นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของแผนกสารสนเทศ บริษัท เอเชียนน้ำมันปาล์ม จำกัด (มหาชน) (“บริษัท”) จัดทำขึ้นเพื่อเป็นกรอบแนวทางการดำเนินงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้บรรลุผลตามนโยบายของบริษัท เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือ ความสูญเสียได้ทั้งทางตรงและทางอ้อม บริษัทต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อเลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นได้

บทสรุปผู้บริหาร

ฝ่ายเทคโนโลยีสารสนเทศ บริษัท เอเชียนน้ำมันปาล์ม จำกัด (มหาชน) (“บริษัท”) ตระหนักถึงความสำคัญของการบริหารความเสี่ยง จึงได้จัดทำแผนบริหารความเสี่ยง (Enterprise Risk Management Policy) ขึ้น เพื่อเป็นกรอบแนวทางการพัฒนาระบบการบริหารความเสี่ยงให้มีคุณภาพและมีมาตรฐาน โดยคำนึงถึงความสอดคล้องกับนโยบายและเป้าหมายการดำเนินงานของบริษัท เอเชียนน้ำมันปาล์ม จำกัด (มหาชน) ทั้งนี้เพื่อให้แผนบริหารความเสี่ยงมีประสิทธิภาพและมีประสิทธิผลในการบริหารความเสี่ยง ตลอดจนมีความมั่นใจว่า กระบวนการทำงานได้ปฏิบัติตามกฎ ระเบียบ ประกาศ คำสั่ง และมาตรฐานที่ดี เพื่อบรรลุถึงผลตามเป้าหมายของบริษัทที่เกิดจากการมีส่วนร่วม ของหน่วยงานและบุคลากรทุกระดับในบริษัท

หลักการและวัตถุประสงค์

บริษัท เอเชียนน้ำมันปาล์ม จำกัด (มหาชน) ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อเพิ่มประสิทธิภาพการดำเนินงานและให้บริการแผนกต่างๆ ให้ได้รับความสะดวกมากขึ้น ขณะเดียวกัน ระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการปรับเปลี่ยนกลยุทธ์ โครงสร้าง และทรัพยากรภายในสำนักงาน รวมถึงปัจจัยภายนอก อาทิ เหตุการณ์ไม่สงบทางการเมือง ภัยธรรมชาติ เป็นต้น อาจส่งผลกระทบกับการดำเนินงานของบริษัททำให้ไม่เป็นไปตามเป้าหมายในแผนการดำเนินงาน ซึ่งจะก่อให้เกิดความเสี่ยงต่อบริษัทโดยรวม แผนบริหารความเสี่ยง (Enterprise Risk Management Policy) จัดทำขึ้นเพื่อวัตถุประสงค์ ดังนี้

1. ใช้เป็นแนวทางให้ บุคลากร ทั้งองค์กร เป็นส่วนนึงของการพัฒนากระบวนการบริหารความเสี่ยงเพื่อสนับสนุนการดำเนินงานของบริษัท เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนการดำเนินงาน
2. เพื่อให้แผนกมีกรอบดำเนินงานเพื่อตอบสนองต่อเหตุการณ์ที่อาจส่งผลให้เกิดความเสี่ยงทุกด้านได้อย่างเป็นระบบและมีมาตรฐาน
3. เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม ทำให้ต้องคำนึงถึงสิ่งที่อาจมีผลกระทบต่อการดำเนินงานพร้อมเตรียมมาตรการรองรับเพื่อจัดการความเสี่ยงไว้อย่างเป็น ระบบ ทำให้การจัดการความเสี่ยงประสบความสำเร็จสามารถลดความสูญเสียที่อาจจะเกิดขึ้นได้อย่างมี ประสิทธิภาพ

กระบวนการจัดการบริหารความเสี่ยง 5 ขั้นตอน ได้แก่

1) ระบุปัจจัยเสี่ยง
2) วิเคราะห์ความเสี่ยง
3) กำหนดมาตรการจัดการความเสี่ยง
4) ติดตาม รายงาน ประเมินผล
5) ทบทวนการ บริหารความเสี่ยง

โดยสามารถระบุปัจจัยความเสี่ยงได้เป็น 4 ด้าน ดังนี้

1) ความเสี่ยงด้านความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ
2) ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ
3) ความเสี่ยงด้านความมั่นคงและปลอดภัยของระบบฐานข้อมูล
4) ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ

โดยได้วิเคราะห์และกำหนดมาตรการจัดการความเสี่ยง กำหนดเป็นแนวทางการควบคุม ดังนี้

1) จัดทำการสำรองฐานข้อมูลสารสนเทศ รวมทั้งจัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถ ทำงานได้
2) ดำเนินการทดสอบการกู้คืน ฐานข้อมูลสารสนเทศ และระบบสารสนเทศ
3) ตรวจสอบระบบเครือข่ายสื่อสารหลัก ระบบสำรองไฟฟ้า (UPS) ระบบป้องกันการบุกรุก ระบบ เครือข่าย(Firewall)
4) ติดตั้งโปรแกรมป้องกันไวรัสและทำการปรับปรุง ฐานข้อมูล Anti-Virus ให้ทันสมัย
5) ตรวจสอบระบบรักษาความปลอดภัยในการเข้า-ออก ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย
6) ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง
7) กำหนดสิทธิ์ในการเข้าถึงข้อมูลระหว่างผู้ใช้งาน และผู้ดูแลระบบเทคโนโลยีสารสนเทศ

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ การกำหนดนโยบาย โครงสร้าง และกระบวนการ เพื่อให้คณะกรรมการ ผู้บริหารและบุคลากรขององค์กรนำไปปฏิบัติในการกำหนดกลยุทธ์และปฏิบัติงานทั่วทั้งองค์กร เพื่อให้เกิดความเชื่อมั่นในระดับหนึ่งว่าการดำเนินการในองค์กร จะบรรลุตามวัตถุประสงค์ที่กำหนดไว้

1. ระบุปัจจัยเสี่ยงและผลกระทบด้านต่างๆที่จะเกิดขึ้น

ที่มาปัจจัยความเสี่ยง	ผลกระทบด้านต่างๆ	
	ระบบ/อุปกรณ์	ผู้ที่ได้รับผลกระทบ
1. ความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ		
1.1 ระบบงานที่ให้บริการ/ระบบฐานข้อมูล	- ทำให้ระบบสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักหรือหยุดทำงาน - ข้อมูลเสียหาย	ผู้ใช้งานระบบสารสนเทศดำเนินงานล่าช้า
1.2 อุปกรณ์บันทึกข้อมูลชำรุด (Hard disk)	- ทำให้การปฏิบัติงานด้านสารสนเทศหยุดชะงัก ข้อมูลชำรุดสูญหาย	ผู้ใช้งานระบบสารสนเทศดำเนินงานล่าช้า
2. ด้านภัยพิบัติระบบสารสนเทศ		
2.1 ไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	- เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์และฐานข้อมูลถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก	ผู้ใช้งานไม่สามารถใช้งานระบบได้
2.2 ระบบเครือข่ายขัดข้อง	- ระบบประมวลผลใช้งานไม่ได้ เกิดการชะงัก ไม่สามารถใช้ระบบอย่างมีประสิทธิภาพ	ผู้ใช้งานไม่สามารถใช้งานระบบได้
2.3 สถานการณ์ไม่สงบเรียบร้อยในบ้านเมือง การประชุมประท้วง การจลาจล การก่อการร้าย		เกิดความรุนแรงทำให้ผู้ใช้งานไม่สามารถปฏิบัติงานได้ตามปกติ
3. ด้านความมั่นคงและปลอดภัยของระบบฐานข้อมูล		
3.1 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ทำให้การปฏิบัติงานด้านสารสนเทศหยุดชะงัก - ทำความเสียหายระยะยาวให้แก่อุปกรณ์คอมพิวเตอร์	ผู้ใช้งานไม่สามารถใช้งานระบบได้
3.2 ถูกเจาะหรือลักลอบเข้าระบบ	- การทำงานของระบบถูกแก้ไขเปลี่ยนแปลง ทำลายหรือแก้ไขสิทธิ์ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบได้	- บุคคลที่มีหน้าที่รับผิดชอบไม่สามารถเข้าใช้งานระบบได้ ทำให้ไม่สามารถปฏิบัติงานได้ตามปกติ
3.3 ถูกเจาะหรือลักลอบระบบฐานข้อมูล	- ข้อมูลการทำงานเสียหายส่งผลให้มีการประมวลผลไม่ครบถ้วน - ข้อมูลมีการแก้ไขเปลี่ยนแปลง	- ข้อมูลรั่วไหล อาจนำไปสู่การแสวงหาผลกำไรโดยมิชอบ - ข้อมูลไม่ถูกต้อง

ที่มาปัจจัยความเสี่ยง	ผลกระทบด้านต่างๆ	
	ระบบ/อุปกรณ์	ผู้ที่ได้รับผลกระทบ
3.4 ความเสียหายจากไวรัสคอมพิวเตอร์	- ไวรัสรบกวนการทำงานของระบบ - ปริมาณข้อมูลมีมากขึ้นผิดปกติ - มีการส่งข้อมูลในเครือข่ายเป็นจำนวนมาก	- ผู้ใช้งานระบบสารสนเทศดำเนินงานล่าช้า
4. ด้านสิทธิ์การใช้งานของผู้ใช้งานในแต่ละระดับ		
4.1 การลักลอบเข้าห้อง Server	- บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงห้อง Server - ขโมยข้อมูลอุปกรณ์	- ข้อมูลรั่วไหลสูญหาย - อุปกรณ์สูญหาย
4.2 การเข้าใช้ระบบโดยไม่ได้รับอนุญาต	- ข้อมูลเปลี่ยนแปลงแก้ไขได้	- บุคลากรที่ไม่มีส่วนเกี่ยวข้องล่วงรู้ข้อมูลและนำไปแสวงหาผลประโยชน์โดยมิชอบ - ผู้ใช้ที่เกี่ยวข้องอาจถูกเปลี่ยนเปลงสิทธิ์การเข้าถึง - ข้อมูลมีการเปลี่ยนแปลง

2. ประเมินความเสี่ยง

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	ระดับความเสี่ยง
1. ความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ	1.1 ระบบงานที่ให้บริการ/ระบบฐานข้อมูล	2	3	ปานกลาง
	1.2 อุปกรณ์บันทึกข้อมูลชำรุด (Hard disk)	2	4	ปานกลาง
2. ด้านภัยพิบัติระบบสารสนเทศ	2.1 ไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	1	5	ปานกลาง
	2.2 ระบบเครือข่ายขัดข้อง	2	5	ปานกลาง
	2.3 สถานการณ์ไม่สงบเรียบร้อยในบ้านเมือง การประชุมประท้วง การจลาจล การก่อการร้าย	1	5	ปานกลาง
3. ด้านความมั่นคงและปลอดภัยของระบบฐานข้อมูล	3.1 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	1	4	ปานกลาง
	3.2 ถูกเจาะหรือลักลอบเข้าระบบ	2	4	ปานกลาง
	3.3 ถูกเจาะหรือลักลอบระบบฐานข้อมูล	2	4	ปานกลาง

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	ระดับความเสี่ยง
	3.4 ความเสียหายจากไวรัสคอมพิวเตอร์	3	4	สูง
4. ด้านสิทธิ์การใช้งานของผู้ใช้งานในแต่ละระดับ	4.1 การลักลอบเข้าห้อง Server	1	4	ปานกลาง
	4.2 การเข้าใช้ระบบโดยไม่ได้รับอนุญาต	1	4	ปานกลาง

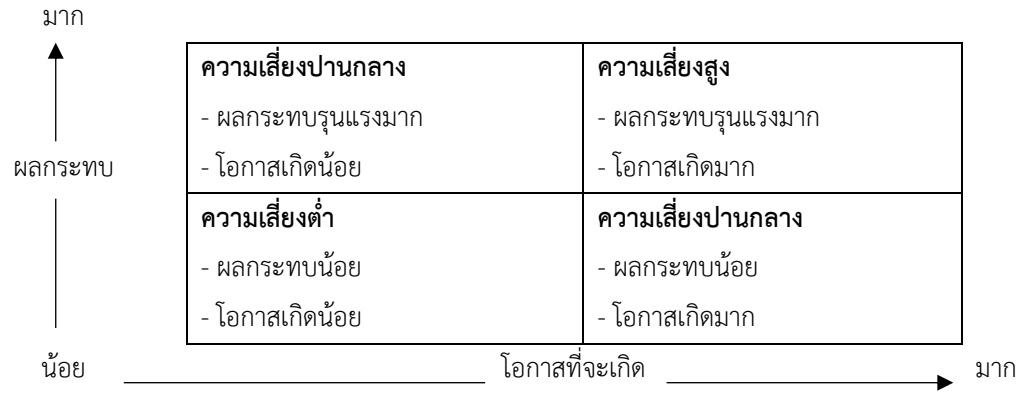
หมายเหตุ : เกณฑ์การให้คะแนนโอกาสที่จะเกิดและผลกระทบจากต่ำไปสูงคือ 1 ถึง 5

1 = น้อยที่สุด / 2 = น้อย / 3 = ปานกลาง / 4 = มาก / 5 = มากที่สุด

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
5	สูงมาก	5 ครั้ง/ปี
4	สูง	4 ครั้ง/ปี
3	ปานกลาง	3 ครั้ง/ปี
2	น้อย	2 ครั้ง/ปี
1	น้อยมาก	ไม่เกิน 1 ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	**ผลกระทบ**	**คำอธิบาย**
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบ ความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

แผนภูมิความเสี่ยง
การวัดระดับความเสี่ยง



3. การจัดการความเสี่ยง

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	แนวทางการควบคุม
1. ความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ	1.1 ระบบงานที่ให้บริการ/ระบบฐานข้อมูล	- จัดทำการสำรอง ฐานข้อมูลสารสนเทศ - ทดสอบการกู้คืน ฐานข้อมูลสารสนเทศและระบบสารสนเทศ
	1.2 อุปกรณ์บันทึกข้อมูลชำรุด (Hard disk)	- จัดทำการสำรอง ฐานข้อมูลสารสนเทศ - ทดสอบการกู้คืน ฐานข้อมูลสารสนเทศและระบบสารสนเทศ
2. ด้านภัยพิบัติระบบสารสนเทศ	2.1 ไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	- ตรวจสอบความ พร้อมใช้งานของอุปกรณ์ ดับเพลิง -จัดหาระบบสำรอง เพื่อให้ระบบสารสนเทศ สามารถทำงานได้ -สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ใน สถานที่อื่นอีกหนึ่งชุด
	2.2 ระบบเครือข่ายขัดข้อง	- ตรวจสอบระบบ เครือข่ายสื่อสารหลัก - มีเครือข่ายสำรองอีก 1 ชุด
	2.3 สถานการณ์ไม่สงบเรียบร้อยในบ้านเมือง การประชุมประท้วง การจลาจล การก่อการร้าย	- จัดหาระบบสำรอง เพื่อให้ระบบสารสนเทศ สามารถทำงานได้
	3.1 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ตรวจสอบระบบสำรอง ไฟฟ้า (UPS)

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	แนวทางการควบคุม
3. ด้านความมั่นคงและปลอดภัยของระบบฐานข้อมูล	3.2 ถูกเจาะหรือลักลอบเข้าระบบ	- ตรวจสอบระบบ ป้องกันการบุกรุกระบบเครือข่าย (Firewall)
	3.3 ถูกเจาะหรือลักลอบระบบฐานข้อมูล	- ตรวจสอบระบบ ป้องกันการบุกรุกระบบเครือข่าย (Firewall)
	3.4 ความเสียหายจากไวรัสคอมพิวเตอร์	- มีโปรแกรมป้องกัน ไวรัสและทำการปรับปรุง ฐานข้อมูล Anti-Virus ให้ทันสมัย
4. ด้านสิทธิ์การใช้งานของผู้ใช้งานในแต่ละระดับ	4.1 การลักลอบเข้าห้อง Server	- ตรวจสอบระบบรักษา ความปลอดภัยในการ เข้า-ออก ห้อง Server
	4.2 การเข้าใช้ระบบโดยไม่ได้รับอนุญาต	- กำหนดสิทธิ์ในการ เข้าถึงข้อมูลระหว่าง ผู้ใช้งาน และผู้ดูแลระบบ

4. รายการกิจกรรมในการจัดการความเสี่ยง

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมในการควบคุม	กำหนดการดำเนินงาน
1. ความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ	1.1 ระบบงานที่ให้บริการ/ระบบฐานข้อมูล 1.2 อุปกรณ์บันทึกข้อมูลชำรุด (Hard disk)	- มีการทำสำรองข้อมูลทั้งหมดที่ เครื่องแม่ข่ายทั้งหมดทุกวันโดยสำรองข้อมูลที่เพิ่มเติมแต่ละวัน สำรองข้อมูลที่ nas storage และ Cloud	- จัดทำการสำรองข้อมูลแบบอัตโนมัติทุกวัน ทุกสัปดาห์ - ทดสอบการกู้คืน (Data Recovery) ทุก 1 ปี
2. ด้านภัยพิบัติระบบสารสนเทศ	2.1 ไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง และ สัญญาณเตือนภัยให้อยู่ในสถานะ พร้อมใช้งาน - จัดทำแผนรองรับภาวะฉุกเฉินและภัยธรรมชาติ และมี การซักซ้อมแผน ปีละ 1 ครั้ง	- ทุก 3 เดือน - ทุก 1 ปี
	2.2 ระบบเครือข่ายขัดข้อง	ตรวจสอบระบบเครือข่ายสื่อสารหลัก	เดือนละ 1 ครั้ง

ประเภทความเสี่ยง	ปัจจัยเสี่ยง	กิจกรรมในการควบคุม	กำหนดการดำเนินงาน
3. ด้านความมั่นคงและปลอดภัยของระบบฐานข้อมูล	3.1 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	ตรวจสอบสถานะระบบสำรองไฟ อุปกรณ์ UPS	- ทุก 3 เดือน
	3.2 ถูกเจาะหรือลักลอบเข้าระบบ	ตรวจสอบสถานะระบบป้องกันการบุกรุก (Firewall)	- ทุก 3 เดือน
	3.3 ถูกเจาะหรือลักลอบระบบฐานข้อมูล	ตรวจสอบสถานะระบบป้องกันการบุกรุก (Firewall)	เดือนละ 1 ครั้ง
	3.4 ความเสียหายจากไวรัสคอมพิวเตอร์	ตรวจสอบสถานะระบบป้องกันการบุกรุก (Firewall)	เดือนละ 4 ครั้ง
4. ด้านสิทธิ์การใช้งานของผู้ใช้งานในแต่ละระดับ	4.1 การลักลอบเข้าห้อง Server	- ตรวจสอบระบบรักษาความ ปลอดภัยเครื่องสแกนลายนิ้วมือ เพื่อจะเข้า-ออกห้องควบคุม ระบบ	- ทุก 3 เดือน
	4.2 การเข้าใช้ระบบโดยไม่ได้รับอนุญาต	กำหนดสิทธิ์ในการเข้าถึงข้อมูล ผู้ใช้และผู้ดูแลระบบสารถสนเทศ - กำหนดสิทธิ์เมื่อเข้ามาเป็นพนักงานใหม่ - ปรับปรุงข้อมูลเมื่อมีการโยกย้ายตำแหน่ง หรือลาออก	กระทำเมื่อ พนักงานเริ่มงาน โยกย้าย ลาออก

บริษัทได้ดำเนินการวางแผนบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ดังนี้

1) มีการสำรองข้อมูลและกู้คืนจากความเสียหาย (Backup and Recovery)
2) มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน หรือภัยพิบัติที่อาจเกิดกับระบบ สารสนเทศ (IT Contingency Plan)
3) มีการตรวจสอบควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย
4) มีระบบการรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Antivirus , ระบบสำรองไฟฟ้า, ระบบ Firewall, ระบบ Backup
5) มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access rights)
6) มีการบันทึกเพื่อตรวจสอบ (audit logs) เช่น ให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์ แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบ ป้องกันการบุกรุก โดยการบันทึกการเข้าออกระบบ (login-logout log)

การประเมินสถานการณ์ความเสี่ยงแนวทางในการดำเนินการเพื่อลดความเสี่ยง

จากการตรวจสอบความเสี่ยงต่างๆ พบว่ามีความเสี่ยง ที่อาจเป็นอันตรายและมีแนวทางดำเนินการ ดังนี้

1) เกิดจากเจ้าหน้าที่หรือบุคลากร (Human error) ขาดความรู้ความเข้าใจใน เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเสริมสร้าง ความรู้ ความเข้าใจ ในการใช้ระบบ จึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรมให้มีความรู้ ความเข้าใจ ในด้าน Hardware และ Software เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด
2) เกิดจากไวรัสคอมพิวเตอร์ สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือ ระบบเครือข่ายคอมพิวเตอร์ มีการดำเนินการดังนี้
   2.1. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสเสมอ
   2.2. ติดตั้ง firewall ทำหน้าที่ป้องกันการบุกรุกจากภายนอก
   2.3. ใช้ซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์ ไม่ติดตั้งหรือใช้งานซอฟท์แวร์อื่นใดที่ไม่มีลิขสิทธิ์
   2.4. ไม่ให้ผู้ใช้งานดาวน์โหลดซอฟท์แวร์โดยไม่ได้รับอนุญาต
3) เกิดจากระบบไฟฟ้าขัดข้อง โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่าย กระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง มีการดำเนินการดังนี้
   3.1 ติดตั้งเครื่องสำรองไฟฟ้า (UPS) เพื่อป้องกันความเสียหายที่ อาจจะเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งจะมีระยะเวลาในการสำรองไฟฟ้าได้ประมาณ 20 - 30 นาที

3.2 เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานคอมพิวเตอร์ และบำรุงรักษาเครื่อง สำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

3.3 เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลทันที และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์

4) เกิดความเสียหายจากเพลิงไหม้ ได้ติดตั้งระบบดับเพลิงอัตโนมัติ (Fire Suppression System) ทั้งเหนือพื้นยกและบริเวณใต้พื้นยกโดยใช้ระบบ Inert Gas System ชนิด IG-55 ซึ่งเป็นสารสะอาดดับเพลิงที่ไม่ เป็นอันตรายต่อสิ่งมีชีวิตและสิ่งแวดล้อม ไม่ทำความเสียหายต่ออุปกรณ์คอมพิวเตอร์, อิเล็กทรอนิกส์ และได้ติดตั้งระบบตรวจจับควันความไวสูง (High Sensitivity Smoke Detect) บริเวณ Return air ของเครื่องปรับอากาศ ซึ่งจะมีการดำเนินการดังนี้

4.1 กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดป้ายเตือนต่างๆ

4.2 อบรมขั้นต้นสำหรับพนักงานทุกคนในแผนป้องกันและระงับอัคคีภัยและมีการซ้อม ดับเพลิงหนีไฟ ให้มีการซักซ้อมอย่างน้อยปีละ 1 ครั้ง

4.3 จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์แม่ข่ายเพื่อ ประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

5) เกิดจากการบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล มีการดำเนินการดังนี้

5.1 สแกนหาจุดอ่อนและอัพเดทโปรแกรม เพื่อปิดกั้นช่องโหว่และจุดอ่อน

5.2 ติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

5.3 ไม่ให้ผู้ใช้ นำอุปกรณ์ Wireless มาติดตั้งเปิดใช้เองโดยไม่ได้รับอนุญาต

6) เกิดจาก Software และข้อมูลสูญหาย Software ระบบปฏิบัติการไม่สามารถใช้งาน เกิดจากมี ไวรัสเข้าสู่ระบบ มี Hacker/Spyware, หนอนอินเตอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan horse) หรือมี Software รบกวนการทำงาน สามารถสร้างความเสียหายต่อระบบฐานข้อมูลได้ จึงเห็นควร มีการดำเนินการดังนี้

6.1. มีการตรวจสอบการทำงานของระบบปฏิบัติการอยู่เสมอ

6.2. มีการติดตั้งระบบป้องกันไวรัส / ไฟร์วอลล์ที่ทันสมัย

6.3. มีการจำกัดสิทธิในการเข้าใช้ระบบงานข้อมูล

7) เกิดจากระบบเครือข่าย Internet ขัดข้อง อาจเกิดจากระบบแม่ข่ายล่ม มีผู้ใช้บริการจำนวนมาก มีผลให้การทำงานของระบบหยุดชะงักไม่สามารถให้บริการข้อมูลได้ จึงเห็นควร มีการดำเนินการดังนี้

7.1 ให้เจ้าหน้าที่ด้านเทคนิคตรวจสอบการทำงานของระบบเครือข่าย

7.2 มีการตรวจสอบบำรุงรักษาช่องสัญญาณเครือข่ายเดือนละ 1 ครั้ง

นโยบายนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ประกาศ และบริษัทอาจทบทวนหรือปรับปรุงได้ตามความเหมาะสมกับสภาวะการดำเนินธุรกิจในแต่ละปี นโยบายนี้ได้รับอนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 6/2568 เมื่อวันที่ 11 พฤศจิกายน 2568

พล.อ. ร. กสิวุฒิ

(พลเอก ดร.รุจ กสิวุฒิ)

ประธานกรรมการบริษัท

บริษัท เอเชียนน้ำมันปาล์ม จำกัด (มหาชน)