(ฉบับปรับปรุง ครั้งที่ 2)

ประกาศใช้ ณ วันที่ 30 ธันวาคม 2565

มหาวิทยาลัยราชภัฏสวนสุนันทา

Suan Sunandha Rajabhat University

คู่มือปฏิบัติงาน Work Manual

กระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

คำนำ

คู่มือการปฏิบัติงานกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต นี้ จัดทำขึ้นเพื่อให้ผู้ปฏิบัติงานใช้เป็นแนวทางในการดำเนินงาน คู่มือการปฏิบัติงานงานนี้คลอบคลุมขั้นตอนการดำเนินการตามกระบวนการจัดการความรู้เพื่อพัฒนาองค์กรของมหาวิทยาลัยราชภัฏสวนสุนันทา ให้สามารถนำกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต ไปปฏิบัติในรูปแบบเดียวกัน

คู่มือฉบับนี้ประกอบด้วย 1) ความเป็นมาและความสำคัญ 2) วัตถุประสงค์การจัดทำคู่มือ 3) ประโยชน์ที่คาดว่าจะได้รับ 4) ขอบเขตของคู่มือ 5) นิยามศัพท์เฉพาะ 6) โครงสร้างของหน่วยงาน 7) ภาระหน้าที่ของหน่วยงาน 8) บทบาทและหน้าที่ความรับผิดชอบของตำแหน่ง 9) ขั้นตอนการปฏิบัติ 10) หลักเกณฑ์วิธีการปฏิบัติงาน 11) เทคนิคการปฏิบัติงาน 12) ขั้นตอนการปฏิบัติงาน 13) ข้อจำกัด ปัญหาอุปสรรค และแนวทางการพัฒนา

คณะผู้จัดทำจะติดตามและประเมินผลความสำเร็จของมาตรฐานการปฏิบัติงานที่กำหนดของคู่มือฉบับนี้ เพื่อนำผลไปทบทวนและปรับปรุงกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต

คณะผู้จัดทำ
30 ธันวาคม 2565

สารบัญ

บทที่ 1 บทนำ

1.1 ความเป็นมาและความสำคัญ

ด้วยมหาวิทยาราชภัฏสวนสุนันทา เป็นมหาวิทยาลัยที่ได้รับการยอมรับในการเป็นมหาวิทยาลัยราชภัฏอันดับ 1 ของประเทศไทย อันเนื่องมาจากศักยภาพด้านการเรียนการสอนการวิจัยทั้งภายในประเทศและนานาชาติด้วยการประยุกต์ใช้เทคโนโลยีสารสนเทศในการเรียนการสอน ตามแผนยุทธศาสตร์ในการพัฒนามหาวิทยาลัย และสอดรับกับแผนแม่บทเทคโนโลยีสารสนเทศของประเทศไทยและแผนแม่บทเทคโนโลยีสารสนเทศของกระทรวงอุดมศึกษาและวิทยาศาตร์ วิจัยและนวัตกรรม วิเคราะห์ปัจจัยภายในและภายนอกต่าง ๆ การสร้างเครือข่ายในทุกภาคส่วนตามพันธกิจของมหาวิทยาลัย จึงได้กำหนดแนวทางการปฏิบัติพัฒนาระบบสารสนเทศและเครือข่ายความสัมพันธ์ระหว่าง มหาวิทยาลัยกับนักศึกษาศิษย์เก่าและชุมชนส่งเสริมและสนับสนุนการสร้างเครือข่ายความร่วมมือทำวิชาการด้านการวิจัยและด้านอื่นๆ ในการสนับสนุนภารกิจของมหาวิทยาลัยกับประชาคมอาเซียนปฏิรูปกระบวนการผลิต และพัฒนาครู บุคลากรทำการศึกษา โดยการสร้างเครือข่ายและความร่วมมือกับสถานศึกษาในการพัฒนา และ ผลิตครูให้มีคุณภาพตามมาตรฐานวิชาชีพสร้างเครือข่ายความร่วมกับองค์กรหน่วยงานภายนอกในการให้บริการ วิชาการเพื่อพัฒนาคุณภาพชีวิต สังคม และสิ่งแวดล้อมของชุมชนให้เข้มแข็ง ยั่งยืน นำไปสู่การพึ่งพาตนเองได้ สนับสนุนให้มีการสร้างเครือข่ายทางวัฒนธรรมแลกเปลี่ยนเพื่อการอนุรักษ์และเผยแพร่ทั้งภายในประเทศและต่างประเทศ เพื่อให้เหมาะสมกับสภาวะเศรษฐกิจและสังคมดิจิตอลทันสมัยต่อความก้าวหน้าทางเทคโนโลยีในอนาคต

ระบบเทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ซึ่งมีหน้าที่ดำเนินการเกี่ยวกับการเสนอนโยบายการกำกับ ดูแล การสนับสนุน ส่งเสริม วางแผนและติดตามผลการนำเทคโนโลยีสารสนเทศมาใช้พัฒนาระบบเทคโนโลยีสารสนเทศที่เชื่อถือได้ ถูกต้อง รวดเร็วเป็นปัจจุบัน ผู้ใช้เข้าถึงได้ง่าย และเชื่อมโยงกับเครือข่ายทั้งในและต่างประเทศ

ทั้งนี้ เพื่อให้การดำเนินการได้สอดคล้องกับนโยบายและแนวปฏิบัติกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต ประจำปีงบประมาณ 2566 เพื่อป้องกันและลดผลกระทบต่อจัดการปฏิบัติงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงเล็งเห็นความสำคัญต่อผู้ใช้งานเป็นอย่างมาก เพื่อให้เกิดการปฏิบัติงานอย่างมีประสิทธิภาพ

1.2 วัตถุประสงค์การจัดทำคู่มือ

1. เพื่อเป็นแนวทางในการปฏิบัติงานของกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต สำหรับบุคลากรที่เกี่ยวข้อง

2. เพื่อเป็นประโยชน์ในการประเมินผลการปรับปรุงคุณภาพกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต ให้เป็นมาตรฐานเดียวกัน

1.3 ประโยชน์คาดว่าจะได้รับ

1. เพื่อรายงานผลการดำเนินงานตามกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต ประจำปีงบประมาณ พ.ศ.2566

2. เพื่อเป็นกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต ประจำปีงบประมาณ พ.ศ.2566

1.4 ขอบเขตของคู่มือ

คู่มือการปฏิบัติงานนี้ ครอบคลุมการจัดการการประกันคุณภาพการศึกษาภายใน หน่วยงานได้ดำเนินการจัดการความรู้เป็นประจำทุกปี เพื่อให้เป็นไปตามมาตรฐานการอุดมศึกษาข้อที่ 3 มาตรฐานด้านการสร้างและพัฒนาสังคมฐานความรู้ และสังคมแห่งการเรียนรู้ และตอบสนองนโยบายของมหาวิทยาลัยที่ทุกหน่วยงานต้องดำเนินการจัดการความรู้ให้สามารถสร้างองค์ความรู้และนวัตกรรมที่สามารถทำให้เป้าประสงค์ของแต่ละยุทธศาสตร์สำเร็จ รวมทั้งเพื่อให้เป็นไปตามเกณฑ์การประกันคุณภาพ

1.5 นิยามศัพท์เฉพาะ

ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง การใช้ความรู้ทางวิทยาศาสตร์คอมพิวเตอร์มาปรับปรุงแก้ไขและพัฒนาระบบโครงข่ายเทคโนโลยีสารสนเทศ

ระบบโครงข่ายเทคโนโลยีสารสนเทศ หมายถึง ระบบฮาร์ดแวร์ ซอฟต์แวร์ และเครือข่ายของระบบคอมพิวเตอร์

การวางแผนพัฒนาและบริหารระบบ ICT หมายถึง การจัดทำแผนแม่บทเทคโนโลยีสารสนเทศ ให้สอดคล้องกับแผนแม่บทเทคโนโลยีสารสนเทศของประเทศไทย เพื่อนำมาพัฒนาและบริหารระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏสวนสุนันทาให้ตอบสนองต่อภารกิจและยุทธศาสตร์มหาวิทยาลัยราชภัฏสวนสุนันทา

มาตรฐานด้าน ICT หมายถึง แนวทาง กรอบ กติกาและการจัดการเพื่อใช้อ้างอิงในงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศทั้งทางด้านฮาร์ดแวร์ ซอฟแวร์เครือข่ายและอุปกรณ์ที่เกี่ยวข้อง เพื่อให้ทิศทางการใช้เทคโนโลยีสารสนเทศในองค์กรเป็นไปในแนวทางเดียวกัน นำไปสู่การลดต้นทุน ลดความซ้ำซ้อนในการใช้งาน รวมทั้งก่อให้เกิดความต่อเนื่องของการใช้เทคโนโลยีสารสนเทศในองค์กร

การออกแบบและพัฒนาระบบ ICT หมายถึง การดำเนินการออกแบบและพัฒนาระบบเทคโนโลยีสารสนเทศ เพื่อใช้ประโยชน์ในมหาวิทยาลัยราชภัฏสวนสุนันทา ตามความจำเป็นและความต้องการของหน่วยงาน การจัดทำเว็บไซต์ต่าง ๆ การพัฒนาระบบ e – service เช่น e – mail คลังวิดีโอ การพัฒนาระบบซอฟแวร์ เช่น ระบบเครือข่าย Internet

การสร้างวัฒนธรรมการใช้ ICT หมายถึง การเผยแพร่และสร้างบรรยากาศรวมทั้งพฤติกรรมการใช้เทคโนโลยีสารสนเทศให้เหมาะสมถูกต้อง เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

การพัฒนาบุคลากรด้าน ICT หมายถึง การดำเนินการจัดทำองค์ความรู้และสร้างการเรียนรู้ เพื่อเพิ่มพูนความรู้และทักษะด้านเทคโนโลยีสารสนเทศให้กับบุคลากรที่เกี่ยวข้อง โดยการฝึกอบรม ระบบสำนักงานอัตโนมัติ เป็นต้น

ระบบเครือข่ายคอมพิวเตอร์ (Computer Network) หมายถึง การนำเครื่องคอมพิวเตอร์ มาเชื่อมต่อเข้าด้วยกัน โดยอาศัยช่องทางการสื่อสารข้อมูลอย่างใดอย่างหนึ่ง เช่น สายเคเบิล สายโทรศัพท์ คลื่นวิทยุ คลื่นอินฟราเรด หรือสัญญาณดาวเทียม ทำให้เครื่องคอมพิวเตอร์แต่ละเครื่องในเครือข่ายนั้นสามารถติดต่อ และแลกเปลี่ยนข้อมูลข่าวสารระหว่างเครื่องคอมพิวเตอร์ รวมทั้งการใช้ทรัพยากรของระบบร่วมกัน (Shared Resource) ในเครือข่ายนั้น

คอมพิวเตอร์แม่ข่าย หมายถึง คอมพิวเตอร์ ที่ทำหน้าที่เป็นผู้ให้บริการทรัพยากร(Resources) ต่าง ๆ ซึ่งได้แก่ หน่วยประมวลผล หน่วยความจำ หน่วยความจำสำรองฐานข้อมูล และ โปรแกรมต่าง ๆ เป็นต้น

ระบบเครือข่ายแบบ LAN หมายถึง ระบบเครือข่ายเฉพาะบริเวณ เป็นระบบเครือข่ายส่วนตัว องค์กรที่ต้องการใช้งานเครือข่ายแบบนี้ จะต้องทำการสร้างเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อกันเป็นระบบเครือข่ายในระยะใกล้ ๆ

อินเตอร์เน็ต (Internet) หมายถึง เครือข่ายคอมพิวเตอร์นานาชาติ ที่มีสายตรงเชื่อมต่อไปยังสถาบันหรือหน่วยงานต่าง ๆ เพื่ออำนวยความสะดวกให้แก่ผู้ใช้ทั่วโลก ผู้ใช้เครือข่ายนี้สามารถสื่อสารถึงกันได้ทางอีเมล์ สามารถสืบค้นข้อมูลและสารสนเทศ รวมทั้งคัดลอกแฟ้มข้อมูลและโปรแกรมมาใช้ได้

อินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายภายในองค์กร เป็นบริการ และการเชื่อมต่อคอมพิวเตอร์เหมือนกับอินเทอร์เน็ต แต่จะเปิดให้ใช้เฉพาะสมาชิกในองค์กรเท่านั้น

การเชื่อมโยงเครือข่าย หมายถึง การสร้างเส้นทางการสื่อสารเพื่อส่งข้อมูลจากอุปกรณ์หนึ่งไปยังอีกอุปกรณ์หนึ่ง

ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ หมายถึง ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบ ดูแล รักษา ระบบเครือข่ายคอมพิวเตอร์ และสามารถเข้าถึงโปรแกรมรวมทั้งอุปกรณ์เครือข่ายคอมพิวเตอร์เพื่อการบริหารจัดการ

การรักษาความปลอดภัย หมายถึง มาตรการที่ใช้ในการปกป้องทรัพยากรจากภัยคุกคามทางกายภาพและระบบ ทั้งโดยเจตนาและไม่เจตนา เป็นวิธีการที่ช่วยลดความเสี่ยงด้านความปลอดภัย โดยการจำกัดให้เฉพาะผู้ที่จำเป็นต้องใช้งาน

ระบบสารสนเทศ (Information System หรือ IS) หมายถึง ระบบพื้นฐานของการทำงาน เพื่อช่วยการตัดสินใจ และการควบคุมในองค์กร ในการทำงานของระบบสารสนเทศประกอบไปด้วยกิจกรรม 3 อย่าง คือ การนำข้อมูลเข้าสู่ระบบ (Input) การประมวลผล (Processing) และ การนำเสนอผลลัพธ์ (Output)

ข้อมูลสารสนเทศ หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้วมีความหมายมีคุณค่า และเป็นประโยชน์ต่อผู้ใช้ สามารถนำไปใช้ในการดำเนินงานหรือการตัดสินใจได้ทันที สารสนเทศที่ได้อาจจะเป็นตัวเลข ตัวหนังสือ สัญลักษณ์ ภาพ หรือเสียงก็ได้

การนำเข้าข้อมูล (Input data) หมายถึง กระบวนการบันทึกข้อมูลเข้าสู่คอมพิวเตอร์ เพื่อการสร้างฐานข้อมูลที่ละเอียดถูกต้อง

การวิเคราะห์และการออกแบบระบบ (System Analysis and Design) หมายถึง วิธีการที่ใช้ในการสร้างระบบสารสนเทศขึ้นมาใหม่ เพื่อช่วยในการแก้ไขระบบสารสนเทศเดิมที่มีอยู่แล้วให้ดีขึ้น

การวิเคราะห์ระบบ คือ การหาความต้องการ (Requirements) ของระบบสารสนเทศว่าคืออะไร หรือต้องการเพิ่มเติมอะไรเข้ามาในระบบ

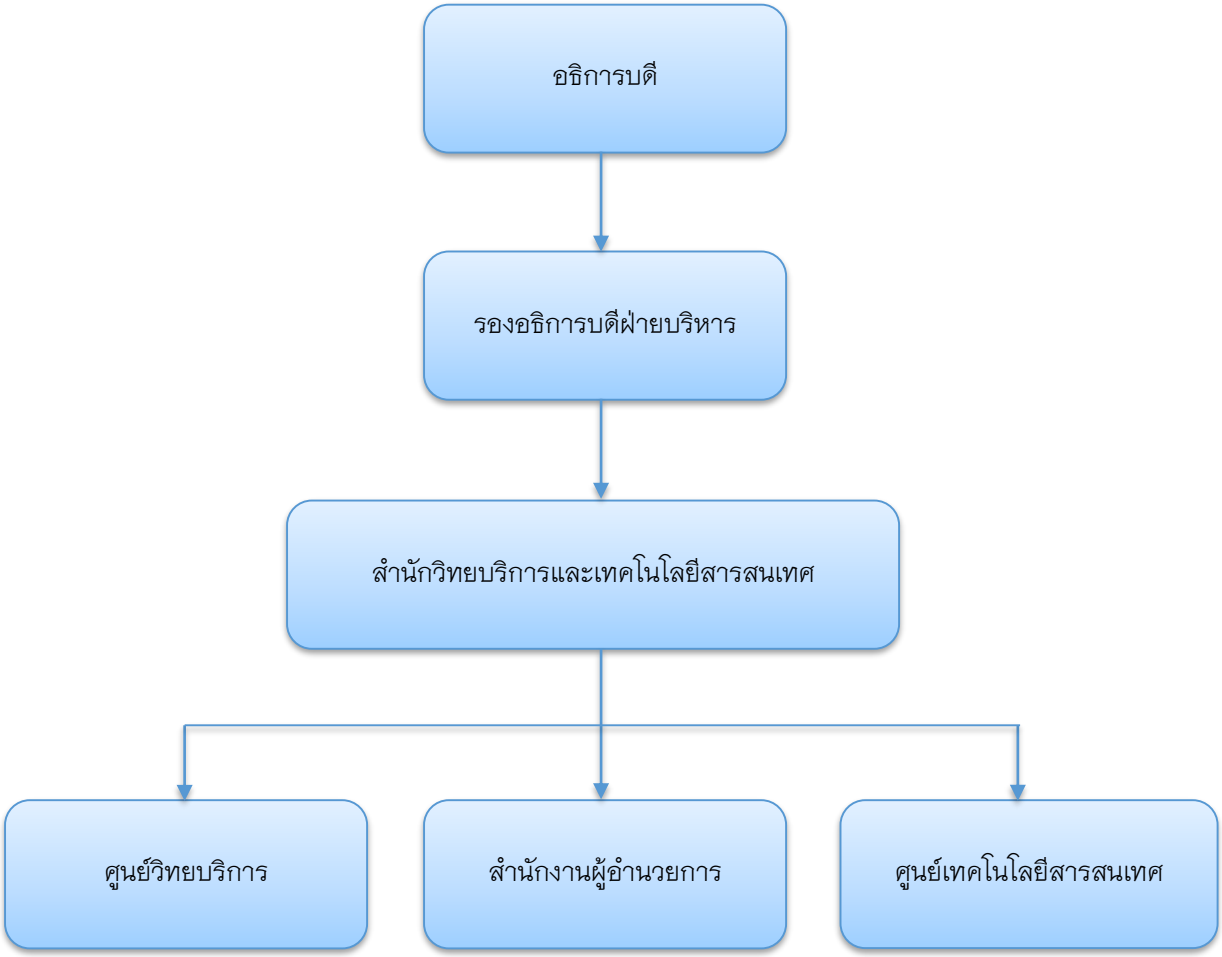
การออกแบบระบบ คือ การนำเอาความต้องการของระบบมาเป็นแบบแผน หรือเรียกว่าพิมพ์เขียวในการสร้างระบบสารสนเทศนั้นให้ใช้งานได้จริง

การประมวลผลข้อมูล (Data processing) หมายถึง วิธีการจัดการกับข้อมูลซึ่งอาจเป็นการบวก ลบ คูณ หาร หรือการคำนวณ และเปรียบเทียบลักษณะต่างๆ ที่กำหนดไว้ เพื่อให้ข้อมูลนั้นๆ อยู่ในรูปแบบที่เป็นประโยชน์ หรือตรงตามวัตถุประสงค์ของผู้ใช้งาน

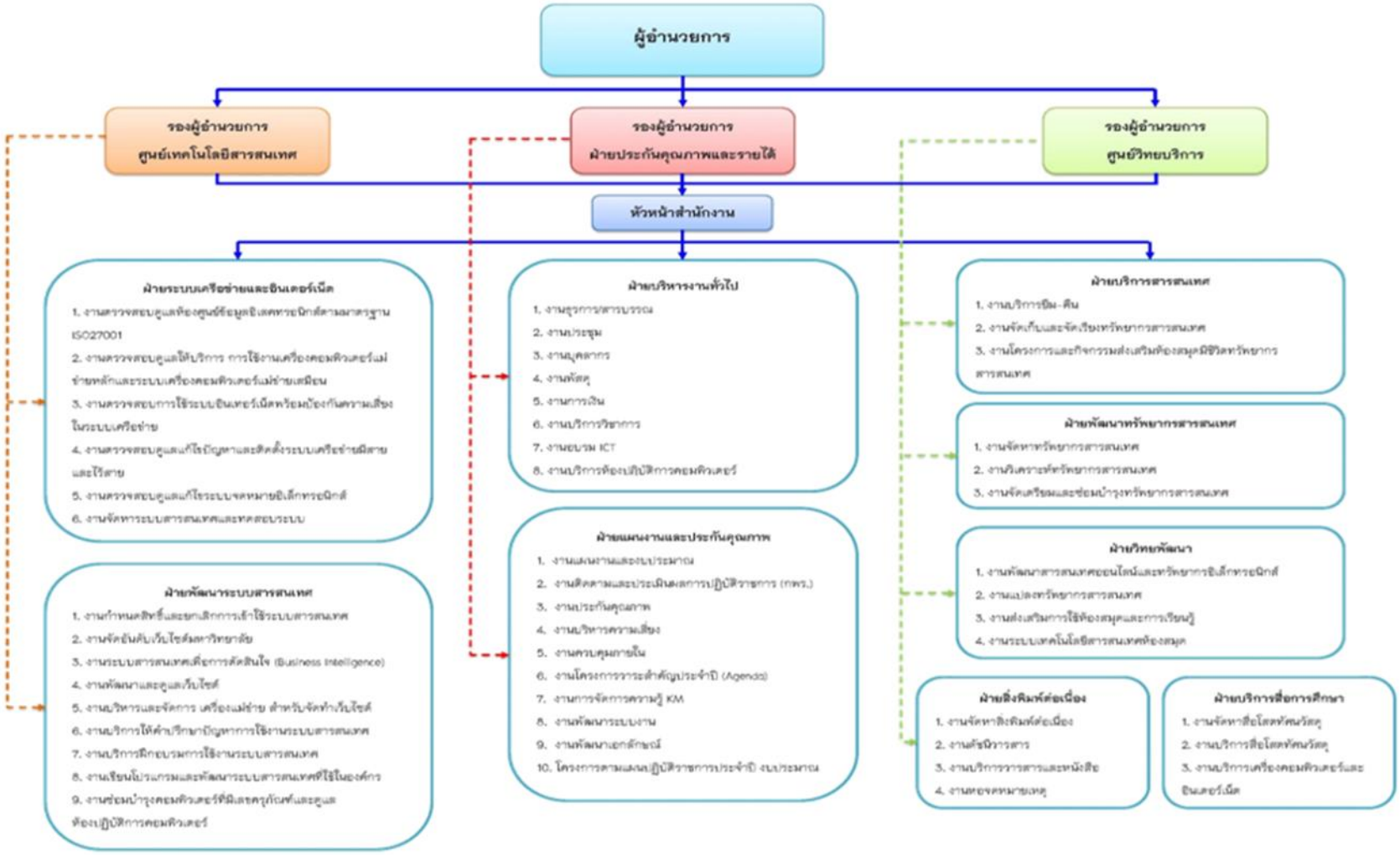
การรายงานผล หมายถึง ขั้นตอนการดำเนินการเพื่อสรุปความสำคัญของข้อมูลสารสนเทศ ให้ตรงสภาพที่เป็นจริงตรงตามวัตถุประสงค์ก่อนที่จะนำข้อมูลมาใช้

บทที่ 2 โครงสร้าง และหน้าที่ความรับผิดชอบ

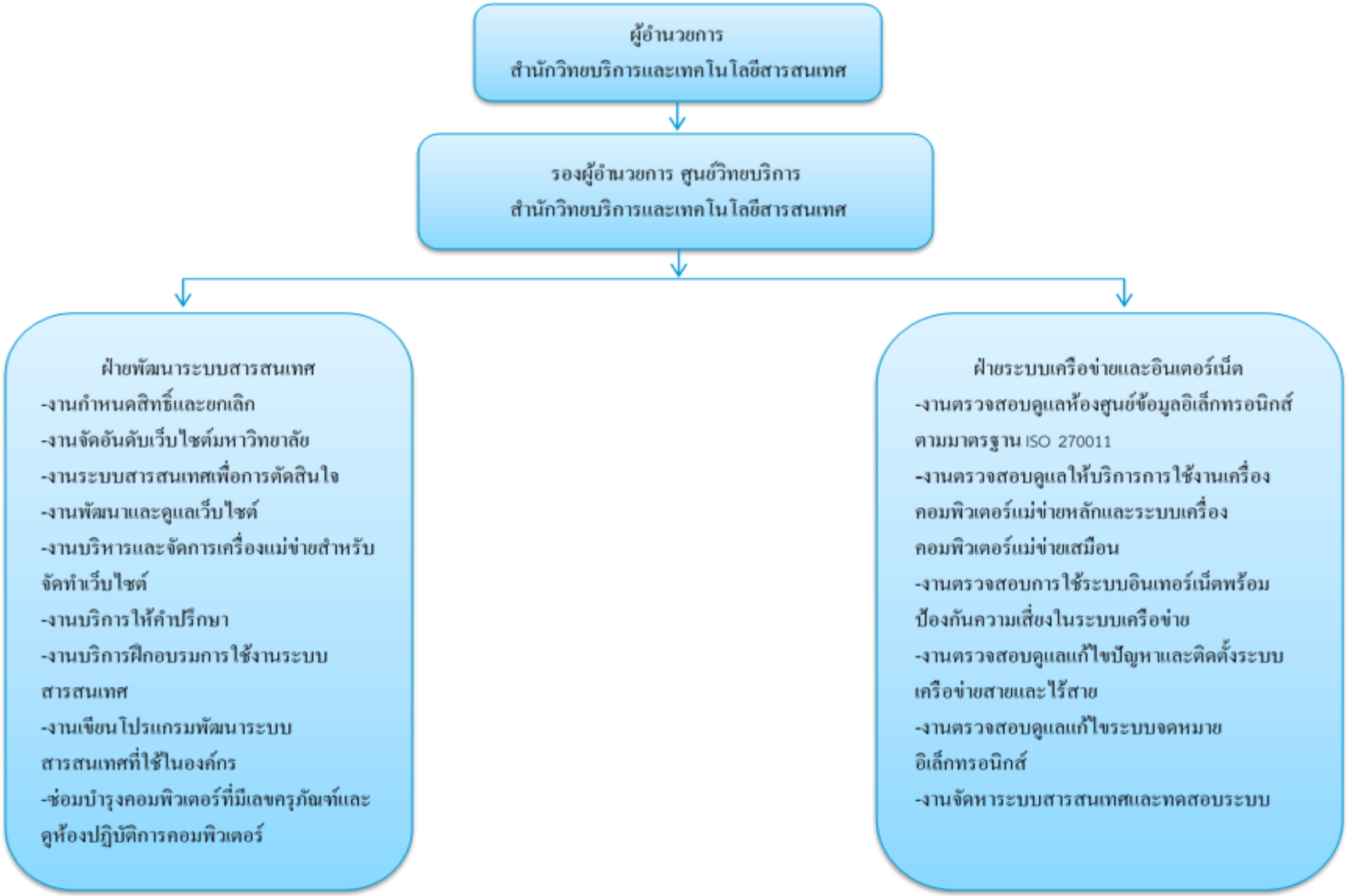
2.1 โครงสร้างของหน่วยงาน



2.2 โครงสร้างการบริหาร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ



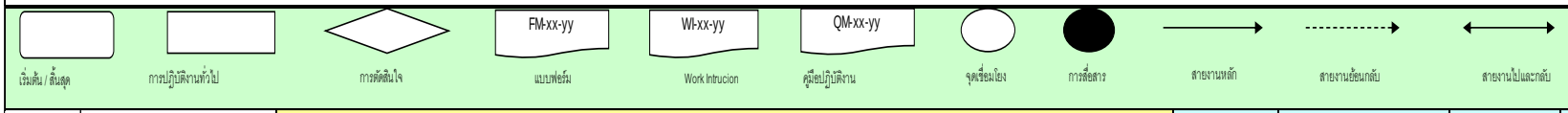
2.3 โครงสร้างของศูนย์เทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ



2.4 ขั้นตอนการปฏิบัติงาน

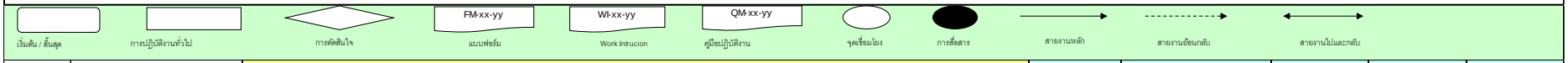
ผังกระบวนการปฏิบัติงาน (Quality Work Procedure)

กระบวนการปฏิบัติงาน : รักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต



ลำดับขั้นตอน	กิจกรรมหลัก	รายละเอียดกิจกรรมรอง					เวลา			เอกสารที่เกี่ยวข้อง (รหัส)	จุดควบคุม (control item)	ตัวชี้วัด (kqi)	เป้าหมาย
		งานรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต	หัวหน้าฝ่าย	หัวหน้าสำนักงานผู้อำนวยการ	รองผู้อำนวยการ	ผู้อำนวยการ	นาที	ชม.	วัน				
1	งานตรวจสอบดูแลให้บริการป้องกันไวรัสในระบบเครือข่าย	เริ่มต้น ↓ ตรวจเช็คไวรัสบนเครื่องคอมพิวเตอร์แม่ข่าย ↓ เก็บข้อมูลไวรัสและแสดงผลออกมาว่ามีการถูกไวรัสโจมตีในแต่ละเดือน ↓ Update โปรแกรมป้องกันไวรัสและปรับปรุงฐานข้อมูลและ Export Report ไวรัส ด้วยโปรแกรมป้องกันไวรัส ↓ จัดเก็บข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายระบบป้องกันไวรัส ↓					10 30 10 10			1.รายงานการตรวจสอบเบื้องต้น 2.รายงานข้อมูลไวรัสที่ตรวจสอบได้ 3.รายงานการปรับปรุงและผลการตรวจสอบ 4.รายงานฐานข้อมูลระบบป้องกันวัสบนเครื่องคอมพิวเตอร์แม่ข่ายเสมือน	-รายงานฐานข้อมูลระบบป้องกันวัสบนเครื่องคอมพิวเตอร์แม่ข่ายเสมือน	ระยะเวลาดำเนินการที่แล้วเสร็จตามกำหนด	แล้วเสร็จตามระยะเวลาที่กำหนด

กระบวนการปฏิบัติงาน : รักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต



ขั้นตอน	กิจกรรมหลัก	รายละเอียดกิจกรรมรอง					เวลา			เอกสารที่เกี่ยวข้อง (รหัส)	จุดควบคุม (control item)	ตัวชี้วัด (kqi)	เป้าหมาย
		งานรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต	หัวหน้าฝ่าย	หัวหน้าสำนักงานผู้อำนวยการ	รองผู้อำนวยการ	ผู้อำนวยการ	นาที	ชม.	วัน				
2	งานตรวจสอบและป้องกันความเสี่ยงระบบเครือข่าย	ตรวจเช็คโดยรวมอุปกรณ์ Firewall ในการทำงาน					10			1.รายงานเข้าอุปกรณ์ Firewall ผ่านหน้าเว็บไซต์เพื่อดูการทำงานโดยรวมของอุปกรณ์ 2.รายงานการตรวจสอบการทำงานของอุปกรณ์ 3.รายงานการตรวจสอบข้อมูลการบุกรุก 4.รายงานวิเคราะห์การบุกรุกต่างๆจากภายนอก 5.รายงานวิเคราะห์และประเมินความเสี่ยงจากระบบ ผ่านหน้าเว็บไซต์ผ่านอุปกรณ์ Firewall 6.รายงานกิจกรรมในการทำงานการโจมตีบนอุปกรณ์ที่เกิดขึ้นทั้งภายในและภายนอกองค์กร	รายงานกิจกรรมในการทำงานการโจมตีบนอุปกรณ์ที่เกิดขึ้นทั้งภายในและภายนอกองค์กร	ระยะเวลาดำเนินการที่แล้วเสร็จตามกำหนด	แล้วเสร็จตามระยะเวลาที่กำหนด
		↓ ตรวจเช็คข้อมูลจราจร(Log file)บนอุปกรณ์(Firewall)ดูการบุกรุกและทำการป้องกันถ้ามีการโจมตีเข้ามาในระบบเครือข่าย					20						
		↓ ประเมินความเสี่ยง(Risk Assessment)					10						
		↓ ทดสอบความเสี่ยง(Testing)					10						
		↓ บันทึก(Record)					10						
		↓											
3	สรุปผลการตรวจสอบความมั่นปลอดภัยทางเครือข่ายอินเทอร์เน็ต	จัดทำรายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต						1		1.รายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต 2.รายงานแจ้งผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเตอร์เน็ต	รายงานแจ้งผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเตอร์เน็ต	ระยะเวลาดำเนินการที่แล้วเสร็จตามกำหนด	แล้วเสร็จตามระยะเวลาที่กำหนด
		↓ จัดทำรายงานและจัดเก็บทางจดหมายอิเล็กทรอนิกส์					20						
		↓ สิ้นสุด											
รวม							140	1					

ผู้อนุมัติ	ผศ.ดร.ศิริลักษณ์ เกตุฉาย	**ตัวชี้วัดที่สำคัญ (KQI)**	**เป้าหมาย**
ตำแหน่ง	ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	ร้อยละความพึงพอใจการให้บริการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	≥4.94
วันที่	30/พฤศจิกายน/2564		

บทที่ 3 หลักเกณฑ์วิธีการปฏิบัติงาน

3.1 หลักเกณฑ์วิธีการปฏิบัติงานกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต

1.งานตรวจสอบดูแลให้บริการป้องกันไวรัสในระบบเครือข่าย

1.1 ตรวจเช็คไวรัสบนเครื่องคอมพิวเตอร์แม่ข่าย

1.2 เก็บข้อมูลไวรัสและแสดงผลออกมาว่ามีการถูกไวรัสโจมตีในแต่ละเดือน

1.3 Update โปรแกรมป้องกันไวรัสและปรับปรุงฐานข้อมูลและ Export Report ไวรัส ด้วยโปรแกรมป้องกันไวรัส

1.4 จัดเก็บข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายระบบป้องกันไว้รัส

2. งานตรวจสอบและป้องกันความเสี่ยงระบบเครือข่าย

2.1 ตรวจเช็คโดยรวมอุปกรณ์ Firewall ในการทำงาน

2.2 ตรวจเช็คข้อมูลจราจร(Log file) บนอุปกรณ์ (Firewall) ดูการบุกรุกและทำการป้องกันถ้ามีการโจมตีเข้ามาในระบบเครือข่าย

2.3 ประเมินความเสี่ยง (Risk Assessment)

2.4 ทดสอบความเสี่ยง(Testing)

2.5 บันทึก (Record)

3. สรุปผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต

3.1 จัดทำรายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต

3.2 จัดทำรายงานและจัดเก็บทางจดหมายอิเล็กทรอนิกส์

กฎระเบียบ ข้อบังคับ และอื่นๆ ที่เกี่ยวข้องในกระบวนการปฏิบัติงาน

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

2. ปฏิบัติตามแผนแม่บท ICT ฉบับปี 2552-2556 และแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา กระทรวงศึกษาธิการ 2554 – 2556

หน้า ๒๔
เล่ม ๑๓๔ ตอนที่ ๑๐ ก ราชกิจจานุเบกษา ๒๔ มกราคม ๒๕๖๐

พระราชบัญญัติ
ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)
พ.ศ. ๒๕๖๐

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร

ให้ไว้ ณ วันที่ ๒๓ มกราคม พ.ศ. ๒๕๖๐
เป็นปีที่ ๒ ในรัชกาลปัจจุบัน

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร มีพระราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้ยกเลิกความในมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่กับออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงและประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้"

มาตรา ๔ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๑๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกินสองแสนบาท

ให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับและลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย"

มาตรา ๕ ให้ยกเลิกความในมาตรา ๑๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท"

มาตรา ๖ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๒/๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"มาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท"

มาตรา ๗ ให้เพิ่มความต่อไปนี้เป็นวรรคสอง วรรคสาม วรรคสี่ และวรรคห้าของมาตรา ๑๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสามหรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว"

มาตรา ๘ ให้ยกเลิกความในมาตรา ๑๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้"

มาตรา ๙ ให้ยกเลิกความในมาตรา ๑๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๕ ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ"

มาตรา ๑๐ ให้ยกเลิกความในมาตรา ๑๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย"

มาตรา ๑๑ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๖/๑ และมาตรา ๑๖/๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี"

มาตรา ๑๒ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๗/๑ ในหมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"มาตรา ๑๗/๑ ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๑๑ มาตรา ๑๓ วรรคหนึ่ง มาตรา ๑๖/๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๗ ให้คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งมีอำนาจเปรียบเทียบได้

คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคนหนึ่งต้องเป็นพนักงานอัยการตามประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ต้องหาไม่ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว"

มาตรา ๑๓ ให้ยกเลิกความในมาตรา ๑๘ และมาตรา ๑๙ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิด หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวนอาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รีบรวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (๑) (๒) และ (๓) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงาน

เจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดระยะเวลาที่ต้องดำเนินการที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง"

มาตรา ๑๔ ให้ยกเลิกความในมาตรา ๒๐ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๒๐ ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ดังต่อไปนี้ พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้

(๑) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัตินี้

(๒) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาค ๒ ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา

(๓) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญาหรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและเจ้าหน้าที่ตามกฎหมายนั้นหรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ

ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์จะมอบหมายให้พนักงานเจ้าหน้าที่ยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้ ทั้งนี้ ให้นำบทบัญญัติว่าด้วยคณะกรรมการที่มีอำนาจดำเนินการพิจารณาทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับกับการประชุมของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์โดยอนุโลม

ให้รัฐมนตรีแต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ตามวรรคสองขึ้นคณะหนึ่งหรือหลายคณะ แต่ละคณะให้มีกรรมการจำนวนเก้าคนซึ่งสามในเก้าคนต้องมาจากผู้แทนภาคเอกชนด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ หรือด้านอื่นที่เกี่ยวข้อง และให้กรรมการได้รับค่าตอบแทนตามหลักเกณฑ์ที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

การดำเนินการของศาลตามวรรคหนึ่งและวรรคสอง ให้นำประมวลกฎหมายวิธีพิจารณาความอาญามาใช้บังคับโดยอนุโลม ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ตามวรรคหนึ่งหรือวรรคสอง พนักงานเจ้าหน้าที่จะทำการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นเองหรือจะสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้รัฐมนตรีประกาศกำหนดหลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการให้เป็นไปในแนวทางเดียวกันโดยคำนึงถึงพัฒนาการทางเทคโนโลยีที่เปลี่ยนแปลงไป เว้นแต่ศาลจะมีคำสั่งเป็นอย่างอื่น

ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่จะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่จะได้รับความเห็นชอบจากรัฐมนตรี หรือพนักงานเจ้าหน้าที่โดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์จะยื่นคำร้องตามวรรคสองไปก่อนที่รัฐมนตรีจะมอบหมายก็ได้ แต่ทั้งนี้ต้องรายงานให้รัฐมนตรีทราบโดยเร็ว"

มาตรา ๑๕ ให้ยกเลิกความในวรรคสองของมาตรา ๒๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่ง หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง เว้นแต่เป็นชุดคำสั่งไม่พึงประสงค์ที่อาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดรายชื่อ ลักษณะ หรือรายละเอียดของชุดคำสั่งไม่พึงประสงค์ซึ่งอาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์ก็ได้"

มาตรา ๑๖ ให้ยกเลิกความในมาตรา ๒๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่และพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสอง เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นในกรณีตามมาตรา ๑๘ วรรคสอง หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือกับพนักงานสอบสวนในส่วนที่เกี่ยวกับการปฏิบัติหน้าที่ตามมาตรา ๑๘ วรรคสอง โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสอง ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้หรือที่พนักงานสอบสวนได้มาตามมาตรา ๑๘ วรรคสอง ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วย

การสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น"

มาตรา ๑๗ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้"

มาตรา ๑๘ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ อาจได้รับค่าตอบแทนพิเศษตามที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

ในการกำหนดให้ได้รับค่าตอบแทนพิเศษต้องคำนึงถึงภาระหน้าที่ ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่หรือมีการสูญเสียผู้ปฏิบัติงานออกจากระบบราชการเป็นจำนวนมาก คุณภาพของงาน และการดำรงตนอยู่ในความยุติธรรมโดยเปรียบเทียบค่าตอบแทนของผู้ปฏิบัติงานอื่นในกระบวนการยุติธรรมด้วย"

มาตรา ๑๙ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๓๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"มาตรา ๓๑ ค่าใช้จ่ายในเรื่องดังต่อไปนี้ รวมทั้งวิธีการเบิกจ่ายให้เป็นไปตามระเบียบที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

(๑) การสืบสวน การแสวงหาข้อมูล และรวบรวมพยานหลักฐานในคดีความผิดตามพระราชบัญญัตินี้

(๒) การดำเนินการตามมาตรา ๑๘ วรรคหนึ่ง (๔) (๕) (๖) (๗) และ (๘) และมาตรา ๒๐

(๓) การดำเนินการอื่นใดอันจำเป็นแก่การป้องกันและปราบปรามการกระทำความผิดตามพระราชบัญญัตินี้"

มาตรา ๒๐ บรรดาระเบียบหรือประกาศที่ออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ยังคงใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติแห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ จนกว่าจะมีระเบียบหรือประกาศที่ต้องออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ ใช้บังคับ

การดำเนินการออกระเบียบหรือประกาศตามวรรคหนึ่ง ให้ดำเนินการให้แล้วเสร็จภายในหกสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

มาตรา ๒๑ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้

ผู้รับสนองพระราชโองการ
พลเอก ประยุทธ์ จันทร์โอชา
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็วและโดยที่มีการจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งมีภารกิจในการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศสมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวกับผู้รักษาการตามกฎหมาย กำหนดฐานความผิดขึ้นใหม่ และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ตลอดจนกำหนดให้มีคณะกรรมการเปรียบเทียบซึ่งมีอำนาจเปรียบเทียบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และแก้ไขเพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้

บทที่ 4
เทคนิคการปฏิบัติงาน

4.1 เทคนิคการปฏิบัติงานกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต

เทคนิค	เครื่องมือ	วิธีการใหม่ที่ทำมาใช้	เทคโนโลยีลดระยะเวลา ลดขั้นตอน
-นำรายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ตปีที่ผ่านมาปรับปรุง เพื่อใช้จัดทำรายงานปีปัจจุบัน	- รายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ตปีที่ผ่าน	- รายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ตปีที่ผ่าน	ระยะเวลาในการทำรายงานในปีถัดไป ลดลง 30 นาที

4.2 ขั้นตอนการปฏิบัติงาน

4.2.1 การวิเคราะห์กิจกรรมที่ต้องการพัฒนา

กระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต

กิจกรรมวิเคราะห์ตรวจสอบดูแลให้บริการป้องกันไวรัสในระบบเครือข่าย

ขั้นตอน	วิธีการปฏิบัติงานเดิม		วิธีการพัฒนางานใหม่		ผลลัพธ์ที่เกิดขึ้น
	กิจกรรม/วิธีการ	ระยะเวลา	กิจกรรม/วิธีการ	ระยะเวลา	
1.เก็บข้อมูลไวรัสและแสดงผลออกมาว่ามีการถูกไวรัสโจมตีในแต่ละเดือน	3	30 นาที	นำผลการตรวจจับไวรัสเดือนที่ผ่านมาปรับปรุงเพื่อทำเป็นรายงานในเดือนถัดไป	10 นาที	ระยะเวลาในการทำรายงานในเดือนถัดไป ลดลง 20 นาที
รวม	3	30 นาที	**รวม**	10 นาที	

กระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต
กิจกรรมวิเคราะห์สรุปผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต

ขั้นตอน	วิธีการปฏิบัติงานเดิม		วิธีการพัฒนางานใหม่		ผลลัพธ์ที่เกิดขึ้น
	กิจกรรม/วิธีการ	ระยะเวลา	กิจกรรม/วิธีการ	ระยะเวลา	
1.จัดทำรายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต	1	1 ชม.	นำรายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ตปีที่ผ่านมาปรับปรุง เพื่อใช้จัดทำรายงานปีปัจจุบัน	30 นาที	ระยะเวลาในการทำรายงานในปีถัดไปลดลง 30 นาที
2.จัดทำรายงานและจัดเก็บทางจดหมายอิเล็กทรอนิกส์	1	20 นาที	นำรายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ตปีที่ผ่านมาปรับปรุง เพื่อใช้จัดทำรายงานปีปัจจุบัน	15 นาที	ระยะเวลาในการทำรายงานในปีถัดไปลดลง 15 นาที
รวม	3	1ชม.20 นาที	**รวม**	45 นาที	

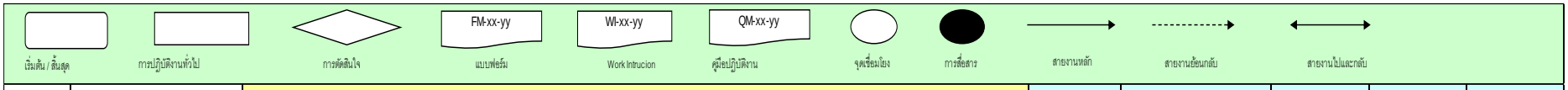
4.2.2 วิธีการปฏิบัติงาน(ใหม่)

ผังกระบวนการปฏิบัติงาน (Quality Work Procedure)

กระบวนการปฏิบัติงาน : รักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต

เริ่มต้น / สิ้นสุด | การปฏิบัติงานทั่วไป | การตัดสินใจ | FM-xx-yy แบบฟอร์ม | WI-xx-yy Work Intrucion | QM-xx-yy คู่มือปฏิบัติงาน | จุดเชื่อมโยง | การสื่อสาร | สายงานหลัก | สายงานย้อนกลับ | สายงานไปและกลับ

ลำดับ	กิจกรรมหลัก	รายละเอียดกิจกรรมรอง					เวลา			เอกสารที่เกี่ยวข้อง (รหัส)	จุดควบคุม (control item)	ตัวชี้วัด (kqi)	เป้าหมาย
		งานรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต	หัวหน้าฝ่าย	หัวหน้าสำนักงานผู้อำนวยการ	รองผู้อำนวยการ	ผู้อำนวยการ	นาที	ชม.	วัน				
1	งานตรวจสอบดูแลให้บริการป้องกันไวรัสในระบบเครือข่าย	เริ่มต้น ↓ ตรวจเช็คไวรัสบนเครื่องคอมพิวเตอร์แม่ข่าย ↓ เก็บข้อมูลไวรัสและแสดงผลออกมาว่ามีการถูกไวรัสโจมตีในแต่ละเดือน ↓ Update โปรแกรมป้องกันไวรัสและปรับปรุงฐานข้อมูลและ Export Report ไวรัส ด้วยโปรแกรมป้องกันไวรัส ↓ จัดเก็บข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายระบบป้องกันไวรัส ↓					10 10 10 10			1.รายงานการตรวจสอบเบื้องต้น 2.รายงานข้อมูลไวรัสที่ตรวจสอบได้ 3.รายงานการปรับปรุงและผลการตรวจสอบ 4.รายงานฐานข้อมูลระบบป้องกันวัสบนเครื่องคอมพิวเตอร์แม่ข่ายเสมือน	-รายงานฐานข้อมูลระบบป้องกันวัสบนเครื่องคอมพิวเตอร์แม่ข่ายเสมือน	ระยะเวลาดำเนินการที่แล้วเสร็จตามกำหนด	แล้วเสร็จตามระยะเวลาที่กำหนด



ลำดับขั้นตอน	กิจกรรมหลัก	รายละเอียดกิจกรรมรอง					เวลา			เอกสารที่เกี่ยวข้อง (รหัส)	จุดควบคุม (control item)	ตัวชี้วัด (kqi)	เป้าหมาย
		งานรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต	หัวหน้าฝ่าย	หัวหน้าสำนักงานผู้อำนวยการ	รองผู้อำนวยการ	ผู้อำนวยการ	นาที	ชม.	วัน				
2	งานตรวจสอบและป้องกันความเสี่ยงระบบเครือข่าย	ตรวจเช็คโดยรวมอุปกรณ์ Firewall ในการทำงาน ↓ ตรวจเช็คข้อมูลจราจร(Log file)บนอุปกรณ์(Firewall)ดูการบุกรุกและทำการป้องกันถ้ามีการโจมตีเข้ามาในระบบเครือข่าย ↓ ประเมินความเสี่ยง(Risk Assessment) ↓ ทดสอบความเสี่ยง(Testing) ↓ บันทึก(Record) ↓					10 20 10 10 10			1.รายงานเข้าอุปกรณ์ Firewall ผ่านหน้าเว็บไซต์เพื่อดูการทำงานโดยรวมของอุปกรณ์ 2.รายงานการตรวจสอบการทำงานของอุปกรณ์ 3.รายงานการตรวจสอบข้อมูลการบุกรุก 4.รายงานวิเคราะห์การบุกรุกต่างๆจากภายนอก 5.รายงานวิเคราะห์และประเมินความเสี่ยงจากระบบ ผ่านหน้าเว็บไซต์ผ่านอุปกรณ์ Firewall 6.รายงานกิจกรรมในการทำงานการโจมตีบนอุปกรณ์ที่เกิดขึ้นทั้งภายในและภายนอกองค์กร	รายงานกิจกรรมในการทำงานการโจมตีบนอุปกรณ์ที่เกิดขึ้นทั้งภายในและภายนอกองค์กร	ระยะเวลาดำเนินการที่แล้วเสร็จตามกำหนด	แล้วเสร็จตามระยะเวลาที่กำหนด
3	สรุปผลการตรวจสอบความมั่นปลอดภัยทางเครือข่ายอินเทอร์เน็ต	จัดทำรายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต ↓ จัดทำรายงานและจัดเก็บทางจดหมายอิเล็กทรอนิกส์ ↓ สิ้นสุด					30 15			1.รายงานผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต 2.รายงานแจ้งผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเตอร์เน็ต	รายงานแจ้งผลการตรวจสอบความมั่นคงปลอดภัยทางเครือข่ายอินเตอร์เน็ต	ระยะเวลาดำเนินการที่แล้วเสร็จตามกำหนด	แล้วเสร็จตามระยะเวลาที่กำหนด
รวม							140	1					

ผู้อนุมัติ	ผศ.ดร.ศิริลักษณ์ เกตุฉาย	**ตัวชี้วัดที่สำคัญ (KQI)**	**เป้าหมาย**
ตำแหน่ง	ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	ร้อยละความพึงพอใจการให้บริการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	≥4.95
วันที่	30/พฤศจิกายน/2565		

บทที่ 5
ข้อจำกัด ปัญหาอุปสรรค และแนวทางการพัฒนา

การดำเนินงานในการจัดทำกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ตมีข้อจำกัดและอุปสรรคในการปฏิบัติงาน และแนวทางการพัฒนา ดังนี้

ข้อจำกัด และปัญหาอุปสรรค	แนวทางการพัฒนา
เนื่องจากไวรัสมีการพัฒนาการตัวใหม่เกิดขึ้นทำให้ถูกไวรัสโจมตีในแต่ละวันต้องเฝ้าระวังในการกำจัดไวรัส	ศึกษาไวรัสตัวใหม่และติดต่อประสานงานกับผู้ที่เกี่ยวข้อง เพื่อกำจัดไวรัส

ภาคผนวก

หนังสืออนุมัติกระบวนการปฏิบัติงาน

หนังสือรับรองกระบวนการปฏิบัติงาน

ข้าพเจ้าผู้ช่วยศาสตราจารย์ ดร.ศิริลักษณ์ เกตุฉาย ตำแหน่งผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้พิจารณาและเห็นชอบกับการปรับปรุงกระบวนการสนับสนุนสร้างคุณค่ากระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต ในฐานะผู้บังคับบัญชาสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

โดยยินยอมให้ศูนย์เทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ นำกระบวนการรักษาความมั่นคงปลอดภัยทางเครือข่ายอินเทอร์เน็ต มาใช้ในหน่วยงานตั้งแต่วันที่ ๓๐ ธันวาคม ๒๕๖๕ เป็นต้นไป

ให้ไว้ ณ วันที่ ๓๐ ธันวาคม ๒๕๖๕

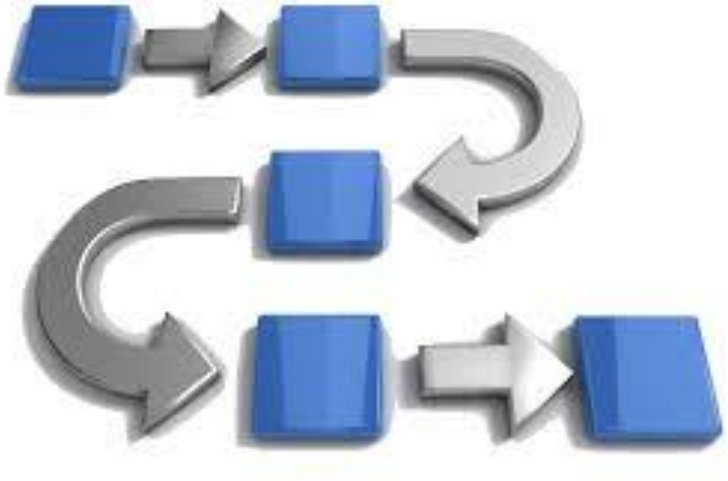
(ผู้ช่วยศาสตราจารย์ ดร.ศิริลักษณ์ เกตุฉาย)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

คณะผู้จัดทำ

คู่มือปฏิบัติงานกระบวนการขับเคลื่อนการจัดอันดับมหาวิทยาลัย

1. อาจารย์อภิรักษ์	ธิตินฤมิต	รองผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ
2. นายอโณทัย	อรุณเรือง	หัวหน้าฝ่ายระบบเครือข่ายและอินเทอร์เน็ต
3. นายอัครเดช	สินแต่ง	หัวหน้าฝ่ายพัฒนาระบบสารสนเทศ
4. นางลลิสา	สหนาวิน	นักวิชาการคอมพิวเตอร์
5. นายจรูญพันธ์	สหนาวิน	นักวิชาการคอมพิวเตอร์
6. นางสาววราภรณ์	นราประเสริฐ	นักวิชาการคอมพิวเตอร์
7. นายสุรวิช	สุนทรเสนีย์กุล	นักวิชาการคอมพิวเตอร์
8. นายรุจิโรจน์	กังเจริญสัมพันธ์	นักวิชาการคอมพิวเตอร์
9. นางสาวสุธาสินี	ยกระดับ	นักวิชาการคอมพิวเตอร์
10.นายณัฐ	พลอยอ่อง	นักวิชาการคอมพิวเตอร์
11.นายปฐมพงศ์	ปุณณภุม	นักวิชาการคอมพิวเตอร์

คู่มือการปฏิบัติงาน (Work Manual)



1 ถนนอู่ทองนอก แขวงวชิระ เขตดุสิต กรุงเทพมหานคร 10300

Suan Sunandha Rajabhat University