การประเมินและการจัดการความเสี่ยงทรัพย์สินและการบริการที่สำคัญ (Asset Risk Asessment and Risk Treatment]

ผู้พิจารณาประเมิน : นางสาว ธิดิยากร สิริพิเดช
ผู้บันทึก : นาย กำชัย เสาเวียง
วันที่ทำการประชุมความเสี่ยงพร้อมบันทึก : 18 มี.ค 69
สถานที่ : ศูนย์ข้อมูล กลุ่มงานประกันสุขภาพ
ที่อยู่ : 303 หมู่.7 ตำบลยางชุมน้อย อำเภอยางชุมน้อย จังหวัดศรีสะเกษ 33190
ระบบบริการที่สำคัญ : All application as HIS

ผลการประเมินความเสี่ยงทรัพย์สินและการบริการที่สำคัญ (เฉลี่ย) โดยรวมขององค์กร	12.6

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

ผลการประเมินความเสี่ยง(เฉลี่ย) โดยรวมขององค์กร หลังจัดการความเสี่ยง	1.0

สี	ความหมาย
แดง	เป็นความเสี่ยงขั้นวิกฤติ ต้องมีการดำเนินการโดยทันที
ส้ม	เป็นความเสี่ยงสูง ต้องมีการดำเนินการบางอย่างเพื่อลดความเสี่ยง
เหลือง	เป็นความเสี่ยงปานกลาง ต้องมีการติดตามและอาจมีมาตรการป้องกัน
เขียว	ต้องมีการติดตามเป็นระยะ แต่ยังไม่ต้องมีการดำเนินการใดๆเพิ่มเติม

	ชนิดของทรัพย์สิน (Type of Asset) / Cluster	ชื่อ (Asset Name)	คำอธิบาย (Description)	ระบบที่เกี่ยวข้อง (Concerned Application)	บริการที่สำคัญ/ฟังก์ชันที่สำคัญ (Critical Service / Function)	ระบุความเสี่ยงด้านไซเบอร์และช่องโหว่ ต่างๆ: ภัยคุกคาม (Threat)	ระบุความเสี่ยงด้านไซเบอร์และช่องโหว่ ต่างๆ: ช่องโหว่ (Vulner.)	กระทบต่อ: C	กระทบต่อ: I	กระทบต่อ: A	ความรุนแรงแต่ละด้าน: F	S	R	I	L	O	Risk Analysis A: โอกาสเกิด (Likelihood)	B: ความรุนแรง (Impact)	C = A*B: ระดับความเสี่ยง (Risk Level)	เจ้าของ (Asset Owner)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk Level) -ของแต่ละ Cluster
1	Application-Major	Himpro	แอปพลิเคชั่นจัดการข้อมูลโรงพยาบาล	ระบบการให้บริการ	ข้อมูลผู้ป่วยทั้งหมดและข้อมูลบุคลากรในโรงพยาบาล	X	X	x	x	x	-	-	x	x	x	x	3	5	15	ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ	15.0
2	HW-Servers	Server for Himpro	Server Ubuntu 22.04	ระบบการให้บริการ	ข้อมูลผู้ป่วยทั้งหมดและข้อมูลบุคลากรในโรงพยาบาล	X	X	x	x	x	-	-	x	x	x	x	3	5	15	ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ	12.5
3	HW-Switch	core switch	อุปกรณ์สวิชสำหรับเครือข่ายหลัก	ระบบความปลอดภัยเครือข่าย	เชื่อมต่อเครือข่ายองค์กร	X	X	x	x	x	-	-	x	x	x	x	2	5	10	ฝ่ายไอที	
4	HW-Router/Firewall	Cisoo router	อุปกรณ์เราเตอร์สำหรับเครือข่าย	ระบบเครือข่าย	เชื่อมต่อเครือข่ายองค์กร	X	X	x	x	x	-	-	x	x	x	x	2	5	10	ฝ่ายไอที	9.0
5	HW-Workstaion	Hp Server	Server สำหรับผู้จัดการ	ระบบจัดเก็บข้อมูล	การจัดการเอกสาร	X	X	x	x	x	-	-	x	x	x	x	2	4	8	ฝ่ายบริหาร	
6	Sw-other	Antivirus Software	ซอฟแวร์ป้องกันไวรัส	ระบบการความปลอดภัย	ป้องกันมัลแวร์	X	X	x	x	x	-	-	x	x	x	x	2	4	8	ฝ่ายไอที	14.0
7	HW-Router/Firewall	fortigate	ป้องกันเชื่อมต่อเครือข่าย	ระบบการความปลอดภัย	ตรวจสอบ log และจัดการเครือข่าย	X	X	x	x	x	-	-	x	x	x	x	4	5	20	ฝ่ายไอที	

	ตัวเลือกการตอบสนอง (Risk Treatment)	No.	แผนจัดการความเสี่ยง (Risk Treatment Plan)		คาดว่าดำเนินการแล้วเสร็จ (Expected finish date)	ผู้รับผิดชอบ (Responsibility)	สถานะความคืบหน้า (Progress Status)	ดำเนินการแล้วเสร็จ
1	Mitigate Risk	1	การป้องกัน: สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง.	ภายใน 30 ก.ย. 67		50%	18 ก.ย. 68
2	Mitigate Risk	1	การป้องกัน: สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง , เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR	ภายใน 30 ก.ย. 67		90%	18 ก.ย. 68
3	Mitigate Risk	1	การป้องกัน: ตั้งค่า Configure ของ switch ให้แน่นหนาและรัดกุม	การแก้ไข: ตรวจสอบ log และประเมินความเสียหาย ว่าเกิดจุดไหน เพื่อให้สถานะการเบาบางลง และ แก้ไข โดยการหามาเปลี่ยนใหม่โดยทันที	ภายใน 30 ก.ย. 67		90%	18 ก.ย. 68
4	Mitigate Risk	1	การป้องกัน: ตั้งค่าความซ้ำซ้อนด้วยเราเตอร์สำรอง (High Availability Setup), ใช้โปรโตคอลการกำหนดเส้นทางแบบไดนามิก (Dynamic Routing Protocols เช่น OSPF หรือ BGP), เฝ้าระวังอุปกรณ์ด้วยระบบ SNMP	การแก้ไข: เปลี่ยนเราเตอร์ด้วยอุปกรณ์สำรองที่กำหนดค่าไว้ล่วงหน้า, รีเซ็ตและโหลดการตั้งค่าคอนฟิกใหม่จากข้อมูลสำรอง, วิเคราะห์เส้นทางการเชื่อมต่อเครือข่ายที่ได้รับผลกระทบ.	ภายใน 30 ก.ย. 67		60%	18 ก.ย. 68
5	Mitigate Risk	1	การป้องกัน: ดำเนินการบำรุงรักษาเชิงป้องกัน, สำรองข้อมูลและตั้งค่า Configure ของระบบ	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง , เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR	ภายใน 30 ก.ย. 67		90%	18 ก.ย. 68
6	Mitigate Risk	1	การป้องกัน: Configure ของระบบให้รัดกุมและปลอดภัย	การแก้ไข: ใช้แผน DR, กู้คืนข้อมูลจากข้อมูลสำรอง.	ภายใน 30 ก.ย. 67		90%	18 ก.ย. 68
7	Mitigate Risk	1	การป้องกัน: ตรวจสอบ logs เพื่อวิเคราะห์ปัญหา , สำรองข้อมูลและตั้งค่า Configure ของระบบให้รัดกุมและปลอดภัย	การแก้ไข: เปลี่ยนไปใช้เซิร์ฟเวอร์สำรองตามแผน DR, ติดตั้ง Web Application Firewall เพื่อป้องกันภัยคุกคามออนไลน์, เฝ้าระวังการทำงานของเซิร์ฟเวอร์อย่างต่อเนื่อง.	ภายใน 30 ก.ย. 67		80%	18 ก.ย. 68

ความเสี่ยงที่คงเหลืออยู่ (Risk Residual)

	กระทบต่อ: C	กระทบต่อ: I	กระทบต่อ: A	ความรุนแรงแต่ละด้าน: F	S	R	I	L	O	โอกาสเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยงที่คงเหลือ (Risk Residual Level)	ดำเนินการเพิ่มเติมเพื่อลดความเสี่ยงให้น้อยลงอีก (Further actions to be taken to further minimize risk)
1	-	-	-	-	-	-	-	-	-	1	1	1	เฝ้าติดตามเป็นระยะ
2	-	-	-	-	-	-	-	-	-	1	1	1	เฝ้าติดตามเป็นระยะ
3	-	-	-	-	-	-	-	-	-	1	1	1	เฝ้าติดตามเป็นระยะ
4	-	-	-	-	-	-	-	-	-	1	1	1	เฝ้าติดตามเป็นระยะ
5	-	-	-	-	-	-	-	-	-	1	1	1	เฝ้าติดตามเป็นระยะ
6	-	-	-	-	-	-	-	-	-	1	1	1	เฝ้าติดตามเป็นระยะ
7	-	-	-	-	-	-	-	-	-	1	1	1	เฝ้าติดตามเป็นระยะ