทุกเครื่อง

๓. ด้านข้อมูล

๓.๑ ต้องมีระบบที่สามารถสำรองข้อมูลได้อย่างน้อยสัปดาห์ละ ๑ ครั้ง

๓.๒ ต้องมีการรักษาความปลอดภัยทุกข้อมูลที่มีความสำคัญ

๓.๓ จำกัดสิทธิการใช้งานของบุคคลที่มีสิทธิเท่านั้น

๓.๔ ข้อมูลที่สำคัญต้องมีการเข้ารหัสก่อนเข้าถึงข้อมูล

๓.๕ เมื่อมีความเสียหายเกิดขึ้นต้องทำการกู้ให้ระบบสามารถทำการได้อย่างเป็นปกติ อย่างช้าไม่เกิน ๑ วัน

๓.๖ เมื่อมีความสงสัยว่าข้อมูลนั้น ๆ ไม่มีความถูกต้อง ต้องสามารถตรวจสอบย้อนกลับได้ว่าข้อมูลนั้นถูกต้องหรือไม่เพียงใด

๔. ด้านบุคลากร

กำหนดให้มีผู้ดูแลระบบที่มีความสามารถต่าง ๆ ดังนี้

๔.๑ ผู้บริหารระบบ (System Administrator) มีความรู้ด้านฮาร์ดแวร์ ซอร์ฟแวร์ระบบ เป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ ดังนี้

๑. บริหารและดูแลอุปกรณ์คอมพิวเตอร์ซึ่งเป็นแม่ข่ายบริการแก่หน่วยงานต่าง ๆ ของส่วนราชการ

๒. ควบคุมและตรวจสอบการใช้งานระบบ

๓. ตรวจสอบ ควบคุม ดูแล การบำรุงรักษาระบบ

๔. รักษาความปลอดภัยระบบ เช่น รักษาความลับ ความคงสภาพและความพร้อมใช้งาน

๔.๒ ผู้จัดการฐานข้อมูล (Database Manager) มีความรู้ด้านการจัดการฐานข้อมูล ระบบคอมพิวเตอร์เป็นอย่างดี และรับมอบหมายให้ปฏิบัติหน้าที่ ดังนี้

๑. ควบคุมดูแลฐานข้อมูล เช่น การรวบรวม การเพิ่ม การเปลี่ยนแปลง การลบ การจัดโครงสร้าง การใช้งาน การเก็บ และการเรียกดู

๒. เลือกตัดตอน และกำหนดรูปแบบข้อมูลที่เก็บในแฟ้มข้อมูล

๓. รักษาความปลอดภัยฐานข้อมูล เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานของฐานข้อมูล

๔. ตรวจสอบฐานข้อมูล และวิเคราะห์ข้อมูล

๕. ควบคุม และบริการการใช้งานฐานข้อมูล

๔.๓ ผู้จัดการเครือข่าย (Network Manager) มีความรู้ด้านฮาร์ดแวร์การสื่อสารข้อมูล และอุปกรณ์ในระบบเครือข่ายเป็นอย่างดี และรับมอบหมายให้ปฏิบัติหน้าที่ ดังนี้

๑. กำหนดเลขที่อยู่ไอพี (IP Address) ให้คอมพิวเตอร์ในเครือข่ายของส่วนราชการ โดยประสานกับหน่วยงานอื่น ๆ

๒. กำหนดบัญชีผู้ใช้ (Account) และรหัสผ่าน (Password) ของผู้ใช้งานในเครือข่ายที่รับผิดชอบ

๓. ดูแลการใช้เครือข่ายคอมพิวเตอร์ภายในส่วนราชการ

๔. ดูแลโครงสร้างพื้นฐานและอุปกรณ์ที่เกี่ยวข้องกับระบบเครือข่าย เช่น โทรศัพท์ โมเด็ม ฮับ เป็นต้น

๕. รักษาความปลอดภัยของระบบเครือข่าย เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานในระบบเครือข่าย

๕. ความเสี่ยงด้านการปฏิบัติ

๕.๑ จัดทำคู่มือขั้นตอนการปฏิบัติงานทุกระบบสารสนเทศที่ใช้งาน

๕.๒ ทุกหน้าที่การปฏิบัติงานต้องมีผู้รับผิดชอบมากกว่า ๑ คน

๕.๓ หัวหน้างานต้องตรวจสอบ กระตุ้นให้ผู้ปฏิบัติทำงานตามหน้าที่อย่างเคร่งครัด
