การประเมินความเสี่ยง และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ฝ่ายไฟฟ้าและเทคโนโลยีสารสนเทศ สำนักงานชลประทานที่ 8

ประเภทความเสี่ยง	ความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
		ปัจจัยเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	1. ความเสี่ยงจากการเกิดระบบกระแสฟ้าขัดข้อง	1. เสี่ยงต่อการให้บริหารของเครื่องคอมพิวเตอร์แม่ข่ายและการบริการของเครือข่ายได้ 2. ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่าย ทั้งส่วนระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (RDBMS) อันเนื่องมาจากเครื่องไม่ได้ ถูกทำการ Shutdown อย่างเหมาะสม	1. ข้อมูลเสียหาย 2. ระบบปฏิบัติการโปรแกรมหรือฐานข้อมูลเสียหาย ต้องมีการติดตั้งใหม่	3	4	3x4=12 ค่อนข้างสูง	1. ตรวจสอบระบบสำรองไฟฟ้า (UPS) 2. การจัดหาและติดตั้งเครื่องกำเนิดไฟฟ้า (Electrical Generator) สำหรับ สชป.8	การควบคุม (Treat)	
	2. ความเสี่ยงจากแมลงหรือสัตว์กัดแทะ อุปกรณ์หรือสายไฟฟ้า/สายสัญญาณ	1. เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	1. เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน 2. ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง	1	5	1x5=5 ค่อนข้างต่ำ	1. ไม่ปล่อยให้มีสายไฟฟ้าหรือสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack 2. ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	การควบคุม (Treat)	หน้าที่ 1

	3. ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง	1. เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	1. เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง 2. เสียเวลาในการกู้ระบบ 3. เสียภาพลักษณ์ของ สชป.8	1	5	1x5=5 ค่อนข้างต่ำ	1. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย 2. ตู้ Rack ที่ติดตั้งอุปกรณ์ เช่น เครื่องแม่ข่าย (Server) อุปกรณ์จัดเก็บข้อมูล (Disk Array) และอุปกรณ์เครือข่ายต้องมีการล็อคด้วยกุญแจตลอดเวลา 3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ ที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ตั้งอยู่	การควบคุม (Treat)	
ด้านบุคลากร (Human Risk)	4. ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	1. เสี่ยงต่อการใช้งานในทางที่ผิด เช่น การดูหนัง ฟังเพลง เป็นต้น 2. การใช้ Resource ทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ที่ไม่มีลิขสิทธิ์ เป็นต้น	1. สูญเสีย Bandwidth ในเครือข่าย 2. อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	2	3	2x3=6 ค่อนข้างต่ำ	1. กำหนด Policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น 2. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ต่าง ๆ ไปใช้ในทางที่ผิด รวมถึงการบันทึกการใช้งานและรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืน	การควบคุม (Treat)	หน้าที่ 2

ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data)	5. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	1. ไม่สามารถใช้ระบบงาน ได้เต็มประสิทธิภาพ 2. เสี่ยงต่อความเสียหาย ของข้อมูลและการกู้คืน ข้อมูล	1. ส่งผลต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล 2. การใช้งานระบบงาน ไม่สามารถใช้ได้ตามปกติ	3	5	3x5=15 สูง	1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล 2. จัดตั้งศูนย์สำรองข้อมูล (Backup Site)	การควบคุม (Treat)	
	6. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	1. เสี่ยงต่อการไม่สามารถใช้งานระบบงานของ สชป.8ผ่านเครือข่ายอินทราเน็ตได้ 2. เสี่ยงต่อการไม่สามารถเชื่อมต่อภายนอก สชป.8ผ่านเครือข่ายอินเทอร์เน็ตได้	1. ขัดขวางการทำงานของเจ้าหน้าที่และผู้บริหารของ สชป.8 2. บุคคลภายนอกไม่สามารถเข้าใช้ Web Server หรือค้นหาข้อมูลที่ต้องการได้	3	4	3x4=12 ค่อนข้างสูง	1. ตรวจสอบระบบเครือข่ายหลักหรือระบบเครือข่ายที่ให้บริการของ สชป.8 อย่างสม่ำเสมอ	การควบคุม (Treat)	
	7. ความเสี่ยงจากการติดไว้รัสคอมพิวเตอร์หรือ Malware	1. เสี่ยงต่อการไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ 2. เสี่ยงต่อการถูกขโมยข้อมูล	1. ใช้คอมพิวเตอร์ไม่ได้ 2. ใช้ระบบงานไม่ได้ 3. ข้อมูลที่สำคัญสูญหาย	2	4	2x4=8 ค่อนข้างสูง	1. ติดตั้งระบบป้องกันกับเครื่องแม่ข่าย 2. อัพเดตข้อมูลไวรัสอย่างสม่ำเสมอ	การควบคุม (Treat)	
	8. ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก	1. เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	1. ทำให้ระบบเครื่องแม่ข่ายหรือลูกข่ายติดไวรัสและแพร่กระจ่ายสู่เครื่องอื่น ๆ ทั้งหมด ในเครือข่าย 2. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพบน Web Site ของ สชป.8	3	4	3x4=12 ค่อนข้างสูง	1. ติดตั้งระบบเครือข่ายเพื่อป้องกัน และเตือนภัย 2. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับ 3. ตรวจสอบ Policy และ Log ของ ระบบ ป้องกันการบุกรุกระบบเครือข่าย	การควบคุม (Treat)	หน้าที่ 3

	9. ความเสี่ยงจากการถูกโจมตีเครือข่ายของ สชป.8 จากภายในและภายนอก ไม่ให้สามารถให้บริการได้	1. เสี่ยงต่อการถูกโจมตีเครือข่ายภายนอกในทุกรูปแบบ ซึ่งจะมีการพัฒนาวิธีการอยู่ตลอดเวลา 2. เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายใน ทั้งที่ไม่ได้ตั้งใจและตั้งใจ	1. ทำให้ไม่สามารถใช้งานเครือข่ายได้ หรือใช้ได้แต่งานได้ แต่ช้ามาก	1	4	1x4=4 ค่อนข้างต่ำ	1. ติดตั้งระบบป้องกันและเตือนภัย Spam, Virus, Malware, Trojan ฯลฯ และมีเจ้าหน้าที่คอยดูแลตรวจสอบ และอัพเดทฐานข้อมูลเป็นประจำ 2. หมั่นตรวจสอบ Policy และ Log ของ Firewall อย่างสม่ำเสมอ 3. มีมาตรการ และกฎระเบียบในการควบคุมให้มีการติดตั้งโปรแกรมต่างๆ บนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายอินทราเน็ตของ สชป.8	การควบคุม (Treat)	
	10. ความเสี่ยงจากการใช้ Wireless เข้าเครือข่ายอินทราเน็ต	1. เสี่ยงต่อผู้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลเข้าใช้เครือข่ายอินทราเน็ต	1. ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้ อันจะนำมาซึ่งการขาดความน่าเชื่อถือ	1	4	1x4=4 ค่อนข้างต่ำ	1. ควบคุมการเข้าใช้เครือข่าย 2. เพิ่มความปลอดภัยในการใช้งาน เพิ่มขึ้นโดยติดตั้งระบบยืนยันตน (Authentication)	การควบคุม (Treat)	
ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	11. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	1. การสูญหายของข้อมูล 2. การถูกฟ้องร้องและเสื่อมเสียชื่อเสียงและความน่าเชื่อถือของ สชป.8	1. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้น ๆ 2. สชป.8 อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้ที่เป็นเจ้าของลิขสิทธิ์นั้น ๆ	2	5	2x5=10 ค่อนข้างสูง	1. การจัดหาซอฟต์แวร์ที่ถูกต้องตามกฎหมายมาใช้ตามความจำเป็น 2. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย	การควบคุม (Treat)	

ด้านระบบข้อมูล (Database Risk)	12. ความเสี่ยงจากการสำรองข้อมูล การทำงานระบบไม่มีความเสถียรภาพหรือทำการสำรองข้อมูลแต่ขาดการอัพเดท	1. เสี่ยงต่อการสูญหายของข้อมูล จนไม่สามารถดำเนินงานได้ตามปกติ 2. เสี่ยงต่อการมีข้อมูลที่ไม่ถูกต้องกับความเป็นจริง	1. เสียค่าใช้จ่ายในการกู้คืนข้อมูล หรือทำใหม่ 2. ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้งานได้ เนื่องจากขาดความมั่นใจในข้อมูล	3	5	3x5=15 สูง	1. มีการบริหารจัดการการสำรองข้อมูล (Backup) เป็นประจำอย่างสม่ำเสมอ 2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	การควบคุม (Treat)	
	13. ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	1. เสี่ยงต่อข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรือ ม้วนเทป (Cartridge Tape) แผ่น DVD/CD	1. ข้อมูลที่อยู่ในชั้นความลับรั่วไหลทำให้เกิดความเสียหายต่อความน่าเชื่อถือของกรมชลประทาน 2. ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	2	3	2x3=6 ค่อนข้างต่ำ	1. มีการบริหารจัดการต่ออุปกรณ์ข้อมูล เช่น Hard Disk ม้วนเทป แผ่น DVD/CD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้น ๆ ทิ้งแล้วหากทำได้	การควบคุม (Treat)	
ด้านกลยุทธ์ (Strategic Risk)	14. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	1. การเปลี่ยนแปลงนโยบายจากรัฐบาล/ผู้บริหาร	การเปลี่ยนแปลงผู้บริหารอาจทำให้ นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการ โครงการต่าง ๆ ได้รับผลกระทบ	2	3	2x3=6 ค่อนข้างต่ำ	-	การยอมรับ (Take)	-
ด้านการเงิน (Financial Risk)	15. ความเสี่ยงต่อการไม่ได้รับ การสนับสนุนงบประมาณด้านเทคโนโลยีสารสนเทศและการสื่อสาร	1. โครงการด้านเทคโนโลยีสารสนเทศและการสื่อสารไม่ได้รับการจัดสรรงบประมาณ	การขาดแคลนเทคโนโลยีสารสนเทศและการสื่อสารส่งผลทำให้การดำเนินงานขาดความต่อเนื่องไร้ซึ่งประสิทธิภาพ			2x3=6 ค่อนข้างต่ำ	-	การยอมรับ (Take)	-