

SUPALAI

แบบประเมินความเสี่ยงด้าน IT และ Cyber Security

สำหรับผู้รับจ้างภายนอก

ส่วนที่ 1 : รายละเอียดของผู้รับจ้างภายนอก		วันที่ประเมิน
ชื่อผู้รับจ้างภายนอก	
ประเภทของกลุ่มที่เข้าถึงข้อมูลของบริษัทฯ	<input type="checkbox"/> ผู้ให้บริการงานด้าน IT <input type="checkbox"/> ผู้ที่สามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าของบริษัท <input type="checkbox"/> ผู้ที่สามารถเข้าใช้ระบบงานภายในของบริษัทฯ ได้ เช่น ระบบ CM / CRM หรืออื่นๆ <input type="checkbox"/> อื่นๆ.....	
รายละเอียดงานที่ดำเนินการให้กับบริษัทฯ :		
.....		
(1) ชื่อผู้จัดทำ..... ตำแหน่ง.....		
โทรศัพท์..... E-mail.....		
(2) ชื่อผู้จัดทำ..... ตำแหน่ง.....		
โทรศัพท์..... E-mail.....		

ส่วนที่ 2 : สำหรับผู้รับจ้างภายนอกประเมินความเสี่ยงของธุรกิจตนเอง

กรุณาทำเครื่องหมาย / หรือกรอกข้อมูลคำตอบ และอธิบายรายละเอียดเพิ่มเติม (ถ้ามี)

สำหรับ บมจ.ศุภาลัย

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมิน ระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติม ประกอบการประเมิน
				1	2	3	4	5		
① นโยบาย/มาตรการรักษาความมั่นคงปลอดภัยด้าน IT (เพื่อให้มั่นใจได้ว่าบริษัทมีการบริหารจัดการความเสี่ยงด้าน IT อย่างเพียงพอและเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล)	1.1 มีกรรมการ หรือที่ปรึกษา อย่างน้อย 1 ท่าน ที่มีคุณสมบัติอย่างใดอย่างหนึ่ง ดังนี้ - จบการศึกษาในสาขา IT - มีความรู้หรือประสบการณ์ด้าน IT - มีประวัติการอบรมหรือการสัมมนา ด้าน IT ในปีล่าสุด เช่น <u>การอบรมเพื่อสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์</u> เป็นต้น									
	1.2 จัดให้มีนโยบาย/มาตรการรักษาความมั่นคงปลอดภัยด้าน IT (IT Policy / Procedure)									
	1.3 จัดให้มีแผนบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT Incident Response Plan) หากเกิดการบุกรุกโจมตีหรือการรั่วไหลของข้อมูลอย่างทันที									

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมิน ระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติม ประกอบการประเมิน
				1	2	3	4	5		
② การรักษาความปลอดภัยขั้นพื้นฐาน / แนวปฏิบัติเรื่องการจัดการความเสี่ยงทางไซเบอร์ (Cyber Security Procedure)	2.1 มีเครื่องมือป้องกันความเสี่ยงด้าน Cyber Security อะไรบ้าง เช่น <ul style="list-style-type: none"> ○ Antivirus ○ Firewall ○ VPN ○ การติดตั้ง Patch 									
	2.2 มีวิธีการควบคุมการเข้าถึงข้อมูลภายในของบริษัทอย่างไร (Data Access Procedure) ตัวอย่างเช่น <ul style="list-style-type: none"> ○ กำหนดหน้าที่ผู้อนุมัติการเข้าถึงข้อมูล (Access) ซึ่งต้องมีการอนุมัติก่อนการยินยอมให้มีการเข้าถึงข้อมูล ○ กำหนดรูปแบบ / วิธีการยืนยันตัวตน (Authentication) ○ กำหนดสิทธิ์ และมีการบันทึกการเข้าใช้งาน (Authentication, Authorization, and Accounting) 									

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมิน ระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติม ประกอบการประเมิน
				1	2	3	4	5		
③ ประวัติการถูกโจมตีทางไซเบอร์ หรือระบบเทคโนโลยีสารสนเทศอย่างมี นัยสำคัญ (Significant Cyber- Attack History)	3.1 ประวัติเกี่ยวกับการรั่วไหลของ ข้อมูล (Data Breach History) ของ บริษัท									
	3.2 ประวัติการถูกบุกรุกโจมตี โดย Computer Virus, Ransomware และ Malware <u>ในปีล่าสุด</u>	โปรดระบุ : <input type="checkbox"/> ไม่พบการบุกรุกโจมตี <input type="checkbox"/> ตรวจพบการบุกรุกโจมตี แต่สามารถป้องกัน ได้จากระบบตรวจจับของบริษัท เช่น Firewall, Antivirus, Gateway, Proxy <input type="checkbox"/> ตรวจพบ Computer Virus ที่อุปกรณ์ ผู้ใช้งาน เช่น ระบบ Antivirus เครื่อง คอมพิวเตอร์ <input type="checkbox"/> ตรวจพบ Computer Virus ที่เครื่องแม่ข่าย องค์กร (ไม่นับรวม Gateway) <input type="checkbox"/> ตรวจพบ Computer Virus แต่ไม่ทราบ/ไม่ สามารถระบุได้ว่ามาจากที่ใด <input type="checkbox"/> อื่นๆ (โปรดระบุ).....								

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมิน ระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติม ประกอบการประเมิน
				1	2	3	4	5		
	3.3 ประวัติการถูกร้องเรียน หรือแจ้งเหตุการณ์ เกี่ยวกับภัยไซเบอร์จากผู้มีส่วนได้เสีย <u>ในปีล่าสุด</u> เช่น โดเมนโฮสติงผู้ใช้งาน หรือข้อมูลส่วนบุคคลรั่วไหล เป็นต้น และมีแนวทางแก้ไขอย่างไร	โปรดระบุ : <input type="checkbox"/> ไม่เคยมีประวัติดังกล่าว <input type="checkbox"/> เคยมีประวัติ (โปรดระบุเหตุการณ์ และจำนวนครั้งที่ถูกร้องเรียนหรือแจ้งเหตุ <u>ในปีล่าสุด</u>)								
④ การใช้งาน Cloud หรือ Hosting Service	4.1 ลักษณะรูปแบบที่บริษัทใช้ Cloud Service หรือ Hosting Service	โปรดระบุ : <input type="checkbox"/> ไม่มีการใช้งาน (ข้ามไปข้อ 5) <input type="checkbox"/> Private Cloud หรือ Hosting Service หรือบริษัทในเครือ <input type="checkbox"/> Public Cloud, Hybrid <input type="checkbox"/> อื่นๆ (โปรดระบุ).....								
	4.2 จำนวนระบบงาน หรือ Application ที่สำคัญ ที่ใช้ในการประมวลผลหรือสนับสนุนกิจกรรมของบริษัทซึ่งอยู่บน Cloud หรือ Hosting Services <u>ซึ่งเมื่อหยุดชะงักแล้วส่งผลกระทบต่อ</u> การดำเนินธุรกิจ	โปรดระบุจำนวนระบบงานหรือ Application ที่สำคัญ ระบบที่(1)..... ระบบที่(2)..... โปรดระบุชื่อ Cloud Provider / Hosting Service ที่ใช้บริการอยู่								

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมิน ระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติม ประกอบการประเมิน
				1	2	3	4	5		
⑤ บริษัทที่มีผู้ให้บริการภายนอกที่สามารถเข้าถึงเครือข่าย/ ระบบงานภายในบริษัทได้ (Third Parties, Vendor, Outsourcer, Sub-Contractor)	5.1 จัดให้มีสัญญาจ้างงานระบุเงื่อนไขหรือข้อตกลงครอบคลุมหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยเกี่ยวกับ IT Policy หรือไม่ เช่น มีการระบุความจำเป็นในการทำสัญญาไม่เปิดเผยความลับระหว่างองค์กรกับผู้รับจ้างภายนอก									
	5.2 จำนวนบริษัทผู้ให้บริการภายนอกที่สามารถเข้าถึงเครือข่ายภายในของบริษัทได้ (Third Parties, Vendor, Outsourcer, Sub-Contractor)	โปรดระบุจำนวนผู้ให้บริการภายนอกและประเภทบริการที่ใช้ ○ จำนวนผู้ให้บริการราย ○ ประเภทบริการ รายที่ 1 รายที่ 2 รายที่ 3..... รายที่ 4.....								
	5.3 วิธีการหรือช่องทางที่ผู้ให้บริการภายนอกเข้าถึงเครือข่าย หรือทรัพยากรภายในของบริษัท	โปรดระบุ <input type="checkbox"/> ผู้ให้บริการต้องเข้ามา Onsite เท่านั้น <input type="checkbox"/> ผู้ให้บริการสามารถใช้ช่องทางเฉพาะ เช่น Leased Line หรือ VPN เข้ามาให้บริการ <input type="checkbox"/> อื่นๆ								

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมิน ระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติม ประกอบการประเมิน
				1	2	3	4	5		
	5.4 แนวทางการบริหารจัดการ Sub-Contract (การจ้างช่วง) เช่น ○ การจ้างผู้ประกอบการธุรกิจ เมื่อมีการใช้งานหรือเปลี่ยนแปลง Sub-Contract ○ ความรับผิดชอบของผู้ให้บริการ ในกรณีที่มีการใช้งาน Sub-Contract									
⑥ การรับประกันความเสียหาย	6.1 บริษัทได้ทำประกันภัยกรณีเกิดความเสียหายจากภัยคุกคามทางไซเบอร์ไว้ครอบคลุมหรือไม่									
⑦ การอบรม/สร้างความตระหนัก (Training / Awareness)	7.1 การจัดทำแผนการอบรมเพื่อสร้างความตระหนักและให้ความรู้แก่พนักงาน ลูกจ้าง ผู้ให้บริการภายนอก หรือผู้ที่เกี่ยวข้องอื่นๆ เช่น การอบรมด้านนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยด้าน IT อย่างสม่ำเสมอ									

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมิน ระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติม ประกอบการประเมิน
				1	2	3	4	5		
⑧ การจัดให้มีผลการตรวจสอบด้าน IT โดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล	8.1 จัดให้มีผู้ตรวจสอบการดำเนินงาน และการควบคุมภายในด้าน IT จากหน่วยงานภายนอก	การตรวจสอบตามมาตรฐาน <input type="checkbox"/> SSAE 18 (SOC 2 Type 2 Report) <input type="checkbox"/> PCI-DSS Attestation of Compliance (AOC) <input type="checkbox"/> อื่นๆ (โปรดระบุ)								
รวมคะแนนทั้งสิ้น										

สรุปผลการประเมินความเสี่ยงด้าน IT และ Cyber Security
 สำหรับผู้รับจ้างภายนอก

.....

.....

.....