SUPALAI

แบบประเมินความเสี่ยงด้าน IT และ Cyber Security

สำหรับผู้รับจ้างภายนอก

<u>ส่วนที่ 1</u> : รายละเอียดของผู้รับจ้างภายนอก	**วันที่ประเมิน** .....
ชื่อผู้รับจ้างภายนอก	....
ประเภทของกลุ่มที่เข้าถึงข้อมูลของบริษัทฯ	☐ ผู้ให้บริการงานด้าน IT ☐ ผู้ที่สามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าของบริษัท ☐ ผู้ที่สามารถเข้าใช้ระบบงานภายในของบริษัทฯ ได้ เช่น ระบบ CM / CRM หรืออื่นๆ ☐ 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					คะแนนประเมินระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติมประกอบการประเมิน
				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 - มีประวัติการอบรมหรือการสัมมนาด้าน IT ในปีล่าสุด เช่น <u>การอบรมเพื่อสร้างความตระหนักด้านความปลอดภัยทางไซเบอร์</u> เป็นต้น								
	1.2 จัดให้มีนโยบาย/มาตรการรักษาความมั่นคงปลอดภัยด้าน IT (IT Policy / Procedure)									
	1.3 จัดให้มีแผนบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT Incident Response Plan) หากเกิดการบุกรุกโจมตีหรือการรั่วไหลของข้อมูลอย่างทันท่วงที									

สำหรับ บมจ.ศุภาลัย

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมินระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติมประกอบการประเมิน
				1	2	3	4	5		
② การรักษาความปลอดภัยขั้นพื้นฐาน / แนวปฏิบัติเรื่องการจัดการความเสี่ยงทางไซเบอร์ (Cyber Security Procedure)	2.1 มีเครื่องมือป้องกันความเสี่ยงด้าน Cyber Security อะไรบ้าง เช่น O Antivirus O Firewall O VPN O การติดตั้ง Patch									
	2.2 มีวิธีการควบคุมการเข้าถึงข้อมูลภายในของบริษัทอย่างไร (Data Access Procedure) ตัวอย่างเช่น O กำหนดหน้าที่ผู้อนุมัติการเข้าถึงข้อมูล (Access) ซึ่งต้องมีการอนุมัติก่อนการยินยอมให้มีการเข้าถึงข้อมูล O กำหนดรูปแบบ / วิธีการยืนยันตัวตน (Authentication) O กำหนดสิทธิ์ และมีการบันทึกการเข้าใช้งาน (Authentication, Authorization, and Accounting)									

สำหรับ บมจ.ศุภาลัย

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมินระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติมประกอบการประเมิน
				1	2	3	4	5		
③ ประวัติการถูกโจมตีทางไซเบอร์หรือระบบเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ (Significant Cyber-Attack History)	3.1 ประวัติเกี่ยวกับการรั่วไหลของข้อมูล (Data Breach History) ของบริษัท									
	3.2 ประวัติการถูกบุกรุกโจมตี โดย Computer Virus, Ransomware และ Malware ในปีล่าสุด	โปรดระบุ : ☐ ไม่พบการบุกรุกโจมตี ☐ ตรวจพบการบุกรุกโจมตี แต่สามารถป้องกันได้จากระบบตรวจจับของบริษัท เช่น Firewall, Antivirus, Gateway, Proxy ☐ ตรวจพบ Computer Virus ที่อุปกรณ์ผู้ใช้งาน เช่น ระบบ Antivirus เครื่องคอมพิวเตอร์ ☐ ตรวจพบ Computer Virus ที่เครื่องแม่ข่ายองค์กร (ไม่นับรวม Gateway) ☐ ตรวจพบ Computer Virus แต่ไม่ทราบ/ไม่สามารถระบุได้ว่ามาจากที่ใด ☐ อื่นๆ (โปรดระบุ).....								

สำหรับ บมจ.ศุภาลัย

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมินระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติมประกอบการประเมิน
				1	2	3	4	5		
	3.3 ประวัติการถูกร้องเรียน หรือแจ้งเหตุการณ์ เกี่ยวกับภัยไซเบอร์จากผู้มีส่วนได้เสียในปีล่าสุด เช่น โดนขโมยบัญชีผู้ใช้งาน หรือข้อมูลส่วนบุคคลรั่วไหล เป็นต้น และมีแนวทางแก้ไขอย่างไร	โปรดระบุ : ☐ ไม่เคยมีประวัติดังกล่าว ☐ เคยมีประวัติ (โปรดระบุเหตุการ และจำนวนครั้งที่ถูกร้องเรียนหรือแจ้งเหตุ ในปีล่าสุด)								
④ **การใช้งาน Cloud หรือ Hosting Service**	4.1 ลักษณะรูปแบบที่บริษัทใช้ Cloud Service หรือ Hosting Service	โปรดระบุ : ☐ ไม่มีการใช้งาน (ข้ามไปข้อ 5) ☐ Private Cloud หรือ Hosting Service หรือบริษัทในเครือ ☐ Public Cloud, Hybrid ☐ อื่นๆ (โปรดระบุ).....								
	4.2 จำนวนระบบงาน หรือ Application ที่สำคัญ ที่ใช้ในการประมวลผลหรือสนับสนุนกิจกรรมของบริษัทซึ่งอยู่บน Cloud หรือ Hosting Services ซึ่งเมื่อหยุดชะงักแล้วส่งผลกระทบต่อการดำเนินธุรกิจ	โปรดระบุจำนวนระบบงานหรือ Application ที่สำคัญ ระบบที่(1)..... ระบบที่(2)..... โปรดระบุชื่อ Cloud Provider / Hosting Service ที่ใช้บริการอยู่								

สำหรับ บมจ.ศุภาลัย

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมินระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติมประกอบการประเมิน
				1	2	3	4	5		
⑤ บริษัทมีผู้ให้บริการภายนอกที่สามารถเข้าถึงเครือข่าย/ ระบบงานภายในบริษัทได้ (Third Parties, Vendor, Outsourcer, Sub-Contractor)	5.1 จัดให้มีสัญญาจ้างงานระบุเงื่อนไขหรือข้อตกลงครอบคลุมหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยที่เกี่ยวกับ IT Policy หรือไม่ เช่น มีการระบุความจำเป็นในการทำสัญญาไม่เปิดเผยความลับระหว่างองค์กรกับผู้รับจ้างภายนอก									
	5.2 จำนวนบริษัทผู้ให้บริการภายนอกที่สามารถเข้าถึงเครือข่ายภายในของบริษัทได้ (Third Parties, Vendor, Outsourcer, Sub-Contractor)	โปรดระบุจำนวนผู้ให้บริการภายนอกและประเภทบริการที่ใช้ ○ จำนวนผู้ให้บริการ .....ราย ○ ประเภทบริการ รายที่ 1 ..... รายที่ 2 ..... รายที่ 3..... รายที่ 4.....									
	5.3 วิธีการหรือช่องทางที่ผู้ให้บริการภายนอกเข้าถึงเครือข่าย หรือทรัพยากรภายในของบริษัท	โปรดระบุ ☐ ผู้ให้บริการต้องเข้ามา Onsite เท่านั้น ☐ ผู้ให้บริการสามารถใช้ช่องทางเฉพาะ เช่น Leased Line หรือ VPN เข้ามาให้บริการ ☐ อื่นๆ									

สำหรับ บมจ.ศุภาลัย

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมินระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติมประกอบการประเมิน
				1	2	3	4	5		
	5.4 แนวทางการบริหารจัดการ Sub-Contract (การจ้างช่วง) เช่น ○ การแจ้งผู้ประกอบธุรกิจ เมื่อมีการใช้งานหรือเปลี่ยนแปลง Sub-Contract ○ ความรับผิดชอบของผู้ให้บริการในกรณีที่มีการใช้งาน Sub-Contract									
⑥ **การรับประกันความเสียหาย**	6.1 บริษัทได้ทำประกันภัยกรณีเกิดความเสียหายจากภัยคุกคามทางไซเบอร์ไว้ครอบคลุมหรือไม่									
⑦ **การอบรม/สร้างความตระหนัก (Training / Awareness)**	7.1 การจัดทำแผนการอบรมเพื่อสร้างความตระหนักและให้ความรู้แก่พนักงาน ลูกจ้าง ผู้ให้บริการภายนอก หรือผู้ที่เกี่ยวข้องอื่นๆ เช่น การอบรมด้านนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยด้าน IT อย่างสม่ำเสมอ									

สำหรับ บมจ.ศุภาลัย

หัวข้อการประเมิน	รายละเอียดการประเมิน	คำตอบแบบประเมิน และรายละเอียดประกอบการตอบ	ค่าน้ำหนัก	ระดับความเสี่ยง					คะแนนประเมินระดับความเสี่ยง (ค่าน้ำหนัก x ระดับความเสี่ยง)	ความคิดเห็นเพิ่มเติมประกอบการประเมิน
				1	2	3	4	5		
⑧ **การจัดให้มีผลการตรวจสอบด้าน IT โดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล**	8.1 จัดให้มีผู้ตรวจสอบการดำเนินงานและการควบคุมภายในด้าน IT จากหน่วยงานภายนอก	การตรวจสอบตามมาตรฐาน ☐ SSAE 18 (SOC 2 Type 2 Report) ☐ PCI-DSS Attestation of Compliance (AOC) ☐ อื่นๆ (โปรดระบุ)								
		รวมคะแนนทั้งสิ้น								

สรุปผลการประเมินความเสี่ยงด้าน IT และ Cyber Security สำหรับผู้รับจ้างภายนอก

.....

.....

.....