บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (กลุ่มคอมพิวเตอร์และระบบเครือข่าย โทร. ๒๓๔๒)

ที่ กษ ๐๖๐๘/ ๕๑๐ **วันที่** ๒๕ มิถุนายน ๒๕๖๗

เรื่อง ขออนุมัติแผนรับมือภัยคุกคามทางไซเบอร์ และแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์

เรียน อธิบดีกรมปศุสัตว์

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยแห่งชาติ เรื่องมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ เพื่อให้หน่วยงานจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ และแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ ทั้งในส่วนของประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐาน นั้น

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ และแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ เพื่อกำหนดวิธีการในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ ป้องกัน และลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ และเตรียมความพร้อมด้านบุคลากรของกรมปศุสัตว์ ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์ และให้การปฏิบัติงานเป็นอย่างมีระบบ และต่อเนื่องสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดอนุมัติแผนรับมือภัยคุกคามทางไซเบอร์ และแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ ทั้งนี้เป็นอำนาจของรองอธิบดี โสภัชย์ ชวาลกุล ตามคำสั่งกรมปศุสัตว์ ที่ ๘๔๔/๒๕๖๖ ลงวันที่ ๒๘ กันยายน ๒๕๖๖

(นางสาวบุณิกา จุลละโพธิ)
ผู้อำนวยการ
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

อนุมัติ
ลงนามแล้ว

(นายโสภัชย์ ชวาลกุล)
รองอธิบดี ปฏิบัติราชการแทน
อธิบดีกรมปศุสัตว์
๒๗ มิ.ย. ๒๕๖๗

กรมปศุสัตว์

Department of Livestock Development

แผนรับมือภัยคุกคามทางไซเบอร์
และ
แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมปศุสัตว์
มิถุนายน 2567

ประวัติการแก้ไขเอกสาร

เวอร์ชัน	รายละเอียดการแก้ไข	วันที่จัดทำ
01	เอกสารเวอร์ชันตั้งต้น	

การอนุมัติเอกสาร

ผู้จัดทำเอกสาร	
ชื่อ นางสาวภาณุตา บุนนาค ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ วันที่	ลงชื่อ ..... (นางสาวภาณุตา บุนนาค)
ผู้ตรวจทานเอกสาร	
ชื่อ นางสาวบุณิกา จุลละโพธิ ตำแหน่ง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร วันที่	ลงชื่อ ..... (นางสาวบุณิกา จุลละโพธิ)
ผู้อนุมัติเอกสาร	
ชื่อ นายโสภัชย์ ชวาลกุล ตำแหน่ง รองอธิบดีกรมปศุสัตว์ วันที่	ลงชื่อ ..... (นายโสภัชย์ ชวาลกุล)

สารบัญ

เรื่อง **หน้า**

แผนรับมือภัยคุกคามทางไซเบอร์

กรมปศุสัตว์

1. หลักการและเหตุผล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยต้องประกอบด้วยเรื่องดังต่อไปนี้

1.1 แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจ ประเมินผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปละหนึ่งครั้ง

1.2 แผนรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กรมปศุสัตว์ จึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่มาในรูปแบบ ไวรัสคอมพิวเตอร์ และการโจมตีระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ โดยการดำเนินงานตามแผนจะมุ่งเน้นในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึง การกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางให้สามารถใช้งานได้

2. วัตถุประสงค์

2.1 เพื่อกำหนดวิธีการในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2.2 เพื่อกำหนดวิธีการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ ให้สามารถใช้งานได้

2.3 เพื่อเตรียมความพร้อมตานบุคลากรของกรมปศุสัตว์ ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์

2.4 เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอน

3. รูปแบบภัยคุกคามไซเบอร์

3.1 ซอฟต์แวรประสงค์ร้าย (Malicious Software) หรือมัลแวร (Malware) ซึ่งเป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

3.2 ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวรชนิดหนึ่ง ที่สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ซึ่งไวรัสคอมพิวเตอร์จะแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่นๆ โดยใช้พาหะ เช่น แฟลชไดรว์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

3.3 หนอนคอมพิวเตอร์ (Computer Worm) เปนมัลแวรชนิดหนึ่ง สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่นๆ โดยที่เจาของเครื่องคอมพิวเตอร์ไมอนุญาต โดยหนอนคอมพิวเตอร์จะตางกับไวรัสตรงที่ไวรัสจะแพรกระจายตัวเองไปสูคอมพิวเตอร์เครื่องอื่นๆ โดยอาศัยพาหะ แตหนอนคอมพิวเตอร์จะใชวิธีสแกนเครื่องคอมพิวเตอร์ที่อยูในระบบเครือข่ายและตรวจหาชองโหวของระบบปฏิบัติการหรือชองโหวของแอพพลิเคชั่น จากนั้นจึงทำการคัดลอกตัวเองเขาไปฝงตัวโดยใชชองโหวดังกล่าว

3.4 มาโทรจัน (Trojan Horse) เปนมัลแวรชนิดหนึ่ง ที่มีจุดประสงคเพื่อบุกรุก เขาถึง และควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟลข้อมูลสำคัญ หรือทำการคัดลอกข้อมูลดังกล่าวสงใหแกผูคุกคามผ่านระบบเครือข่ายอินเทอรเน็ต ซึ่งข้อมูลสำคัญที่ผูคุกคามต้องการอาจเปนชื่อผูใช รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่นๆ ลักษณะของการติดตั้งมาโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัยพาหะซึ่งอาจมาจากแฟลชไดรว หรือทางอีเมล

3.5 สปายแวร (Spyware) เปนมัลแวรชนิดหนึ่ง ที่มีวัตถุประสงคเพื่อบันทึกการกระทำของผูใชบนเครื่องคอมพิวเตอร์และสงผ่านอินเทอรเน็ตโดยที่ผูใชไมไดรับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูลสถิติการใชงานจากผูใชไดหลายอย่างขึ้นอยูกับการออกแบบของโปรแกรม

3.6 ซอฟตแวรเรียกคาไถ (Ransomware) เปนมัลแวรชนิดหนึ่ง ที่มีพฤติกรรมเขารหัสไฟลตางๆ ที่อยูบนเครื่องคอมพิวเตอร์ไมวาจะเปนไฟลเอกสาร รูปภาพ วิดีโอ ผูใชงานจะไมสามารถเปดไฟลใดๆ ไดเลยหากไฟล์เหล่านั้นถูกเขารหัส ซึ่งการถูกเขารหัสก็หมายความวาจะต้องใชคียในการปลดล็อคเพื่อกูข้อมูลคืนมาผูใชงานจะต้องทำการจายเงินตามข้อความ "เรียกคาไถ" ที่ปรากฏ

3.7 ประตูหลัง (Backdoor) เปนชองทางพิเศษที่ใชเขาถึงระบบงานคอมพิวเตอร์โดยที่ไมต้องผ่านการพิสูจน์ทราบตัวตน ซึ่งสวนใหญเมื่อผูบุกรุกสามารถเจาะเขาระบบไดแล้ว ก็จะสร้างประตูหลังเอาไวเพื่อใชในการบุกรุกเขาสูระบบงานคอมพิวเตอร์ในภายหลัง

3.8 Rootkit เปนโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบ หรือขโมยข้อมูลที่อยูในระบบคอมพิวเตอร์ ทั้งนี้ นอกจากใชสำหรับบุกรุกเขาสูระบบงานแล้ว Rootkit ยังอาจใชเพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ดวย

3.9 การโจมตีแบบ DoS/DDOS มีจุดประสงคเพื่อทำใหเครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตีมีเครื่องเดียว เรียกวาการโจมตีแบบ Denial of Service (DoS) แตหากมีเครื่องคอมพิวเตอร์ที่โจมตีมีมากกวา 1 เครื่องและกระทำพรอมๆ กัน ไมวาจะโดยตั้งใจหรือไมตั้งใจ จะเรียกวา การโจมตีแบบ Distributed Denial of Service (DDoS)

3.10 Botnet เปนกลุมของอุปกรณ์ที่ติดมัลแวรและถูกเปลี่ยนเปน Bot (ยอมาจาก Robot) ไมวาจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราทเตอร หรืออุปกรณ์ IoT อื่นๆ เพื่อรอรับคำสั่งจากผูบุกรุก (Hacker) โดยผูบุกรุก (Hacker) จะนำ Botnet ที่มีไปใชในการโจมตีขนาดใหญ เชนการทำ DDoS เปนตน

3.11 Spam Mail หรืออีเมลขยะ เปนขยะออนไลนที่สงตรงถึงผูรับ โดยที่ผูรับสารนั้นไมต้องการ และสร้างความเดือดรอนรำคาญให้กับผูรับไดในลักษณะของการโฆษณาสินค้า หรือบริการ การชักชวนเข้า ไปยังเว็บไซต ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเขามาดวย ดวยเหตุนี้จึงควรติดตั้งระบบ Anti-Spam หรือหากใชฟรีอีเมลก็จะมีโปรแกรมคัดกรองอีเมลขยะในชั้นหนึ่งแลว

3.12 Phishing คือการหลอกลวงทางอินเทอรเน็ต เพื่อขอข้อมูลที่สำคัญเชน รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการสงข้อความผ่านทางอีเมลหรือเมสเซนเจอร ตัวอย่างของการฟชชิง เชน การบอกแกผูรับปลายทางวา เปนธนาคารหรือบริษัทที่นาเชื่อถือ และแจงวามีสาเหตุทำให้คุณต้องเข้าสูระบบและ ใสข้อมูลที่สำคัญใหม โดย เว็บไซตที่ลิงกไปนั้น จะมีหนาตาคลายคลึงกับเว็บที่กล่าวถึง Phishing

3.13 Sniffing เปนการดักข้อมูลที่สงจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เปนวิธีการหนึ่งที่ผูบุกรุกระบบนิยมใช

3.14 Hacking เปนการเจาะระบบเครือข่ายคอมพิวเตอร์ไมวาจะกระทำดวยมนุษยหรืออาศัยโปรแกรมด้วยวัตถุประสงคต่างๆ กัน ทั้งนี้โดยทั่วไปแลวการ Hacking เปนสิ่งที่ผิดกฎหมาย แต่อย่างไรก็ตามหากไดรับอนุญาตก็ไมใชสิ่งผิดกฎหมายโดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เชน การเจาะระบบเพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายขององคกร

3.15 ผูบุกรุก (Hacker) หมายถึง ผูที่ไมไดรับอนุญาตในการใช้งานระบบ แตพยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงคต่างๆ ไมวาจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจสวนบุคคลก็ตามความเสียหายจากผูบุกรุกเป็นภัยคุกตามที่หนัก

4. การเตรียมความพรอมในการรับมือปญหาภัยคุกคามทางไซเบอร์

เพื่อให้กรมปศุสัตว์ มีความพรอมในการรับมือปญหาภัยคุกคามทางไซเบอร์ตามที่ระบุในข้อ 3 กรมปศุสัตว์จะดำเนินการเตรียมความพรอมในด้านต่างๆ ดังนี้

4.1 การเตรียมพรอมด้านอุปกรณ์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ สามารถรับมือกับภัยคุกคามทาง ไซเบอร์ได กรมปศุสัตว์ จึงควรจัดหาอุปกรณ์และซอฟตแวรที่จำเปนดังนี้

4.1.1 อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท DoS/DDoS BOTNET Phishing Sniffing Hacker ทั้งนี้อุปกรณ์ป้องกันระบบเครือข่ายที่จัดหานอกจากความสามารถในการเปน Firewall แล้วยังต้องมีความสามารถอื่นๆ เพิ่มเติม ซึ่งได้แกความสามารถในด้านการตรวจจับการบุกรุก (IPS) ความสามารถในการคัดกรองเว็บไซตอันตราย (Web filtering) และ การควบคุมการใช้งานซอฟตแวร (Application Control) เปนอย่างนอย

4.1.2 ซอฟตแวรตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์

4.1.3 อุปกรณ์ web app firewall ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบงานคอมพิวเตอร์ของกรมปศุสัตว์ ที่พัฒนาขึ้นมาให้บริการผ่าน web browser ได้แก การคุกคามทางไซเบอร์ประเภท Hacker โดยสามารถป้องกันเทคนิคการบุกรุกเชน Cross-site scripting และ sql injection ได้เปนอย่างนอย

4.1.4 ซอฟตแวรสำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และการกู้ข้อมูลของระบบเครือข่ายคอมพิวเตอร์ของกรมปศุสัตว์ รวมทั้งยังสามารถสำรองข้อมูลแบบเขารหัสได

4.1.5 ระบบคลาวด์กลางภาครัฐ GDCC Cloud) ใช้ในระดับกรม (Agency Cloud) เพื่อเป็นโครงสร้างพื้นฐานด้านดิจิทัลรองรับหน่วยงานรัฐให้เข้าถึงทรัพยากรด้านคลาวต์ด้วยมาตรฐานสากลระดับ Tier 4 พร้อม SLA 99.99% ซึ่งเป็นไปตามเป้าหมายของกระทรวงดิจิทัลฯ ในการพัฒนาคลังข้อมูลดิดิจิทัลภาครัฐ และใช้ประโยชน์ Big Data จากคลังข้อมูลให้สามารถการบูรณาการข้อมูลข้ามหน่วยงานกันได้อย่างเป็นระบบเพื่อนำสู่การปรับปรุงเพิ่มประสิทธิภาพบริการดิจิทัลให้แห้แก่ประชาชนและเป็นข้อมูลในการพัฒนาประเทศในทุกมิติ

4.1.6 ระบบงานคอมพิวเตอร์สำรอง ใชในกรณีที่ไมสามารถกูระบบงานคอมพิวเตอร์ขึ้นมาได

4.1.7 อุปกรณ์จัดเก็บ Log file ใชสำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์

4.1.8 อุปกรณ์วิเคราะห Log file ใชสำหรับวิเคราะหข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ ซึ่งข้อมูลที่ถูกวิเคราะหดังกล่าวจะชวยระบุถึงหมายเลข IP Address ของผูโจมตี และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ และใชประกอบการทำรายงานให้แกคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

4.1.9 ซอฟตแวรป้องกันไวรัสคอมพิวเตอร์แบบคอรปอเรต (Corporate Antivirus Software) ใชสำหรับติดตั้งบนเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์ แม่ข่ายของกรมปศุสัตว์ ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware, Computer Virus, Computer worm, Trojan, Spyware, Ransomware, BOTNET, Spam Mail

4.2แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา กรมปศุสัตว์จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปละ 1 ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้อาจสามารถดันหาภัยคุกคามไซเบอร์ประเภท Backdoor ที่ถูกซอนเอาไว้จากขั้นตอนการพัฒนาระบบงานคอมพิวเตอร์ได

4.3 การเตรียมพรอมด้านบุคลากร

4.3.1 การให้ความรู้ เพื่อให้บุคลากรของกรมปศุสัตว์ มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ กรมปศุสัตว์จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการจัดฝึกอบรมให้ความรู้แกบุคลากรของกรมปศุสัตว์

4.3.2 การแจ้งรายชื่อเจ้าหน้าที่ สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตราที่ 46 กำหนดให้หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยกรมปศุสัตว์จะกำหนดระดับภัยคุกคามทางไซเบอร์ ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตราที่ 60 และจะแจ้งรายชื่อผู้เจ้าหน้าที่เพื่อประสานงานด้านการรักษาความปลอดภัยไซเบอร์ในระดับต่างๆ

4.3.3 มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์

4.4 การเตรียมพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรอง ในกรณีที่ภัยคุกคามทางไซเบอร์ก่อให้เกิดความเสียหายแกระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์อย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน กรมปศุสัตว์จะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ สามารถกลับมาใช้งานได้อย่างรวดเร็วที่สุด ทั้งนี้แนวทางในการกู้คืนข้อมูล และการใช้ระบบคอมพิวเตอร์สำรองจะกำหนดอยู่ในเอกสารแผนสำรองและกู้คืนระบบของกรมปศุสัตว์

5. ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์

ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทาง ปฏิบัติและกรอบมาตรฐานของแตละหน่วยงานให้สอดคล้องกับนโยบายและแผนวาด้วยการรักษาความมั่นคง ปลอดภัยไซเบอร์โดยเร็ว ทั้งนี้ทางกรมปศุสัตว์ ไดมีมาตรการสำหรับรับมือกับภัยคุกคามทางไซเบอร์ 3 มาตรการดังนี้

5.1 มาตรการตรวจสอบและเฝาระวังภัยคุกคามทางไซเบอร์ (Detect) มีขั้นตอนดังนี้ การตรวจสอบและเฝาระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) คือ การที่ต้องสร้างกลไกและกระบวนการเพื่อ

- ตรวจจับเหตุการณที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของกรมปศุสัตว์
- การจัดประเภทและวิเคราะหเหตุการณที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ
- การระบุวามีภัยคุกคามทางไซเบอร์หรือเหตุการณที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับบริการที่สำคัญของกรมปศุสัตว์หรือไม และดำเนินการทบทวนกลไก และกระบวนการอย่างน้อยปละ 1 ครั้ง เพื่อให้แนใจวากลไก และกระบวนการตางๆ ยังคงมีประสิทธิภาพ

5.2 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response) มี 3 ขั้นตอน ดังนี้

5.2.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปละ 1 ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

5.2.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

1) ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ

2) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต มีการดำเนินการต่อไปนี้

- จัดตั้งทีมสื่อสารในภาวะวิกฤต เพื่อเปิดใช้งานในช่วงวิกฤต
- ระบุสถานการณ์จำลองเหตุการณ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง
- ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท
- ระบุผู้แทนหน่วยงานหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน
- ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

3) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

4) ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปละ 1 ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

5.2.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

1) กรมปศุสัตว์ ต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์หาก ได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำ โดยคณะกรรมการการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ ทั้งในระดับชาติ หรือระดับภาคส่วน กรมปศุสัตว์ต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกข้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

2) ต้องปฏิบัติตามคำขอใดๆ ของคณะกรรมการ เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญกรมปศุสัตว์ เพื่อวัตถุประสงค์ในการวางแผน และดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตและขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของกรมป้องกัน และบรรเทาสาธารณภัย

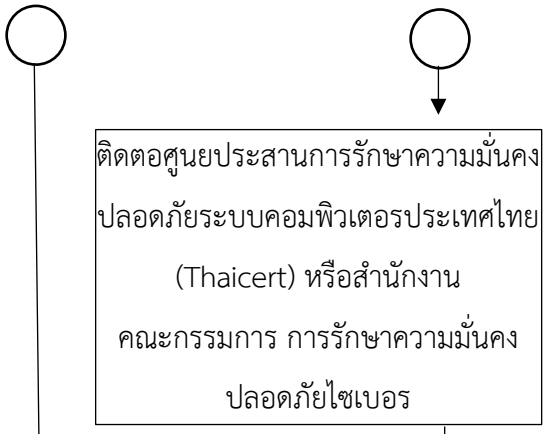
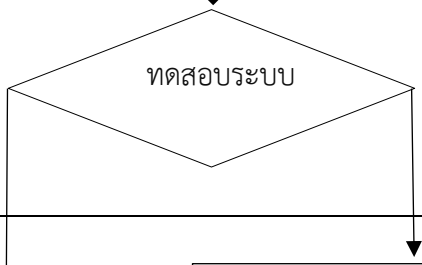
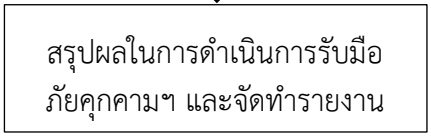
5.3 มาตรการรักษาและฟนฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)

5.3.1 ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย สามารถให้บริการที่จำเปนต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เชน ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เปนตน

5.3.2 ต้องตรวจสอบให้แน่ใจวามีการฝกซอม BPC อย่างนอยปละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

กรมปศุสัตว์ได้จัดทำขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอรซึ่งเปนการดำเนินการเบื้องตันดังนี้

ขั้นตอน	รายละเอียด
ตรวจพบภัยคุกคามทางไซเบอร	มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจจับการคุกคามทางไซเบอรได้จากอุปกรณ์ป้องกันระบบเครือข่าย หรือเครื่องมือต่างๆ ตามที่กำหนดในข้อ 3.1 ซึ่งจะช่วยให้กรมปศุสัตว์ สามารถตรวจพบการคุกคามทางไซเบอร์อย่างรวดเร็ว
ตรวจสอบภัยคุกคามทางไซเบอร	ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัยคุกคามตามที่กำหนดใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร พ.ศ. 2562 มาตรา 62
การควบคุมภัย คุกคามทางไซเบอร์	ดำเนินการควบคุมภัยคุกคามทางไซเบอร ให้สงผลกระทบน้อยที่สุดและป้องกันไม่ให้เกิดการแพรกระจายไปยังสวนอื่นๆ ซึ่งในกรณีที่เรงด่วนกรมปศุสัตว์ จะทำการปิดระบบ หรือตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว
แกไขปญหา	ดำเนินการแกไขหรือกำจัดภัยคุกคามทางไซเบอรในเบื้องตนในทันที

ขั้นตอน	รายละเอียด
	ในกรณีที่ไมสามารถแกไขปญหาได้จะดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร แหงชาติ เพื่อขอคำแนะนำหรือขอความชวยเหลือ
	หลังจากแกไขปญหาภัยคุกคามไซเบอรแลว กรมปศุสัตว์จะดำเนินการตรวจหาชองโหว โดยอุปกรณ์ ตรวจสอบช่อโหวระบบเครือข่าย หรือเครื่องมืออื่นๆ และหาวิธีเพื่อป้องกันการเกิดภัยคุกคาม ไซเบอรในลักษณะเดิม
	ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกรมปศุสัตว์วาสามารถทำงานไดสมบูรณหรือไม ในกรณีที่พบวาการทำงานไม่สมบูรณ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกูคืนระบบงาน
	ดำเนินการตามขั้นตอนการกูคืนข้อมูลตามที่ระบุในแผนการสำรองและกูคืนระบบ ในกรณีที่กูคืนระบบไมได กรมปศุสัตว์จะพิจารณาเปดใชระบบงานคอมพิวเตอร์สำรอง และเรงกูระบบงานคอมพิวเตอร์หลัก
	เมื่อโครงสรางพื้นฐานสำคัญทางสารสนเทศของกรมปศุสัตว์สามารถทำงานได้ตามปกติแล้ว หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศของกรมปศุสัตว์จะดำเนินการสรุปผลในการ ดำเนินการรับมือภัยคุกคามไซเบอร์
	สรุปผลในการรับมือภัยคุกคามทางไซเบอร และแจ้งผลการดำเนินงานใหแกผู้เกี่ยวข้อง เชน ผูอำนวยการกองผูบริหารระดับสูงด้านสารสนเทศ

6. การเตรียมพรอมรับมือภัยคุกคามทางไซเบอรในสวนของเจาหนาที่กรมปศุสัตว์

เมื่อเกิดการคุกคามทางไซเบอรแล้ว ในบางครั้งผลกระทบที่เกิดขึ้นอาจสงผลใหการทำงานของเครื่องคอมพิวเตอร์ของเจาหนาที่กรมปศุสัตว์ทำงานผิดพลาดหรือลาชาลง หรือสงผลใหไฟลข้อมูลที่ถูกจัดเก็บเอาไวในเครื่องคอมพิวเตอร์ไมสามารถใชงานได้ และยากต่อการกูคืนใหเปนปกติ ดังนั้นเจาหนาที่ของกรมปศุสัตว์ควรดำเนินการเตรียมพรอมรับมือภัยคุกคามทางไซเบอรดังนี้

6.1 ดำเนินการตามนโยบายการใชงานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์อย่างเคร่งครัด

6.2 ดำเนินการตามนโยบายการใชงานเครื่องคอมพิวเตอร์สวนบุคคล และ นโยบายการใชงานเครื่อง คอมพิวเตอร์แบบพกพาอย่างเคร่งครัด

7. การประเมินความเสี่ยง (Risk Assessment)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ประเมินความเสี่ยง (Risk Assessment) ของภัยพิบัติและสถานการณ์ฉุกเฉินที่สำคัญ ส่งผลกระทบต่อระบบสารสนเทศกรมปศุสัตว์ โดยพิจารณาจากปัจจัยสภาพแวดล้อมต่างๆ มาตรการ เครื่องมือ การดำเนินงานในปัจจุบัน ดังนี้

7.1 ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้

ปัจจัยเสี่ยงที่เกิด	ผลกระทบที่เกิดขึ้น
ไฟฟ้าดับ/ขัดข้อง	ทำให้ไม่สามารถเข้าถึงข้อมูล เกิดความเสียหายต่อฐานข้อมูลและระบบสารสนเทศ
เพลิงไหม้	ทำลายระบบสารสนเทศ /ฐานข้อมูล /เอกสาร /อาคาร สถานที่ทรัพย์สิน ของทางราชการ และความปลอดภัยของบุคลากร
บุกรุกระบบคอมพิวเตอร์	ทำให้ไม่สามารถเข้าถึงข้อมูล เกิดความเสียหายต่อฐานข้อมูล และระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นเหตุการณ์ที่มีโอกาสเกิดขึ้นบ่อยครั้ง
เครือข่ายขัดข้อง	ระบบสารสนเทศหยุดชะงัก ทำให้ไม่สามารถใช้งานระบบได้

7.2 โอกาสที่จะเกิด (Likelihood: L) ปัญหาความเสี่ยงในแง่ของโอกาสที่จะเกิดเหตุ (Likelihood) หรือเหตุการณ์ (Event) ของภัยพิบัติที่สำคัญว่ามีมากน้อยเพียงไร และผลกระทบ (Impact) ที่ติดตามมาว่ามีความเสียหายรุนแรง มากน้อยเพียงใด โดยใช้เกณฑ์ในการประเมินระดับโอกาส (Likelihood) การเกิด แบ่งเป็น 5 ระดับ ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood)		
ระดับ	**โอกาสที่จะเกิด (ความเป็นไปได้)**	**คำอธิบาย**
5	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง
4	สูง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
3	ปานกลาง	มีโอกาสเกิดบางครั้ง
2	ต่ำ	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
1	ต่ำมาก	มีโอกาสเกิดในกรณียกเว้น

7.3 ผลกระทบ (Impact: I) หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้น หากเกิดเหตุการณ์ความเสี่ยง

เกณฑ์ที่ใช้ในการประเมินผลกระทบ (Impact) ที่จะเกิดความเสี่ยง แบ่งออกเป็น 5 ระดับ ดังนี้

ระดับความรุนแรงของผลกระทบ (Impact)		
ระดับ	**ระดับผลกระทบ**	**คำอธิบาย**
5	สูงมาก	เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายต่อความปลอดภัยของข้อมูลต่างๆ บางส่วน
3	ปานกลาง	ระบบ IT มีปัญหา และมีความเสียหายไม่มาก
2	ต่ำ	ระบบ IT มีปัญหา และมีความเสียเพียงเล็กน้อย และสามารถแก้ไขได้
1	ต่ำมาก	ระบบ IT มีปัญหา ซึ่งไม่เกิดผลกระทบต่อข้อมูลต่างๆ

7.4 ระดับความเสี่ยง (Degree of Risk: D) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง มีค่าเป็นเชิงปริมาณ ซึ่งคำนวณได้จากสูตรต่อไปนี้

คะแนนระดับความเสี่ยง = ระดับโอกาส X ระดับผลกระทบของความเสี่ยง หรือ D = L x I

การประเมินผลกระทบและความรุนแรงภัยพิบัติและสถานการณ์ฉุกเฉินที่สำคัญ

ปัจจัยความเสี่ยงที่เกิด	**โอกาสที่จะเกิด**	**ระดับผลกระทบ**	**คะแนนระดับความเสี่ยง**	**ลำดับที่**
เครือข่ายขัดข้อง	3	5	15	1
บุกรุกระบบคอมพิวเตอร์	3	5	15	1

ปัจจัยความเสี่ยงที่เกิด	โอกาสที่จะเกิด	ระดับผลกระทบ	คะแนนระดับความเสี่ยง	ลำดับที่
ไฟฟ้าดับ/ขัดข้อง	3	4	12	2
เพลิงไหม้	3	4	12	2
อุปกรณ์ไม่สามารถทำงานได้ โดยไม่ทราบสาเหตุ	3	4	12	2
จลาจล การชุมนุม/เหตุการณ์ความไม่สงบ	2	3	6	3
อุทกภัย	1	3	3	4
แผ่นดินไหว	1	2	2	5

โดย ระดับความเสี่ยงจำแนกตามสีใน Risk Matrix เป็นดังนี้

ระดับความเสี่ยง	สูงมาก	สูง	ปานกลาง	ต่ำ
คะแนนระดับความเสี่ยง	16 - 25	10 - 15	5 - 9	1 - 4

ระดับความเสี่ยง	ระดับคะแนน	สีสัญลักษณ์	ความหมาย
ต่ำ	1 - 4	สีเขียว	ยอมรับความเสี่ยง โดยไม่จำเป็นต้องมีมาตรการ จัดการเพิ่มเติม
ปานกลาง	5 - 9	สีเหลือง	ยอมรับความเสี่ยง แต่มีแผนควบคุมความเสี่ยง โดย กำหนดผู้รับผิดชอบและกรอบระยะเวลาที่ชัดเจน
สูง	10 - 15	สีส้ม	มีแผนลดความเสี่ยง ไม่สามารถยอมรับได้ต้อง จัดการความเสี่ยงเพื่ออยู่ในระดับที่ยอมรับได้
สูงมาก	16 - 25	สีแดง	มีแผนลดและประเมินซ้ าหรือถ่ายโอนความเสี่ยง จะต้องมีการกำหนดมาตรการในการจัดการความ เสี่ยงเพิ่มเติมโดยทันที

7. การประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
1. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)							
1) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	1. ระบบคอมพิวเตอร์ และระบบเครือข่ายถูกทำลาย 2. ระบบสารสนเทศ และระบบฐานข้อมูลถูกทำลาย	1	5	5	1. ตรวจสอบระบบดับเพลิง แบบอัตโนมัติตามมาตรฐานทุก 3 เดือน 2. ตรวจสอบการทำงานของ ศูนย์สำรอง Disaster Recovery Site (DR Site)ทุก 3 เดือน	การควบคุม (Treat)	นายศิริพล พจนวิเศษ, นายพยุง ตรีกมล
2) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	1. ไม่สามารถใช้งานระบบคอมพิวเตอร์ และระบบเครือข่ายได 2. ไม่สามารถใช้งานระบบสารสนเทศและระบบฐานข้อมูลได 3. ระบบปฏิบัติการ และระบบฐานข้อมูล เกิดความเสียหายจากการที่เครื่องไม่ได้ถูกทำการปิดอย่างเหมาะสม	1	4	4	1. ตรวจสอบระบบสำรอง ไฟฟ้า (UPS) ในศูนย์คอมพิวเตอร์แม่ข่ายกลางทุก 3 เดือน	การถ่ายโอน (Transfer)	นายศิริพล พจนวิเศษ, นายพยุง ตรีกมล

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
3) ความเสี่ยงจากอุณหภูมิ และความชื้นของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)	เกิดความเสียหายต่อเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย	1	4	4	ตรวจสอบเครื่องปรับอากาศ ที่ควบคุมอุณหภูมิ และความชื้นทุก 3 เดือน	การถ่ายโอน (Transfer)	นายศิริพล พจนวิเศษ
4) ความเสี่ยงจากแมลง สัตวกัดแทะอุปกรณ์เครือข่าย และระบบไฟฟ้า	1. ไม่สามารถใช้งานระบบเครือข่ายได้ 2. ไม่สามารถให้บริการระบบเครือข่ายได้อย่างต่อเนื่อง	1	3	3	ตรวจสอบอุปกรณ์เครือข่าย และระบบไฟฟ้าทุก 3 เดือน	การยอมรับ (Take)	นายศิริพล พจนวิเศษ
5) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง	1. อุปกรณ์ และข้อมูลที่มีความสำคัญสูญหาย 2. เสียภาพลักษณ์ของหน่วยงาน	1	3	3	1. ติดตั้งระบบรักษาความ ปลอดภัยในการควบคุมการ เข้า-ออกห้องคอมพิวเตอร์แม่ข่าย 2. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ๆ มีเครื่องคอมพิวเตอร์ และอุปกรณ์ติดตั้ง 3. ตรวจสอบการทำงานของ ศูนย์สำรอง Disaster Recovery Site (DR Site) ทุก 3 เดือน	การยอมรับ (Take)	นายศิริพล พจนวิเศษ, นายพยุง ตรีกมล

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
2. ความเสี่ยงด้านบุคลากร (Human Risk)							
6) ความเสี่ยงจากผู้ดูแลระบบ	ข้อมูลที่อยู่ในชั้นความลับรั่วไหล ทำให้เสียหายต่อความน่าเชื่อถือของหน่วยงาน	1	3	3	1. การทำ Authentication การเข้าใช้ระบบสารสนเทศ รวมถึงการยกเลิกทะเบียน (เกษียณอายุ/ลาออก ฯลฯ) ย้าย 2. การจัดระดับการเข้าถึง ข้อมูลอย่างเป็นระบบ และสิทธิในการกระทำกับข้อมูล	การยอมรับ (Take)	นายศิริพล พจนวิเศษ
7) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์ และระบบเครือข่าย	1. สูญเสีย Bandwidth ในระบบเครือข่ายทำให้ต้องเพิ่ม Bandwidth ให้มากขึ้น เนื่องจากการใช้งานนอกเหนือจากงานราชการ 2. เครื่องคอมพิวเตอร์เสียหาย และเสื่อมอายุการใช้งานเร็วกว่าปกติ	2	3	6	1. กำหนด Policy ของ Firewall ให้เหมาะสมต่อการใช้งาน 2. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ไปใช้นอกเหนือจากงานราชการ และรายงานการใช้การปฏิบัติของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา	การควบคุม (Treat)	นายศิริพล พจนวิเศษ, นายพยุง ตรีกมล ,บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					3. ตรวจสอบและแนะนำ ผู้ใช้งานให้ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์ต่อพ่วงอย่างเหมาะสม		
3. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)							
8) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	1. เกิดความเสียหายต่อระบบสารสนเทศ และระบบฐานข้อมูล 2. ไม่สามารถใช้งานระบบสารสนเทศที่ความสำคัญ และต้องใช้งานอย่างเร่งด่วน	3	4	12	1. ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายหลักทุกวัน 2. สำรองระบบและข้อมูล (Backup) ทุกวัน 3. ทดสอบการกู้คืนระบบแม่ข่ายหลักเดือนละ 1 ครั้ง	การควบคุม (Treat)	นายศิริพล พจนวิเศษ
9) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร	1. โปรแกรมหรือข้อมูลถูกทำลาย 2. ไม่สามารถเรียกใช้โปรแกรม หรือระบบงานได้ตามปกติ 3. การถูกขโมยข้อมูลที่สำคัญ	3	2	6	1. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ (อัตโนมัติ) 2. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและใหมีผลบังคับใช้อย่างเคร่งครัด	การควบคุม (Treat)	นายศิริพล พจนวิเศษ

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
10) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่าย จากภายในและภายนอกองคกร	1. ระบบสารสนเทศของหน่วยงาน ไมสามารถใหบริการได 2. ทำใหระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัส และแพรกระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย 3. ถูกแกไขหรือเปลี่ยนแปลงข้อมูลหรือรูปภาพบน Web Site ของหน่วยงาน 4. ถูกโจรกรรมข้อมูลที่เปนความลับ 5. ไมสามารถเข่าใช่ระบบสารสนเทศได	4	4	16	1. อัพเดตโปรแกรมป้องกัน ไวรัสใหสามารถป้องกันไวรัสไดทุกรูปแบบ 2. ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และระบบเฝ้าระวัง เครือข่ายทุกวัน	การควบคุม (Treat)	นายศิริพล พจนวิเศษ, นายพยุง ตรีกมล ,บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
11) ความเสี่ยงจากการเชื่อมต่อ ระบบเครือข่ายอินทราเน็ต และอินเทอร์เน็ตภายใน และภายนอก สถานที่ทำงาน	1. ระบบเครือข่ายอินทราเน็ต และอินเทอรเน็ตไมสามารถใชงานได 2. ไมสามารถเข่าใช่งานระบบสารสนเทศผ่านเครือข่ายอินทราเน็ตและอินเทอรเน็ตได	2	3	6	1. ตรวจสอบระบบเครือข่ายสื่อสารหลักทุกวัน 2. ควบคุมการเข่าใช่เครือข่ายอินทราเน็ต และอินเทอรเน็ต โดยใชระบบยืนยันตน (Authentication)	การยอมรับ (Take)	นายศิริพล พจนวิเศษ, นายพยุง ตรีกมล

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
12) ความเสี่ยงจากการถูกบล็อกจากผู้ใหบริการเครือข่าย (Black List)	1. ผู้ใช้งานที่ต้องการข้อมูลของหน่วยงาน หรือประชาชนทั่วไปไม่สามารถเขาใชงาน Web Server ได 2. ลดความนาเชื่อถือของหน่วยงาน	1	3	3	1. อัพเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสไดทุกรูปแบบ 2. ปรับปรุง Policy Firewall 3. Monitoring ระบบเครือข่ายเป็นประจำทุกวัน	การยอมรับ (Take)	นางสุวรรณี กาญจนภูสิต, นายเอกพงศ์ สุวรรณพงศ์
13) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)	ระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference) ขัดข้อง ทำให้ผู้บริหาร และหน่วยงานที่เกี่ยวข้อง ไม่สามารถเข้าร่วมประชุมได ผู้ไม่เกี่ยวข้องเข้าร่วมประชุมแบบไม่ได้เชิญ	1	3	3	ตรวจสอบการเชื่อมต่ออุปกรณ์การทำงานของระบบชุดประชุมทางไกลผ่านเครือข่าย (VDO Conference) ก่อนใชงาน	การยอมรับ (Take)	นายวัชรพงศ์ ชื่นพิมลชาญกิจ ,นายสุรชัย ถมวิจิตร
4. ความเสี่ยงดานโปรแกรมคอมพิวเตอร์ (Software Risk)							
14) ความเสี่ยงจากการใชซอฟตแวร ที่ไมมีลิขสิทธิ์	1. การถูกฟองร้อง และเสื่อมเสียชื่อเสียง และความนาเชื่อถือของหน่วยงาน 2. การใชงานอาจไมได้ประสิทธิภาพตามความสามารถของซอฟตแวรนั้นๆ	1	3	3	1. การจัดหาซอฟตแวรที่ถูก กฎหมายมาใชงานตามความจำเป็น 2. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใชงาน Open Source	การยอมรับ (Take)	นายศิริพล พจนวิเศษ, นายพยุง ตรีกมล

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
	3. หน่วยงานอาจถูกฟองร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ						
15) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	1. สร้างความเสียหายต่อระบบคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศและระบบฐานข้อมูล 2. ลดความน่าเชื่อถือต่อหน่วยงาน	1	3	3	1. อัพเดทเครื่องมือ และโปรแกรมที่ใช้พัฒนาอย่างสม่ำเสมอ 2. ตรวจสอบช่องโหว่ และดำเนินการแก้ไขทุก 3 เดือน	การยอมรับ (Take)	นายศิริพล พจนวิเศษ, นายพยุง ตรีกมล
16) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	1. ไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่ และแก้ไขการทำงานที่ ผิดพลาดได้อย่างทันท่วงที 2. ขาดการดูแลบำรุงรักษาโปรแกรม และข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว เนื่องจากโปรแกรมหมด ลิขสิทธิ์ และขาดการปรับปรุง (Update) โปรแกรม 3. ไม่สามารถเชื่อมโยงข้อมูลกับระบบ Big Data ของกรมปศุสัตว์ได้ ในกรณีมีการปรับปรุง	1	3	3	1. กำหนดให้มีการส่งมอบเอกสารที่ใช้ในการวิเคราะห์ออกแบบการพัฒนาระบบ และชุดคำสั่ง (Source Code) ฉบับสมบูรณ์ ทั้งในกรณีพัฒนาเสร็จสิ้น และเมื่อมีการปรับปรุงแก้ไข 2. ส่งมอบชุดคำสั่ง (Source Code) ชุดสมบูรณ์ 3. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่	การควบคุม (Treat)	นายศิริพล พจนวิเศษ, นายพยุง ตรีกมล ,บริษัท ที่รับ MA

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					4. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรม และข้อมูลให้มีความทันสมัยและใช้งานได้อย่างต่อเนื่อง		
5. ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)							
17) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน	1. ระบบฐานข้อมูลไม่สามารถนำไปใช้สนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ 2. ลดความน่าเชื่อถือของหน่วยงาน 3. ข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน	1	3	3	1. จัดทำรายการข้อมูล และความถี่ในการปรับปรุง 2. กำหนดมาตรการ แนวทางการปรับปรุง และช่องทางการเข้าถึงข้อมูล เพื่อให้ผู้ดูแลข้อมูลถือปฏิบัติ	การยอมรับ (Take)	นางสาวภาณุตา บุนนาค, นายวัชรพงศ์ ชื่นพิมลชาญกิจ
18) ความเสี่ยงจากการไม่สำรองข้อมูลและไม่สามารถกู้คืนระบบฐานข้อมูล	1. เกิดการสูญหายของข้อมูล และกระทบต่อการทำงานตามปกติ 2. ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้สนับสนุนการปฏิบัติงานได้	1	3	3	1. มีการสำรองระบบฐานข้อมูลเป็นประจำทุกวัน 2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) ทุกสัปดาห์	การยอมรับ (Take)	นางสาวภาณุตา บุนนาค, นายวัชรพงศ์ ชื่นพิมลชาญกิจ
19) ความเสี่ยงจากการโจมตีระบบฐานข้อมูล	1. ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ 2. ข้อมูลที่สำคัญสูญหาย และถูกทำลาย	1	4	4	1. ตรวจสอบระบบป้องกันการบุกรุกและระบบตรวจสอบ และเฝ้าระวังเครือข่ายเป็นประจำทุกวัน	การยอมรับ (Take)	นางสาวภาณุตา บุนนาค,

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					2. ตรวจสอบ Policy และLog ของระบบป้องกัน การบุกรุก และระบบเฝาระวังเครือข่ายเป็นประจำทุกวัน		นายวัชรพงศ์ ชื่นพิมลชาญกิจ

เกณฑ์การประเมินความเสี่ยง

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
5	สูงมาก	16 ครั้งขึ้นไป/ปี
4	สูง	11 - 15 ครั้ง/ปี
3	ปานกลาง	6 - 10 ครั้ง/ปี
2	น้อย	2 – 5 ครั้ง/ปี
1	น้อยมาก	1 ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	**ผลกระทบ**	**คำอธิบาย**
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	เกิดเหตุร้ายแรงหรือระบบมีปัญหา แต่มีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

ระดับ	จัดระดับความเสี่ยง	กลยุทธในการจัดการความเสี่ยง	พื้นที่สี
1 – 8	ต่ำ	ยอมรับความเสี่ยง (มีแผนรองรับ)	**ขาว**
9 – 16	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	**เหลือง**
17 – 24	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	**ฟ้า**
25	สูงมาก	ถ่ายโอนความเสี่ยง	**แดง**