บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ส่วนยุทธศาสตร์และมาตรฐานเทคโนโลยี โทร. ๒๖๒๕

ที่ ศทส. ๐๓๗๗/๒๕๖๕ **วันที่** ๒๔ พฤษภาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ข้อมูลความเสี่ยงด้านเทคโนโลยีดิจิทัล

เรียน ผู้อำนวยการสำนัก/กอง/กลุ่ม

ด้วยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีความประสงค์รวบรวมข้อมูลความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือเทคโนโลยีดิจิทัล รวม ๕ ด้าน สำหรับกรณีที่หน่วยงานของท่านมีระบบงานที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลในปัจจุบัน หรือกำลังจะมีใน ๑-๒ ปีนี้ เพื่อจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของกรมชลประทาน ประจำปี พ.ศ. ๒๕๖๖ – ๒๕๖๘ ต่อไป ดังข้อมูลหรือเอกสาร qr code ที่แนบมาพร้อมนี้

ทั้งนี้ ขอความกรุณากรอกข้อมูลพร้อมส่งเอกสารกลับภายในวันที่ ๓๐ มิถุนายน ๒๕๖๕

จึงเรียนมาเพื่อโปรดพิจารณา

(นายนรเศรษฐ ส่องทอง)
ผอ.ทส.

(นายธเนศร์ สมบูรณ์)
ผส.บอ.

ตัวอย่าง/ฟอร์มกรอกข้อมูล แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล ประจำปี พ.ศ. ๒๕๖๖ - ๒๕๖๘
http://ictstrategy.rid.go.th/files/risk/doc/request-risk-data.docx

ตัวอย่าง แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปี งบประมาณ พ.ศ. ๒๕๖๓ – ๒๕๖๕
http://ictstrategy.rid.go.th/files/risk/doc/Risk-2562.pdf

ตัวอย่าง / ร่าง

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล
ประจำปี พ.ศ.๒๕๖๖ - ๒๕๖๘

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมชลประทาน กระทรวงเกษตรและสหกรณ์

คำนำ

เพื่อเป็นมาตรการตามมาตรฐานเบื้องต้นในการรักษาความปลอดภัยของระบบสารสนเทศ จากภัยคุกคามอันเกิดจากปัจจัยภายในและปัจจัยภายนอกที่จะทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมชลประทาน จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศประจำปี พ.ศ. ๒๕๖๖ - ๒๕๖๘เพื่อเป็นแนวทางปฏิบัติงานในการป้องกันภัยคุกคามที่อาจเกิดขึ้นซึ่งจะส่งผลกระทบต่อประสิทธิภาพการให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมชลประทาน

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารประจำปี พ.ศ.๒๕๖๖ - ๒๕๖๘กรมชลประทานฉบับนี้ประกอบด้วยความเสี่ยง ๕ ด้าน คือ ด้านกายภาพและสิ่งแวดล้อม ด้านบุคลากร ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร ด้านโปรแกรมคอมพิวเตอร์ และด้านระบบข้อมูลทั้งนี้เพื่อให้การดำเนินงานตามมาตรฐานอย่างเป็นระบบ มีการบริหารจัดการเพื่อลดหรือขจัดความเสี่ยง สามารถกำหนดแผนปฏิบัติและพัฒนาทักษะความรู้บุคลากรผู้ปฏิบัติงานด้วยเทคโนโลยีสารสนเทศและการสื่อสารได้ถูกต้องและมีประสิทธิภาพ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมชลประทาน

สารบัญ

บทที่๑
บทนำ

๑.๑ภารกิจ

จากกฎกระทรวงแบ่งส่วนราชการกรมชลประทาน กระทรวงเกษตรและสหกรณ์ พ.ศ. ๒๕๕๗ให้กรมชลประทานมีภารกิจเกี่ยวกับการพัฒนาแหล่งน้ำตามศักยภาพของลุ่มน้ำให้เพียงพอและจัดสรรน้ำให้กับผู้ใช้น้ำทุกประเภทเพื่อให้ผู้ใช้น้ำได้รับน้ำอย่างทั่วถึงและเป็นธรรมตลอดจนป้องกันความเสียหายอันเกิดจากน้ำโดยให้มีอำนาจหน้าที่ดังต่อไปนี้

๑. ดำเนินการจัดให้ได้มาซึ่งน้ำหรือกักเก็บรักษาควบคุมส่งระบายหรือจัดสรรน้ำเพื่อการเกษตรการพลังงานการสาธารณูปโภคหรือการอุตสาหกรรมตามกฎหมายว่าด้วยการชลประทานกฎหมายว่าด้วยคันและคูน้ำและกฎหมายอื่นที่เกี่ยวข้อง

๒. ดำเนินการเกี่ยวกับการป้องกันความเสียหายอันเกิดจากน้ำความปลอดภัยของเขื่อนและอาคารประกอบและการคมนาคมทางน้ำที่อยู่ในเขตชลประทานตลอดจนดำเนินการเกี่ยวกับกิจกรรมพิเศษต่างๆที่ไม่ได้เป็นแผนงานประจำปีของกรม

๓. ดำเนินการจัดรูปที่ดินเพื่อเกษตรกรรมตามกฎหมายว่าด้วยการจัดรูปที่ดินเพื่อเกษตรกรรม

๔. ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกรมหรือตามที่รัฐมนตรีหรือคณะรัฐมนตรีมอบหมาย

๑.๒ แผนปฏิบัติการดิจิทัลกรมชลประทาน ปี พ.ศ. ๒๕๖๔ – ๒๕๖๘

ด้วยกรมชลประทานได้เล็งเห็นความสำคัญของการใช้เทคโนโลยีสารสนเทศในการขับเคลื่อนนโยบายด้านต่าง ๆ รองรับภารกิจของกรมชลประทานและนโยบายของประเทศ จึงได้มีการจัดทำแผนปฏิบัติการดิจิทัล กรมชลประทาน ปีพ.ศ. ๒๕๖๔ – ๒๕๖๘ ขึ้น โดยใช้หลักการของการพัฒนาสถาปัตยกรรมองค์กรที่ประกอบไปด้วยขั้นตอนที่สำคัญ ได้แก่

๑. การสร้างองค์ความรู้ในด้านการพัฒนาสถาปัตยกรรมองค์กรแก่บุคลากรและเจ้าหน้าที่ ที่เกี่ยวข้องทุกระดับภายในกรมชลประทาน

๒. การศึกษา วิเคราะห์สถานภาพของสถาปัตยกรรมองค์กรที่มีอยู่ในปัจจุบัน กรมชลประทานที่ครอบคลุมในด้านการดำเนินงานขององค์กร การใช้ข้อมูลและการแลกเปลี่ยนข้อมูล ระบบสารสนเทศ ระบบโครงสร้างพื้นฐาน และการรักษาความมั่นคงปลอดภัยสารสนเทศ

๓. การออกแบบสถาปัตยกรรมองค์กรเป้าหมาย กรมชลประทาน ที่ครอบคลุมในด้านต่าง ๆได้แก่ การออกแบบระบบงานและกระบวนการสำคัญขององค์กร ข้อมูลสารสนเทศหลัก ระบบสารสนเทศที่ต้องการ ระบบโครงสร้างพื้นฐาน และการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

๔. การประเมินช่องว่างระหว่างสถาปัตยกรรมองค์กรเป้าหมายกับสถาปัตยกรรมองค์กรที่มีอยู่ในปัจจุบันโดยผลการประเมินช่องว่างดังกล่าวได้ถูกนำไปกำหนดเป็นประเด็นสำคัญในการออกแบบยุทธศาสตร์การพัฒนาเทคโนโลยีดิจิทัล

๕. การจัดทำแผนพัฒนาเทคโนโลยีดิจิทัลเพื่อปิดช่องว่างจากผลการประเมินโดยแปลงเป็นแผนปฏิบัติการตามรายยุทธศาสตร์ในระยะเวลา ๕ ปี พ.ศ. ๒๕๖๔ – ๒๕๖๘ จากการดำเนินการตามขั้นตอนข้างต้น กรมชลประทานจึงได้กำหนดวิสัยทัศน์ พันธกิจ และยุทธศาสตร์การพัฒนาเทคโนโลยีดิจิทัล แผนงาน และตัวชี้วัดสำคัญ ดังนี้

๑) วิสัยทัศน์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

"ประยุกต์ใช้เทคโนโลยีดิจิทัลในการเปลี่ยนถ่ายองค์กรสู่องค์กรอัจฉริยะเพื่อบริการที่ทันสมัย มั่นคง ปลอดภัย ตามแนวทางมาตรฐานสากล"

๒) พันธกิจ ด้านเทคโนโลยีดิจิทัล

๑) สร้างกลไกการบริหารจัดการเทคโนโลยีดิจิทัลของกรมชลประทานอย่างมีธรรมาภิบาล ตามแนวทางมาตรฐานสากล

๒) บริหารจัดการโครงสร้างพื้นฐานดิจิทัลให้เพียงพอ ทันสมัย และมีประสิทธิภาพ

๓) พัฒนาและเพิ่มประสิทธิภาพระบบสารสนเทศ และระบบฐานข้อมูลที่สามารถสนับสนุนภารกิจขององค์กรได้อย่างถูกต้อง และรวดเร็ว

๔) เป็นศูนย์กลางการจัดเก็บข้อมูลสารสนเทศด้านน้ำของกรมชลประทานที่เป็นมาตรฐานแบบบูรณาการ และสามารถใช้ข้อมูลร่วมกันได้ทั้งองค์กรอย่างยั่งยืน

๕) เพิ่มประสิทธิภาพระบบสารสนเทศและการบริการข้อมูลที่ถูกต้อง รวดเร็ว แก่ประชาชนและหน่วยงานที่เกี่ยวข้องผ่านช่องทางต่าง ๆ ที่หลากหลายแผนปฏิบัติการดิจิทัล กรมชลประทาน ปี พ.ศ. ๒๕๖๔ – ๒๕๖๘) พัฒนาบุคลากรทุกระดับ ให้มีขีดสมรรถนะและทักษะด้านเทคโนโลยีดิจิทัลที่เหมาะสมกับการปฏิบัติงาน

๓) ยุทธศาสตร์ ด้านเทคโนโลยีดิจิทัล

<u>ประเด็นยุทธศาสตร์ที่ ๑</u>การยกระดับการจัดการทรัพยากรและข้อมูลสารสนเทศที่มีประสิทธิภาพตามแนวทางสากล

เป้าประสงค์	แผนงาน	ตัวชี้วัด
๑. มีการบริหารทรัพยากรดิจิทัลที่มีประสิทธิภาพ ๒. มีการบริหารและการกำกับดูแลข้อมูลสารสนเทศสอดคล้องตามมาตรฐาน ๓. มีกระบวนการในการบริหารคุณภาพการบริการเทคโนโลยีดิจิทัล	๑.๑ การบริหารและการกำกับดูแลข้อมูลหลักองค์กร	๑. มีการประกาศใช้นโยบายและโครงสร้างการบริหารและการกำกับดูแลข้อมูลองค์กรอย่างเป็นทางการ ๒. มีการจัดการข้อมูลหลักองค์กรและข้อมูลองค์กรมีความเป็นเอกภาพบนฐานข้อมูลองค์กรเดียวกัน
	๑.๒ การพัฒนากระบวนการบริหารเทคโนโลยีดิจิทัลตามมาตรฐานสากล	กรมชลประทานมีกระบวนการในการบริหารคุณภาพบริการเทคโนโลยีตามมาตรฐานสากล

ประเด็นยุทธศาสตร์ที่ ๒ การพัฒนาเทคโนโลยีดิจิทัลเพื่อสนับสนุนงานปฏิบัติการหลักองค์กร

เป้าประสงค์	แผนงาน	ตัวชี้วัด
๑. มีการนำเทคโนโลยีดิจิทัลไปปรับใช้ในงานปฏิบัติการเพื่อเพิ่มประสิทธิภาพ ๒. มีการพัฒนาเทคโนโลยีและนวัตกรรมเทคโนโลยีดิจิทัลกับกระบวนการปฏิบัติการหลัก	๒.๑ การพัฒนาเทคโนโลยีตามภารกิจหลักองค์กร	๑. ความสำเร็จตามแผนงาน ๒. ประสิทธิภาพในการทำงานที่เพิ่มขึ้นจากการนำเทคโนโลยีดิจิทัลไปปรับใช้
	๒.๒ การใช้เทคโนโลยีดิจิทัลที่เป็นมิตรกับสิ่งแวดล้อมและสร้างความยั่งยืน	๑. จำนวนระบบเทคโนโลยีดิจิทัลที่นำมาใช้งานและเป็นมิตรกับสิ่งแวดล้อม ๒. ปริมาณการใช้พลังงานไฟฟ้าที่ลดน้อยลงจากการนำเทคโนโลยีที่เป็นมิตรกับสิ่งแวดล้อมมาปรับใช้งาน

ประเด็นยุทธศาสตร์ที่ ๓ การปรับเปลี่ยนบริการสู่บริการ Platform ดิจิทัล

เป้าประสงค์	แผนงาน	ตัวชี้วัด
๑. มีการพัฒนา Platform เพื่อบริการแก่ผู้มีส่วนได้ส่วนเสียและภาคประชาชน ๒. มีการบูรณาการระบบงานภายในองค์กรเพื่อลดความซ้ำซ้อน	๓.๑ การพัฒนาบริการแก่ผู้มีส่วนได้ส่วนเสียด้วย Platform ดิจิทัล	๑. จำนวน Platform ที่พัฒนาขึ้นเพื่อให้บริการแก่ภาคประชาชน ๒. ระดับความพึงพอใจของผู้รับบริการ
	๓.๒ การพัฒนาระบบงานรองรับการดำเนินงานภายในองค์กร	๑. ความสำเร็จตามแผน ๒. ระดับความพึงพอใจของผู้ใช้บริการ

ประเด็นยุทธศาสตร์ที่ ๔การปรับปรุงระบบโครงสร้างพื้นฐานที่มีประสิทธิภาพและความมั่นคงปลอดภัย

เป้าประสงค์	แผนงาน	ตัวชี้วัด
๑. มีระบบโครงสร้างพื้นฐานที่เหมาะสม เพียงพอและมีประสิทธิภาพในการบริการ ๒. มีการจัดการด้านความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพและสอดคล้องตามมาตรฐานสากล	๔.๑ การปรับปรุงระบบโครงสร้างพื้นฐาน	ประสิทธิภาพของระบบโครงสร้างพื้นฐานและความพร้อมใช้งานของระบบ
	๔.๒ การจัดการความมั่นคงปลอดภัยระบบเครือข่ายและสารสนเทศ	จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่ลดน้อยลง

<u>ประเด็นยุทธศาสตร์ที่ ๕</u>ยกระดับทักษะบุคลากรสู่บุคลากรสายพันธุ์ดิจิทัล

เป้าประสงค์	แผนงาน	ตัวชี้วัด
บุคลากรกรมชลประทานมีทักษะด้านเทคโนโลยีดิจิทัลที่สอดคล้องตามมาตรฐานอาชีพ	การพัฒนาทักษะบุคลากรด้านเทคโนโลยีดิจิทัล	จำนวนบุคลากรกรมชลประทานที่ผ่านการประเมินคุณวุฒิวิชาชีพด้านเทคโนโลยีดิจิทัลจากสำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สคช.)

บทที่๒
ความเป็นมา และความสำคัญของการบริหารความเสี่ยง

๒.๑ ความเป็นมา

ระบบข้อมูลสารสนเทศมีความสำคัญยิ่งต่อการดำเนินงานของกรมชลประทานจึงต้องมีมาตรการระบบรักษาความปลอดภัยของระบบข้อมูลสารสนเทศเพื่อป้องกันภัยคุกคามอันเกิดจากปัจจัยภายในและปัจจัยภายนอกที่จะทำให้เกิดความเสียหายต่อระบบเทคโนโลยีดิจิทัล ซึ่งจะมีผลต่อประสิทธิภาพการดำเนินงานของกรมชลประทาน

๒.๒ หลักการและเหตุผล

กรมชลประทานได้นำเทคโนโลยีดิจิทัลมาใช้งานเพื่อช่วยเพิ่มประสิทธิภาพการดำเนินงานภายในองค์กรให้ได้รับความสะดวกรวดเร็วขณะเดียวกันระบบเทคโนโลยีดิจิทัลอาจได้รับความเสียหายจากการถูกโจมตีไวรัสคอมพิวเตอร์บุคลากรปัญหาไฟฟ้าขัดข้องอัคคีภัยซึ่งส่งผลกระทบต่อการดำเนินงานของกรมชลประทานดังนั้นเพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมชลประทาน มีความมั่นคงและปลอดภัยจึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลและปฏิบัติงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลรวมทั้งมีการทบทวนและปรับปรุงนโยบายและแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลให้เป็นปัจจุบันอยู่เสมอ

๒.๓ วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลสารสนเทศให้มีเสถียรภาพและพร้อมใช้งาน

๒. เพื่อให้ระบบเทคโนโลยีดิจิทัลดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๓. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีดิจิทัล

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีดิจิทัล

๒.๔ ผลที่คาดว่าจะได้รับ

๑. สามารถลดความเสี่ยงทางด้านระบบเทคโนโลยีดิจิทัลได้

๒. บุคลากรมีความรู้ความเข้าใจระบบรักษาความปลอดภัยด้านเทคโนโลยีดิจิทัลมากขึ้น

บทที่ ๓
กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล

๓.๑ นิยามความเสี่ยง

ความเสี่ยง หมายถึงเหตุการณ์หรือการกระทำใดๆ ที่อาจเกิดขึ้นในสถานการณ์ที่ไม่แน่นอน และอาจส่งผลกระทบสร้างความเสียหาย หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมายและวัตถุประสงค์ขององค์กร

ระบบบริหารความเสี่ยง หมายถึง ระบบการบริหารปัจจัยและการควบคุมกิจกรรมการดำเนินงานต่างๆ โดยลดมูลเหตุของโอกาสที่องค์กรจะเกิดความเสียหาย เพื่อให้ระดับความเสียหายที่อาจเกิดขึ้นอยู่ในระดับที่สามารถควบคุมและยอมรับได้

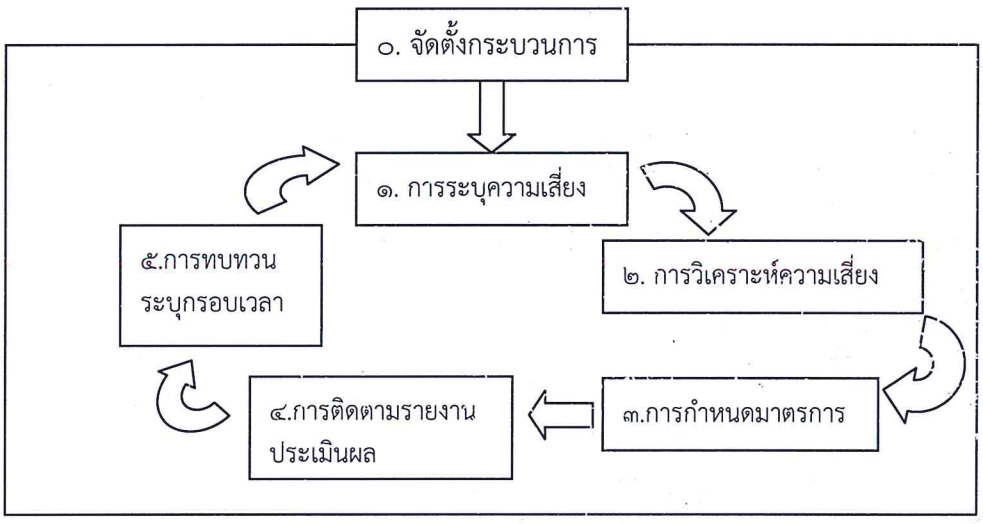
ปัจจัยเสี่ยง หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่สามารถบรรลุเป้าประสงค์ที่กำหนดไว้

๓.๒กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยงเป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดลำดับความเสี่ยงที่มีผลต่อการดำเนินงานของหน่วยงานการบริหารความเสี่ยงอย่างมีประสิทธิภาพต้องมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้

๑. การระบุความเสี่ยงหรือปัจจัยเสี่ยง
๒. การวิเคราะห์และประเมินความเสี่ยง
๓. การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม
๔. การติดตาม รายงานผลการดำเนินการตามมาตรการจัดการความสี่ยงที่ได้กำหนดไว้
๕. การทบทวนการบริหารความเสี่ยงโดยการระบุกรอบเวลาในการทบทวนอย่างชัดเจน

กระบวนการของการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมชลประทาน มีขั้นตอนของกระบวนการ ดังรูป



รูปที่ ๓-๑ กระบวนการของการบริหารความเสี่ยง

เริ่มต้นโดยการจัดตั้งกระบวนการ เพื่อให้การปฏิบัติงานการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลเป็นไปอย่างมีประสิทธิภาพและบรรลุตามวัตถุประสงค์ โดยมีคำสั่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารที่ .....รอเสนอแต่งตั้งใหม่..... เรื่องแต่งตั้งคณะทำงานจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล โดยมีหน้าที่ความรับผิดชอบ ดังนี้

๑. ศึกษา วิเคราะห์ ระบุความเสี่ยงด้านเทคโนโลยีดิจิทัล

๒. จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยียีดิจิทัล

๓. ติดตาม ประเมินผล การจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล

๓.๒.๑ การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

๑. การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

๒. การใช้ Checklist

๓. การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

๔. การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

๕. การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๓.๒.๒ การวิเคราะห์และประเมินความเสี่ยง

เป็นการประเมินถึงผลกระทบของความเสี่ยงและโอกาสที่จะเกิดความเสี่ยง โดยการให้คะแนนความน่าจะเป็น และหามาตรการในการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้หรือต่ำลงน้อยลง ประกอบด้วย ๔ ขั้นตอน

๑.การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๒.การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยงซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้นก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

โดยมีเกณฑ์การพิจารณาให้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีผลกระทบจากการเกิดความเสี่ยงต่อการปฏิบัติงานที่หน่วยงานได้ ดังนี้

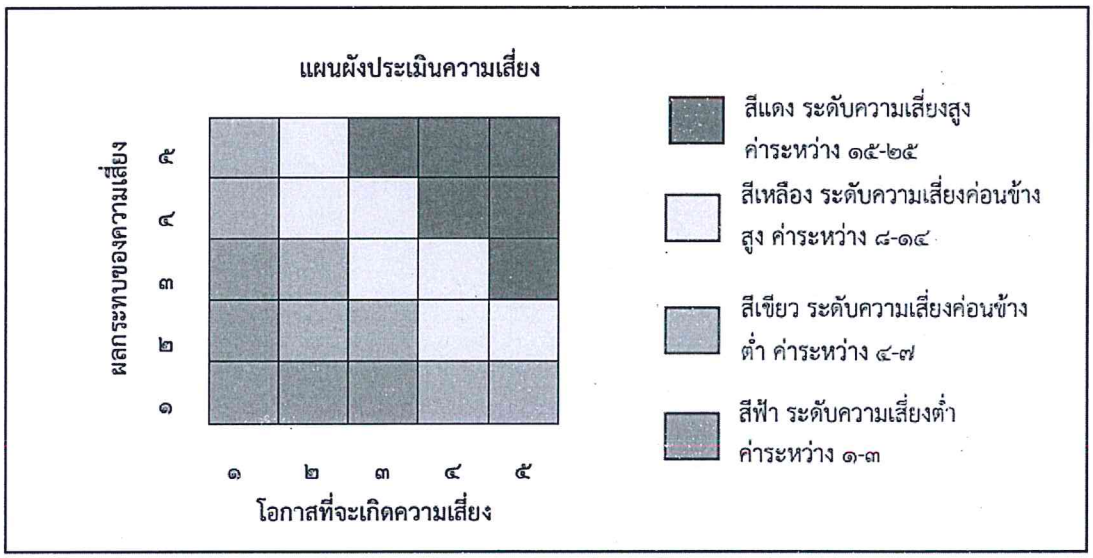
เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง (Likelihood)

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
๕	สูงมาก	เกิดขึ้นทุกวัน
๔	สูง	เกิดขึ้นทุกสัปดาห์
๓	ปานกลาง	เกิดขึ้นทุกเดือน
๒	น้อย	เกิดขึ้นทุกไตรมาส
๑	น้อยมาก	นานๆ เกิดที (ปีละ ๑ ครั้ง)

เกณฑ์การประเมิน ผลกระทบ (Impact)

ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบ ความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

๓.การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังรูปที่ ๒



รูปที่ ๓-๒แสดงแผนผังประเมินความเสี่ยง

๔. การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณาการกำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๓.๓.๓. การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุม ผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

๓.๓.๓.๑ ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

๓.๓.๓.๒ การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

๓.๓.๓.๓ การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๓.๓.๓.๔การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

๑) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมีเพื่อป้องกัน ความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

๒) พิจารณาหรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

๓) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

๓.๓.๔. การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติเพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรม ที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอและนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

๓.๓.๔.๑ พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๓.๓.๔.๒ เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๓.๓.๔.๓ กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๓.๓.๔.๔ ในรอบปีต่อไปให้พิจารณาผลการติดตามการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมิน และบริหารจัดการความเสี่ยงว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหาร เพื่อทราบและสั่งการ

๓.๓.๕.การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

๓.๓ ความเสี่ยงด้านเทคโนโลยีดิจิทัล

กรมชลประทาน ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยียีดิจิทัลตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้ เป็น ๕ ประเภท ดังนี้

๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่ มีประสิทธิภาพเพียงพอ

๒. ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดเพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

๓.ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายในและมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือ จากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งทางกรมชลประทานอาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

๕.ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูลเพื่อการโจรกรรมข้อมูลที่สำคัญการลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความ เสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรงรวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยีและการสื่อสาร

๓.๔ การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

การหลีกเลี่ยง (Terminate)เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือการเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น

การยอมรับ (Take)เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat)เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์ เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

๓.๕ ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของกรมชลประทาน ได้แก่

๓.๕.๑ ปัจจัยภายนอก ได้แก่

๑. ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

๒. การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓. การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

๔. ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

๕. ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๖. การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๓.๕.๒ ปัจจัยภายใน ได้แก่

๑. ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒. การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร

๓. เจ้าหน้าที่หรือบุคลการของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร เสียหายใช้งานไม่ได้ หรือหยุดการทำงาน

๓.๖การประเมินความเสียหาย

๓.๖.๑ ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๓.๖.๒ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

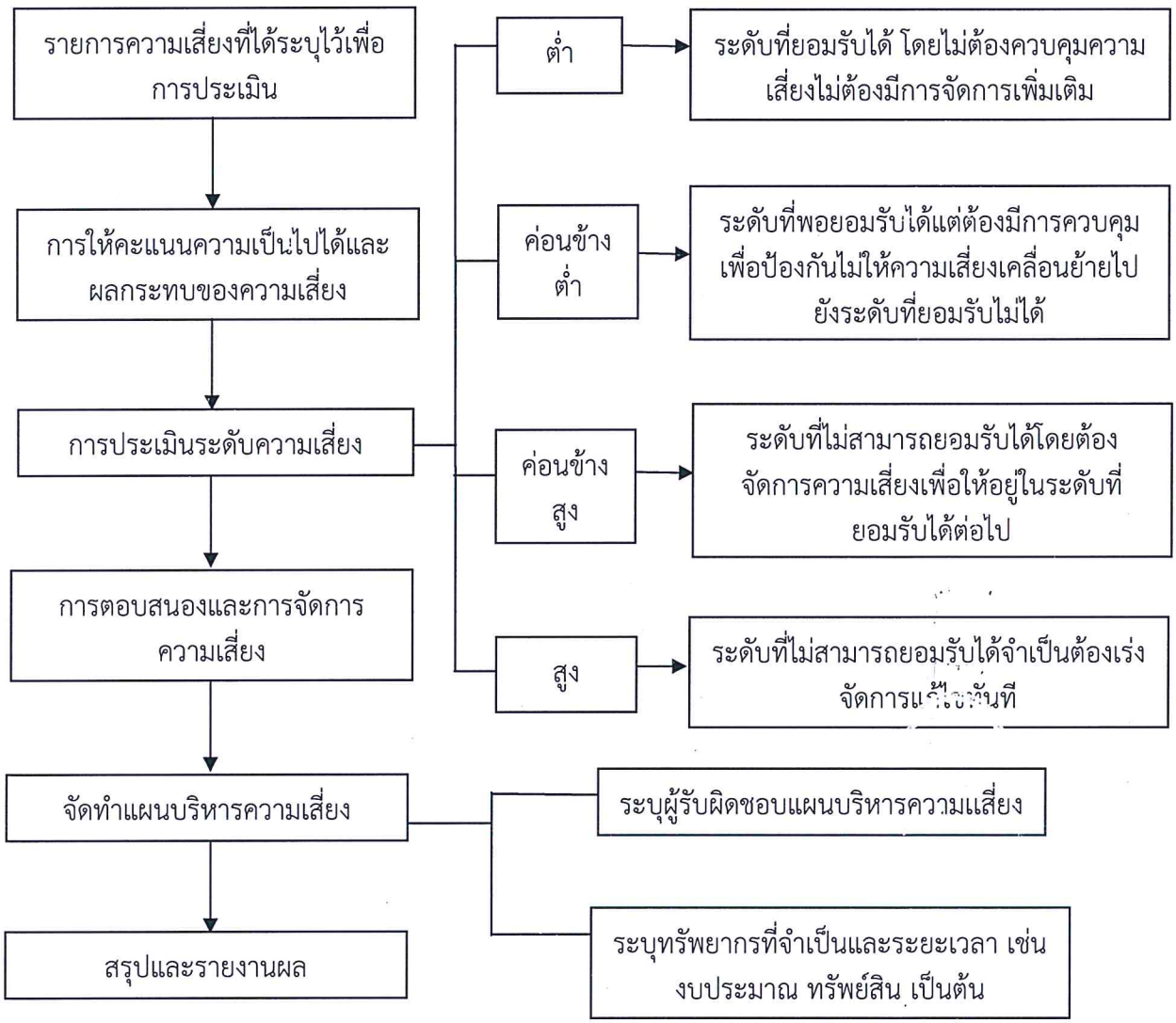
๓.๗ การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบตามรอบการรายงานผล และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

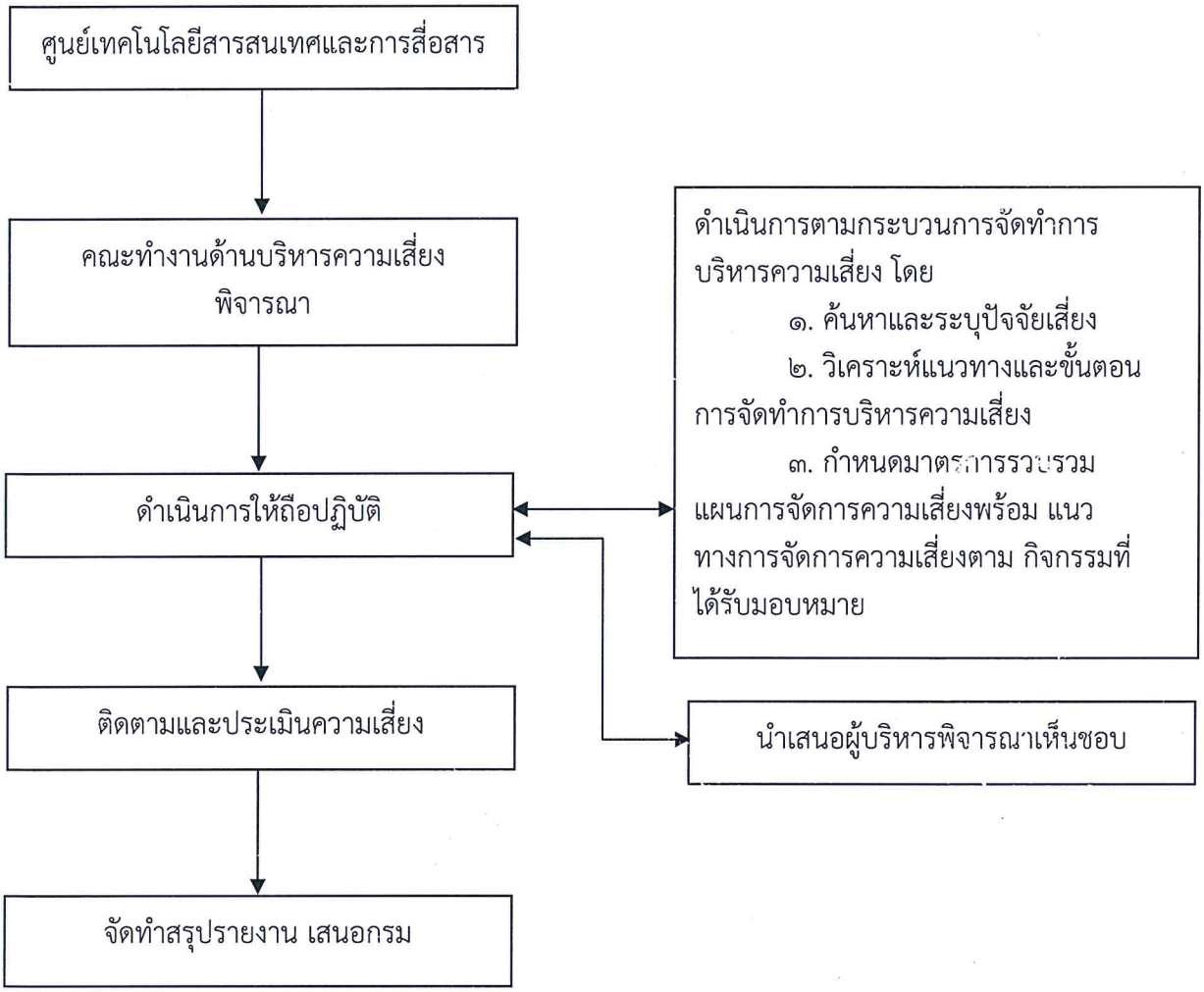
บทที่ ๔
การวิเคราะห์และการบริหารจัดการความเสี่ยง

กรมชลประทาน ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ทำแผนบริหารความเสี่ยงด้านเทคโนโลยียีดิจิทัลประจำปี ๒๕๖๖ - ๒๕๖๘ ให้สอดคล้องกับความเสี่ยงด้านเทคโนโลยียีดิจิทัลของ กรมชลประทาน กระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยียีดิจิทัล และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงาน ด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

๔.๑แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



๔.๒ กระบวนการจัดทำการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล



ส่วนที่ต้องนำส่ง ศทส. เฉพาะ ตาราง ข้อ ๔.๓

กรณีหน่วยงานของท่าน มีระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือเทคโนโลยีดิจิทัลในหน่วยงานของท่าน

๔.๓ การประเมินความเสี่ยงด้านเทคโนโลยีดิจิทัลกรมชลประทาน

ความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
	ปัจจัยเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)ตัวอย่าง								
๑. ความเสี่ยงจากการเกิดอัคคีภัย วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม แผ่นดินไหว หรือวินาศภัยการก่อการร้าย ที่มีผลต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร	๑. การสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร ๒. ความเสียหายด้านโครงสร้างอาคารอาจทำลายระบบเครื่องและข้อมูล ๓. ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์	๑. เสียงบประมาณในการจัดหาระบบทดแทน ๒. ไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทน ๓. เสียเวลาในการกู้ระบบ ๔. เสียภาพลักษณ์ของกรมชลประทาน	๓	๕	สูง ๓x๕=๑๕	๑. ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง งานอุปกรณ์ดับเพลิง ๒. จัดทำแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ๓. จัดทำแผน การบริหารความต่อเนื่อง Business Continuity Plan (BCP) ๔. ทำการสำรองข้อมูลต่างที่กัน ๕. จัดทำศูนย์สำรอง Disaster Recovery Site (DR Site)	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	

ความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
	ปัจจัยเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๒. ความเสี่ยงด้านบุคลากร (Human Risk)ตัวอย่าง								
๑. ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	๑. เสี่ยงต่อการใช้งานในทางที่ผิด เช่น การดูหนัง ฟังเพลง เป็นต้น ๒. การใช้ Resource ทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรมที่ไม่มีลิขสิทธิ์ เป็นต้น	๑. สูญเสีย Bandwidth ในเครือข่าย ๒. อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	๒	๓	ค่อนข้างต่ำ ๒x๓=๖	๑. กำหนด Policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	
						๒. การเสริมสร้างองค์ความรู้ให้บุคลากรอย่างสม่ำเสมอ	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	
๒. ความเสี่ยงจากเจ้าหน้าที่ใช้สายพ่วงไม่ได้มาตรฐาน ทำให้ไฟกระชากจากสายพ่วง (Extension Cord)	เสี่ยงต่อไฟไหม้ ไฟดูด ทำให้อุปกรณ์เครื่องคอมพิวเตอร์เสียหายทั้งหมดได้	๑. ไม่สามารถใช้งานเครื่องคอมพิวเตอร์ได้ตามปกติ ๒. ไฟอาจลัดวงจรทำให้เครื่องเสียหาย	๒	๒	ค่อนข้างต่ำ ๒x๒=๔	๑. ตรวจสอบสายพ่วง/สายสัญญาณ ให้มีมาตรฐาน ม.อ.ก. และมีการเชื่อมต่อสายดิน/การติดตั้ง Breaker ตามจุด/พื้นที่/โซน ที่จำเป็น ๒. การสำรองสายพ่วง (ตามมาตรฐาน) สำหรับกรณีฉุกเฉิน	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	

ความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
	ปัจจัยเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๓. ความเสี่ยงด้านอุปกรณ์/เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)ตัวอย่าง								
๑. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๑. ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ ๒. เสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล	๑. การใช้งานระบบงาน ไม่สามารถใช้ได้ตามปกติ	๓	๕	สูง ๓x๕=๑๕	๑. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล ๒. การทำ replication/redundancy หรือ มีระบบ Virtual Desktop Infrastructure :VDI	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	
						๒. หมั่นตรวจสอบ Policy และ Log ของ Firewall อย่างสม่ำเสมอ และเปิด port / service ที่จำเป็นต้องใช้งานเท่านั้น	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	
						๓. มีมาตรการ และกฎระเบียบในการควบคุมให้มีการติดตั้งโปรแกรมต่างๆ บนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายอินทราเน็ตของกรม	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	

ความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
	ปัจจัยเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)ตัวอย่าง								
๑. ความเสี่ยงจากช่องโหว่ จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๑. การถูกขโมยข้อมูล ๒. โปรแกรมเสียหาย ๓. การใช้ช่องโหว่ของโปรแกรมหรือซ่อน Script ไว้เพื่อวัตถุประสงค์แอบแฝง ๔. รูปแบบในการพัฒนาแตกต่างกัน ทำให้เปลี่ยนคนพัฒนาหรือรับงานต่อยาก	๑. ลดความน่าเชื่อถือต่อกรมชลประทาน หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ ๒. กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหาย เป็นอย่างยิ่ง ๓. การใช้งานหรือพัฒนาโปรแกรมไม่ต่อเนื่อง	๓	๕	สูง ๓x๕=๑๕	๑. มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ ๒. ตรวจสอบช่องโหว่และดำเนินการปิดช่องโหว่ ๓. การใช้โปรแกรมประยุกต์ให้น้อยที่สุด	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	
						๒. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	
๕. ความเสี่ยงด้านระบบข้อมูล (Database Risk)ตัวอย่าง								
๑. ความเสี่ยงจากการสำรองข้อมูล การทำงานระบบไม่มีความเสถียรภาพหรือทำการสำรองข้อมูลแต่ขาดการอัพเดท	๑. เสี่ยงต่อการสูญหายของข้อมูล จนไม่สามารถดำเนินงานได้ตามปกติ ๒. เสี่ยงต่อการมีข้อมูลที่ไม่ถูกต้องกับความเป็นจริง	๑. เสียค่าใช้จ่ายในการกู้คืนข้อมูล หรือการจัดทำขึ้นมาใหม่ ๒. ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้งานได้	๓	๕	สูง ๓x๕=๑๕	๑. มีการบริหารจัดการการสำรองข้อมูล (Backup/replicate) เป็นประจำอย่างสม่ำเสมอ	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	
						๒. มีการทดสอบการนำข้อมูลกลับคืนสู่	☐การยอมรับ ☑การควบคุม	

ความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
	ปัจจัยเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
						ระบบ (Restore)	☐การถ่ายโอน	
						๒. การถ่ายทอดองค์ความรู้ด้านการรักษาความปลอดภัย	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	
						๓. มีการบริหารจัดการด้านการเข้าถึงข้อมูล	☐การหลีกเหลี่ยง ☐การยอมรับ ☑การควบคุม ☐การถ่ายโอน	

ใส่ข้อมูลความเสี่ยงทั้ง ๕ ด้าน ที่หน่วยงานของท่านมีระบบงานด้านเทคโนโลยีดิจิทัล

ความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
	ปัยจัยเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)(ใส่ข้อมูลหน่วยงานของท่าน)								
๒. ความเสี่ยงด้านบุคลากร (Human Risk)(ใส่ข้อมูลหน่วยงานของท่าน)								
๓. ความเสี่ยงด้านอุปกรณ์/เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)(ใส่ข้อมูลหน่วยงานของท่าน)								
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)(ใส่ข้อมูลหน่วยงานของท่าน)								
๕. ความเสี่ยงด้านระบบข้อมูล (Database Risk)(ใส่ข้อมูลหน่วยงานของท่าน)								

จบในส่วนที่ต้องนำส่ง ศทส. เฉพาะ ตาราง ข้อ ๔.๓

บทที่ ๕
สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือกระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแลตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อน การดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกหน่วยงานภายในกรมชลประทานในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายและถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้นหนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัยซึ่งก็คือ การจัดการความเสี่ยงในองค์กร นั่นเอง

๕.๑ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีดิจิทัล

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีผลคะแนนสูงสุด ๕ อันดับแรก ได้ข้อสรุป ดังนี้

๑. ความเสี่ยงจากการเกิดอัคคีภัย มีแนวทางปฏิบัติดังนี้

- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง
- ติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง
- มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ

๒. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย มีแนวทางปฏิบัติดังนี้

- ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักและสำรองฐานข้อมูล
- การจัดตั้งหรือติดตาม ตรวจสอบ ศูนย์สำรองข้อมูล (Backup Site)

๓. ความเสี่ยงจากการสำรองข้อมูล การทำงานระบบไม่มีความเสถียรภาพหรือทำการสำรองข้อมูลแต่ขาดการอัพเดทมีแนวทางปฏิบัติดังนี้

- การบริหารจัดการในการทำสำรองข้อมูล (Backup) เป็นประจำอย่างสม่ำเสมอ
- มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)

๔. ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร มีแนวทางปฏิบัติดังนี้

- มาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ
- ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่

๕. ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource) การขาดแผนบริหารความต่อเนื่อง มีแนวทางปฏิบัติดังนี้

- การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level
- การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล ER-Diagram
- ให้มีการส่งมอบ Source Code ในรูปแบบที่ไม่เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้
- หากมีการพัฒนา Library ด้วยตนเอง ต้องส่ง Source Code Library ที่สามารถแก้ไขได้
- มีการถ่ายทอดความรู้ เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่
- มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม
- จัดทำข้อตกลงการรักษาข้อมูลความลับของหน่วยงานระหว่างผู้รับจ้างกับผู้ว่าจ้าง
- มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัพเดท เมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล(Database) เกิดความเสียหาย เป็นต้น

๕.๒ สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลได้ดำเนินการจัดทำเพื่อ

๔.๒.๑ เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศและการสื่อสาร

๔.๒.๒ เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๔.๒.๓ ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๕.๓ ข้อเสนอแนะ

๔.๓.๑ การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

๔.๓.๑.๑ พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

๔.๓.๑.๒ พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความ เสี่ยงนั้น

๔.๓.๑.๓ กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่

๔.๓.๒ การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่าง ถูกต้องได้อย่างมีประสิทธิภาพ