



ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
เลขที่รับ 5/๐
วันที่ 27 มิ.ย. 2567
เวลา

กลุ่มช่วยอำนวยความสะดวก
เลขที่รับ 2892
วันที่ 25 มิ.ย. 2567
เวลา 1620
✓ 4

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 และต่อเนื่องสามารถแก้ไขสถานการณ์ได้อย่างทันที่

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดอนุมัติแผนรับมือภัยคุกคามทางไซเบอร์ และแผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์ ทั้งนี้เป็นอำนาจของรองอธิบดี โสภชัย ขวาลกุล ตามคำสั่งกรมปศุสัตว์ ที่ ๘๔๔/๒๕๖๖ ลงวันที่ ๒๘ กันยายน ๒๕๖๖

UNV

(นางสาวบุณิกา จุลละโพธิ์)
ผู้อำนวยการ
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

อนุมัติ

ลงนามแล้ว

95501

(นายโสภชัย ขวาลกุล)
รองอธิบดี ปฏิบัติราชการแทน
อธิบดีกรมปศุสัตว์

๒๗ มิ.ย. ๒๕๖๗



กรมปศุสัตว์
Department of Livestock Development

แผนรับมือภัยคุกคามทางไซเบอร์
และ
แผนบริหารความเสี่ยงและความปลอดภัยทางไซเบอร์

การอนุมัติเอกสาร

ผู้จัดทำเอกสาร	
ชื่อ นางสาวภาณุตา บุนนาค ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ วันที่	ลงชื่อ  (นางสาวภาณุตา บุนนาค)
ผู้ตรวจทานเอกสาร	
ชื่อ นางสาวบุณิกา จุลละโพธิ ตำแหน่ง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร วันที่	ลงชื่อ  (นางสาวบุณิกา จุลละโพธิ)
ผู้อนุมัติเอกสาร	
ชื่อ นายโสภชัย ขวาลกุล ตำแหน่ง รองอธิบดีกรมปศุสัตว์ วันที่	ลงชื่อ  (นายโสภชัย ขวาลกุล)

สารบัญ

เรื่อง	หน้า
1. หลักการและเหตุผล	1
2. วัตถุประสงค์	1
3. รูปแบบภัยคุกคามทางไซเบอร์	1
4. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์	3
5. ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์	4
5.1 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	4
5.2 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)	5
5.3 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)	5
6. การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ในส่วนของเจ้าหน้าที่กรมปศุสัตว์	7
7. การประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์	9

แผนรับมือภัยคุกคามทางไซเบอร์

กรมปศุสัตว์

1. หลักการและเหตุผล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติ และกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเร็ว ซึ่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยต้องประกอบด้วยเรื่องดังต่อไปนี้

1.1 แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

1.2 แผนรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กรมปศุสัตว์ จึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ที่มาในรูปแบบไวรัสคอมพิวเตอร์ และการโจมตีระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ โดยการทำงานตามแผนจะมุ่งเน้นในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางให้สามารถใช้งานได้

2. วัตถุประสงค์

2.1 เพื่อกำหนดวิธีการในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ เพื่อป้องกัน และลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2.2 เพื่อกำหนดวิธีการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ ให้สามารถใช้งานได้

2.3 เพื่อเตรียมความพร้อมด้านบุคลากรของกรมปศุสัตว์ ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์

2.4 เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบ และต่อเนื่องสามารถแก้ไขปัญหาสถานการณ์ได้อย่างทันทั่วถึง

3. รูปแบบภัยคุกคามไซเบอร์

3.1 ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือมัลแวร์ (Malware) ซึ่งเป็นโปรแกรมที่มิดการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

3.2 ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวร์ชนิดหนึ่ง ที่สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ซึ่งไวรัสคอมพิวเตอร์จะแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่นๆ โดยใช้พาหะ เช่น แฟลชไดรฟ์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

3.3 หนอนคอมพิวเตอร์ (Computer Worm) เป็นมัลแวร์ชนิดหนึ่ง สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่นๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต โดยหนอนคอมพิวเตอร์จะต่างกับไวรัสตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่นๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์จะใช้วิธีสแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอปพลิเคชัน จากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังตัวโดยใช้ช่องโหว่ดังกล่าว

3.4 ม้าโทรจัน (Trojan Horse) เป็นมัลแวร์ชนิดหนึ่ง ที่มีจุดประสงค์เพื่อบุกรุก เข้าถึง และควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูลดังกล่าวส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการอาจเป็นชื่อผู้รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่นๆ ลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัยพาหะ ซึ่งอาจมาจากแฟลชไดรฟ์ หรือทางอีเมล

3.5 สพายแวร์ (Spyware) เป็นมัลแวร์ชนิดหนึ่งที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูลสถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

3.6 ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ชนิดหนึ่งที่มีพฤติกรรมเข้ารหัสไฟล์ต่างๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆ ได้เลยหากไฟล์ เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าต้องจ่ายค่าไถ่ในการปลดล็อคเพื่อกู้ข้อมูลคืนมาผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ "เรียกค่าไถ่" ที่ปรากฏ

3.7 ประตูหลัง (Backdoor) เป็นช่องทางพิเศษที่ใช้เข้าถึงระบบงานคอมพิวเตอร์โดยที่ไม่ต้องผ่านการพิสูจน์ทราบตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลังเอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบงานคอมพิวเตอร์ในภายหลัง

3.8 Rootkit เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ทั้งนี้นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ด้วย

3.9 การโจมตีแบบ DoS/DDOS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตีมีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมีมากกว่า 1 เครื่องและกระทำพร้อมๆ กัน ไม่ว่าจะเป็นโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS)

3.10 Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่นๆ เพื่อรอรับคำสั่งจากผู้บุกรุก (Hacker) โดยผู้บุกรุก (Hacker) จะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่ เช่นการทำ DDoS เป็นต้น

3.11 Spam Mail หรืออีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับโดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อนรำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการการชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ Anti-Spam หรือหากใช้ฟรีอีเมลก็จะมีโปรแกรมคัดกรองอีเมลขยะในขั้นหนึ่งแล้ว

3.12 Phishing คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชซิง เช่น การบอกแก่ผู้รับปลายทางว่า เป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบ และใส่ข้อมูลที่สำคัญใหม่โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

3.13 Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งเป็นวิธีการหนึ่งที่ผู้บุกรุกระบบนิยมใช้

3.14 Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์ หรืออาศัยโปรแกรมด้วยวัตถุประสงค์ต่างๆ กัน ทั้งนี้โดยทั่วไปแล้วการ Hacking เป็นสิ่งที่ผิดกฎหมาย แต่อย่างไรก็ตามหากได้รับอนุญาตก็

ไม่ใช่สิ่งผิดกฎหมาย โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบเพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายขององค์กร

3.15 ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่างๆ ไม่ว่าจะเป็นเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกคามที่หนัก

4. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์

เพื่อให้กรมปศุสัตว์ มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ตามที่ระบุในข้อ 3 กรมปศุสัตว์ จะดำเนินการเตรียมความพร้อมในด้านต่างๆ ดังนี้

4.1 การเตรียมพร้อมด้านอุปกรณ์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ กรมปศุสัตว์จึงควรจัดหาอุปกรณ์และซอฟต์แวร์ที่จำเป็นดังนี้

4.1.1 อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท DoS/DDoS BOTNET Phishing Sniffing Hacker ทั้งนี้อุปกรณ์ป้องกันระบบเครือข่ายที่จัดหา นอกจากความสามารถในการเป็น Firewall แล้วยังต้องมีความสามารถอื่นๆ เพิ่มเติม ซึ่งได้แก่ความสามารถในการตรวจจับการบุกรุก (IPS) ความสามารถในการคัดกรองเว็บไซต์อันตราย (Web filtering) และ การควบคุมการใช้งานซอฟต์แวร์ (Application Control) เป็นอย่างน้อย

4.1.2 ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์

4.1.3 อุปกรณ์ web app firewall ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบงานคอมพิวเตอร์ของกรมปศุสัตว์ ที่พัฒนาขึ้นมาให้บริการผ่าน web browser ได้แก่ การคุกคามทาง ไซเบอร์ประเภท Hacker โดยสามารถป้องกันเทคนิคการบุกรุกเช่น Cross-site scripting และ SQL Injection ได้ เป็นอย่างน้อย

4.1.4 ซอฟต์แวร์สำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และการกู้ข้อมูลของระบบเครือข่ายคอมพิวเตอร์ของกรมปศุสัตว์ รวมทั้งยังสามารถสำรองข้อมูลแบบเข้ารหัสได้

4.1.5 ระบบคลาวด์กลางภาครัฐ GDCC Cloud ใช้ในระดับกรม (Agency Cloud) เพื่อเป็นโครงสร้างพื้นฐานด้านดิจิทัลรองรับหน่วยงานรัฐให้เข้าถึงทรัพยากรด้านคลาวด์ด้วยมาตรฐานสากลระดับ Tier 4 พร้อม SLA 99.99% ซึ่งเป็นไปตามเป้าหมายของกระทรวงดิจิทัลฯ ในการพัฒนาคloudข้อมูลดิจิทัลภาครัฐ และใช้ประโยชน์ Big Data จากคลังข้อมูล ให้สามารถบูรณาการข้อมูลข้ามหน่วยงานกันได้อย่างเป็นระบบ เพื่อนำสู่การปรับปรุงเพิ่มประสิทธิภาพบริการดิจิทัลให้แก่ประชาชนและเป็นข้อมูลในการพัฒนาประเทศในทุกมิติ

4.1.6 ระบบงานคอมพิวเตอร์สำรอง ใช้ในกรณีที่ไม่สามารถกู้ระบบงานคอมพิวเตอร์ขึ้นมาได้

4.1.7 อุปกรณ์จัดเก็บ Log file ใช้สำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์

4.1.8 อุปกรณ์วิเคราะห์ Log file ใช้สำหรับวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ ซึ่งข้อมูลที่ถูวิเคราะห์ดังกล่าวจะช่วยระบุถึง หมายเลข IP Address ของผู้โจมตี และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ และใช้ประกอบการทำรายงานให้แก่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

4.1.9 ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์ แมข่ายของกรมปศุสัตว์ ซึ่งสามารถป้องกันภัยคุกคามทางไซเบอร์ประเภท Malware, Computer Virus, Computer worm, Trojan, Spyware, Ransomware, BOTNET, Spam Mail

4.2 แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา กรมปศุสัตว์จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปีละ 1 ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้อาจสามารถค้นหาภัยคุกคามทางไซเบอร์ประเภท Backdoor ที่ถูกซ่อนเอาไว้จากขั้นตอนการพัฒนาระบบงานคอมพิวเตอร์ได้

4.3 การเตรียมพร้อมด้านบุคลากร

4.3.1 การให้ความรู้ เพื่อให้บุคลากรของกรมปศุสัตว์มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ กรมปศุสัตว์ จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากรของกรมปศุสัตว์

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

4.3.3 มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์

4.4 การเตรียมพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรอง ในกรณีที่ภัยคุกคามทางไซเบอร์ ก่อให้เกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์อย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน กรมปศุสัตว์จะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ สามารถกลับมาใช้งานได้อย่างรวดเร็วที่สุด ทั้งนี้แนวทางในการกู้คืนข้อมูล และการใช้ระบบคอมพิวเตอร์สำรองจะกำหนดอยู่ในเอกสารแผนสำรองและกู้คืนระบบของกรมปศุสัตว์

5. ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์

ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติ และกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ทั้งนี้ทางกรมปศุสัตว์ได้มีมาตรการสำหรับรับมือกับภัยคุกคามทางไซเบอร์ 3 มาตรการดังนี้

5.1 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) มีขั้นตอนดังนี้ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) คือ การที่ต้องสร้างกลไกและกระบวนการเพื่อ

- ตรวจสอบเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของกรมปศุสัตว์

- การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

- การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของกรมปศุสัตว์หรือไม่ และดำเนินการทบทวนกลไก และกระบวนการอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ากลไก และกระบวนการต่างๆ ยังคงมีประสิทธิภาพ

5.2 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response) มี 3 ขั้นตอน ดังนี้

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

5.2.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

1) ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์

2) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต มีการดำเนินการต่อไปนี้

- จัดตั้งทีมสื่อสารในภาวะวิกฤต เพื่อเปิดใช้งานในช่วงวิกฤต

- ระบุสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง

- ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

- ระบุผู้แทนหน่วยงานหลัก และผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

- ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

3) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

4) ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

5.2.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

1) กรมปศุสัตว์ ต้องมีส่วนร่วมในการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำ โดยคณะกรรมการการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ทั้งในระดับชาติ หรือระดับภาคส่วน กรมปศุสัตว์ต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

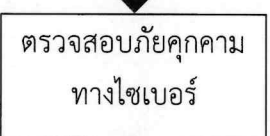
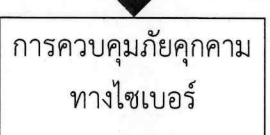
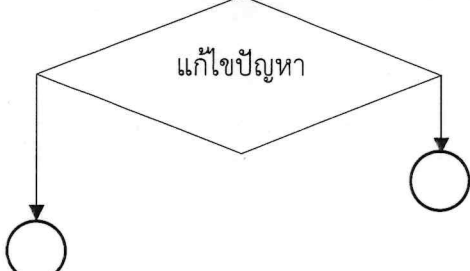
2) ต้องปฏิบัติตามคำขอใดๆ ของคณะกรรมการ เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ กรมปศุสัตว์ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤต และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของกรมปศุสัตว์

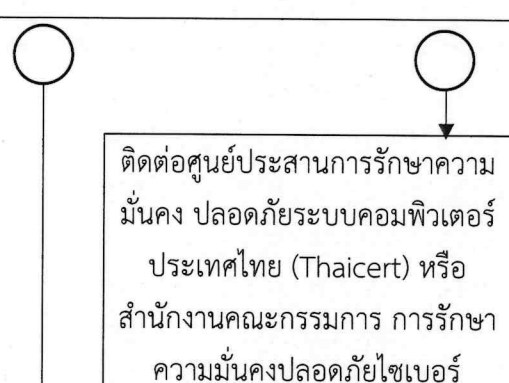
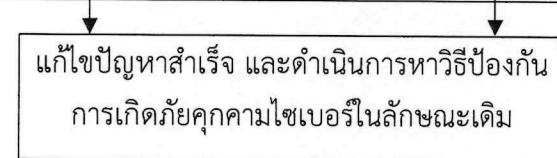
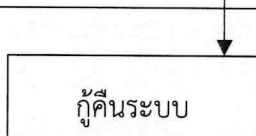
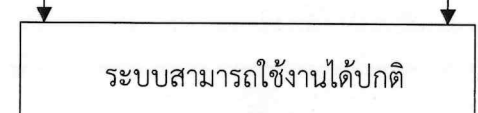
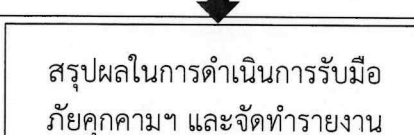
5.3 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)

5.3.1 ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของกรมปศุสัตว์สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตค่านิยมและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

5.3.2 ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BPC อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

กรมปศุสัตว์ได้จัดทำขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์ซึ่งเป็นการดำเนินการเบื้องต้นดังนี้

ขั้นตอน	รายละเอียด
	มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจจับการคุกคามทางไซเบอร์ได้จากอุปกรณ์ป้องกันระบบเครือข่าย หรือเครื่องมือต่างๆ ตามที่กำหนดในข้อ 3.1 ซึ่งจะช่วยให้กรมปศุสัตว์ สามารถตรวจพบการคุกคามทางไซเบอร์อย่างรวดเร็ว
	ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัยคุกคามตามที่กำหนดใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 62
	ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ให้ส่งผลกระทบน้อยที่สุดและป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่นๆ ซึ่งในกรณีที่เร่งด่วนกรมปศุสัตว์ จะทำการปิดระบบ หรือตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว
	ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์ในเบื้องต้นในทันที

ขั้นตอน	รายละเอียด
 <pre> graph TD Start(()) --> Contact[ติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ] Contact --> Fix[แก้ไขปัญหาสำเร็จ และดำเนินการหาวิธีป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม] </pre>	ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อขอคำแนะนำหรือขอความช่วยเหลือ
 <pre> graph TD Fix[แก้ไขปัญหาสำเร็จ และดำเนินการหาวิธีป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม] --> Check[ทดสอบระบบ] </pre>	หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์แล้ว กรมปศุสัตว์จะดำเนินการตรวจหาช่องโหว่ โดยอุปกรณ์ ตรวจสอบช่องโหว่ระบบเครือข่าย หรือเครื่องมืออื่นๆ และหาวิธีเพื่อป้องกันการเกิดภัยคุกคาม ไซเบอร์ในลักษณะเดิม
 <pre> graph TD Check{ทดสอบระบบ} --> Pass[ระบบสามารถใช้งานได้ตามปกติ] Check --> Fail[กู้คืนระบบ] </pre>	ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกรมปศุสัตว์ว่าสามารถทำงานได้สมบูรณ์หรือไม่ ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกู้คืนระบบงาน
 <pre> graph TD Fail[กู้คืนระบบ] --> Restore[ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรองและกู้คืนระบบ] </pre>	ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้ กรมปศุสัตว์จะพิจารณาเปิดใช้ระบบงานคอมพิวเตอร์สำรอง และเร่งกู้ระบบงานคอมพิวเตอร์หลัก
 <pre> graph TD Pass[ระบบสามารถใช้งานได้ตามปกติ] --> RestoreNormal[สรุปผลในการดำเนินการรับมือภัยคุกคามฯ และจัดทำรายงาน] </pre>	เมื่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกรมปศุสัตว์สามารถทำงานได้ตามปกติแล้ว หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศของกรมปศุสัตว์จะดำเนินการสรุปผลในการ ดำเนินการรับมือภัยคุกคามไซเบอร์
 <pre> graph TD RestoreNormal[สรุปผลในการดำเนินการรับมือภัยคุกคามฯ และจัดทำรายงาน] --> End[] </pre>	สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้อำนวยการกอง ผู้บริหารระดับสูงด้านสารสนเทศ

6. การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ในส่วนของผู้บริหารกรมปศุสัตว์

เมื่อเกิดการคุกคามทางไซเบอร์แล้ว ในบางครั้งผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของเครื่องคอมพิวเตอร์ของผู้บริหารกรมปศุสัตว์ทำงานผิดพลาดหรือล่าช้าลง หรือส่งผลให้ไฟล์ข้อมูลที่ถูกจัดเก็บเอาไว้ในเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติ ดังนั้นเจ้าหน้าที่ของ สดช. ควรดำเนินการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ดังนี้

6.1 ดำเนินการตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์อย่างเคร่งครัด

6.2 ดำเนินการตามนโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และ นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างเคร่งครัด

7. การประเมินความเสี่ยงการรักรักษาความมั่นคงปลอดภัยไซเบอร์

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการจัดการความเสี่ยง	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, นายพยุ่ง ตีร์กิล
2) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	1. ไม่สามารถใช้งานระบบคอมพิวเตอร์ และระบบเครือข่ายได้ 2. ไม่สามารถใช้งานระบบสารสนเทศ และระบบฐานข้อมูลได้ 3. ระบบปฏิบัติการ และระบบฐานข้อมูล เกิดความเสียหายจากการที่เครื่องไม่ได้อุปกรณ์การปิดอย่างเหมาะสม	1	4	4	1. ตรวจสอบระบบสำรอง ไฟฟ้า (UPS) ในศูนย์คอมพิวเตอร์แม่ข่าย กลางทุก 3 เดือน	การถ่ายโอน (Transfer)	นายศิริพล พจนวิเศษ, นายพยุ่ง ตีร์กิล
3) ความเสี่ยงจากอุปกรณ์ภูมิ และความชื้นของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)	เกิดความเสียหายต่อเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย	1	4	4	ตรวจสอบเครื่องปรับอากาศ ที่ควบคุมอุณหภูมิ และความชื้นทุก 3 เดือน	การถ่ายโอน (Transfer)	นายศิริพล พจนวิเศษ

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
4) ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่าย และระบบไฟฟ้า	1. ไม่สามารถใช้งานระบบเครือข่ายได้ 2. ไม่สามารถให้บริการระบบเครือข่ายได้อย่างต่อเนื่อง	1	3	3	ตรวจสอบอุปกรณ์เครือข่าย และระบบไฟฟ้าทุก 3 เดือน	การยอมรับ (Take)	นายศิริพล พจนวิเศษ
5) ความเสี่ยงจากการโจรกรรม อุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง	1. อุปกรณ์ และข้อมูลที่มีความสำคัญ สูญหาย 2. เสียภาพลักษณ์ของหน่วยงาน	1	3	3	1. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการ เข้า - ออกห้องคอมพิวเตอร์แม่ข่าย 2. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ๆ มีเครื่องคอมพิวเตอร์ และอุปกรณ์ติดตั้ง 3. ตรวจสอบการทำงานของ ศูนย์สำรอง Disaster Recovery Site (DR Site) ทุก 3 เดือน	การยอมรับ (Take)	นายศิริพล พจนวิเศษ, นายพยุ่ง ตรีภณ
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

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
7) ความเสี่ยงจากผู้ใช้งานเครือข่ายคอมพิวเตอร์ และระบบเครือข่าย	1. สูญเสีย Bandwidth ในระบบเครือข่ายทำให้ต้องเพิ่ม Bandwidth ให้มากขึ้น เนื่องจากการใช้งานนอกเหนือจากงานราชการ 2. เครื่องคอมพิวเตอร์เสียหาย และเสื่อมอายุการใช้งานเร็วกว่าปกติ	2	3	6	1. กำหนด Policy ของ Firewall ให้เหมาะสมต่อการใช้งาน 2. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ไปใช้ออกนอกหน่วยงานราชการ และรายงานการใช้การปฏิบัติงานของผู้ที่ฝ่าฝืนต่อผู้บังคับบัญชา 3. ตรวจสอบและแนะนำ ผู้ใช้งาน ให้ใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์ต่อพ่วงอย่างเหมาะสม	การควบคุม (Treat)	นายศิริพล พจนวิเศษ, นายพยุ่ง ตริภมล, บริษัท โทรคมนาคม แห่งชาติ จำกัด (มหาชน)
3. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)							
8) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	1. เกิดความเสียหายต่อระบบสารสนเทศ และระบบฐานข้อมูล 2. ไม่สามารถใช้งานระบบสารสนเทศที่สำคัญ และต้องใช้งานอย่างเร่งด่วน	3	4	12	1. ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายหลักทุกวัน 2. สำรองระบบ และ ข้อมูล (Backup) ทุกวัน 3. ทดสอบการกู้คืนระบบแม่ข่ายหลักเดือนละ 1 ครั้ง	การควบคุม (Treat)	นายศิริพล พจนวิเศษ

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการควบคุมความเสี่ยง	ผู้รับผิดชอบ
9) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	1. โปรแกรมหรือข้อมูลถูกทำลาย 2. ไม่สามารถเรียกใช้โปรแกรม หรือระบบงานได้ตามปกติ 3. การถูกขโมยข้อมูลที่สำคัญ	3	2	6	1. อัปเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ (อัตโนมัติ) 2. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และให้ผลบังคับใช้อย่างเคร่งครัด	การควบคุม (Treat)	นายศิริพล พจนวิเศษ
10) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่าย จากภายในและภายนอกองค์กร	1. ระบบสารสนเทศของหน่วยงาน ไม่สามารถให้บริการได้ 2. ทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัส และแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย 3. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพบน Web Site ของหน่วยงาน 4. ถูกโจรกรรมข้อมูลที่เป็นความลับ 5. ไม่สามารถเข้าใช้ระบบสารสนเทศได้	4	4	16	1. อัปเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ 2. ตรวจสอบ Policy และการทำงานของระบบป้องกันการบุกรุก DDoS, IPS และระบบเฝ้าระวังเครือข่ายทุกส่วน	การควบคุม (Treat)	นายศิริพล พจนวิเศษ, นายพยุ่ง ตรีภณ บริษัท โทรคมนาคม แห่งชาติ จำกัด (มหาชน)

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
11) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินเทอร์เน็ตภายใน และภายนอกสถานที่ทำงาน	1. ระบบเครือข่ายอินเทอร์เน็ต และอินเทอร์เน็ตไม่สามารถใช้งานได้ 2. ไม่สามารถเข้าใช้จากระบบสารสนเทศผ่านเครือข่ายอินเทอร์เน็ตและอินเทอร์เน็ตได้	2	3	6	1. ตรวจสอบระบบเครือข่ายสื่อสารหลักทุกวัน 2. ควบคุมการเข้าใช้เครือข่ายอินเทอร์เน็ต และอินเทอร์เน็ต โดยใช้ระบบยืนยันตน(Authentication)	การยอมรับ (Take)	นายศิริพล พจนวิเศษ, นายพยุ่ง ตริภณ
12) ความเสี่ยงจากการถูกล็อกจากผู้ใช้บริการเครือข่าย (Black List)	1. ผู้ใช้งานที่ต้องการข้อมูลของหน่วยงาน หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน Web Server ได้ 2. ลดความน่าเชื่อถือของหน่วยงาน	1	3	3	1. อัปเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัสได้ทุกรูปแบบ 2. ปรับปรุง Policy Firewall 3. Monitoring ระบบเครือข่ายเป็นประจำทุกวัน	การยอมรับ (Take)	นางสุวรรณี กาญจนกุลิต, นายเอกพงศ์ สุวรรณพงศ์
13) ความเสี่ยงจากการใช้งานระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference)	ระบบประชุมทางไกลผ่านเครือข่าย (VDO Conference) ขัดข้อง ทำให้ผู้ใช้ และหน่วยงานที่เกี่ยวข้อง ไม่สามารถเข้าร่วมประชุมได้ ผู้ไม่เกี่ยวข้องเข้าร่วมประชุมแบบไม่ได้เชิญ	1	3	3	ตรวจสอบการเชื่อมต่ออุปกรณ์ การทำงานของระบบชุดประชุมทางไกลผ่านเครือข่าย (VDO Conference) ก่อนใช้งาน	การยอมรับ (Take)	นายวัชรพงศ์ ชื่นพิณสขญกิจ, นายสุรัชชัย ภูมิวิจิตร
4. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)							
14) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์	1. การถูกฟ้องร้อง และเสื่อมเสียชื่อเสียง และความน่าเชื่อถือของหน่วยงาน	1	3	3	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น	การยอมรับ (Take)	นายศิริพล พจนวิเศษ, นายพยุ่ง ตริภณ

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการจัดการความเสี่ยง	ผู้รับผิดชอบ
	2. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้นๆ 3. หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ				2. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งาน Open Source		
15) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	1. สร้างความเสียหายต่อระบบคอมพิวเตอร์แม้ขาย ระบบสารสนเทศและระบบฐานข้อมูล 2. ลดความน่าเชื่อถือต่อหน่วยงาน	1	3	3	1. อัปเดตเครื่องมือ และโปรแกรมที่ใช้พัฒนาอย่างสม่ำเสมอ 2. ตรวจสอบช่องโหว่ และดำเนินการแก้ไขทุก 3 เดือน	การยอมรับ (Take)	นายศิริพล พจนวิเศษ, นายพยุ่ง ตริภค
16) ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือดูแลระบบโดยผู้รับจ้างภายนอก (Outsource)	1. ไม่สามารถแก้ไขโปรแกรมให้รองรับกระบวนการใหม่ และแก้ไขการทำงานที่ผิดพลาดได้อย่างทั่วถึง 2. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว เนื่องจากโปรแกรมหมดลิขสิทธิ์ และขาดการปรับปรุง (Update) โปรแกรม 3. ไม่สามารถเชื่อมโยงข้อมูลกับระบบ Big Data ของกรมบัญชีตัวได้ ในกรณีมีการปรับปรุง	1	3	3	1. กำหนดให้มีการส่งมอบเอกสารที่ใช้ในการวิเคราะห์ออกแบบการพัฒนา ระบบ และชุดคำสั่ง (Source Code) ฉบับสมบูรณ์ ทั้งในกรณีพัฒนาเสร็จสิ้น และเมื่อมีการปรับปรุงแก้ไข 2. ส่งมอบชุดคำสั่ง (Source Code) ชุดสมบูรณ์ 3. มีการถ่ายทอดความรู้ เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่	การควบคุม (Treat)	นายศิริพล พจนวิเศษ, นายพยุ่ง ตริภค, บริษัท ที่รับ MA

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการ ความเสี่ยง	ผู้รับผิดชอบ
					4. จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรม และข้อมูลให้มีความทันสมัย และใช้งานได้อย่างต่อเนื่อง		
5. ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)							
17) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน	1. ระบบฐานข้อมูลไม่สามารถนำไปใช้สนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ 2. ลดความน่าเชื่อถือของหน่วยงาน 3. ข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน	1	3	3	1. จัดทำรายการการข้อมูล และความถี่ในการปรับปรุง 2. กำหนดมาตรการ แนวทางการปรับปรุง และช่องทางการเข้าถึงข้อมูล เพื่อให้ผู้ดูแลข้อมูลปฏิบัติตาม	การยอมรับ (Take)	นางสาวภาณุตา บุญนาค, นายวัชรพงษ์ ชื่นพินสขัญกิจ
18) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล	1. เกิดการสูญหายของข้อมูล และกระทบต่อการทำงานตามปกติ 2. ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้สนับสนุนการปฏิบัติงานได้	1	3	3	1. มีการสำรองระบบฐานข้อมูลเป็นประจำทุกวัน 2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) ทุกสัปดาห์	การยอมรับ (Take)	นางสาวภาณุตา บุญนาค, นายวัชรพงษ์ ชื่นพินสขัญกิจ
19) ความเสี่ยงจากการโจมตีระบบฐานข้อมูล	1. ข้อมูลที่สำคัญรั่วไหลสู่ภายนอก หรือสาธารณะ 2. ข้อมูลที่สำคัญสูญหาย และถูกทำลาย	1	4	4	1. ตรวจสอบระบบป้องกันการบุกรุก และระบบตรวจสอบ และเฝ้าระวังเครือข่ายเป็นประจำทุกวัน 2. ตรวจสอบ Policy และ Log ของระบบป้องกัน การบุกรุก และระบบเฝ้าระวังเครือข่ายเป็นประจำทุกวัน	การยอมรับ (Take)	นางสาวภาณุตา บุญนาค, นายวัชรพงษ์ ชื่นพินสขัญกิจ

