9.2.5 มีการนำผลการประเมินหรือความสี่ยงที่ยังคงเหลืออยู่ มาปรับปรุงแผนการจัดการความเสี่ยงอย่างต่อเนื่อง

Risk Assessment of Cybersecurity
Risk Assessment of Cybersecurity Report to MGT

การประเมินและการจัดการความเสี่ยงทรัพย์สินและการบริการที่สำคัญ (Asset Risk Asessment and Risk Treatment]

ผู้พิจารณาประเมิน : สมาชิกคณะกรรมการพิจารณาความเสี่ยง

ผู้บันทึก :สันต์ สิงห์ไกร, สมาชิกคณะกรรมการพิจารณาความเสี่ยง

วันที่ทำการประชุมความเสี่ยงพร้อมบันทึก : 18 มีนาคม 2569

สถานที่ : ห้องประชุมสุนีย์ อินฉัตร

ที่อยู่ : 84/2 หมู่ 1 ตำบลพิมา อำเภอปรางค์กู่ จังหวัดศรีสะเกษ 33170

ระบบบริการที่สำคัญ : All application as HIS

ผลการประเมินความเสี่ยง	8

แดง (สูง) = 17 เอกสาร เป็นอย่างน้อย
เหลือง (ปานกลาง) = 13 เอกสาร เป็นอย่างน้อ
เขียว (ต่ำ) = 10 เอกสาร เป็นอย่างน้อย

No.	ชนิดของทรัพย์สิน (Type of Asset) / Cluster	ชื่อ (Asset Name)	คำอธิบาย (Description)	ระบบที่เกี่ยวข้อง (Concerned Application)	บริการที่สำคัญ/ฟังก์ชันที่สำคัญ (Critical Service/ Function)	ระบุความเสี่ยงด้านไซเบอร์และช่องโหว่ ต่างๆ		ระทบต่			ามรุนแรงแต่ละด้					Risk Analysis		
																A	B	C = A*B
						ภัยคุกคาม (Threat)	ช่องโหว่ (Vulner.)	C	I	A	F	S	R	I	L	O	โอกาสเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)
1	Application-Major	Himpro	โปรแกรมสำหรับให้บริการผู้ป่วย	ระบบบริการผู้ป่วย	รองรับการรับระบบการให้บริการผู้ป่วย	x	x	x	x	x	-	-	x	x	x	x	2	5	10
2	Application-Major	INFINITT	โปรแกรมสำหรับดูลภาพทางการแพทย์	ระบบ X-ray	รองรับระบบการดูภาพถ่ายทางการแพทย์ในการให้บริการผู้ป่วย	x	x	x	x	x	-	-	x	x	x	x	2	4	8
3	Application-Major	HRM	โปรแกรมสำหรับจัดทำข้อมูลการเบิกจ่ายค่าบริการ	ระบบเบิกจ่ายค่าบริการทางการแพทย์	รองรับระบบเบิกจ่ายค่าบริการทางการแพทย์	x	x	x	x	x	-	-	x	x	x	x	2	5	10
4	Application-Major	HM	โปรแกรมสำหรับบันทึกข้อมูลผู้ป่วยใน	ระบบเวชระเบียนผู้ป่วยใน	รองรับระบบเวชระเบียนผู้ป่วยใน	x	x	x	x	x	-	-	x	x	x	x	2	5	10

5	HW-Servers	Server for Himpro	เครื่องแม่ข่ายสำหรับฐานข้อมูลหลัก	ระบบจัดเก็บข้อมูล	รองรับระบบให้บริการผู้ป่วยและระบบบิกจ่ายรักษาพยาบาล	x	x	x	x	x	-	-	x	x	x	x	2	5	10
6	HW-Servers	Server for INFINITT	เครื่องแม่ข่ายสำหรับฐานข้อมูลภาพทางการแพทย์	ระบบจัดเก็บข้อมูล	รองรับระบบการดูภาพถ่ายทางการแพทย์ในการให้บริการผู้ป่วย	x	x	x	x	x	-	-	x	x	x	x	2	4	8

7	HW-Servers	Server for HRM	เครื่องแม่ข่ายสำหรับฐานข้อมูลการเบิกจ่ายค่าบริการ	ระบบจัดเก็บข้อมูล	รองรับระบบเบิกจ่ายค่าบริการทางการแพทย์	x	x	x	x	x	-	-	x	x	x	x	2	4	8
8	HW-Servers	Server for HM	เครื่อวแม่ข่ายสำหรับบันทึกข้อมูลผู้ป่วยใน	ระบบบริการเวชระเบียนผู้ป่วยใน	รองรับระบบเวชระเบียนผู้ป่วยใน												2	4	8

9	HW-Switch	core switch	เครื่องอุปกรณ์สวิตช์หลัก (Core Switch)	ระบบบริการผู้ป่วย	รองรับระบบบริการผู้ป่วย	x	x	x	x	x	-	-	x	x	x	x	2	4	8
10	SW-Others	Antivirus Software	ซอฟต์แวร์ป้องกันไวรัส	ระบบความปลอดภัย	ป้องกันมัลแวร์	x	x	x	x	x	-	-	x	x	x	x	1	4	4
11	SW-Others	HeidiSQL	ซอฟต์แวร์จัดการฐานข้อมูล	ระบบฐานข้อมูล	จัดการข้อมูลองค์กร	x	x	x	x	x	-	-	x	x	x	x	1	4	4
12	SW-Others	Backup Software	ซอฟต์แวร์สำรองข้อมูล	ระบบสำรองข้อมูล	ป้องกันการสูญหายของข้อมูล	x	x	x	x	x	-	-	x	x	x	x	2	4	8

วย

เจ้าของ (Asset Owner)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk Level) -ของแต่ละ Cluster	ตัวเลือกการตอบสนอง (Risk Treatment)	No.	แผนจัดการความเสี่ยง (Risk Treatment Plan)		คาดว่าดำเนินการแล้วเสร็จ (Expected finish date)	ผู้รับผิดชอบ (Responsibility)	สถานะความคืบหน้า (Progress Status)
กลุ่มงานสุขภาพดิจิทัล	9.5	Mitigate Risk	1	การป้องกัน: ดำเนินการบำรุงรักษาเชิงป้องกัน, สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	
กลุ่มงานสุขภาพดิจิทัล		Mitigate Risk	1	การป้องกัน: ดำเนินการบำรุงรักษาเชิงป้องกัน, สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	
กลุ่มงานสุขภาพดิจิทัล		Mitigate Risk	1	การป้องกัน: ดำเนินการบำรุงรักษาเชิงป้องกัน, สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	
กลุ่มงานสุขภาพดิจิทัล		Mitigate Risk	1	การป้องกัน: ดำเนินการบำรุงรักษาเชิงป้องกัน, สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	

							จนท.กลุ่มงานสุขภาพดิจิทัล	
กลุ่มงานสุขภาพดิจิทัล		Mitigate Risk	1	การป้องกัน: ใช้การจัดกลุ่มเซิร์ฟเวอร์ (Server Clustering) เพื่อการโหลดบาลานซ์, สำรองข้อมูลทุกวัน, เฝ้าระวังการทำงานของเซิร์ฟเวอร์อย่างต่อเนื่อง.	การแก้ไข: เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR, กู้คืนระบบจากข้อมูลที่สำรองไว้, ตรวจสอบ logs เพื่อวิเคราะห์ปัญหาการป้องกัน: ใช้การจัดกลุ่มเซิร์ฟเวอร์ (Server Clustering) เพื่อการโหลดบาลานซ์, สำรองข้อมูลทุกวัน, เฝ้าระวังการทำงานของเซิร์ฟเวอร์อย่างต่อเนื่อง. การแก้ไข: เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR, กู้คืนระบบจากข้อมูลที่สำรองไว้, ตรวจสอบ logs เพื่อวิเคราะห์ปัญหา.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	**90%**
กลุ่มงานสุขภาพดิจิทัล	8.5	Mitigate Risk	1	การป้องกัน: ใช้การจัดกลุ่มเซิร์ฟเวอร์ (Server Clustering) เพื่อการโหลดบาลานซ์, สำรองข้อมูลทุกวัน, เฝ้าระวังการทำงานของเซิร์ฟเวอร์อย่างต่อเนื่อง.	การแก้ไข: เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR, กู้คืนระบบจากข้อมูลที่สำรองไว้, ตรวจสอบ logs เพื่อวิเคราะห์ปัญหาการป้องกัน: ใช้การจัดกลุ่มเซิร์ฟเวอร์ (Server Clustering) เพื่อการโหลดบาลานซ์, สำรองข้อมูลทุกวัน, เฝ้าระวังการทำงานของเซิร์ฟเวอร์อย่างต่อเนื่อง. การแก้ไข: เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR, กู้คืนระบบจากข้อมูลที่สำรองไว้, ตรวจสอบ logs เพื่อวิเคราะห์ปัญหา.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	**50%**

กลุ่มงานสุขภาพดิจิทัล		Mitigate Risk	1	การป้องกัน: ใช้การจัดกลุ่มเซิร์ฟเวอร์ (Server Clustering) เพื่อการโหลดบาลานซ์, สำรองข้อมูลทุกวัน, เฝ้าระวังการทำงานของเซิร์ฟเวอร์อย่างต่อเนื่อง.	การแก้ไข: เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR, กู้คืนระบบจากข้อมูลที่สำรองไว้, ตรวจสอบ logs เพื่อวิเคราะห์ปัญหาการป้องกัน: ใช้การจัดกลุ่มเซิร์ฟเวอร์ (Server Clustering) เพื่อการโหลดบาลานซ์, สำรองข้อมูลทุกวัน, เฝ้าระวังการทำงานของเซิร์ฟเวอร์อย่างต่อเนื่อง. การแก้ไข: เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR, กู้คืนระบบจากข้อมูลที่สำรองไว้, ตรวจสอบ logs เพื่อวิเคราะห์ปัญหา.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	**50%**
กลุ่มงานสุขภาพดิจิทัล		Mitigate Risk	1	การป้องกัน: ใช้การจัดกลุ่มเซิร์ฟเวอร์ (Server Clustering) เพื่อการโหลดบาลานซ์, สำรองข้อมูลทุกวัน, เฝ้าระวังการทำงานของเซิร์ฟเวอร์อย่างต่อเนื่อง.	การแก้ไข: เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR, กู้คืนระบบจากข้อมูลที่สำรองไว้, ตรวจสอบ logs เพื่อวิเคราะห์ปัญหาการป้องกัน: ใช้การจัดกลุ่มเซิร์ฟเวอร์ (Server Clustering) เพื่อการโหลดบาลานซ์, สำรองข้อมูลทุกวัน, เฝ้าระวังการทำงานของเซิร์ฟเวอร์อย่างต่อเนื่อง. การแก้ไข: เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR, กู้คืนระบบจากข้อมูลที่สำรองไว้, ตรวจสอบ logs เพื่อวิเคราะห์ปัญหา.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	

กลุ่มงานสุขภาพดิจิทัล	**8.0**	Mitigate Risk	**1**	การป้องกัน: ดำเนินการบำรุงรักษาเชิงป้องกัน, สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	**60%**
กลุ่มงานสุขภาพดิจิทัล	**5.3**	Continue Monitoring	**1**	การป้องกัน: ดำเนินการบำรุงรักษาเชิงป้องกัน, สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	**90%**
กลุ่มงานสุขภาพดิจิทัล		Continue Monitoring	**1**	การป้องกัน: ดำเนินการบำรุงรักษาเชิงป้องกัน, สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	**55%**
กลุ่มงานสุขภาพดิจิทัล		Mitigate Risk	**1**	การป้องกัน: ดำเนินการบำรุงรักษาเชิงป้องกัน, สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง.	ภายใน 30 ก.ย. 69	**จนท.กลุ่มงานสุขภาพดิจิทัล**	**90%**

	เป็นความเสี่ยงขั้นวิกฤติ ต้องมีการดำเนินการโดยทันที	
	เป็นความเสี่ยงสูง ต้องมีการดำเนินการบางอย่างเพื่อลดความเสี่ยง	
	เป็นความเสี่ยงปานกลาง ต้องมีการติดตามและอาจมีมาตรการป้องกัน	
	ต้องมีการติดตามเป็นระยะ แต่ยังไม่ต้องมีการดำเนินการใดๆเพิ่มเติม	

ıual)

L	O	โอกาสเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยงที่คงเหลือ (Risk Residual Level)	ดำเนินการเพิ่มเติมเพื่อลดความเสี่ยงให้น้อยลงอีก (Further actions to be taken to further minimize risk)
				0	
				0	
				0	
				0	

-	-	1	1	1	เฝ้าติดตามเป็นระยะ
-	-	1	1	1	เฝ้าติดตามเป็นระยะ

-	-	1	1	1	เฝ้าติดตามเป็นระยะ

-	-	1	1	1	เฝ้าติดตามเป็นระยะ
-	-	1	1	1	เฝ้าติดตามเป็นระยะ
-	-	1	1	1	เฝ้าติดตามเป็นระยะ
-	-	1	1	1	เฝ้าติดตามเป็นระยะ

โรงพยาบาลปรางค์กู่

รายงานการประเมินความเสี่ยงไซเบอร์ (Cybersecurity Risk Assessment Report)
วันที่ทำประเมิน : 17 มีนาคม 2569
ผู้จัดทำรายงาน : นายสันต์ สิงห์ไกร
ชื่อระบบ : Critical Core Application เช่น HIMPRO, LIS

1. สรุปสำหรับผู้บริหาร (Executive Summary)

วันที่ทำการประเมิน : 17 มีนาคม 2569

วัตถุประสงค์ : การประเมินความเสี่ยงของระบบบริหารจัดการโรงพยาบาล (Himpro) เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับข้อมูลลูกค้าที่ใช้บริการ รวมถึงหาวิธีการควบคุมที่เหมาะสม

ประเภทของการประเมิน : การประเมินความเสี่ยงครั้งแรก

ระดับความเสี่ยงโดยรวม : ระดับความเสี่ยงโดยรวมถูกประเมินว่าอยู่ในระดับ สูง

จำนวนความเสี่ยงที่ระบุทั้งหมด : 16 รายการ

ความเสี่ยงที่ยอมรับได้ (ความเสี่ยงต่ำ) : 4 รายการ

ความเสี่ยงปานกลาง: 11 รายการ

ความเสี่ยงสูง: 1 รายการ

2. รายละเอียดของรายงาน (Body of the Report)

2.1 วัตถุประสงค์ของการประเมินความเสี่ยง

1. ประเมินความเสี่ยงของระบบบริหารจัดการโรงพยาบาล (Himpro) ที่เกี่ยวข้องกับความลับ (Confidentiality), ความถูกต้อง (Integrity), และความพร้อมใช้งาน (Availability) ของผู้ใช้บริการ

2. ระบุความเสี่ยงที่อาจก่อให้เกิดปัญหากับระบบบริหารจัดการโรงพยาบาล (Himpro) รวมถึงการจัดการข้อมูลลูกค้าที่มาใช้บริการ

3. ตรวจสอบการใช้มาตรการควบคุมเพื่อปกป้องระบบจากภัยคุกคามไซเบอร์

2.2 โมเดลความเสี่ยงและวิธีการประเมิน

ใช้โมเดลความเสี่ยงตาม NIST SP 800-30 Rev. 1 ซึ่งประเมินตามความรุนแรงและโอกาสของความเสี่ยง โดยใช้คะแนนจาก 1 ถึง 5 (1 = ต่ำสุด, 5 = สูงสุด) และคำนวณคะแนนรวมเพื่อประเมินระดับความเสี่ยง

รายละเอียดความเสี่ยง (Detailed Risk Assessment) ในแต่ละ Cluster (เน้นเฉพาะ Cluster ที่มีระดับความเสี่ยงสูง เป็นหลัก

	ความเสี่ยง	ระดับความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	การควบคุมที่มีอยู่ปัจจุบัน	คำแนะนำเพิ่มเติม	คาดว่าจะเสร็จสิ้น
1	การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks)	สูง	เสี่ยงการโจรกรรมข้อมูลการเงินหรือการเรียกค่าไถ่ (Ransomware) ระบบล่ม ทำให้สูญเสียรายได้ ข้อมูลลูกค้าหรือผู้ใช้บริการถูก	ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ในทุกอุปกรณ์ใช้ระบบ Endpoint Security เพื่อสแกนหาไวรัสโดยใช้	ทดสอบระบบการป้องกันมัลแวร์อย่างสม่ำเสมอค้นหาช่องโหว่ที่อาจถูกใช้โจมตี, จัดอบรมเกี่ยวกับการ	30 ก.ย. 2569

			ขโมยทำให้สูญเสียความเชื่อมั่น ความน่าเชื่อถือขององค์กรลดลง	ระบบ IDS/IPS ตั้งค่าการอัปเดตอัตโนมัติ ใช้กลยุทธ์ 3-2-1 Backup สำรองข้อมูล 3 ชุด ใน 2 สื่อที่ต่างกัน และเก็บ 1 ชุดนอกสถานที่)	หลีกเลี่ยงการดาวน์โหลดไฟล์หรือเข้าเว็บไซต์ที่ไม่น่าเชื่อถือ	

จึงเรียนมาเพื่อทราบ

ลงชื่อ ผู้จัดทำ :

(นายสันต์ สิงห์ไกร) (Lead Implementer)

รับทราบ :

(นายแพทย์อัครเดช บุญเย็น)

ตำแหน่ง ผู้อำนวยการโรงพยาบาลปรางค์กู่ (CISO)