แผนบริหารจัดการความเสี่ยง

และความปลอดภัยทางไซเบอร์

กรมปศุสัตว์

สิงหาคม 2568

คำนำ

แผนบริหารจัดการความเสี่ยงและความปลอดภัยทางไซเบอร์ กรมปศุสัตว์ ปี 2568 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ในการระบุ ความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากเหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่เกิด (Likelihood) ของเหตุการณ์ องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการได้อย่างเหมาะสมในการบริหารความเสี่ยงให้อยู่ในระดับที่องค์กรสามารถรองรับได้และทำให้องค์กรบรรลุวัตถุประสงค์ ได้อย่างมีประสิทธิภาพมากขึ้น ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หวังเป็นอย่างยิ่งว่าแผนบริหารจัดการความเสี่ยงและความปลอดภัยทางไซเบอร์ฉบับนี้ จะเป็นแนวทางในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการ บริหารงานด้านเทคโนโลยีสารสนเทศของ กรมปศุสัตว์ ต่อไป

สารบัญ

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงาน และการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์การติดตาม ควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสีย และโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูลการใช้งานอุปกรณ์คอมพิวเตอร์การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรดังนั้น ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร/ส่วนราชการ วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยงแล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

วัตถุประสงค์ของการบริหารความเสี่ยง

1. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ
2. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
3. เพื่อทำให้การปฏิบัติงานเป็นไปอย่างมีระบบต่อเนื่องง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

ความสำคัญของการบริหารความเสี่ยง และ นิยาม

ความเสี่ยง (Risk) หมายถึง ความเป็นได้ของเหตุการณ์ที่อาจเกิดขึ้นและเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ของหน่วยงาน

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการระบุความเสี่ยง การวิเคราะห์ความเสี่ยงและการกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยง

ความเสี่ยงในการบริหารองค์กร หมายถึง เหตุการณ์ที่ไม่มีความแน่นอนที่อาจเกิดขึ้นและส่งผลกระทบในด้านลบต่อการบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กร

ระบบบริหารความเสี่ยง หมายถึง ระบบบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่าง ๆ โดยลดมูลเหตุแต่ละโอกาสที่จะทำให้เกิดความเสียหายเพื่อให้ระดับของความเสี่ยงและ

ผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายของหน่วยงานเป็นสำคัญ

การดำเนินงานใด ๆ ย่อมมีความเสี่ยงเกิดขึ้นได้เสมอ ความเสี่ยงที่อาจจะก่อให้เกิดความเสียหายทั้งที่เป็นตัวเงินและไม่เป็นตัวเงินมีสาเหตุสำคัญจาก 2 ปัจจัยหลัก ได้แก่

- ปัจจัยภายใน เช่น ขั้นตอนการปฏิบัติงาน คุณภาพและจริยธรรมของบุคลากร ระเบียบและข้อบังคับของกรมปศุสัตว์ เป็นต้น

- ปัจจัยภายนอก เช่น นโยบายของรัฐบาล กฎหมาย ระเบียบ ข้อบังคับของทางราชการ สภาวะแวดล้อมทั้งทางเศรษฐกิจและการเมืองระหว่างประเทศ ภัยพิบัติ ปัญหาความขัดแย้งในประเทศหรือระหว่างประเทศ เป็นต้น การบริหารจัดการความเสี่ยง หมายความว่า กระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐสามารถดำเนินงานให้บรรลุวัตถุประสงค์ของหน่วยงาน รวมถึงเพื่อเพิ่มศักยภาพและขีดความสามารถให้หน่วยงานของรัฐ

การจัดการความเสี่ยง เป็นแนวทางหนึ่งในการป้องกันปัญหาและอุปสรรคที่อาจจะเกิดขึ้นในอนาคตเนื่องจากการเปลี่ยนแปลงของสภาวะแวดล้อมทั้งภายในและภายนอกองค์กร ซึ่งส่งผลกระทบต่อ การดำเนินงานขององค์กร รวมทั้งเป็นเครื่องมือหนึ่งที่องค์กรนำมาใช้ในการวางแผนการดำเนินธุรกิจเพื่อสร้างมูลค่าเพิ่มให้กับองค์กร ดังนั้นจึงจำเป็นต้องมีการบริหารจัดการปัจจัยต่าง ๆ เพื่อควบคุมกิจกรรม และกระบวนการดำเนินงานด้านต่างๆ เพื่อลดมูลเหตุของระดับผลกระทบและโอกาสที่จะทำให้เกิดความเสียหายให้อยู่ในระดับที่สามารถยอมรับได้ และควบคุมได้ รวมทั้งตรวจสอบได้อย่างเป็นระบบ

กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) ส่วนราชการต้องมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์ ประเมินและจัดการความเสี่ยงอย่างเหมาะสม โดยดำเนินการครอบคลุม 7 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

เป็นการกำหนดวัตถุประสงค์ที่ชัดเจนทำเพื่อให้องค์กรมั่นใจว่าวัตถุประสงค์ที่กำหนดขึ้นมีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ โดยทั่วไปวัตถุประสงค์และกลยุทธ์ควรได้รับการบันทึกเป็นลายลักษณ์อักษรและสามารถพิจารณาได้ในด้านต่าง ๆ ดังนี้ ด้านกลยุทธ์เกี่ยวข้องกับ เป้าหมายและพันธกิจในภาพรวมขององค์กร ด้านปฏิบัติงาน เกี่ยวข้องกับประสิทธิภาพผลการปฏิบัติงานหรือ ความสามารถในการบริหารด้านการปฏิบัติตามกฎ ระเบียบ เกี่ยวข้องกับการปฏิบัติตามกฎหมาย และกฎระเบียบต่างๆ

ขั้นตอนที่ 2 การระบุความเสี่ยงต่างๆ (Event Identification)

องค์กรมีการระบุสถานการณ์ที่อาจเกิดความเสี่ยง ซึ่งองค์กรไม่สามารถมั่นใจได้ว่าเหตุการณ์ใด เหตุการณ์หนึ่งจะเกิดขึ้นหรือไม่ หรือมีผลลัพธ์ที่เกิดขึ้นจะเป็นอย่างไร ต้องพิจารณาทั้งปัจจัยภายในและ ภายนอกองค์กร อาจวิเคราะห์มาจากเหตุการณ์ในอดีตหรือแนวโน้มการเปลี่ยนแปลงในอนาคต

ขั้นตอนที่ 3 การประเมินความเสี่ยง (Risk Assessment)

ขั้นตอนนี้เน้นการประเมินโอกาสเกิดและผลกระทบของเหตุการณ์ที่อาจเกิดขึ้นต่อวัตถุประสงค์ขณะที่เกิดเหตุกรณ์ใดเหตุการณ์หนึ่งอาจส่งผลกระทบในระดับต่ำ เหตุการณ์ที่เกิดขึ้นอย่างต่อเนื่องอาจมีผลกระทบในระดับสูงต่อวัตถุประสงค์

ทั้งนี้ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Risk) คือ ความเสี่ยงของผลลัพธ์ที่ไม่พึงประสงค์ ความเสียหาย การสูญเสีย การละเมิด ความล้มเหลวหรือการหยุดชะงักใดๆ ที่อาจเกิดขึ้นจากการใช้หรือการพึ่งพาฮาร์ดแวร์คอมพิวเตอร์ ซอฟต์แวร์ อุปกรณ์ ระบบ แอปพลิเคชัน และเครือข่าย ความเสี่ยงนี้มักเกี่ยวข้องกับข้อบกพร่องของระบบ ข้อผิดพลาดในการประมวลผล ข้อบกพร่องของซอฟต์แวร์ ข้อผิดพลาดในการทำงานความล้มเหลวของฮาร์ดแวร์ ความล้มเหลวของระบบความไม่เพียงพอของความจุ ช่องโหว่ของเครือข่ายจุดอ่อนในการควบคุม ภัยคุกคามทางไซเบอร์ การรั่วไหลของข้อมูล รวมถึงข้อมูลอ่อนไหว

การประเมินความเสี่ยงประกอบด้วย 2 มิติ คือ โอกาสที่อาจเกิดขึ้น (Likelihood) เหตุการณ์มีโอกาสเกิดขึ้นมาก น้อยเพียงใด ผลกระทบ (Impact) หากมีเหตุการณ์เกิดขึ้นองค์กรจะได้รับผลกระทบมาก น้อยเพียงใด เกณฑ์การประเมินระดับความเสี่ยง เป็นหลักเกณฑ์เพื่อให้สามารถระบุระดับโอกาสและระดับผลกระทบว่ามากน้อยเพียงใด โดยเปรียบเทียบเป็นระดับคะแนน

ความเสี่ยงเชิงปริมาณ หมายถึง ความเสี่ยงที่เกิดขึ้นเนื่องจากการปฏิบัติงานซึ่งสามารถรวบรวมข้อมูล เพื่อนำมาวิเคราะห์ และวัดผลกระทบได้เป็นตัวเลขที่นับจำนวนได้ในการวัดกำหนดให้เป็นจำนวนจริง

ระดับโอกาสเกิดความเสี่ยง (Likelihood) เชิงปริมาณ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มากกว่า 12 ครั้งต่อปี
4	สูง	2-11 ครั้งต่อปี
3	ปานกลาง	1 ครั้งต่อปี
2	น้อย	1 ครั้งต่อ 2-3 ปี
1	น้อยมาก	1 ครั้งต่อ 4-5 ปี

ระดับความรุนแรงของผลกระทบความเสี่ยง (Impact) เชิงปริมาณ		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	การหยุดชะงักของระบบมากกว่า 24 ชม.
4	สูง	การหยุดชะงักของระบบระหว่าง 12-24 ชม.
3	ปานกลาง	การหยุดชะงักของระบบระหว่าง 3-12 ชม.
2	น้อย	การหยุดชะงักของระบบระหว่าง 1-3 ชม.
1	น้อยมาก	การหยุดชะงักของระบบน้อยกว่า 1 ชม.

ความเสี่ยงเชิงคุณภาพ คือ ความเสี่ยงที่เกิดขึ้นเนื่องจากการปฏิบัติงานซึ่งสามารถรวบรวมข้อมูล เพื่อนำมาวิเคราะห์ และวัดผลกระทบได้ในเชิงคุณภาพความเสี่ยงบางเรื่องต้องใช้การพิจารณาตัดสินใจโดยผู้เชี่ยวชาญ

ระดับโอกาสเกิดความเสี่ยง (Likelihood) เชิงคุณภาพ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง
4	สูง	มีโอกาสในการเกิดค่อนข้างสูง
3	ปานกลาง	มีโอกาสเกิดบางครั้ง
2	น้อย	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
1	น้อยมาก	มีโอกาสเกิดในกรณี ยกเว้น

ระดับความรุนแรงของผลกระทบความเสี่ยง (Impact) เชิงคุณภาพ		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดขึ้นอย่างต่อเนื่อง และไม่มีการปรับปรุงแก้ไข
4	สูง	เกิดขึ้นอย่างต่อเนื่อง และมีการปรับปรุงแก้ไข แต่ยังไม่ดีขึ้น
3	ปานกลาง	เกิดขึ้นเป็นบางครั้ง มีการปรับปรุงแก้ไขได้ส่วนใหญ่
2	น้อย	เกิดขึ้นน้อยและแก้ไข ได้เป็นส่วนใหญ่
1	น้อยมาก	ไม่เกิดขึ้นหรือหากเกิด สามารถแก้ไขได้

การจัดลำดับความเสี่ยง โดยการใช้ตารางจัดลำดับความรุนแรงตามปัจจัยเสี่ยง (Risk Ranking) โดยใช้ตารางประเมินความเสี่ยง (Risk matrix หรือ Heat Map) เป็นการพิจารณาจากความสัมพันธ์ระหว่างโอกาสที่จะเกิด ความเสี่ยง และผลกระทบของความเสี่ยงต่อองค์กรว่าก่อให้เกิดความเสี่ยงในระดับใด

ระดับผลกระทบ (Impact)	5	สูง	สูง	สูงมาก	สูงมาก	สูงมาก
	4	ปานกลาง	สูง	สูง	สูงมาก	สูงมาก
	3	ปานกลาง	ปานกลาง	ปานกลาง	สูง	สูงมาก
	2	ต่ำ	ต่ำ	ปานกลาง	สูง	สูงมาก
	1	ต่ำ	ต่ำ	ปานกลาง	สูง	สูง
		1	2	3	4	5
		ระดับโอกาสเกิด (Likelihood)				

สูงมาก - ระดับที่ไม่สามารถยอมรับได้ ต้องมีการบริหารจัดการหรือมาตรการจัดการความเสี่ยงเพื่อไม่ให้เกิดความเสียหายทันที

สูง - ระดับที่ไม่สามารถยอมรับได้ ต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ต่อไป ต้องมีการบริหารจัดการหรือมาตรการจัดการความเสี่ยง

ปานกลาง - ระดับที่ยอมรับได้ แต่ต้องควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเลื่อนระดับไปยังระดับที่ยอมรับไม่ได้ ต้องมีการติดตามเพื่อเฝ้าระวังสม่ำเสมอ

ต่ำ - ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมหรือจัดการเพิ่มเติม แต่ต้องมีการติดตามเฝ้าระวังสม่ำเสมอ

ขั้นตอนที่ 4 กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)

ผู้บริหารต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสเกิดและผลกระทบของเหตุการณ์ให้อยู่ในห้วงที่องค์กรสามารถยอมรับได้ โดยหลักการการตอบสนองความเสี่ยงมี 4 วิธีการ ดังนี้ (หลัก 4 T)

- Take การยอมรับความเสี่ยง (Accept) หมายถึง การตกลงกันที่จะยอมรับเนื่องจากไม่คุ้มค่าในการจัดการหรือป้องกัน แต่การเลือกบริหารความเสี่ยงด้วยวิธีนี้ต้องมีการติดตามเฝ้าระวังอย่างสม่ำเสมอ

- Treat การลด/การควบคุมความเสี่ยง (Control) หมายถึง การปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อลด โอกาสที่จะเกิดความเสียหาย หรือลดผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เช่นการ จัดอบรมพนักงาน การจัดทำคู่มือการปฏิบัติงาน

- Transfer การกระจาย หรือโอนความเสี่ยง (Transfer) หมายถึง การกระจายหรือถ่ายโอนความเสี่ยงให้หน่วยงานอื่นช่วยแบ่งความรับผิดชอบไปเช่น การทำประกันภัยกับบริษัทภายนอก หรือการจ้างบุคคลภายนอกดำเนินการแทน (Outsource)

- Terminate การหลีกเลี่ยงความเสี่ยง (Avoid) หมายถึง การจัดการความเสี่ยงที่อยู่ในระดับสูงมาก และไม่อาจยอมรับได้ จึงต้องตัดสินใจยกเลิกโครงการ/กิจกรรมที่จะก่อให้เกิดความเสี่ยงนั้นไป

ขั้นตอนที่ 5 กิจกรรมการบริหารความเสี่ยง (Control Activities)

การกำหนดกิจกรรม มาตรการและการปฏิบัติต่างๆ เพื่อช่วยลด หรือ ควบคุมความเสี่ยง เพื่อสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้อง และทำให้การดำเนินงานบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ป้องกันและลดระดับความเสี่ยงให้อยู่ในระดับที่ องค์กร ยอมรับได้ โดยมีหลักในการควบคุม 4 มาตรการ คือ

- ควบคุมเพื่อป้องกันไม่ให้เกิดข้อผิดพลาด
- ควบคุมเพื่อให้ตรวจพบข้อผิดพลาด
- ควบคุมโดยการชี้แนะหรือกระตุ้นให้เกิดผลสำเร็จของงานตามวัตถุประสงค์
- ควบคุมเพื่อการแก้ไขข้อผิดพลาดที่เกิดขึ้น

ขั้นตอนที่ 6 ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

จะต้องมีระบบสารสนเทศ และการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยง ต่อไปตามกรอบและขั้นตอนการปฏิบัติที่องค์กรกำหนด

ขั้นตอนที่ 7 การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

การติดตามผลการดำเนินงาน การนำกลยุทธ์มาตรการ หรือแนวทางมาใช้ปฏิบัติเพื่อลดโอกาสที่ เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรม ควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยง มีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยงเมื่อองค์กรทราบความเสี่ยง ที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณา

ความเป็นไปได้และค่าใช้จ่าย แต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

1. พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

2. เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจาก มาตรการดังกล่าวว่าคุ้มค่าหรือไม่

3. กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

4. ในครั้งต่อไป ให้พิจารณาผลการติดตามการบริหารความเสี่ยงในครั้งก่อนหน้า มาใช้ประกอบการ ดำเนินการบริหารความเสี่ยงตามกระบวนการ หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์ และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผล การวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ถ้ามีเหลืออยู่ให้วิเคราะห์ ว่ามีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบ และสั่งการ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

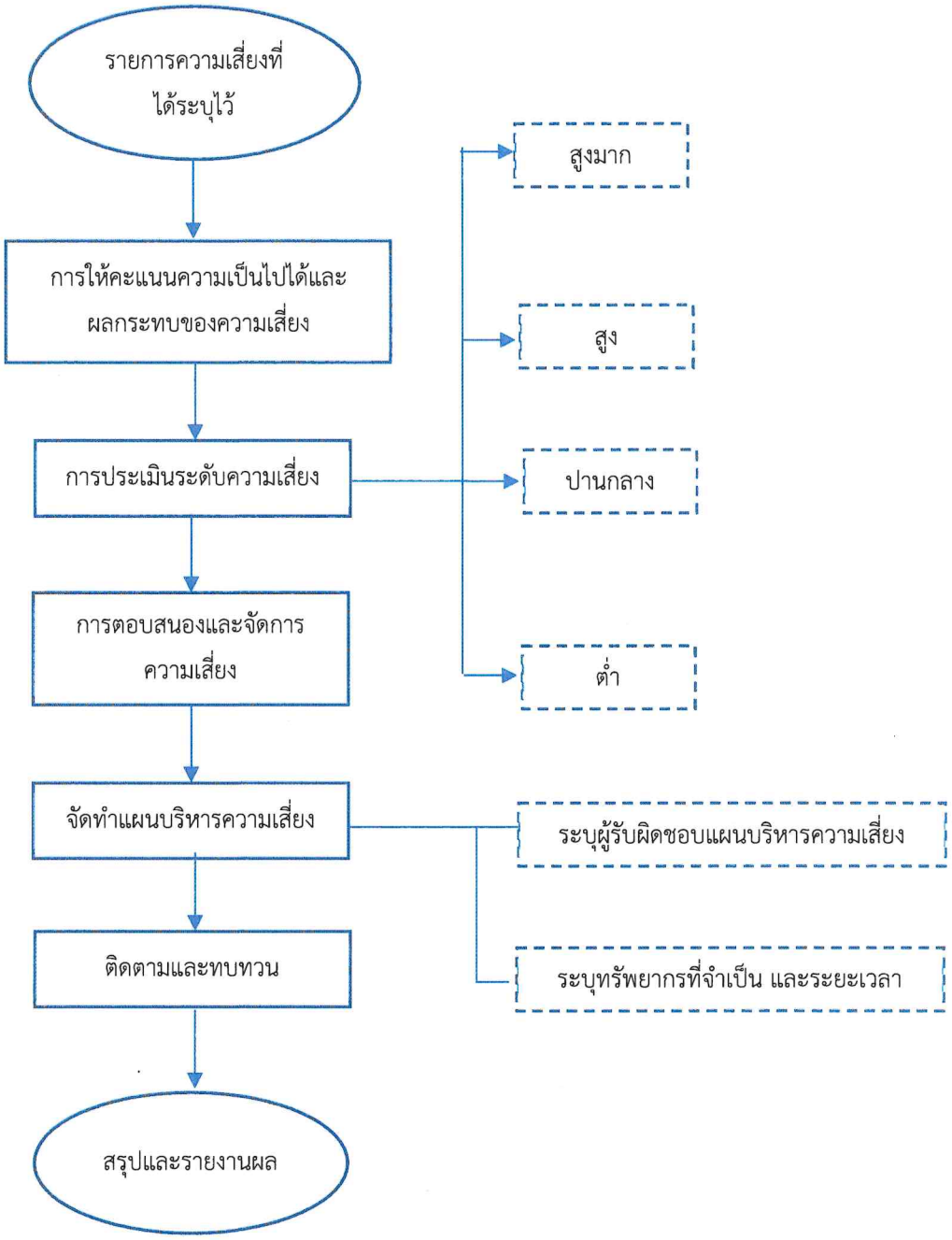
1. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์สร้างขึ้น เช่น วาตภัยอุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

2. ความเสี่ยงด้านระบบเครือข่ายและความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ หมายถึงความเสี่ยงที่เกิดขึ้น กับระบบเครือข่ายเทคโนโลยีสารสนเทศต่างๆเช่น ระบบเครือข่ายอินเทอร์เน็ตขัดข้อง ไวรัสคอมพิวเตอร์ภัยคุกคาม ทางคอมพิวเตอร์ต่าง ๆ

3. ความเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล หมายถึงความเสี่ยงที่เกิดจากการทำงานของระบบสารสนเทศ และการจัดเก็บฐานข้อมูลสารสนเทศ ที่อาจเกิดความเสียหายจากการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ไม่มีการอัพเดทโปรแกรม ให้ทันสมัยเพื่อลดช่องโหว่ที่อาจเกิดจากBug ของซอฟต์แวร์นั้น ๆตลอดจนความเสี่ยงจากการถูกบุกรุกข้อมูลการสูญหาย ของข้อมูลความถูกต้องน่าเชื่อถือของข้อมูลและรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ

4. ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึงความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผนการตรวจสอบการทำงาน การมอบหมายหน้าที่ และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากร มีความรู้ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้ง บุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



ตารางการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมปศุสัตว์ ปีงบประมาณ พ.ศ. 2568

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
1. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)							
1. ความเสี่ยง ไฟฟ้าดับ น้ำท่วม ไฟไหม้ หรือเหตุการณ์ภัยพิบัติอื่น ๆ ที่ส่งผลต่ออุปกรณ์ไอทีห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง	1. ระบบคอมพิวเตอร์และระบบเครือข่ายถูกทำลาย 2. ระบบสารสนเทศ และระบบฐานข้อมูลถูกทำลาย	1	5	สูง	1. ตรวจสอบระบบไฟฟ้า ปลั๊กพ่วง และสายไฟอย่างสม่ำเสมอ เพื่อหาจุดชำรุด ฉนวนแตก หรือการเสื่อมสภาพ 2. ติดตั้งอุปกรณ์ตัดกระแสไฟฟ้าลัดวงจร (Circuit Breaker) หรือเครื่องป้องกันกระแสไฟฟ้ารั่วไหล (ELCB/RCBO) ในแผงควบคุมไฟฟ้า 3. ติดตั้งเครื่องตรวจจับควันหรือความร้อนในบริเวณที่มีเครื่องคอมพิวเตอร์และอุปกรณ์จำนวนมาก 4. จัดเตรียมถังดับเพลิงชนิดที่เหมาะสมสำหรับเพลิงไหม้จากอุปกรณ์ไฟฟ้า และวางในจุดที่เข้าถึงง่าย พร้อมฝึกอบรมการใช้งาน 5. สำรองข้อมูล โดยกำหนดความถี่ ชนิด และสถานที่ในการสำรองข้อมูลที่สำคัญ เช่น ระบบฐานข้อมูล	การควบคุม (Treat) และการกระจาย (Transfer)	ศูนย์โทรคมนาคมนนทบุรี บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) และศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					ทะเบียนอาหารสัตว์, ข้อมูลสูตรอาหารสัตว์ 6. ศูนย์คอมพิวเตอร์แม่ข่ายกลาง (NT นนทบุรี) มีมาตรการป้องกันไฟฟ้าลัดวงจร ตรวจสอบระบบดับเพลิงอย่างสม่ำเสมอ สำรองข้อมูลสม่ำเสมอ		
2. ความเสี่ยงจากการเกิดชุมนุม ประท้วงภายในบริเวณรอบ ๆ พื้นที่สำนักงาน	เกิดการปิดล้อมบริเวณพื้นที่ราชการ กรณีเกิดการชุมนุมประท้วงทางการเมือง ทำให้ไม่สามารถเข้าถึงพื้นที่ภายในสำนักงาน และไม่สามารถเข้าระบบคอมพิวเตอร์แม่ข่ายได้	1	2	ต่ำ	1. สำรองข้อมูลทุกเดือน 2. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายเป็นประจำ	การควบคุม (Treat)	ผู้ดูแลระบบ กอง/สำนักที่เกี่ยวข้อง
3. อุปกรณ์เก็บข้อมูลชำรุด ไม่สามารถเก็บข้อมูลได้	พื้นที่เก็บข้อมูลลดลง หรือไม่สามารถใช้ข้อมูลในอุปกรณ์ที่ชำรุดได้	2	3	ปานกลาง	1. พิจารณาวิธีการสำรองข้อมูลที่เหมาะสม เช่น (RAID3 หรือ RAID5) เพื่อให้ระบบสามารถดำเนินการต่อได้เมื่ออุปกรณ์เก็บข้อมูลผิดปกติ และแจ้งเจ้าของอุปกรณ์ทันทีที่ตรวจพบ 2.ตรวจสอบสถานะของอุปกรณ์เก็บข้อมูลอยู่เสมอ หากพบโอกาสเสี่ยงควรพิจารณาเปลี่ยนทันที	การควบคุม (Treat)	ผู้ดูแลระบบ กอง/สำนักที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
2. ความเสี่ยงด้านบุคลากร (Human Risk)							
4. บุคลากรขาดความรู้ ความเข้าใจ เกี่ยวกับการใช้ระบบไอทีหรือความตระหนักด้านความปลอดภัยของระบบไอที อาจกระทำ/ปฏิบัติผิดพลาดโดยไม่ได้ตั้งใจ	บุคลากรขาดความรู้ ความเข้าใจเกี่ยวกับการใช้ระบบไอทีหรือความตระหนักด้านความปลอดภัยของระบบไอที อาจกระทำ/ปฏิบัติผิดพลาดโดยไม่ได้ตั้งใจ ข้อมูลผิดพลาด/สูญหาย ระบบเสียหาย หรือถูกโจมตีทางไซเบอร์จากการเปิดช่องทางความเสี่ยงที่เกิดจากการใช้งานผิดพลาด	1	3	ปานกลาง	จัดฝึกอบรมด้านไอที ความปลอดภัยข้อมูล และการใช้งานระบบเป็นประจำอย่างสม่ำเสมอ มีคู่มือปฏิบัติงานชัดเจน และจัดระบบอนุญาตใช้งานตามสิทธิ์	การควบคุม (Treat)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
5. ความเสี่ยงจากรหัสผู้ใช้งานรั่วไหล/เปิดเผยรหัสผู้ใช้งานให้บุคคลอื่นทราบ (ใช้บัญชีผู้ใช้งานร่วมกัน)	1. ข้อมูลที่อยู่ในชั้นความลับรั่วไหล เช่น ข้อมูลส่วนบุคคล เป็นต้น 2. ฐานข้อมูลเกิดความเสียหาย	3	3	ปานกลาง	- แจ้งเวียนข้อสั่งการให้ดำเนินการตามนโยบายและประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการ	การควบคุม (Treat)	ผู้ดูแลระบบ กอง/สำนักที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
6. ความเสี่ยงจากภัยคุกคามทางไซเบอร์เนื่องจากเจ้าหน้าที่ไม่ติดตั้งโปรแกรม Antivirus	1. ข้อมูลที่อยู่ในชั้นความลับรั่วไหล เช่น ข้อมูลส่วนบุคคล เป็นต้น 2. ฐานข้อมูลเกิดความเสียหาย 3. ส่งผลเสียต่อชื่อเสียงและความน่าน่าเชื่อถือของหน่วยงาน	3	3	ปานกลาง	รักษาความมั่นคงปลอดภัยไซเบอร์ของกรมปศุสัตว์ - ผู้ดูแลระบบตรวจสอบ/ทบทวนบัญชีผู้ใช้งานระบบสารสนทศ รวมถึงการยกเลิกบัญชี (เกษียณอายุ/ลาออก/โอนย้าย ฯลฯ) - การจัดระดับสิทธิการเข้าถึงข้อมูลอย่างเป็นระบบ และสิทธิในการกระท่ากับข้อมูล การก่าหนดบัญชีผู้ใช้งาน 1 บัญชี ต่อ 1 บุคคล - ผู้ดูแลระบบสารสนเทศเปลี่ยนรหัสผ่านทุก 6 เดือน และตั้งรหัสที่คาดเดายาก - มีระบบการสำรองข้อมูล		

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
7. เจ้าหน้าที่เข้าเว็บไซต์ที่ก่อให้เกิดมัลแวร์ภายในเครื่อง	1. ทำให้ระบบคอมพิวเตอร์เกิดความล่าช้าและไม่มีประสิทธิภาพตามความสามารถในการทำงานของระบบคอมพิวเตอร์นั้น ๆ 2. เกิดช่องโหว่ให้ผู้ไม่หวังดี เข้ามาควบคุมคอมพิวเตอร์ หรือโจรกรรมข้อมูล	3	2	ปานกลาง	1. กำชับให้เจ้าหน้าที่ไม่เข้าเว็บไซต์ที่เป็นอันตราย หรือสุ่ม เสี่ยง พร้อมทั้งมีการกำหนด นโยบายที่เกี่ยวข้องการ เข้าถึงเว็บไซต์อย่างมั่นคง ปลอดภัยไว้เป็นลายลักษณ์อักษร 2. หลีกเลี่ยงการดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ 3.ทำการ Clean Malware และสแกน Virus เป็นประจำ	การควบคุม (Treat)	เจ้าหน้าที่ทุกกอง/สำนัก
8. การกดลิงค์ในอีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	1. โดนหลอกลวงเพื่อขอรหัสผ่านข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นความลับ 2. โดนหลอกเพื่อติดตั้งไวรัสลงบนคอมพิวเตอร์ หรือคอมพิวเตอร์แม่ข่าย	3	2	ปานกลาง	- จัดอบรมให้ความตระหนักรู้แก่เจ้าหน้าที่ในองค์กร - มีการแจ้งข่าวสารให้เจ้าหน้าที่ในองค์กรทราบเมื่อมีการพบเจออีเมลหรือหน้าเว็บไซต์หลอกลวง	การควบคุม (Treat)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้ดูแลระบบทุกกอง/สำนัก
9. การใช้งานไม่ถูกต้อง หรือมีช่องโหว่ เช่น ตั้งรหัสผ่านที่คาดเดาได้ง่าย ไม่เปลี่ยนรหัสผ่านเป็นประจำ การเข้าเว็บไซต์ที่อาจมีความเสี่ยง	1. ระบบสารสนเทศ และระบบฐานข้อมูลถูกทำลาย เกิดการจู่โจม 2. ข้อมูลเสียหาย สูญหาย	3	4	สูง	1. มีมาตรการในการรักษาความมั่นคงปลอดภัยระบบ เช่น การตั้งรหัสผ่าน การควบคุมการงานคอมพิวเตอร์เพื่อลดความเสี่ยง ให้ความรู้การใช้งานที่ถูกต้องให้	การควบคุม (Treat)	เจ้าหน้าที่ทุกกอง/สำนัก

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
10. ความผิดพลาดโดยไม่ตั้งใจ เช่น การลบไฟล์ผิด					ผู้ใช้งาน การจัดการสิทธิ์ผู้ใช้งาน 2. เพิ่มความตระหนักให้แก่เจ้าหน้าที่ที่เข้าถึงฐานข้อมูลการจำกัดสิทธิ์การเข้าถึงข้อมูลที่สำคัญ 3. อบรมบุคลากรด้าน cybersecurity ให้ผู้ใช้ทุกระดับ		
11. เปิดเผยรหัสผ่านแก่ผู้อื่น ทั้งโดยความตั้งใจและไม่ตั้งใจ	บุคลที่มีรหัสผ่านสามารถเข้าใช้งานระบบภายใต้ชื่อผู้ใช้นั้นได้	3	4	สูง	1. อบรมให้ความรู้แก่ผู้ใช้งานในด้านความปลอดภัยของข้อมูลรวมถึงการจัดการหากตรวจพบความผิดปกติกับบัญชีผู้ใช้ของตน 2. จัดทำระบบยืนยันตัวตนให้มีมากกว่า 1 ขั้นตอน เพื่อเป็นการป้องกันการถูกละเมิดในขั้นต้นและแจ้งเจ้าของข้อมูลเมื่อเกิดกิจกรรมผิดปกติกับบัญชีผู้ใช้ของตน	การควบคุม (Treat)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และเจ้าหน้าที่ทุกกอง/สำนัก

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
12. การละเมิดข้อมูลโดยเจ้าหน้าที่	1. องค์กรอาจถูกปรับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของไทย นอกจากนี้ยังอาจต้องจ่ายค่าชดเชยความเสียหายให้กับเจ้าของข้อมูลที่ได้รับผลกระทบ 2. ทำให้ภาพลักษณ์ขององค์กรเสียหายอย่างรุนแรง โดยเฉพาะอย่างยิ่งหากข้อมูลที่รั่วไหลมีความอ่อนไหวสูง เช่น ข้อมูลส่วนบุคคลของเกษตรกร ข้อมูลสูตรอาหารสัตว์ที่เป็นความลับทางการค้า	4	3	สูง	1. พิจารณาใช้การเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งในขณะจัดเก็บและส่งผ่าน 2. ทบทวนสิทธิ์การเข้าถึงข้อมูลของเจ้าหน้าที่เป็นประจำทุก 6 เดือน หรือเมื่อมีการโยกย้ายตำแหน่ง 3. จัดเก็บบันทึก (Log) กิจกรรมการเข้าถึงและใช้งานระบบของเจ้าหน้าที่อย่างละเอียด	การควบคุม (Treat)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และเจ้าหน้าที่ทุกกอง/สำนัก
3. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)							
13. ระบบเครือข่ายล่ม, อุปกรณ์เครือข่ายขัดข้อง, การเชื่อมต่อภายนอกที่ไม่ปลอดภัย หรือถูกโจมตีจากภายนอก เช่น DDoS หรือ Malware	ผู้ใช้งานไม่สามารถเข้าระบบได้ ข้อมูลไม่ปลอดภัย ระบบให้บริการออนไลน์หยุดชะงัก ข้อมูลรั่วไหล เสียภาพลักษณ์องค์กร	3	4	สูง	- ติดตั้ง Firewall, ระบบเฝ้าระวังภัยคุกคาม (IDS/IPS), VPN, เครือข่ายส่วนตัวเสมือน (Virtual Private Network) สำหรับการเชื่อมต่อระยะไกล, จัดระบบสำรองอุปกรณ์เครือข่าย และดูแลบำรุงรักษาอย่างต่อเนื่อง	การกระจาย (Transfer) และการควบคุม (Treat)	ศูนย์โทรคมนาคมนนทบุรี บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) และเจ้าหน้าที่ กอง/สำนัก ที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					- มีระบบสำรองข้อมูล (Backup) ทดสอบ - มีการทดสอบการกู้คืนระบบแม่ข่ายหลัก อย่างน้อยเดือนละ 1 ครั้ง		
14. ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	1. เกิดความเสียหายจากการจัดหาครุภัณฑ์ อุปกรณ์ที่ไม่ได้มาตรฐาน 2. การติดตั้งที่ไม่ได้มาตรฐาน	1	3	ปานกลาง	1. ทำการตรวจสอบลักษณะของงานเพื่อจัดหาอุปกรณ์ที่เหมาะสม 2. ตรวจสอบมาตรฐานของอุปกรณ์	การควบคุม (Treat)	เจ้าหน้าที่ กอง/สำนักที่เกี่ยวข้อง
15. ความเสี่ยงจากการภัยคุกคามทางไซเบอร์จากการไม่ได้ติดตั้งโปรแกรม Antivirus บนเครื่องคอมพิวเตอร์แม่ข่าย (Server)	1. ข้อมูลรั่วไหล/สูญหาย 2. ระบบสารสนเทศไม่สามารถใช้งานได้ 3. ระบบสารสนเทศ และฐานข้อมูลถูกทำลาย 4. ส่งผลเสียต่อชื่อเสียงและความน่าน่าเชื่อถือของหน่วยงาน	2	5	สูง	- ดำเนินการตามนโยบายและประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมปศุสัตว์ - ผู้ดูแลระบบตรวจสอบ/ทบทวนบัญชีผู้ใช้งานระบบสารสนทศ รวมถึงการยกเลิกบัญชี (เกษียณอายุ/ลาออก/โอนย้าย ฯลฯ) - การจัดระดับสิทธิการเข้าถึงข้อมูลอย่างเป็นระบบ และสิทธิในการกระทำกับข้อมูล การกำหนดบัญชีผู้ใช้งาน 1 บัญชี ต่อ 1 บุคคล - ผู้ดูแลระบบสารสนเทศเปลี่ยน	การควบคุม (Treat)	เจ้าหน้าที่ กอง/สำนักที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					รหัสผ่านทุก 6 เดือน และตั้งรหัสที่คาดเดายาก - มีระบบการสำรองข้อมูล		
16. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายไม่ได้รับการบำรุงรักษา เกิดความชำรุด/เสียหาย หรือไม่สามารถให้บริการได้	1. เกิดความผิดพลาดในการให้บริการระบบสารสนเทศ หรือ ไม่สามารถให้บริการต่อเนื่องได้ 2. ระบบฐานข้อมูลเสียหาย/ถูกทำลาย หน่วยงานไม่สามารถให้บริการ ได้สูญเสียข้อมูลสำคัญที่เก็บอยู่ภายในเครื่องคอมพิวเตอร์แม่ข่าย	3	4	สูง	- กำหนดแนวทางการปรับปรุง/พัฒนาระบบสารสนเทศ - จัดหางบประมาณเพื่อดำเนินการบำรุงรักษาระบบสารสนเทศ (MA) - มีระบบการสำรองข้อมูล - มีแผนการบำรุงรักษา ตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการจ้างผู้เชี่ยวชาญภายนอก (Outsource) ที่มีความเชี่ยวชาญเพื่อบำรุงรักษาระบบ - มีการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่อง	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง
17. ไม่มีการควบคุม/จัดทำบัญชี/ ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ครุภัณฑ์คอมพิวเตอร์ ครุภัณฑ์เครือข่าย หรืออุปกรณ์สูญหาย	1	4	ปานกลาง	- จัดทำทะเบียนครุภัณฑ์ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และระบบสารสนเทศสำคัญของสำนักฯ	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
18. ขาดการบริหารจัดการสิทธิ์ การใช้งานอุปกรณ์เทคโนโลยี สารสนเทศและการสื่อสารในทุก ๆ ระดับ ของผู้ใช้งาน	1. เกิดความผิดพลาดในการให้บริการ ระบบสารสนเทศและการสื่อสารทั้งระบบ 2. ไม่สามารถระบุตัวตนผู้ใช้งานได้	1	3	ปานกลาง	1. มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับ 2. มีการทบทวนสิทธิ์การเข้าใช้งานเป็นประจำทุก 6 เดือน หรือเมื่อมีการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข	การควบคุม (Treat)	เจ้าหน้าที่ กอง/สำนักที่เกี่ยวข้อง
19. SSL certificate หมดอายุ	การเข้าใช้งานระบบทำได้ยากและเสี่ยงต่อความปลอดภัยเนื่องจากข้อมูลอาจไม่ได้ถูกเข้ารหัส	3	4	สูง	ทำการต่ออายุ ssl certificate ก่อนหมดอายุ	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง
20. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตไม่เสถียร	ผู้ใช้งานไม่สามารถเข้าใช้ระบบอินทราเน็ต และอินเทอร์เน็ตได้	1	5	สูง	1. ตรวจสอบระบบเครือข่ายสื่อสารหลักทุกวัน 2. ควบคุมการเข้าใช้เครือข่ายอินทราเน็ตและอินเทอร์เน็ต	การยอมรับ (Take)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
4. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)							
21. ซอฟต์แวร์มีข้อผิดพลาด, ช่องโหว่หรือไม่ได้รับการอัปเดต, ขาดการบำรุงรักษา ไม่มีระบบตรวจสอบความถูกต้อง ส่งผลให้ถูกโจมตีได้	ข้อมูลถูกขโมยหรือเปลี่ยนแปลง, ระบบหยุดทำงาน ระบบล่ม หรือใช้งานไม่ได้, ผู้ใช้งานไม่สามารถดำเนินงานได้อย่างต่อเนื่อง และมีประสิทธิภาพ ไม่สามารถอัพเดตได้ หรือเกิดช่องโหว่ ไม่ได้รับการ support	1	3	ปานกลาง	มีนโยบายการจัดการ Patch และอัปเดตซอฟต์แวร์ตามรอบอย่างสม่ำเสมอ, จัดให้มีการทดสอบก่อนใช้งานจริง, มีระบบแจ้งเตือนความผิดปกติของโปรแกรม	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
22. ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	1. ข้อมูลถูกเปลี่ยนแปลงหรือถูกทำลาย 2. ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ 3. ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง 4. ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	3	4	สูง	1. มีการติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall 2. ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ 3. ตรวจสอบ ติดตาม และเฝ้าระวังการบุกรุกเครือข่าย อย่างสม่ำเสมอ 4. ติดตามข่าวสารภัยคุมคามทางไซเบอร์อย่างสม่ำเสมอ 5. ติดตั้งโปรแกรมป้องกันไวรัส 6. ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ 7. เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
23. ความเสี่ยงจากความเข้ากันได้ของ browser version ระหว่างระบบกับเครื่องผู้ใช้งาน หรือระบบปฏิบัติการ	ผู้ใช้งานที่ไม่ได้อัพเดท browser หรือใช้ระบบปฏิบัติการเก่าที่ระบบไม่รองรับจะไม่สามารถใช้ความสามารถบางอย่างได้	1	5	สูง	1.แจ้งผู้ใช้อัพเดท browser เพื่อให้สามารถใช้งานระบบได้อย่างเต็มประสิทธิภาพ 2. แจ้งผู้ใช้ทำการอัพเกรดระบบปฏิบัติการให้สอดคล้องกับที่ระบบรองรับ	การควบคุม (Treat)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้ดูแลระบบกอง/สำนัก ที่เกี่ยวข้อง
24. ความเสี่ยงจากการติดตั้งโปรแกรมคอมพิวเตอร์ ที่ไม่มีลิขสิทธิ์ และไม่ทราบแหล่งที่มา	1. องค์กรอาจถูกฟ้องร้องดำเนินคดีตามพระราชบัญญัติลิขสิทธิ์ ซึ่งมีโทษปรับสูง และอาจมีโทษจำคุกสำหรับผู้บริหารหรือผู้ที่เกี่ยวข้อง 2. เจ้าของลิขสิทธิ์สามารถเรียกค่าเสียหายจากองค์กรได้ 3. โปรแกรมคอมพิวเตอร์ที่ไม่มีลิขสิทธิ์หรือติดตั้งจากแหล่งที่ไม่น่าเชื่อถือ มีการฝังมัลแวร์ (Malware) ต่างๆ เช่น ไวรัส (Virus) สปายแวร์ (Spyware) แรนซัมแวร์ (Ransomware) โทรจัน (Trojan), หรือ Backdoor เพื่อให้ผู้โจมตีสามารถควบคุมเครื่องคอมพิวเตอร์หรือเข้าถึงข้อมูลได้ 4. อาจมีการทำงานที่ไม่เสถียร	1	3	ต่ำ	1. กำหนดนโยบายให้ชัดเจนว่า ไม่อนุญาต ให้ติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หรือซอฟต์แวร์ที่ไม่ได้มาจากแหล่งที่เชื่อถือได้โดยเด็ดขาด 2. จัดซื้อ จัดหา และติดตั้งซอฟต์แวร์อย่างเป็นทางการ เพื่อให้มั่นใจว่าซอฟต์แวร์ทั้งหมดมีลิขสิทธิ์ถูกต้อง 3. กำหนดสิทธิ์ผู้ใช้ไม่ให้สามารถติดตั้งโปรแกรมใดๆ ได้เอง โดยไม่มีสิทธิ์ผู้ดูแลระบบ (Administrator Privileges)	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนัก ที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
	เกิดข้อผิดพลาดบ่อยครั้ง หรือทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง						
24. ความเสี่ยงจากการติดตั้งโปรแกรมคอมพิวเตอร์ ที่ไม่มีลิขสิทธิ์ และไม่ทราบแหล่งที่มา	1. องค์กรอาจถูกฟ้องร้องดำเนินคดีตามพระราชบัญญัติลิขสิทธิ์ ซึ่งมีโทษปรับสูง และอาจมีโทษจำคุกสำหรับผู้บริหารหรือผู้ที่เกี่ยวข้อง 2. เจ้าของลิขสิทธิ์สามารถเรียกค่าเสียหายจากองค์กรได้ 3. โปรแกรมคอมพิวเตอร์ที่ไม่มีลิขสิทธิ์หรือได้จากแหล่งที่ไม่น่าเชื่อถือมักจะมีการฝังมัลแวร์ (Malware) ต่างๆ เช่น ไวรัส (Virus) สปายแวร์ (Spyware) แรนซัมแวร์ (Ransomware) โทรจัน (Trojan), หรือ Backdoor เพื่อให้ผู้โจมตีสามารถควบคุมเครื่องคอมพิวเตอร์หรือเข้าถึงข้อมูลได้ 4. อาจมีการทำงานที่ไม่เสถียร เกิดข้อผิดพลาดบ่อยครั้ง หรือทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง	1	3	ต่ำ	1. กำหนดนโยบายให้ชัดเจนว่า ไม่อนุญาต ให้ติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หรือซอฟต์แวร์ที่ไม่ได้มาจากแหล่งที่เชื่อถือได้โดยเด็ดขาด 2. จัดซื้อ จัดหา และติดตั้งซอฟต์แวร์อย่างเป็นทางการ เพื่อให้มั่นใจว่าซอฟต์แวร์ทั้งหมดมีลิขสิทธิ์ถูกต้อง 3. กำหนดสิทธิ์ผู้ใช้ไม่ให้สามารถติดตั้งโปรแกรมใดๆ ได้เอง โดยไม่มีสิทธิ์ผู้ดูแลระบบ (Administrator Privileges)	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
5. ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)							
25. ข้อมูลสูญหาย ถูกดัดแปลง หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต	สูญเสียข้อมูลสำคัญ ข้อมูลรั่วไหล สร้างความเสียหายทางกฎหมายและภาพลักษณ์	1	3	ปานกลาง	จัดให้มีระบบสำรองข้อมูลสม่ำเสมอ, กำหนดสิทธิ์เข้าถึงตามบทบาท และการเข้ารหัสข้อมูล	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง
26. ฐานข้อมูลถูกเข้าถึงโดยไม่ได้รับอนุญาต	- ข้อมูลสำคัญสูญหาย หรือหลุดรั่วไปยังภายนอกหน่วยงาน - อาจถูกดำเนินคดีหรือถูกฟ้องเรียกค่าเสียหายร่วมด้วย - หน่วยงานเสื่อมเสียชื่อเสียงและความน่าเชื่อถือ	1	5	สูง	1. มีระบบพิสูจน์ตัวตนก่อนเข้าใช้งานระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศ 2. มีกระบวนการทบทวนสิทธิผู้ใช้งานเป็นประจำ 3. มีการเก็บประวัติการเข้าใช้งานคอมพิวเตอร์ 4. มีกระบวนการบริหารจัดการคอมพิวเตอร์และอุปกรณ์ 5. มีแนวปฏิบัติในการลบหรือทำลายข้อมูลหลังจากไม่ได้ใช้งาน	การควบคุม (Treat)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารและผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง
27. ความเสี่ยงจากผู้ใช้งานนำเข้าข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน	1. ระบบสารสนเทศมีประสิทธิภาพลดลง 2. ลดความน่าเชื่อถือของหน่วยงาน 3. ข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน	3	3	ปานกลาง	1. จัดทำรายการข้อมูล ความถี่ในการนำเข้าข้อมูลผิดพลาด 2. กำหนดแนวทางการปรับปรุง/พัฒนาระบบสารสนเทศ	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					- จัดทำคู่มือ การใช้ระบบสารสนเทศให้ถูกต้อง		
28. ความเสี่ยงจากความผิดพลาดหรือข้อบกพร่อง (BUG) ที่เกิดขึ้นในระบบสารสนเทศ	1. ระบบสารสนเทศไม่สามารถใช้งานหรือประสิทธิภาพการใช้งานลดลง 2. ลดความน่าเชื่อถือของหน่วยงาน 3. ข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน	2	3	ปานกลาง	- จัดทำรายการข้อมูล ความถี่ ในผิดพลาดของระบบ - กำหนดมาตรการ แนวทางการปรับปรุงระบบสารสนเทศ - จัดหางบประมาณเพื่อดำเนินการปรับปรุงระบบสารสนเทศ	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง
29. ความเสี่ยงจากการไม่จำกัดสิทธิ์เข้าถึงระบบฐานข้อมูลภายในสำนักงาน	1. อาจทำให้ข้อมูลเกิดการสูญหาย 2. ข้อมูลอาจเกิดการบิดเบือนจากความเป็นจริงและไม่ถูกต้อง	1	3	ปานกลาง	1. กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มต่าง ๆ เช่น ผู้ดูแลระบบ, ผู้ใช้งานทั่วไป เป็นต้น 2. จัดการบัญชีต่าง ๆ (User) ให้เป็นปัจจุบัน ปิดบัญชีผู้ใช้ที่ไม่มีการใช้งาน	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง
30. ฐานข้อมูลจะถูกโจมตี ถูกบุกรุก เสียหาย ไม่สามารถเข้าถึงได้ หรือข้อมูลภายในถูกเปิดเผย/แก้ไขโดยไม่ได้รับอนุญาต	1. ข้อมูลในฐานข้อมูลถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ทำให้ไม่ถูกต้องหรือไม่น่าเชื่อถือ 2. ฐานข้อมูลล่มหรือไม่สามารถเข้าถึงได้ ทำให้แอปพลิเคชันหรือบริการที่ต้องพึ่งพาฐานข้อมูลไม่สามารถทำงานได้	1	3	ปานกลาง	1. ตรวจสอบความถูกต้องของฐานข้อมูลอย่างสม่ำเสมอ 2. พัฒนาความรู้และทักษะด้านความปลอดภัยของฐานข้อมูลอย่างต่อเนื่อง	การยอมรับ (Take)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
	3. องค์กรอาจถูกมองว่าไร้ความสามารถในการปกป้องข้อมูลสำคัญ						
31. ฐานข้อมูลถูกใช้เต็มพื้นที่	ไม่สามารถเพิ่มข้อมูลใหม่ได้	1	5	สูง	1. พิจารณาพื้นที่จัดเก็บข้อมูลในปัจจุบัน หากพื้นที่ใกล้เต็ม ควรพิจารณาจัดซื้อหน่วยจัดเก็บข้อมูลเพิ่มเติม 2. ดำเนินการตามแนวปฏิบัติในการลบหรือทำลายข้อมูลหลังจากไม่ได้ใช้งาน	การควบคุม (Treat)	ผู้ดูแลระบบกอง/สำนักที่เกี่ยวข้อง