การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมบัญชีกลาง

โดย

นายเกียรติณรงค์ วงศ์น้อย
ที่ปรึกษาด้านพัฒนาระบบการเงินการคลัง
กรมบัญชีกลาง กระทรวงการคลัง

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 61
ประจำปีการศึกษา พุทธศักราช 2561 - 2562

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมบัญชีกลาง” ลักษณะวิชาวิทยาศาสตร์และเทคโนโลยี ของ นายเกียรติณรงค์ วงศ์น้อย เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 61 ประจำปีการศึกษา พุทธศักราช 2561 – 2562

พลโท

(ขจรฤทธิ์ นิลกำแหง)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง **การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมบัญชีกลาง**

ลักษณะวิชา **วิทยาศาสตร์และเทคโนโลยี**

ผู้วิจัย **นายเกียรติณรงค์ วงศ์น้อย** **หลักสูตร วปอ. รุ่นที่ 61**

งานวิจัยนี้คืองานวิจัยที่เกี่ยวข้องกับศึกษากฎหมาย กฎระเบียบ ข้อบังคับ ที่เกี่ยวข้องกับสารสนเทศ ผู้วิจัยได้รวบรวมข้อมูล และศึกษาความเหมาะสมของการทำงานของบุคลากร รวมทั้งอุปกรณ์ที่ใช้ในการดำเนินการ และนำมาจัดทำเป็นพัฒนานโยบายการรักษาควบคุมความมั่นคงทางไซเบอร์ของกรมบัญชีกลาง เพื่อนำมาสื่อสารให้บุคลากรที่เกี่ยวข้อง พร้อมทั้งบังคับใช้นโยบายฯ ให้เหมาะสมกับการทำงาน รวมถึงการบังคับให้ระบบสารสนเทศของกรมบัญชีกลางต้องปฏิบัติตามนโยบายฯ เพื่อให้ระบบสารสนเทศมีความพร้อมกับการรับมือกับภัยคุกคามทางไซเบอร์ และวางแผนการปรับปรุงอุปกรณ์และเทคโนโลยีในอนาคตให้ทันสมัย และสามารถตอบสนองต่อภัยคุกคามทางไซเบอร์เพื่อลดผลกระทบที่เกิดขึ้นจากภัยคุกคาม โดยการศึกษาได้มีการศึกษาบุคลากร อุปกรณ์ ระบบงานของศูนย์เทคโนโลยีสารสนเทศ ของกรมบัญชีกลาง ผลการวิจัยนี้ชี้ให้เห็นว่า บุคลากรของศูนย์เทคโนโลยีสารสนเทศมีไม่เพียงพอต่อการเฝ้าระวังภัยคุกคามทางไซเบอร์ และอุปกรณ์ของศูนย์เทคโนโลยีสารสนเทศยังมีไม่เพียงพอต่อการรับมือและการวิเคราะห์ภัยคุกคามเนื่องระบบงานของกรมที่ให้บริการกับหน่วยงานภายนอกมีค่อนข้างเยอะ ผลการพัฒนานโยบายการรักษาควบคุมความมั่นคงทางไซเบอร์ของกรมบัญชีกลาง จะช่วยในการควบคุมบุคลากรและระบบงานของกรมบัญชีกลางให้สามารถรับมือต่อภัยคุกคามทางไซเบอร์ได้

Abstract

Title Cyber Security of the Comptroller General's Department
Field Science and Technology
Name Mr.Kiatnarong Wongnoi **Course** NDC **Class** 61

This research is involving the study of laws, regulations, and principles concerning with information system. The researcher gathered and researched the proper working process of personnel, also the working equipment, and apply it to develop a cybersecurity strategy of The Comptroller General' s Department for communicating for concerned personnel. And properly enforcing the strategy to the working process including enforcing the information technology system of The Comptroller General' s Department to act according to the strategy. To make the information technology system ready to encounter with a cyber threat and planning for improving future devices and technologies to be modern and able to encounter with a cyber threat to reduce its effect. The researcher studied from the personnel, devices, and the working system of The Comptroller General' s Department' s Information Technology Center and the result of this research found that the Information Technology Center doesn't have enough personnel to monitor for the cyber threat. Its devices also not enough to encounter and analyze the threat because the department has many working systems for serving the outsider agencies. The result of the development of the cybersecurity strategy of The Comptroller General's Department will help to control the personnel and the working system of The Comptroller General's Department to be able to encounter with a cyber threat.

คำนำ

เอกสารวิจัยฉบับนี้ เป็นส่วนหนึ่งของหลักสูตรการป้องกันราชอาณาจักร มีเนื้อหาเพื่อการจัดทำนโยบายการรักษาควบคุมความมั่นคงทางไซเบอร์ ของกรมบัญชีกลาง มีวัตถุประสงค์เพื่อรักษาระบบสารสนเทศให้คงไว้ซึ่งคุณสมบัติหลัก 3 ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การคงสภาพความถูกต้องและความน่าเชื่อถือของข้อมูล (Integrity) และความพร้อมใช้งาน (Availability) ของระบบสารสนเทศของกรมบัญชีกลาง

ผู้จัดทำวิจัยหวังเป็นอย่างยิ่งว่า เอกสารวิจัยฉบับนี้จะเป็นประโยชน์ต่อบุคลากรของกรมบัญชีกลางที่เป็นผู้ใช้งานทั่วไป ผู้ปฏิบัติงานด้านระบบสารสนเทศและผู้ที่สนใจ สามารถนำไปเป็นแนวทางในการใช้และป้องกันภัยคุกคามทางด้านไซเบอร์ของเทคโนโลยีสารสนเทศได้อย่างปลอดภัย

(นายเกียรติณรงค์ วงศ์น้อย)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 61
ผู้วิจัย

กิตติกรรมประกาศ

เอกสารวิจัยฉบับนี้สำเร็จเรียบร้อยได้ก็ด้วยความเสียสละ ความอนุเคราะห์ อาจารย์ที่ปรึกษาที่ได้ให้ความรู้ ให้คำปรึกษา ให้แนวคิดและช่วยตรวจแก้ไขในส่วนที่บกพร่องต่าง ๆ ตั้งแต่เริ่มต้นจนกระทั่งสำเร็จเป็นรูปเล่ม และข้อเสนอแนะจนสมบูรณ์ ข้าพเจ้าขอกราบขอบพระคุณในความกรุณาของทุกท่านมา ณ โอกาส

ขอขอบพระคุณในความเอื้อเฟื้อของทีมงานนักศึกษาวิทยาลัยป้องกันราชอาณาจักร ที่ได้ให้ความช่วยเหลือด้านเอกสารคำแนะนำ และวิธีการจัดทำเอกสารวิจัย จนกระทั่งบรรลุผลสำเร็จเป็นอย่างดี

ท้ายที่สุดนี้ คุณความดีและกุศลที่พึงบังเกิดมีจากเอกสารวิจัยเล่มนี้ เป็นผลมาจากความเมตตา กรุณา ของบิดา มารดา และครอบครัว ผู้คอยให้กำลังใจ และคณาจารย์ทุกท่าน ผู้ประสิทธิ์ประศาสน์วิชาความรู้แก่ข้าพเจ้า จึงขอยกคุณความดีเหล่านั้นเป็นเครื่องบูชาพระคุณด้วยความเคารพและสักการะ

(นายเกียรติณรงค์ วงศ์น้อย)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 61
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญแผนภาพ

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

กรมบัญชีกลางทำหน้าที่ทั้งการเป็นผู้ให้บริการ (Service Provider) และการกำกับดูแลทางด้านการเงินและบัญชีภาครัฐ (Regulator) มีภารกิจเกี่ยวกับการควบคุมดูแลการใช้จ่ายเงินของแผ่นดินและหน่วยงานภาครัฐ ให้เป็นไปโดยถูกต้อง มีวินัย คุ้มค่า โปร่งใส และสามารถตรวจสอบได้ โดยการวางกรอบหลักเกณฑ์กลางให้หน่วยงานภาครัฐถือปฏิบัติ การให้บริการคำแนะนำปรึกษาด้านการเงิน การคลัง การบัญชี การตรวจสอบภายใน การบริหารเงินนอกงบประมาณ และการพัสดุภาครัฐ การดำเนินการเกี่ยวกับการบริหารเงินคงคลังให้มีใช้จ่ายอย่างเพียงพอ และการเสนอข้อมูลในเชิงนโยบายการคลังแก่ฝ่ายบริหารโดยประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อให้เกิดเสถียรภาพทางการคลัง รวมทั้งดำเนินการเกี่ยวกับการประเมินผลการคลังภาครัฐ การกำกับดูแลนโยบายและมาตรฐานค่าตอบแทน สวัสดิการและสิทธิประโยชน์ของบุคลากรภาครัฐ โดยให้มีอำนาจหน้าที่ ดังต่อไปนี้ ให้คำปรึกษาหรือข้อเสนอแนะเกี่ยวกับการพัฒนระบบริหารการคลังของประเทศในด้านการบริหารเงินคงคลัง ต่อกระทรวงการคลัง และคณะรัฐมนตรี ดำเนินการเกี่ยวกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง และหลักเกณฑ์ด้านการเงิน การคลัง การบัญชี การพัสดุภาครัฐและการตรวจสอบภายใน เพื่อให้ส่วนราชการหรือหน่วยงานของรัฐถือปฏิบัติ ดำเนินการเกี่ยวกับการกำหนดนโยบายและมาตรฐานการจัดซื้อจัดจ้างภาครัฐ ดำเนินการเกี่ยวกับการกำหนดนโยบายและมาตรฐาน การกำกับดูแล และการพัฒนาเกี่ยวกับการตรวจสอบภายในภาครัฐ ดำเนินการเกี่ยวกับการประเมินผลการคลังภาครัฐในความรับผิดชอบของกรม รวมทั้งติดตามการดำเนินงานและการบริหารด้านการคลัง เพื่อประกอบการพิจารณาเสนอแนะนโยบายด้านการคลังของประเทศ ควบคุม ดูแล และตรวจสอบการเบิกจ่ายเงินของหน่วยงานภาครัฐ การก่อหนี้ผูกพัน การนำเงินส่งคลัง และการถอนคืนเงินรายได้แผ่นดิน รวมทั้งพิจารณาทำความตกลงในการเบิกจ่ายเงินงบประมาณตามที่ส่วนราชการขอทำความตกลง ดำเนินการเกี่ยวกับการบริหารเงินคงคลัง พัฒนาระบบบริหารเงินนอกงบประมาณในด้านกำกับดูแล การติดตามประเมินผล การใช้จ่ายเงินนอกงบประมาณ การทบทวนประสิทธิภาพและความจำเป็นในการดำเนินงานของเงินนอกงบประมาณอย่างเป็นระบบที่มีประสิทธิภาพ รวมทั้งการพัฒนากฎระเบียบที่เกี่ยวข้องในการกำกับและบริหารเงินนอกงบประมาณของหน่วยงานภาครัฐ กำหนด ปรับปรุง และพัฒนามาตรฐานค่าตอบแทน สวัสดิการ และสิทธิประโยชน์ของบุคลากรภาครัฐ พัฒนาระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ และกำกับดูแลการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ ดำเนินเกี่ยวกับการกำหนดมาตราฐานการบัญชีภาครัฐ ระบบบัญชี ตลอดจนการจัดทำและวิเคราะห์รายงานการเงินของแผ่นดิน ดำเนินการเกี่ยวกับความรับผิดทางละเมิดของเจ้าหน้าที่ตามกฎหมายว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่ และความรับผิดทางแพ่งของเจ้าหน้าที่ของส่วนราชการ ดำเนินการเกี่ยวกับการพัฒนาระบบการบริหารบุคคลลูกจ้างของส่วนราชการ ดำเนินการเกี่ยวกับการพัฒนาบุคลากรด้านการเงินการคลัง การบัญชี การตรวจสอบภายในและการพัสดุภาครัฐ ให้คำปรึกษา เสนอแนะ และให้ความช่วยเหลือด้านวิชาการและการปฏิบัติงานทางการเงินการคลัง การบัญชี การพัสดุภาครัฐ การตรวจสอบภายใน แก่ส่วนราชการและหน่วยงาน

ของรัฐ ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นหน้าที่และอำนาจของกรมหรือตามที่รัฐมนตรีหรือคณะรัฐมนตรีมอบหมาย ปัจจุบันกรมบัญชีกลางได้พัฒนาเทคโนโลยีสารสนเทศมาช่วยงานกิจกรรม ภารกิจของกรมบัญชีกลาง เช่น ระบบจ่ายตรงเงินเดือนและค่าจ้างประจำ ระบบจัดซื้อจัดจ้างภาครัฐด้วยวิธีอิเล็กทรอนิกส์ ระบบบำเหน็จบำนาญและสวัสดิการค่ารักษาพยาบาล ระบบบูรณาการฐานข้อมูลสวัสดิการภาครัฐ ระบบรับชำระเงินกลางของบริการภาครัฐ เป็นต้น โดยระบบงานต่าง ๆ ของกรมบัญชีกลางเป็นระบบที่ให้บริการภาครัฐที่สำคัญ และมีข้อมูลที่สำคัญทั้งที่เป็นข้อมูลส่วนบุคคลและข้อมูลที่เป็นความลับมากมาย ซึ่งเป็นเป้าหมายของผู้ไม่หวังดีในการที่พยายามเข้าถึงข้อมูลดังกล่าวโดยให้ใช้เทคโนโลยีทางไซเบอร์ในการเข้าถึงระบบงาน พร้อมกันนี้ในปัจจุบันมีภัยคุกคามทางไซเบอร์ (Cyber threat) ที่เป็นปัญหาในหลายประเทศ ซึ่งทางกรมบัญชีกลางได้ตระหนักถึงภัยคุกคามที่คาดว่าอาจเกิดขึ้นกับกรมบัญชีกลางได้ในอนาคต ดังนั้น กรมบัญชีกลางทบทวนกระบวนการหรือการกระทำทั้งหมดที่เกี่ยวข้องกับระบบงานของกรมบัญชีกลาง เพื่อประเมินความเสี่ยง ดำเนินการทำให้องค์กรปราศจากความเสี่ยง รวมถึงการรับมือกับภัยคุกคามที่จะเกิดขึ้น โดยคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล ประกอบด้วย การรักษาความลับของข้อมูล การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ ของข้อมูลและความพร้อมใช้งานของข้อมูล

จึงกล่าวได้ว่าความมั่นคงปลอดภัยไซเบอร์ ถือว่ามีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้นการที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีกระบวนการในการดำเนินการ โดยเลือกมาตรฐานสากลแล้วนำมาประยุกต์ใช้ให้เหมาะสมกับองค์กรและต้องสอดคล้องตามกฎหมายต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ยุทธศาสตร์ชาติ จากเหตุผลข้างต้น จึงนำมาสู่การศึกษาเรื่อง “การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกรมบัญชีกลาง” โดยมีวัตถุประสงค์เพื่อศึกษานโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมบัญชีกลาง

วัตถุประสงค์ของการวิจัย

1. ศึกษานโยบาย ยุทธศาสตร์ และการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมบัญชีกลาง
2. ศึกษามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐาน ISO/IEC 27001
3. วิเคราะห์องค์ประกอบด้านต่างๆ เพื่อกำหนดแนวทางการพัฒนาระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมบัญชีกลาง
4. เสนอแนะแนวทางในการปรับและพัฒนามาตรฐานงานและองค์ประกอบสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ของกรมบัญชีกลาง

ขอบเขตของการวิจัย

การวิจัยเรื่อง “การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ของกรมบัญชีกลาง” ประกอบด้วยขอบเขตของการศึกษา ดังนี้

1. ขอบเขตด้านเนื้อหา

การวิจัยครั้งนี้จะดำเนินการการทบทวนวรรณกรรมที่เกี่ยวข้องกับกฎหมาย กฎระเบียบเกี่ยวข้องกับเทคโนโลยีสารสนเทศ ตลอดจนนโยบายขององค์กร

2. ขอบเขตด้านทักษะและความรู้ของบุคลากร

การวิจัยครั้งนี้จะดำเนินการให้ความรู้ด้านความมั่นคงปลอดภัยให้กับบุคลากรของกรมและสร้างความตระหนักและการรับรู้เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของกรม เพื่อวัดประสิทธิภาพในการดำเนินการด้านความมั่นคงปลอดทางไซเบอร์ และจัดหลักสูตรฝึกอบรมให้บุคลากรมีความรู้ทักษะในการดำเนินการทางด้านความมั่นคงปลอดภัยทางไซเบอร์

3. ขอบเขตด้านเทคโนโลยีสารสนเทศ

การวิจัยครั้งนี้จะดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมบัญชีกลางและการดำเนินงานของศูนย์เทคโนโลยีสารสนเทศ เพื่อจัดหาหรือเตรียมการให้เหมาะสม และเพิ่มขีดความสามารถในการดำเนินการรับมือกับภัยคุกคามทางไซเบอร์

4. ขอบเขตด้านเวลา

การวิจัยครั้งนี้จะดำเนินการรวบรวมข้อมูลทั้งข้อมูลปฐมภูมิและข้อมูลทุติยภูมิในห้วงเวลาตั้งแต่เดือนตุลาคม 2561 – กันยายน 2562

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีการดำเนินการ ดังนี้

1. การรวบรวมข้อมูล

1.1 ข้อมูลทุติยภูมิ รวบรวมข้อมูลเรื่องแนวคิด ทฤษฎี รวมถึงวรรณกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เว็บไซต์ที่เกี่ยวข้อง

1.2 ข้อมูลปฐมภูมิ โดยรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึกจากผู้ให้ข้อมูลสำคัญ

2. การจัดระเบียบข้อมูล

เมื่อรวบรวมข้อมูลทั้งข้อมูลปฐมภูมิและข้อมูลทุติยภูมิดังที่กล่าวแล้ว หลังจากนั้นจะนำข้อมูลมาจัดระเบียบและตรวจสอบ (Validity) ของข้อมูลตามขั้นตอนการวิจัยเชิงคุณภาพเพื่อที่จะเตรียมข้อมูลไว้สำหรับการวิเคราะห์ข้อมูลในขั้นตอนต่อไป

3. การวิเคราะห์ข้อมูล และการสังเคราะห์ข้อมูล

จะดำเนินการวิเคราะห์ข้อมูลโดยวิธีการวิเคราะห์เนื้อหา (Context Analysis) โดยวิเคราะห์เนื้อหาของข้อมูล เพื่อเชื่อมความสัมพันธ์ระหว่างส่วนประกอบต่าง ๆ ของข้อมูล และนำข้อมูลที่ได้มาสังเคราะห์ เพื่อสรุปเป็นตัวแบบในการกำหนดนโยบายด้านความมั่นคงไซเบอร์ของกรมบัญชีกลาง

ประโยชน์ที่ได้รับจากการวิจัย

1. ได้นโยบายความมั่นคงปลอดภัยทางไซเบอร์สอดคลที่เหมาะสมกับระบบงานต่างๆ ของกรมบัญชีกลาง
2. ได้กระบวนการดำเนินงานที่เป็นไปตามมาตรฐานสากลที่เหมาะสมกับการดำเนินงานภายในกรมบัญชีกลาง
3. ได้กำหนดแนวทางในการพัฒนาระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับกรมบัญชีกลาง
4. ได้แนวทางในการปรับปรุงระบบสนับสนุนการรักษาความมั่นคงปลอดภัยทางไซเบอร์

คำจำกัดความ

บุคลากรกรมบัญชีกลาง (ส่วนกลาง)	หมายถึง ข้าราชการ ลูกจ้างประจำ และพนักงานราชการในกรมบัญชีกลาง (ส่วนกลาง)
นโยบายผู้บริหาร	หมายถึง นโยบาย เป้าหมายทางด้านความมั่นคงปลอดภัย ตลอดจนการมอบหมายหน้าที่ในระดับต่าง ๆ และให้การสนับสนุนนโยบายต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
เทคโนโลยีสารสนเทศ	หมายถึง เทคโนโลยีในปัจจุบันทั้งด้าน Hardware และ Software ที่มีผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ
กฎหมายที่เกี่ยวข้อง	หมายถึง กฎหมาย ระเบียบ หรือข้อบังคับทางด้านความมั่นคงปลอดภัย ตลอดจนกฎหนมายคุ้มครองข้อมูลส่วนบุคคล
ISO 27001	หมายถึง คือมาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems : ISMS) มาตรฐานนี้ให้ต้นแบบสำหรับการประเมินความเสี่ยง การออกแบบด้านการรักษาความปลอดภัยและการนำไปปฏิบัติ รวมถึงการบริหารจัดการความปลอดภัยมาตรฐาน ISO 27001 ได้ระบุแนวทางการดำเนินงานและการบริหารจัดการที่จะช่วยในการเก็บรักษาข้อมูลทั้งเป็นดิจิตอลและเอกสารของท่านได้อย่างปลอดภัย

บทที่ 2
การทบทวนวรรณกรรมที่เกี่ยวข้อง

การศึกษา เรื่อง การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมบัญชีกลาง ได้มีการนำแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องมาใช้เพื่อเป็นแนวทางในการศึกษา ดังนี้

1. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
2. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550
3. ระเบียบและข้อกฎหมายที่เกี่ยวข้องกับพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์
4. ระเบียบและข้อกฎหมายที่เกี่ยวข้องกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
5. ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 วันที่ 23 พฤษภาคม 2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต
6. งานวิจัยที่เกี่ยวข้อง
7. กรอบแนวคิดในการวิจัย
8. สรุป

ในบทนี้เป็นการศึกษาระเบียบและข้อกฎหมายที่เกี่ยวข้องกับระบบการรักษาความปลอดภัยด้านสารสนเทศ เพื่อนำมาปรับปรุงระบบการรักษาความปลอดภัยของกรมบัญชีกลาง ให้สอดคล้องกับระเบียบและกฎหมายเกี่ยวข้อง และเหมาะสมกับลักษณะการดำเนินงานของกรมบัญชีกลาง โดยมีระเบียบและข้อกฎหมายที่เกี่ยวข้องที่นำมาศึกษาต่อไปนี้

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 (“สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ”,ออนไลน์, 2562)

ในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ เนื่องจากประเทศไทยได้เริ่มเข้าสู่ยุคสังคมสารสนเทศ ซึ่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น สมควรสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตน โดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับให้หน่วยงานของรัฐสามารถพัฒนา การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่น ของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ ประกอบกับมาตรา 35 วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 บัญญัติว่า คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมาย

กับหน่วยงานของรัฐหรือโดยหน่วยงาน ของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาแล้ว ให้ถือว่ามีผลโดยชอบด้วยกฎหมาย เช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนดพระราชกฤษฎีกาฉบับนี้เกี่ยวกับกรมบัญชีกลาง รายละเอียดมาตรา 3 ถึงมาตรา 9 ดังนี้

มาตรา 3 ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ หน่วยงานของรัฐต้องจัดให้มีระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ในลักษณะ ดังต่อไปนี้

(1) เอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์นั้นต้องอยู่ในรูปแบบที่เหมาะสม โดยสามารถแสดงหรืออ้างอิงเพื่อใช้ในภายหลังและยังคงความครบถ้วนของขอความในรูปแบบของข้อมูลอิเล็กทรอนิกส์

(2) ต้องกำหนดระยะเวลาเริ่มต้นและสิ้นสุดในการยื่นเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์โดยปกติให้ยึดถือวันเวลาของการปฏิบัติงานหน่วยงานของรัฐนั้นเป็นหลัก และอาจกำหนดระยะเวลาในการดำเนินการพิจารณาของหน่วยงานของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ไว้ด้วยก็ได้ เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(3) ต้องกำหนดวิธีการที่ทำให้สามารถระบุตัวเจ้าของลายมือชื่อ ประเภท ลักษณะหรือรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์

(4) ต้องกำหนดวิธีการแจ้งการตอบรับด้วยวิธีการทางอิเล็กทรอนิกส์หรือด้วยวิธีการอื่นใดเพื่อเป็นหลักฐานว่าได้ มีการดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ไปยังอีกฝ่ายหนึ่งแล้ว

มาตรา 4 นอกจากที่บัญญัติไว้ในมาตรา 3 ในกรณีที่หน่วยงานของรัฐจัดทำกระบวนการพิจารณาทางปกครองโดยวิธีการทางอิเล็กทรอนิกส์ระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ต้องมีลักษณะดังต่อไปนี้ด้วย เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(1) มีวิธีการสื่อสารกับผู้ยื่นคำขอในกรณีที่เอกสารมีข้อบกพร่องหรือมีข้อความที่ผิดหลงอันเห็นได้ ชัดว่าเกิดจากความไม่รู้ หรือความเลินเล่อของผู้ ยื่นคำขอ หรือการขอข้อเท็จจริงเพิ่มเติม รวมทั้งมีวิธีการแจ้งสิทธิและหน้าที่ในกระบวนการพิจารณาทางปกครองตามความจำเป็นแก่กรณี ในกรณีที่กฎหมายกำหนดให้ ต้องแจ้งให้คู่กรณีทราบ

(2) ในกรณีมีความจำเป็นตามลักษณะเฉพาะของธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐใด หน่วยงานของรัฐนั้นอาจกำหนดเงื่อนไขว่าคู่กรณียินยอมตกลงและยอมรับการดำเนินการพิจารณาทางปกครองของหน่วยงานของรัฐโดยวิธีการทางอิเล็กทรอนิกส์

มาตรา 5 หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ เพื่อให้ การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(2) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรา 6 ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา 7 แนวนโยบายและแนวปฏิบัติตามมาตรา 5 และมาตรา 6 ให้หน่วยงานของรัฐจัดทำเป็นประกาศและต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจึงมีผลใช้บังคับได้ หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

มาตรา 8 ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้นสำหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

มาตรา 9 การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐตามหลักเกณฑ์และวิธีการตามพระราชกฤษฎีกานี้ ไม่มีผลเป็นการยกเว้นกฎหมายหรือหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนดไว้เพื่อการอนุญาต อนุมัติ การให้ความเห็นชอบหรือการวินิจฉัย

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

(“สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ”,ออนไลน์, 2562)

ประกาศกระทรวงเทคโนโลยีสารสนเทศและสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ประกาศเพื่อให้หน่วยงานต่าง ๆ ดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์พร้อมกำหนดหลักเกณฑ์ในการดำเนินการ โดยมีข้อกำหนดดังนี้

ข้อ 5 ภายใต้บังคับของมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550 ประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แบ่งได้ ดังนี้

(1) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกัน โดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ 4 ประเภท ดังนี้

ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้ เช่าบริการโปรแกรมประยุกต์ต่าง ๆ (Host Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ง. ผู้ให้บริการร้านอินเทอร์เน็ต ดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

(2) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (1) (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่าง ๆ (Application Service Provider) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก. แนบท้ายประกาศนี้ ข.

ข้อ 6 ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการต้องเก็บรักษา ปรากฏดังภาคผนวก ข. แนบท้ายประกาศนี้ ข

ข้อ 7 ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ดังนี้

(1) ผู้ให้บริการตามข้อ 5 (1) ก. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. 1

(2) ผู้ให้บริการตามข้อ 5 (1) ข. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. 2 ตามประเภท ชนิดและหน้าที่การให้บริการ

(3) ผู้ให้บริการตามข้อ 5 (1) ค. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. 2 ตามประเภท ชนิดและหน้าที่การให้บริการ

(4) ผู้ให้บริการตามข้อ 5 (1) ง. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. 3

(5) ผู้ให้บริการตามข้อ 5 (2) มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. 4 ทั้งนี้ ในการเก็บรักษาข้อมูลจราจรตามภาคผนวกต่าง ๆ ที่กล่าวไปข้างต้นนั้นให้ผู้ให้บริการเก็บเพียงเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น

ข้อ 8 การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้ วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(1) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(2) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บและกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น เว้นแต่ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กร กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

(3) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้ง ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้การสงมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

(4) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้ บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้ บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

(5) ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ 1 ถึงข้อ 4 ข้างต้นได้ให้ บริการในนามตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สามเป็นเหตุให้ ผู้ให้บริการในข้อ 1 ถึงข้อ 4 ไม่สามารถรู้ได้ว่าผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใครผู้ให้บริการ เช่นว่านั้นต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

ข้อ 9 เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที

ข้อ 10 ผู้ให้บริการซึ่งมีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ 7 เริ่มเก็บข้อมูลดังกล่าวตามลำดับ ดังนี้

(1) ผู้ให้บริการตามข้อ 5 (1) ก. เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นสามสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

(2) ให้ ผู้ให้บริการตามข้อ 5 (1) ข. เฉพาะผู้ให้บริการเครือข่ายสาธารณะหรือผู้ให้บริการอินเทอร์เน็ต (ISP) เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งร้อยแปดสิบวันนับจากวันประกาศในราชกิจจานุเบกษา ผู้ให้บริการอื่นนอกจากที่กล่าวมาในข้อ 10 (1) และข้อ 10 (2) ข้างต้น ให้เริ่มเก็บข้อมูล จราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งปีนับจากวันประกาศในราชกิจจานุเบกษา

พระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550

(“สำนักงานคณะกรรมการกฤษฎีกา”,ออนไลน์, 2562)

ในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว มีรายละเอียดมีอยู่ทั้งหมด 2 หมวด 26 มาตรา ดังนี้

หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 6 ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา 8 ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา 12 ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10

(1) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(2) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา 13 ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)

มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

มาตรา 16 ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้ ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา 17 ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

หมวด 2 พนักงานเจ้าหน้าที่

มาตรา 18 ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้มาตรา 19 การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิดเท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้นให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา 18 (4) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา 18 (8) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดง

การยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว

พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา 20 ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสอง ลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา 21 ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมาย ถึงชุด คำสั่ง ที่มีผล ทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้นตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา 22 ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา 18 ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 23 พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา 18 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 24 ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา 18 และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 25 ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา 27 ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา18 หรือมาตรา 20 หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา 21 ต้องระวางโทปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา 28 การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา 29 ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา 30 ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้องบัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (“สำนักงานคณะกรรมการกฤษฎีกา”,ออนไลน์, 2562)

ในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็วและโดยที่มีการจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งมีภารกิจในการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ สมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวกับผู้รักษาการตามกฎหมาย กำหนดฐานความผิดขึ้นใหม่ และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ตลอดจนกำหนดให้มีคณะกรรมการเปรียบเทียบซึ่งมีอำนาจเปรียบเทียบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และแก้ไขเพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้นมีรายละเอียด ดังนี้

มาตรา 3 ให้ยกเลิกความในมาตรา 4 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิด

เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน “มาตรา 4 ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการ

ตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่กับออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้ กฎกระทรวงและประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้”

มาตรา 4 ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา 11 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

“ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกินสองแสนบาทให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับและลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย”

มาตรา 5 ให้ยกเลิกความในมาตรา 12 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน

“มาตรา 12 ถ้าการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 หรือมาตรา 11 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความ

มั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”

มาตรา 6 ให้เพิ่มความต่อไปนี้เป็นมาตรา 12/1 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

“มาตรา 12/1 ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 เป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”

มาตรา 7 ให้เพิ่มความต่อไปนี้เป็นวรรคสอง วรรคสาม วรรคสี่ และวรรคห้าของมาตรา 13 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

“ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 12 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา 12 วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา 12 วรรคสองหรือวรรคสี่ หรือมาตรา 12/1 ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 12 วรรคหนึ่งหรือวรรคสาม หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา 12 วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา 12 วรรคสองหรือวรรคสี่ หรือมาตรา 12/1 ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสามหรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว”

มาตรา 8 ให้ยกเลิกความในมาตรา 14 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน

“มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1)(2) (3) หรือ (4)

ถ้าการกระทำความผิดตามวรรคหนึ่ง (1) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้”

มาตรา 9 ให้ยกเลิกความในมาตรา 15 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน

“มาตรา 15 ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ”

มาตรา 10 ให้ยกเลิกความในมาตรา 16 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน

“มาตรา 16 ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสีย

ชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอายผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริต อันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรสหรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย”

มาตรา 11 ให้เพิ่มความต่อไปนี้เป็นมาตรา 16/1 และมาตรา 16/2 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

“มาตรา 16/1 ในคดีความผิดตามมาตรา 14 หรือมาตรา 16 ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง

(1) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(2) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณา หรือเผยแพร่

(3) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

มาตรา 16/2 ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลาย ตามมาตรา 16/1 ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ ในมาตรา 14 หรือมาตรา 16 แล้วแต่กรณี”

มาตรา 12 ให้เพิ่มความต่อไปนี้เป็นมาตรา 17/1 ในหมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

“มาตรา 17/1 ความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 11 มาตรา 13 วรรคหนึ่งมาตรา 16/2 มาตรา 23 มาตรา 24 และมาตรา 27 ให้คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งมีอำนาจเปรียบเทียบได้

คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคนหนึ่งต้องเป็นพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ต้องหาไม่ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว”

มาตรา 13 ให้ยกเลิกความในมาตรา 18 และมาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน

“มาตรา 18 ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดหรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวนอาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รีบรวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (1) (2) และ (3) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายใน

ระยะเวลาที่พนักงานเจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดระยะเวลาที่ต้องดำเนินการที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้

มาตรา 19 การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8)ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8)ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา 18 (4) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา 18 (8) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้วพนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลันหนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง”

มาตรา 14 ให้ยกเลิกความในมาตรา 20 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน

“มาตรา 20 ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ดังต่อไปนี้ พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้

(1) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัตินี้

(2) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาค 2 ลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา

(3) 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 15 ให้ยกเลิกความในวรรคสองของมาตรา 21 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน

“ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่ง หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง เว้นแต่เป็นชุดคำสั่งไม่พึงประสงค์ที่อาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดรายชื่อ ลักษณะ หรือรายละเอียดของชุดคำสั่งไม่พึงประสงค์ซึ่งอาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์ก็ได้”

มาตรา 16 ให้ยกเลิกความในมาตรา 22 มาตรา 23 มาตรา 24 และมาตรา 25 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน

“มาตรา 22 ห้ามมิให้พนักงานเจ้าหน้าที่และพนักงานสอบสวนในกรณีตามมาตรา 18 วรรคสองเปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มาตามมาตรา 18 ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นในกรณีตามมาตรา 18 วรรคสอง หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบหรือกับพนักงานสอบสวนในส่วนที่เกี่ยวกับการปฏิบัติหน้าที่ตามมาตรา 18 วรรคสอง โดยมิชอบหรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 23 พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนในกรณีตามมาตรา 18 วรรคสอง ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มาตามมาตรา 18 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา 24 ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนได้มาตามมาตรา 18 และเปิดเผยข้อมูลนั้นต่อ

ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 25 ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้หรือที่พนักงานสอบสวนได้มาตามมาตรา 18 วรรคสอง ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบ ประการอื่น”

มาตรา 17 ให้ยกเลิกความในวรรคหนึ่งของมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน

“มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้”

มาตรา 18 ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา 28 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

“ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ อาจได้รับค่าตอบแทนพิเศษตามที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

ในการกำหนดให้ได้รับค่าตอบแทนพิเศษต้องคำนึงถึงภาระหน้าที่ ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่หรือมีการสูญเสียผู้ปฏิบัติงานออกจากระบบราชการเป็นจำนวนมาก คุณภาพของงาน และการดำรงตนอยู่ในความยุติธรรมโดยเปรียบเทียบค่าตอบแทนของผู้ปฏิบัติงานอื่น ในกระบวนการยุติธรรมด้วย”

มาตรา 19 ให้เพิ่มความต่อไปนี้เป็นมาตรา 31 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

“มาตรา 31 ค่าใช้จ่ายในเรื่องดังต่อไปนี้ รวมทั้งวิธีการเบิกจ่ายให้เป็นไปตามระเบียบที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

(1) การสืบสวน การแสวงหาข้อมูล และรวบรวมพยานหลักฐานในคดีความผิดตามพระราชบัญญัตินี้

(2) การดำเนินการตามมาตรา 18 วรรคหนึ่ง (4) (5) (6) (7) และ (8) และมาตรา 20

(3) การดำเนินการอื่นใดอันจำเป็นแก่การป้องกันและปราบปรามการกระทำความผิดตามพระราชบัญญัตินี้”

มาตรา 20 บรรดาระเบียบหรือประกาศที่ออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ยังคงใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติแห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ จนกว่าจะมีระเบียบหรือประกาศที่ต้องออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ ใช้บังคับ

การดำเนินการออกระเบียบหรือประกาศตามวรรคหนึ่ง ให้ดำเนินการให้แล้วเสร็จภายในหกสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

มาตรา 21 ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 (“สำนักงานคณะกรรมการกฤษฎีกา”,ออนไลน์, 2562)

ในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ เนื่องจากในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญต่อการดำเนินการของทั้งภาครัฐและภาคเอกชน โดยมีการทำธุรกรรมทางอิเล็กทรอนิกส์กันอย่างแพร่หลาย จึงสมควรส่งเสริมให้มีการบริหารจัดการและรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้มีการยอมรับและเชื่อมั่นในข้อมูลอิเล็กทรอนิกส์มากยิ่งขึ้น ประกอบกับมาตรา 25 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 บัญญัติให้ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกาแล้ว ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้ มีรายละเอียดดังนี้

มาตรา 3 ในพระราชกฤษฎีกานี้

“วิธีการแบบปลอดภัย” หมายความว่า วิธีการแบบปลอดภัยในการทำ ธุรกรรมทางอิเล็กทรอนิกส์

“ทรัพย์สินสารสนเทศ” หมายความว่า

(1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(2) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

“ความมั่นคงปลอดภัยของระบบสารสนเทศ” (information security) หมายความว่า การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

“ความมั่นคงปลอดภัยด้านบริหารจัดการ” (administrative security) หมายความว่า การกระทำในระดับบริหารโดยการจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ เพื่อนำมาใช้ในกระบวนการคัดเลือก การพัฒนา การนำไปใช้ หรือการบำรุงรักษาทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัย

“ความมั่นคงปลอดภัยด้านกายภาพ” (physical security) หมายความว่า การจัดให้มีนโยบายมาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

“การรักษาความลับ” (confidentiality) หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

“การรักษาความครบถ้วน” (integrity) หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอนหรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

“การรักษาสภาพพร้อมใช้งาน” (availability) หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

“โครงสร้างพื้นฐานสำคัญของประเทศ” (critical infrastructure) หมายความว่า บรรดาหน่วยงานหรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กร ซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้น มีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน

มาตรา 4 วิธีการแบบปลอดภัยมีสามระดับ ดังต่อไปนี้

(1) ระดับเคร่งครัด

(2) ระดับกลาง

(3) ระดับพื้นฐาน

มาตรา 5 วิธีการแบบปลอดภัยตามมาตรา 4 ให้ใช้สำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ดังต่อไปนี้

(1) ธุรกรรมทางอิเล็กทรอนิกส์ซึ่งมีผลกระทบต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน

(2) ธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ

มาตรา 6 ให้คณะกรรมการประกาศกำหนดประเภทของธุรกรรมทางอิเล็กทรอนิกส์หรือหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามมาตรา 5 (1) ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน แล้วแต่กรณีทั้งนี้ โดยให้คำนึงถึงระดับความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ผลกระทบต่อมูลค่าและความเสียหายที่ผู้ใช้บริการอาจได้รับ รวมทั้งผลกระทบต่อเศรษฐกิจและสังคมของประเทศ

ให้คณะกรรมการประกาศกำหนดรายชื่อหรือประเภทของหน่วยงานหรือ องค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศตามมาตรา 5 (2) ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน แล้วแต่กรณี

มาตรา 7 วิธีการแบบปลอดภัยตามมาตรา 4 ในแต่ละระดับ ให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด โดยมาตรฐานดังกล่าวสำหรับวิธีการแบบปลอดภัยในแต่ละระดับนั้น อาจมีการกำหนดหลักเกณฑ์ที่แตกต่างกันตามความจำเป็น แต่อย่างน้อยต้องมีการกำหนดเกี่ยวกับหลักเกณฑ์ ดังต่อไปนี้

(1) การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

(2) การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

(3) การบริหารจัดการทรัพย์สินสารสนเทศ

(4) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

(5) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

(6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(7) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

(8) การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(9) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

(10) การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

(11) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

มาตรา 8 เพื่อประโยชน์ในการเป็นแนวทางสำหรับการจัดทำนโยบายหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานหรือองค์กร คณะกรรมการอาจระบุหรือแสดงตัวอย่างมาตรฐานทางเทคโนโลยีซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเป็นมาตรฐานทางเทคโนโลยีที่เชื่อถือได้ไว้ในประกาศตามมาตรา 7 ด้วยก็ได้

มาตรา 9 ธุรกรรมทางอิเล็กทรอนิกส์ใดได้กระทำโดยวิธีการที่มีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในระดับที่เทียบเท่าหรือไม่ต่ำกว่ามาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศตามประกาศตามมาตรา 7 ซึ่งได้กำหนดไว้สำหรับระดับของวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์นั้น ให้ถือว่าธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวได้กระทำตามวิธีการที่เชื่อถือได้ตามมาตรา 25 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา 10 ในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้ผู้กระทำต้องคำนึงถึงหลักการพื้นฐานของการรักษาความลับ การรักษาความครบถ้วน และการรักษาสภาพพร้อมใช้งาน รวมทั้งต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานหรือองค์กรนั้นด้วย

มาตรา 11 ในกรณีที่คณะกรรมการเห็นว่าหน่วยงานหรือองค์กรใด หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กรใด มีการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโดยสอดคล้องกับวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้ คณะกรรมการอาจประกาศเผยแพร่รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้นเพื่อให้สาธารณชนทราบเป็นการทั่วไปก็ได้

มาตรา 12 ให้คณะกรรมการพิจารณาทบทวนหลักเกณฑ์เกี่ยวกับวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้และประกาศที่ออกตามพระราชกฤษฎีกานี้ รวมทั้งกฎหมายอื่นที่เกี่ยวข้องอย่างน้อยทุกรอบระยะเวลาสองปีนับแต่วันที่พระราชกฤษฎีกานี้ใช้บังคับ ทั้งนี้ โดยพิจารณาถึงความเหมาะสมและความสอดคล้องกับเทคโนโลยีที่ได้มีการพัฒนาหรือเปลี่ยนแปลงไป และจัดทำเป็นรายงานเสนอต่อคณะรัฐมนตรีเพื่อทราบต่อไป

มาตรา 13 ให้นายกรัฐมนตรีรักษาการตามพระราชกฤษฎีกานี้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 (“สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ”,ออนไลน์, 2562)

ประกาศฉบับนี้เพื่อช่วยในการแก้ปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทำให้ผู้ประกอบการ ตลอดจนองค์กร ภาครัฐ และภาคเอกชนที่มีการดำเนินงานใด ๆ ในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ขาดความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกรูปแบบ ประกอบกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ตระหนักถึงความจำเป็นที่จะส่งเสริมและผลักดันให้ประเทศสามารถยกระดับการแข่งขันกับประเทศอื่น ๆ โดยการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลายจึงเห็นความสำคัญที่จะนำกฎหมาย ข้อบังคับต่าง ๆ มาบังคับใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งในส่วนที่ต้องกระทำและในส่วนที่ต้องงดเว้นการกระทำ เพื่อช่วยให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

อาศัยอำนาจตามความในมาตรา 5 มาตรา 7 และมาตรา 8 แห่งพระราชกฤษฎีกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศฉบับนี้ เพื่อเป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งอย่างน้อยต้องประกอบด้วยสาระสำคัญ ดังต่อไปนี้

ข้อ 1 ในประกาศนี้

(1) ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

(2) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(3) สินทรัพย์ (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

(4) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(5) ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

(6) เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่ากรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(7) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึง

ประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ 2 หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(2) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำ เนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ 3 หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

(1) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(2) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(3) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

(4) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ข้อ 4 ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ 5 - 15

ข้อ 5 ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(2) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ

(3) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ 6 ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ 7 ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness

training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(2) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(3) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(4) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ 8 ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(2) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(3) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(4) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544

ข้อ 9 ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(2) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

(3) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(4) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(5) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(6) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(7) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ 10 ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(2) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(3) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(4) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(5) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(6) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศ หรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ 11 ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

(1) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(2) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

(3) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(4) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ 12 หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ตามแนวทางต่อไปนี้

(1) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(2) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(3) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(4) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(5) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ข้อ 13 หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(1) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ 1 ครั้ง

(2) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัย

สารสนเทศของหน่วยงาน

ข้อ 14 หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ 15 หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่า ข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

(“สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ”,ออนไลน์, 2562)

ประกาศฉบับนี้เพื่อให้หน่วยงานที่มีการเก็บรวบรวมข้อมูลส่วนบุคคล จัดเก็บ ใช้หรือเผยแพร่ในรูปของข้อมูลอิเล็กทรอนิกส์ เป็นสิทธิมนุษยชนขั้นพื้นฐานที่ได้รับความคุ้มครอง ซึ่งปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย และเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัย ความน่าเชื่อถือ และมีการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการธุรกรรมทางเล็กทรอนิกส์เห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐให้มีมาตรฐานเดียวกัน

อาศัยอำนาจตามความในมาตรา 6 มาตรา 7 และมาตรา 8 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศฉบับนี้ เพื่อเป็นแนวทางเบื้องต้น ให้หน่วยงานของรัฐใช้ในการกำหนดนโยบายและข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสำหรับการทำธุรกรรมทางเล็กทรอนิกส์ดังต่อไปนี้

ข้อ 1 ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยให้มีสาระสำคัญอย่างน้อย ดังนี้

(1) การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

การจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้มีขอบเขตจำกัด และใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม และให้เจ้าของข้อมูลทราบหรือได้รับความยินยอมจากเจ้าของข้อมูลตามแต่กรณี

(2) คุณภาพของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานของรัฐตามกฎหมาย

(3) การระบุวัตถุประสงค์ในการเก็บรวบรวม

ให้บันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลในขณะที่มีการรวบรวมและจัดเก็บ รวมถึงการนำข้อมูลนั้นไปใช้ในภายหลัง และหากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลให้จัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน

(4) ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดซึ่งข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ของการรวบรวมและจัดเก็บข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นกรณีที่มีกฎหมายกำหนดให้กระทำได้

(5) การรักษาความมั่นคงปลอดภัย

ให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ

(6) การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล ให้มีการเปิดเผยการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคลและจัดให้มีวิธีการที่สามารถตรวจดูความมีอยู่ ลักษณะของข้อมูลส่วนบุคคลวัตถุประสงค์ของการนำข้อมูลไปใช้ ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล

(7) การมีส่วนร่วมของเจ้าของข้อมูล

ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งถึงความมีอยู่ หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเมื่อได้รับคำร้องขอภายในระยะเวลาอันสมควรตามวิธีการในรูปแบบ รวมถึงค่าใช้จ่าย (ถ้ามี) ตามสมควรห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธที่จะให้คำชี้แจงหรือให้ข้อมูลแก่เจ้าของข้อมูลผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ ตามกฎหมายให้ผู้ควบคุมข้อมูลจัดทำบันทึกคำคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใด ๆเกี่ยวกับข้อมูลของเจ้าของข้อมูลไว้เป็นหลักฐาน

(8) ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

ให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามมาตรการที่กำหนดไว้ข้างต้นเพื่อให้การเนินงานตามแนวนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานของประกาศฉบับนี้

ข้อ 2 ให้หน่วยงานของรัฐจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการและให้มีรายการอย่างน้อย ดังนี้

(1) ข้อมูลเบื้องต้น ประกอบด้วย

(ก) ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด

(ข) รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานของรัฐรวบรวม จัดเก็บ หรือการใช้ตามวัตถุประสงค์

(ค) ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบและขอความยินยอมก่อนทุกครั้งตามวิธีการและภายในกำหนดเวลาที่ประกาศ เช่น การแจ้งล่วงหน้าให้เจ้าของข้อมูลทราบก่อน 15 วัน โดยการส่งทางจดหมายอิเล็กทรอนิกส์หรือประกาศไว้ในหน้าแรกของเว็บไซต์ เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่น

การขอความยินยอมจากเจ้าของข้อมูลนั้น ให้มีความชัดเจนว่าหน่วยงานของรัฐขอรับ

ความยินยอมเพื่อวัตถุประสงค์ใด

(2) การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐที่ทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์หรือผ่านรูปแบบของการกรอกข้อความทางกระดาษแล้วนำมาแปลงข้อความเข้าระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่น ให้แสดงรายละเอียดของการรวบรวมข้อมูลเป็นชนิด ประเภทรวมถึงข้อมูลที่จะไม่จัดเก็บ และข้อมูลที่รวบรวมและจัดเก็บนั้นจะนำไปใช้ตามวัตถุประสงค์ใดโดยลักษณะหรือด้วยวิธีการที่ทำให้เจ้าของข้อมูลได้ทราบ ทั้งนี้ การรวบรวมและจัดเก็บข้อมูลนั้นให้ทำเป็นประกาศหรือแจ้งรายละเอียดให้เจ้าของข้อมูลทราบ

ให้หน่วยงานของรัฐที่จัดบริการผ่านทางเว็บไซต์ แสดงรายละเอียดของการรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานนั้น รวมถึงการใช้ข้อมูลซึ่งอย่างน้อยต้องระบุว่าอยู่ในส่วนใดของเว็บไซต์หรือในเว็บเพจใดที่มีการรวบรวมและจัดเก็บข้อมูล และให้มีรายละเอียดอย่างแจ้งชัดถึงวิธีการในการรวบรวมและจัดเก็บข้อมูล เช่น การจัดเก็บโดยให้มีการลงทะเบียน หรือการกรอกแบบสอบถามเป็นต้นให้หน่วยงานของรัฐรวบรวม จัดเก็บและใช้ข้อมูลส่วนบุคคลจัดทำรายละเอียด ดังต่อไปนี้

(ก) การติดต่อระหว่างหน่วยงานของรัฐ ให้หน่วยงานของรัฐซึ่งจะติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์บอกกล่าวให้ผู้ใช้บริการทราบล่วงหน้า ทั้งนี้ ผู้ใช้บริการอาจแจ้งความประสงค์ให้ติดต่อโดยวิธีการอื่นได้

(ข) การใช้คุกกี้ (Cookies) ให้หน่วยงานของรัฐระบุบนเว็บไซต์สำหรับการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคลว่าผู้ใช้บริการจะใช้คุกกี้เพื่อวัตถุประสงค์และประโยชน์ใด และให้สิทธิที่จะไม่รับการต่อเชื่อมคุกกี้ได้

(ค) การเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information) ให้หน่วยงานของรัฐมีเว็บไซต์สำหรับการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากรเช่น เพศ อายุ อาชีพที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ ระบุถึงวิธีการรวบรวมและจัดเก็บข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลด้วย และให้ชี้แจงวัตถุประสงค์ของการใช้ข้อมูลดังกล่าว รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย

(ง) บันทึกผู้เข้าชมเว็บ (Log Files) ให้หน่วยงานของรัฐซึ่งจัดบริการเว็บไซต์ที่มีการเก็บบันทึกการเข้าออกโดยอัตโนมัติเช่น หมายเลขไอพี (IP Address) เว็บไซต์ที่เข้าออกก่อนและหลังและประเภทของโปรแกรมบราวเซอร์ (Browser) ที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลซึ่งระบุตัวบุคคลได้ ระบุวิธีการรวบรวมและจัดเก็บข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล และให้ชี้แจงวัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย

(จ) ให้หน่วยงานของรัฐระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูล ที่ประชาชนมีสิทธิเลือกว่า “จะให้หรือไม่ให้” ก็ได้ และให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่นในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์

(3) การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น

การเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานของรัฐและเว็บไซต์ดังกล่าวที่มีการเชื่อมโยงให้ข้อมูลแก่หน่วยงานหรือองค์กรอื่น ให้หน่วยงานของรัฐแสดงไว้อย่างชัดเจนถึงชื่อผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ หรือชื่อผู้มีสิทธิในข้อมูลที่ได้มีการเก็บรวบรวม (Data Subject)และชื่อ

เป็นผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวทั้งหมด รวมถึงประเภทของข้อมูลที่จะใช้ร่วมกับหน่วยงานหรือองค์กรนั้น ๆ ตลอดจนชื่อผู้มีหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ผู้ใช้บริการทราบ

ให้หน่วยงานของรัฐแจ้งให้ผู้ใช้บริการทราบและให้ความยินยอมล่วงหน้าก่อนทำการเปลี่ยนแปลงการเชื่อมโยงข้อมูลตามวรรคแรกกับหน่วยงานหรือองค์กรอื่น

(4) การรวมข้อมูลจากที่มาหลาย ๆ แห่งให้หน่วยงานของรัฐที่ซึ่งได้รับข้อมูลมาจากผู้ใช้บริการเว็บไซต์ และจะนำไปรวมเข้ากับข้อมูลของบุคคลดังกล่าวที่ได้รับจากที่มาแห่งอื่น ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลถึงเจตนารมณ์การรวมข้อมูลดังกล่าวด้วย เช่น เว็บไซต์ได้รับข้อมูลที่เป็นชื่อและที่อยู่ของการส่งจดหมายอิเล็กทรอนิกส์จากผู้ใช้บริการโดยการกรอกข้อมูลตามแบบสอบถามผ่านทางเว็บไซต์ และจะนำข้อมูลดังกล่าวไปรวมเข้ากับข้อมูลเกี่ยวกับประวัติของผู้ใช้บริการที่ได้รับจากที่มาแห่งอื่น

(5) การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลด้วยว่ามีบุคคลอื่นที่จะเข้าถึงหรือใช้ข้อมูลที่หน่วยงานนั้นได้เก็บรวบรวมมาผ่านทางเว็บไซต์ด้วย และให้ระบุไว้ด้วยว่าการให้เข้าถึง ใช้ หรือเปิดเผยข้อมูลดังกล่าวสอดคล้องกับข้อกำหนดตามกฎหมายของหน่วยงานของรัฐที่ดำเนินการดังกล่าว

(6) การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่ประสงค์จะนำไปดำเนินการอื่นนอกเหนือไปจากวัตถุประสงค์ของการรวบรวมข้อมูลส่วนบุคคลตามที่ได้ระบุไว้ เช่น การรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลที่ไม่จำเป็น หรือการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลอื่นระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลถึงสิทธิของผู้ใช้บริการที่จะเลือกว่าจะให้หน่วยงานของรัฐรวบรวม จัดเก็บหรือไม่ให้จัดเก็บ ใช้หรือไม่ให้ใช้ และเปิดเผยหรือไม่เปิดเผยข้อมูลดังกล่าว

การให้ผู้ใช้บริการใช้สิทธิเลือกตามวรรคแรกให้รวมถึงการให้สิทธิเลือกแบบที่หน่วยงานของรัฐจะต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลนั้นก่อน และการให้สิทธิเลือกแบบที่ให้สิทธิแก่ผู้ใช้บริการในการปฏิเสธไม่ให้มีการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวข้างต้นแล้วเท่านั้น ทั้งนี้ การให้สิทธิเลือกต้องกระทำให้สมบูรณ์ก่อนที่เว็บไซต์จะทำการติดต่อกับผู้ใช้บริการในครั้งแรกและหากเป็นการใช้สิทธิเลือกแบบห้ามไม่ให้มีการใช้ข้อมูลส่วนบุคคลแตกต่างไปจากวัตถุประสงค์เดิมหน่วยงานเจ้าของเว็บไซต์ต้องระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ใช้บริการได้รับทราบถึงวิธีการของการส่งการติดต่อครั้งที่สองของเว็บไซต์ด้วย

(7) การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบันให้หน่วยงานของรัฐกำหนดวิธีการที่ผู้ใช้บริการเว็บไซต์สามารถเข้าถึงและแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลเกี่ยวกับตนเองที่หน่วยงานของรัฐรวบรวมและจัดเก็บไว้ในเว็บไซต์ให้ถูกต้อง

(8) การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางจัดให้มีวิธีการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้ให้เหมาะสมกับการรักษาความลับของข้อมูลส่วนบุคคล เพื่อป้องกันการเปลี่ยนแปลง

แก้ไขข้อมูลดังกล่าวโดยมิชอบ รวมถึงการป้องกันการกระทำใดที่จะมีผลทำให้ข้อมูลไม่อยู่ในสภาพพร้อมใช้งาน ซึ่งหน่วยงานของรัฐพึงดำเนินการ ดังนี้

(ก) สร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ

(ข) กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงาน หรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด

(ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง

(ง) กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึกความเชื่อความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐหรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคลเชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น

(จ) ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม

(9) การติดต่อกับเว็บไซต์

เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับหน่วยงานของรัฐ ต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย ข้อมูลติดต่อที่หน่วยงานของรัฐควรจะระบุเอาไว้ อย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้

(ก) ชื่อและที่อยู่

(ข) หมายเลขโทรศัพท์

(ค) หมายเลขโทรสาร

(ง) ที่อยู่จดหมายอิเล็กทรอนิกส์

ข้อ 3 ให้หน่วยงานของรัฐจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภายใต้หลักการตามข้อ 1 และข้อ 2 สำหรับหน่วยงานของรัฐที่ได้รับทรัสต์มาร์คจากหน่วยงานหรือองค์กรอื่นที่ทำหน้าที่ออกทรัสต์มาร์ค (Trust Mark) ให้หน่วยงานของรัฐนั้นแสดงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากหน่วยงานหรือองค์กรที่ออกหรือรับรองทรัสต์มาร์คดังกล่าวต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วย

ทรัสต์มาร์ค (Trust Mark) ตามความในวรรคแรกหมายถึง เครื่องหมายที่รับรองว่าหน่วยงานดังกล่าวมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในการทำธุรกรรมทางอิเล็กทรอนิกส์

ซึ่งออกโดยหน่วยงานหรือองค์กรที่จัดตั้งโดยชอบด้วยกฎหมายเพื่อทำหน้าที่ในการตรวจสอบและรับรองการออกทรัสต์มาร์คให้กับผู้ขอรับการรับรอง

ข้อ 4 ให้หน่วยงานของรัฐกำหนดชื่อเรียกนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ให้ชัดเจน และในกรณีที่มีการปรับปรุงนโยบาย ให้ระบุวัน เวลา และปี ซึ่งจะมีการปรับปรุงหรือเปลี่ยนแปลงนโยบายดังกล่าวไว้ด้วย

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556

(“สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ”,ออนไลน์, 2562)

ประกาศฉบับนี้ ว่าด้วยการปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐให้สอดคล้องกับมาตรฐานสากล อาศัยอำนาจตามความในมาตรา 5 มาตรา 7 และมาตรา 8 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2549 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556”

ข้อ 2 ให้ยกเลิกความในข้อ 14 ของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และให้ใช้ความต่อไปนี้แทน

“ข้อ 14 หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น”

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

(“สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ”,ออนไลน์, 2562)

ประกาศฉบับนี้ คือ ประกาศกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่คณะกรรมการกำหนดเป็นวิธีการที่เชื่อถือได้ ออกประกาศไว้ ดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐาน
การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555”

ข้อ 2 ในกรณีที่จะต้องปฏิบัติให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐานให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่กำหนดในแนบท้ายประกาศฉบับนี้

บัญชีแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

(“สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ”,ออนไลน์, 2562)

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นมาตรการสำหรับใช้ในการควบคุมให้ระบบสารสนเทศมีความมั่นคงปลอดภัย ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและสารสนเทศในระบบ นั้น โดยการทำธุรกรรมทางอิเล็กทรอนิกส์ด้วยระบบสารสนเทศ ต้องดำเนินการตามมาตรการที่เกี่ยวข้องตามบัญชีแนบ ท้ายนี้ และต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน ทั้งนี้ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ แบ่งออกเป็น 11 ข้อ ได้แก่

1. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ
2. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร
3. การบริหารจัดการทรัพย์สินสารสนเทศ
4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
5. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
7. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
8. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
9. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

10.การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

11.การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

1. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานต้องปฏิบัติ ดังนี้

ข้อ 1. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการหน่วยงานต้องกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติและผลักดันโดยผู้บริหารระดับสูง และมีการประกาศนโยบายดังกล่าวให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน

ข้อ 2. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

2.1 ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

2.2 สำหรับระบบสารสนเทศใหม่ มีการกำหนดขั้นตอนการพิจารณาทบทวนเพื่ออนุมัติการสร้างการติดตั้ง หรือการใช้งานในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบหรือความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่

2.3 มีการกำหนดสัญญาการรักษาข้อมูลที่เป็นความลับ (Confidentiality agreement หรือ Non-Disclosure agreement) ที่สอดคล้องกับสถานการณ์และความต้องการของหน่วยงานในการปกป้องข้อมูลสารสนเทศ

2.4 มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน

2.5 สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศ ควรมีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศระบุไว้ในข้อตกลง

ข้อ 3. การบริหารจัดการทรัพย์สินสารสนเทศมีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง

ข้อ 4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

4.1 กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน หรือหน่วยงานหรือบุคคลภายนอกที่ว่าจ้าง โดยให้สอดคล้องกับความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่หน่วยงานประกาศใช้

4.2 ผู้บริหารระดับสูงของหน่วยงานต้องกำหนดให้พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้างปฏิบัติงานตามนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่หน่วยงานประกาศใช้

4.3 กำหนดให้มีขั้นตอนการลงโทษพนักงานที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในหน่วยงาน

4.4 กำหนดหน้าที่ความรับผิดชอบในการยุติการจ้าง หรือการเปลี่ยนแปลงสถานะการจ้างให้ชัดเจน และมอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน

4.5 พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงานเมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับหน่วยงาน

4.6 ให้ยกเลิกสิทธิของพนักงาน หน่วยงานหรือบุคคลภายนอกในการเข้าใช้งานระบบสารสนเทศ เมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน และให้ปรับเปลี่ยนระดับสิทธิในการเข้าใช้งานระบบสารสนเทศให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น

ข้อ 5. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

5.1 ให้มีการป้องกันขอบเขตพื้นที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้ง จัดเก็บ หรือใช้งาน ระบบสารสนเทศและข้อมูลสารสนเทศ

5.2 มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพเพื่อป้องกันภัยจากภายนอกภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

5.3 จัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่าง ๆ และเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

5.4 มีการป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting utilities)

5.5 มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธี เพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

ข้อ 6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

6.1 มีการจัดทำ ปรับปรุง และดูแลเอกสารขั้นตอนการปฏิบัติงานที่อยู่ในสภาพพร้อมใช้งาน เพื่อให้พนักงานสามารถนำไปปฏิบัติได้

6.2 มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่างจ้างปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

6.3 มีการติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ

6.4 จัดให้มีเกณฑ์การตรวจรับระบบสารสนเทศที่มีการปรับปรุง หรือที่มีเวอร์ชั่นใหม่ และควรมีการทดสอบระบบสารสนเทศทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับ

6.5 มีขั้นตอนควบคุมการตรวจสอบ ป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์ และให้มีการสร้างความตระหนักรู้ให้กับผู้ใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศเกี่ยวกับโปรแกรมไม่พึงประสงค์

6.6 มีการสำรองข้อมูลสารสนเทศ และทดสอบการนำกลับมาใช้งาน โดยให้เป็นไปตามนโยบายการสำรองข้อมูลที่หน่วยงานประกาศใช้

6.7 มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่ายดังกล่าว

6.8 มีการกำหนดรูปแบบการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดการบริหารจัดการในข้อตกลงการให้บริการด้านเครือข่ายคอมพิวเตอร์ ไม่ว่าเป็นการให้บริการโดยหน่วยงานเอง หรือจ้างช่วงไปยังผู้ให้บริการภายนอก

6.9 จัดให้มีนโยบายและขั้นตอนปฏิบัติงาน รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์

6.10 จัดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือหน่วยงานภายนอก

6.11 จัดให้มีนโยบายและขั้นตอนการปฏิบัติงาน เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนผ่านระบบสารสนเทศที่มีการเชื่อมต่อกับระบบสารสนเทศต่าง ๆ

6.12 มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำ พาณิชย์อิเล็กทรอนิกส์(Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกงละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต

6.13 มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูลหรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต

6.14 สำหรับข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

6.15 มีการเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวน ในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง

6.16 มีขั้นตอนการเฝ้าติดตามสังเกตการใช้งานระบบสารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ

6.17 มีการป้องกันระบบสารสนเทศที่จัดเก็บ Log และข้อมูล Log เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต

6.18 มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศโดยผู้ดูแลระบบ (System administrator หรือ System operator)

ข้อ 7. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

7.1 จัดให้มีนโยบายควบคุมการเข้าถึง โดยจัดทำเป็นเอกสาร และมีการติดตามทบทวนให้นโยบายดังกล่าวสอดคล้องกับข้อกำหนดหรือความต้องการด้านการดำเนินงานหรือการให้บริการ และด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

7.2 จัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้อย่างเป็นทางการเพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าใช้งานระบบสารสนเทศใด ๆ ของหน่วยงาน

7.3 การกำหนดสิทธิในการเข้าถึงระดับสูง ให้ทำอย่างจำกัดและอยู่ภายใต้การควบคุม

7.4 ผู้ใช้งานต้องดูแลป้องกันอุปกรณ์สารสนเทศใดที่อยู่ภายใต้ความดูแลรับผิดชอบในระหว่างที่ไม่มีการใช้งาน

7.5 จำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึง และข้อกำหนดการใช้งานแอพพลิเคชั่นเพื่อการดำเนินงาน

7.6 ให้ผู้ใช้งานทุกคนมีบัญชีผู้ใช้งานเป็นของตนเอง และให้ระบบสารสนเทศมีเทคนิคการตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้เข้าใช้งานระบบสารสนเทศได้

7.7 ให้ยุติหรือปิดหน้าจอการใช้งานระบบสารสนเทศโดยอัตโนมัติ หากไม่มีการใช้งานเกินระยะเวลาสูงสุดที่กำหนดไว้

7.8 จำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในแอพพลิเคชั่นของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับนโยบายการเข้าถึงที่ได้กำหนดไว้

7.9 กำหนดนโยบายและแนวทางการจัดการด้านความมั่นคงปลอดภัย เพื่อลดความเสี่ยงในการใช้งานอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้ เช่น แล็ปท็อปคอมพิวเตอร์ (Laptop Computer) หรือสมาร์ทโฟน (Smartphone) เป็นต้น

ข้อ 8. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

8.1 ในการจัดทำข้อกำหนดขั้นต่ำของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศไว้ด้วย

8.2 ให้ดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์

ข้อ 9. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดผ่าน ช่องทางการบริหารจัดการที่เหมาะสมโดยเร็วที่สุด

ข้อ 10. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง ให้กำหนดแผนเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ หลังเกิดเหตุการณ์ที่ทำให้ การดำเนินงานหยุดชะงัก เพื่อให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานตามระดับที่กำหนดไว้ ภายในระยะเวลาที่กำหนดไว้

ข้อ 11. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

11.1 ให้มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องตามกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน โดยต้องจัดทำเป็นเอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

11.2 ป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์

11.3 พนักงานของหน่วยงานต้องดูแลให้งานที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่อยู่ในขอบเขตความรับผิดชอบได้ดำเนินการไปโดยสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

2. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน และต้องปฏิบัติเพิ่มเติม ดังนี้

ข้อ 1. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ หน่วยงานต้องวางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ เพื่อปรับปรุงหากมีการเปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้ เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน และคงความมีประสิทธิผลอยู่เสมอ

ข้อ 2. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

2.1 มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน

2.2 มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

2.3 จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้ การพิจารณาทบทวนดังกล่าว ควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน

ข้อ 3. การบริหารจัดการทรัพย์สินสารสนเทศ

3.1 มีการกำหนดบุคคลผู้มีหน้าที่ดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศไว้ชัดเจน

3.2 มีการกำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศไว้อย่างชัดเจน โดยจัดทำเป็นเอกสาร และมีการประกาศใช้ในหน่วยงาน

3.3 มีการจำแนกประเภทของข้อมูลสารสนเทศ โดยจำแนกตามมูลค่าของข้อมูล ข้อกำหนดทางกฎหมายระดับชั้นความลับและความสำคัญต่อหน่วยงาน

3.4 มีการกำหนดและประกาศใช้ขั้นตอนที่เหมาะสมในการจำแนกประเภทของข้อมูลสารสนเทศ และจัดการข้อมูลสารสนเทศ โดยให้สอดคล้องกับแนวทางการจำแนกประเภทของข้อมูลสารสนเทศที่หน่วยงานประกาศใช้

ข้อ 4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร พนักงานหน่วยงานหรือบุคคลภายนอกต้องได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน และได้รับการสื่อสารให้ทราบถึงนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง

ข้อ 5. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

5.1 มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่หรือสถานที่ปฏิบัติงาน หรืออุปกรณ์สารสนเทศต่าง ๆ

5.2 ไม่ควรนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของหน่วยงานหากมิได้รับอนุญาต

ข้อ 6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

6.1 มีการจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ

6.2 มีการติดตามผลการใช้งานทรัพยากรสารสนเทศ และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม

6.3 มีขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บข้อมูลสารสนเทศเพื่อมิให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ผิดประเภท

6.4 มีการจัดเก็บ Log ที่เกี่ยวข้องกับข้อผิดพลาดใด ๆ ของระบบสารสนเทศ มีการวิเคราะห์ Log ดังกล่าว อย่างสม่ำเสมอ และมีการจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม

6.5 ระบบเวลาของระบบสารสนเทศต่าง ๆ ที่ใช้ในหน่วยงานหรือในขอบเขตงานด้านความมั่นคงปลอดภัย(Security domain) ต้องมีความสอดคล้องกัน (Synchronization) โดยให้มีการตั้งค่าพร้อมกับเวลาจากแหล่งเวลาที่เชื่อถือได้

ข้อ 7. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

7.1 มีข้อบังคับให้ผู้ใช้งานปฏิบัติตามขั้นตอนเพื่อการเลือกใช้รหัสผ่านอย่างมั่นคงปลอดภัยตามที่หน่วยงานกำหนด

7.2 ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น

7.3 ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล

7.4 มีการควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและการเชื่อมต่อผ่านคอมพิวเตอร์ สำหรับระบบสารสนเทศที่สามารถเข้าถึงจากระยะไกลได้ เช่น Remote diagnostic หรือ Configuration facility ของอุปกรณ์เครือข่ายคอมพิวเตอร์

7.5 มีการจัดกลุ่มตามประเภทของข้อมูลสารสนเทศที่ให้บริการ ระบบสารสนเทศ กลุ่มผู้ใช้งานโดยมีการแบ่งแยกบนเครือข่ายคอมพิวเตอร์อย่างเป็นสัดส่วน

7.6 กำหนดให้มีการควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์เพื่อไม่ให้ขัดแย้งกับนโยบายควบคุมการเข้าถึงของแอพพลิเคชั่น

7.7 กำหนดขั้นตอนการ Log-on เพื่อควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์

7.8 ให้จัดทำหรือจัดให้มีระบบการบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้งาน (Interactive) และสามารถรองรับการใช้งานรหัสผ่านที่มีความมั่นคงปลอดภัย

ข้อ 8. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

8.1 ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ ที่จะรับเข้าสู่แอพพลิเคชั่นก่อนเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม

8.2 ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของแอพพลิเคชั่น เพื่อให้มั่นใจได้ว่า ข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม

8.3 จัดให้มีแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน

8.4 ให้เลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อการทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล

8.5 ให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม

8.6 หากมีการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการคอมพิวเตอร์ ให้มีการตรวจสอบทบทวนการทำงานของโปรแกรมที่มีความสำคัญ และทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าว จะไม่ส่งผลกระทบใด ๆ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการของหน่วยงาน

ข้อ 9. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

9.1 จัดให้มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน

9.2 กำหนดให้มีกรอบงานหลักสำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน เพื่อให้การพัฒนาแผนต่าง ๆ เป็นไปในทิศทางเดียวกัน รวมทั้งสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย ตลอดจนมีการจัดลำดับความสำคัญก่อนหลังในการทดสอบและการดูแล

9.3 ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ

ข้อ 10. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

10.1 จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

10.2 ใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

10.3 ให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอเพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ

10.4 วางแผนและจัดให้มีข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ

10.5 ป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise)

3. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานและระดับกลาง และต้องปฏิบัติเพิ่มเติม ดังนี้

ข้อ 1. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

1.1 มีการสร้างความร่วมมือระหว่างผู้ที่มีบทบาทเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ในงานหรือกิจกรรมใด ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

1.2 มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

1.3 ก่อนที่จะอนุญาตให้หน่วยงานหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของหน่วยงาน ให้มีการระบุความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนการอนุญาต

ข้อ 2. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

2.1 ในการพิจารณารับพนักงานเข้าทำงาน หรือการว่าจ้างหน่วยงานหรือบุคคลภายนอกให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึงระดับชั้นความลับของข้อมูลสารสนเทศที่จะให้เข้าถึง และระดับความเสี่ยงที่ได้ประเมิน

2.2 ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้ระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญา

ข้อ 3. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

3.1 ในพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) ต้องมีการควบคุมการเข้าออก โดยให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้

3.2 มีการออกแบบแนวทางการป้องกันทางกายภาพสำหรับการทำงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) และกำหนดให้มีการนำไปใช้งาน

3.3 มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึงอาจสามารถเข้าถึงได้ เช่น จุดรับส่งของ เป็นต้น หรือหากเป็นไปได้ให้แยกบริเวณดังกล่าวออกจากพื้นที่ที่มีการติดตั้ง จัดเก็บ หรือใช้งาน ระบบสารสนเทศและข้อมูลสารสนเทศเพื่อหลีกเลี่ยงการเข้าถึงโดยมิได้รับอนุญาต

3.4 มีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสาร หรือสายไฟ เพื่อมิให้มีการดักรับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น

3.5 มีการรักษาความมั่นคงปลอดภัยให้กับอุปกรณ์สารสนเทศที่มีการนำไปใช้งานนอกสถานที่ปฏิบัติงานของหน่วยงาน โดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานในสถานที่ต่าง ๆ

3.6 ก่อนการยกเลิกการใช้งานหรือจำหน่ายอุปกรณ์สารสนเทศที่ใช้ในการจัดเก็บข้อมูลสารสนเทศต้องมีการตรวจสอบอุปกรณ์สารสนเทศนั้นว่า ได้มีการลบ ย้าย หรือทำลาย ข้อมูลที่สำคัญหรือซอฟต์แวร์ที่จัดซื้อและติดตั้งไว้ด้วยวิธีการที่ทำให้ไม่สามารถกู้คืนได้อีก

ข้อ 4. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

4.1 มีการแบ่งแยกหน้าที่และขอบเขตความรับผิดชอบอย่างชัดเจน เพื่อลดโอกาสความผิดพลาดในการเปลี่ยนแปลงหรือใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศที่ผิดประเภท

4.2 มีการแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต

4.3 มีการบริหารจัดการการเปลี่ยนแปลงใด ๆ เกี่ยวกับการจัดเตรียมการให้บริการ และการดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง

4.4 หากหน่วยงานอนุญาตให้มีการใช้งาน Mobile code (เช่น Script บางอย่างของเว็บแอพพลิเคชั่นที่มีการทำงานอัตโนมัติเมื่อเรียกดูเว็บ) ควรมีการตั้งค่าการทำงาน (Configuration) เพื่อให้มั่นใจได้ว่าการทำงานของMobile code นั้นเป็นไปตามความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และห้ามโดยอัตโนมัติมิให้ Mobile code สามารถทำงานได้ในระบบสารสนเทศ หากในนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดห้ามมิให้ประเภทของ Mobile code ดังกล่าวทำงานได้

4.5 มีขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media)

4.6 มีขั้นตอนการปฏิบัติงานในการทำลายอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) อย่างมั่นคงปลอดภัย

4.7 มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) ถูกเข้าถึงโดยมิได้รับอนุญาต

4.8 ในกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูลสารสนเทศ ให้มีการป้องกันอุปกรณ์ที่ใช้จัดเก็บข้อมูลดังกล่าว เพื่อมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือถูกนำไปใช้งานผิดประเภท หรืออุปกรณ์หรือข้อมูลสารสนเทศได้รับความเสียหาย

4.9 ให้มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E - mail) EDI หรือ Instant messaging)

ข้อ 5. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

5.1 จัดให้มีขั้นตอนการบริหารจัดการเรื่องการกำหนดรหัสผ่านอย่างเป็นทางการ

5.2 กำหนดให้ผู้บริหารติดตามทบทวนระดับสิทธิในการเข้าถึงของผู้ใช้งานอย่างเป็นทางการเป็นประจำ

5.3 มีการกำหนดนโยบาย Clear desk สำหรับข้อมูลสารสนเทศในรูปแบบกระดาษและที่จัดเก็บในอุปกรณ์บันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ และนโยบาย Clear screen สำหรับระบบสารสนเทศ

5.4 ให้มีการระบุอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศโดยอัตโนมัติ (Automatic equipment identification) เพื่อตรวจสอบการเชื่อมต่อของอุปกรณ์ดังกล่าวว่ามาจากอุปกรณ์ดังกล่าวจริง หรือจากสถานที่ที่กำหนดไว้เท่านั้น ทั้งนี้ จำเป็นสำหรับการที่ระบบสารสนเทศจะรับการเชื่อมต่อจากเฉพาะอุปกรณ์ที่ได้รับอนุญาต หรือมาจากเฉพาะสถานที่ที่ได้รับอนุญาต

5.5 ให้จำกัดการเข้าถึงการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ อย่างเข้มงวด เนื่องจากโปรแกรมดังกล่าวอาจมีความสามารถควบคุมดูแลและเปลี่ยนแปลงการทำงานของระบบสารสนเทศได้

5.6 จำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่มีระดับความเสี่ยงสูง เพื่อเพิ่มระดับการรักษาความมั่นคงปลอดภัย

5.7 สำหรับระบบสารสนเทศที่มีความสำคัญสูง ต้องจัดให้ระบบสารสนเทศทำงานในสภาพแวดล้อมที่แยกออกมาต่างหาก โดยไม่ใช้ปะปนกับระบบสารสนเทศอื่น

5.8 กำหนดให้มีนโยบาย แผนงานและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับกิจกรรมใด ๆ ที่มีการปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

ข้อ 6. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

6.1 ให้มีการตรวจสอบ (Validate) การทำงานของแอพพลิเคชั่นเพื่อตรวจหาข้อผิดพลาดของข้อมูลที่อาจเกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด

6.2 ให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอพพลิเคชั่น รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

6.3 จัดให้มีนโยบายในการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ

6.4 กำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ

6.5 ให้มีการควบคุมการเปลี่ยนแปลงต่าง ๆ ในการพัฒนาระบบสารสนเทศ โดยมีขั้นตอนการควบคุมที่เป็นทางการ

6.7 ให้จำกัดการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software package) โดยให้เปลี่ยนแปลงเฉพาะเท่าที่จำเป็น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวด

6.8 มีมาตรการป้องกันเพื่อลดโอกาสที่เกิดการรั่วไหลของข้อมูลสารสนเทศ

ข้อ 7. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

7.1 กำหนดให้พนักงานหรือผู้ใช้งานที่เป็นบุคคลภายนอก มีการบันทึกและรายงานจุดอ่อนใด ๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศ

7.2 กำหนดขอบเขตความรับผิดชอบของผู้บริหารและขั้นตอนการปฏิบัติงาน เพื่อตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด อย่างรวดเร็ว มีระเบียบ และมีประสิทธิผล

7.3 หากในขั้นตอนการติดตามผลกับบุคคลหรือหน่วยงานภายหลังจากเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งเกี่ยวข้องกับการดำเนินการทางกฎหมาย (ไม่ว่าทางแพ่งหรือทางอาญา) ให้มีการรวบรวม จัดเก็บ และนำเสนอหลักฐาน ให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

ข้อ 8. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กร เพื่อให้มีความต่อเนื่อง ให้มีการระบุเหตุการณ์ใด ๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงัก และความเป็นไปได้ในการเกิดผลกระทบ ตลอดจนผลต่อเนื่องจากการหยุดชะงักนั้นในแง่ของความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ 9. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

9.1 กำหนดขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าในการใช้งานข้อมูลที่อาจถือเป็นทรัพย์สินทางปัญญาหรือการใช้งานซอฟต์แวร์มีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ

9.2 ป้องกันมิให้ข้อมูลสารสนเทศที่สำคัญเกิดความเสียหาย สูญหายหรือถูกปลอมแปลง โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน และข้อกำหนดการให้บริการ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559 (“สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ”,ออนไลน์, 2562)

ประกาศฉบับนี้ เป็นการประกาศรายชื่อหน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อให้ดำเนินการตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน แล้วแต่กรณี

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559”

ข้อ 2 ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามร้อยหกสิบวันนับแต่วันประกาศในราชกิจจานุเบกษา เป็นต้นไป

ข้อ 3 ให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่มีรายชื่อแนบท้ายประกาศฉบับนี้ ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางเล็กทรอนิกส์พ.ศ. 2553

แนบท้าย รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กร ส่วนราชการ

1. สำนักนายกรัฐมนตรี เฉพาะ

1.1 สำนักงานปลัดสำนักนายกรัฐมนตรี

1.2 กรมประชาสัมพันธ์

1.3 สำนักข่าวกรองแห่งชาติ

1.4 สำนักงบประมาณ

1.5 สำนักงานคณะกรรมการข้าราชการพลเรือน

1.6 สำนักงานคณะกรรมการส่งเสริมการลงทุน

2. กระทรวงกลาโหม เฉพาะ

2.1 สำนักงานปลัดกระทรวงกลาโหม

2.2 กองบัญชาการกองทัพไทย

2.3 กองทัพบก

2.4 กองทัพเรือ

2.5 กองทัพอากาศ

3. กระทรวงการคลัง เฉพาะ

3.1 กรมธนารักษ์

3.2 กรมบัญชีกลาง

3.3 กรมศุลกากร

3.4 กรมสรรพสามิต

3.5 กรมสรรพากร

3.6 สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ

3.7 สำนักงานบริหารหนี้สาธารณะ

4. กระทรวงการต่างประเทศ

5. กระทรวงเกษตรและสหกรณ์ เฉพาะ

5.1 กรมชลประทาน

5.2 กรมประมง

5.3 กรมปศุสัตว์

5.4 กรมวิชาการเกษตร

5.5 กรมส่งเสริมสหกรณ์

6. กระทรวงคมนาคม เฉพาะ

6.1 กรมเจ้าท่า

6.2 กรมการขนส่งทางบก

6.3 กรมท่าอากาศยาน

6.4 กรมทางหลวง

6.5 กรมทางหลวงชนบท

6.6 สำนักงานนโยบายและแผนการขนส่งและจราจร

7. กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม เฉพาะ

7.1 กรมควบคุมมลพิษ

8. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เฉพาะ

8.1 สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

8.2 กรมอุตุนิยมวิทยา

9. กระทรวงพลังงาน เฉพาะ

9.1 กรมเชื้อเพลิงธรรมชาติ

9.2 กรมธุรกิจพลังงาน

10.กระทรวงพาณิชย์ เฉพาะ

10.1 กรมการค้าภายใน

10.2 กรมพัฒนาธุรกิจการค้า

11.กระทรวงมหาดไทย เฉพาะ

11.1 กรมการปกครอง

11.2 กรมที่ดิน

11.3 กรมป้องกันและบรรเทาสาธารณภัย

11.4 กรมโยธาธิการและผังเมือง

12.กระทรวงยุติธรรม เฉพาะ

12.1 กรมบังคับคดี

12.2 กรมราชทัณฑ์

12.3 กรมสอบสวนคดีพิเศษ

12.4 สถาบันนิติวิทยาศาสตร์

12.5 สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด

12.6 สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

13.กระทรวงแรงงาน

13.1 กรมสวัสดิการและคุ้มครองแรงงาน

13.2 สำนักงานประกันสังคม

14.กระทรวงวิทยาศาสตร์และเทคโนโลยี เฉพาะ

14.1 สำนักงานปรมาณูเพื่อสันติ

15.กระทรวงศึกษาธิการ เฉพาะ

15.1 มหาวิทยาลัยขอนแก่น

15.2 มหาวิทยาลัยเชียงใหม่

15.3 มหาวิทยาลัยธรรมศาสตร์

15.4 มหาวิทยาลัยนเรศวร

15.5 มหาวิทยาลัยมหิดล

15.6 มหาวิทยาลัยศรีนครินทรวิโรฒ

15.7 มหาวิทยาลัยสงขลานครินทร์

16.กระทรวงสาธารณสุข เฉพาะ

16.1 สำนักงานปลัดกระทรวงสาธารณสุข

16.2 กรมการแพทย์

16.3 กรมควบคุมโรค

16.4 กรมวิทยาศาสตร์การแพทย์

16.5 กรมอนามัย

16.6 สำนักงานคณะกรรมการอาหารและยา

17.กระทรวงอุตสาหกรรม เฉพาะ

17.1 กรมโรงงานอุตสาหกรรม

17.2 สำนักงานคณะกรรมการอ้อยและน้ำตาลทราย

18.ส่วนราชการไม่สังกัดสำนักนายกรัฐมนตรี กระทรวงหรือทบวง เฉพาะ

18.1 สำนักงานตำรวจแห่งชาติ

19.องค์กรตามรัฐธรรมนูญ

19.1 สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ

19.2 สำนักงานอัยการสูงสุด

20.รัฐวิสาหกิจ

20.1 การเคหะแห่งชาติ

20.2 การทางพิเศษแห่งประเทศไทย

20.3 การท่าเรือแห่งประเทศไทย

20.4 การประปาส่วนภูมิภาค

20.5 การประปานครหลวง

20.6 การไฟฟ้านครหลวง

20.7 การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย

20.8 การไฟฟ้าส่วนภูมิภาค
20.9 การยางแห่งประเทศไทย
20.10 การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
20.11 การรถไฟแห่งประเทศไทย
20.12 ธนาคารกรุงไทย จำกัด (มหาชน)
20.13 ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย
20.14 ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
20.15 ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย
20.16 ธนาคารออมสิน
20.17 ธนาคารอาคารสงเคราะห์
20.18 ธนาคารอิสลามแห่งประเทศไทย
20.19 บรรษัทตลาดรองสินเชื่อที่อยู่อาศัย
20.20 บรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม
20.21 บริษัท กสท โทรคมนาคม จำกัด (มหาชน)
20.22 บริษัท การบินไทย จำกัด (มหาชน)
20.23 บริษัท ขนส่ง จำกัด
20.24 บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)
20.25 บริษัท ทีโอที จำกัด (มหาชน)
20.26 บริษัท ปตท จำกัด (มหาชน)
20.27 บริษัท ไปรษณีย์ไทย จำกัด
20.28 บริษัท วิทยุการบินแห่งประเทศไทย จำกัด
20.29 บริษัท อสมท จำกัด (มหาชน)
20.30 องค์การเภสัชกรรม
20.31 องค์การคลังสินค้า
20.32 องค์การจัดการน้ำเสีย
20.33 องค์การอุตสาหกรรมป่าไม้
20.34 องค์การขนส่งมวลชนกรุงเทพ
20.35 บริษัทบริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (มหาชน)

21.หน่วยงานอื่นของรัฐ

21.1 กองทุนเงินให้กู้ยืมเงินเพื่อการศึกษา
21.2 กองทุนบำเหน็จบำนาญข้าราชการ
21.3 ตลาดหลักทรัพย์แห่งประเทศไทย
21.4 ธนาคารแห่งประเทศไทย
21.5 สถาบันการแพทย์ฉุกเฉินแห่งชาติ
21.6 สภากาชาดไทย
21.7 สำนักงานคณะกรรมการกำกับกิจการพลังงาน

21.8 สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

21.9 สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

22.องค์การมหาชน

22.1 โรงพยาบาลบ้านแพ้ว (องค์การมหาชน)

22.2 สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)

22.3 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

22.4 สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

23.องค์กรปกครองส่วนท้องถิ่น

23.1 กรุงเทพมหานคร

24.หน่วยงานภาคเอกชน

24.1 บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด

24.2 บริษัท สำนักหักบัญชี (ประเทศไทย) จำกัด

24.3 บริษัท ศูนย์รับฝากหลักทรัพย์ (ประเทศไทย) จำกัด

24.4 สมาคมตลาดตราสารหนี้ไทย

ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 วันที่ 23 พฤษภาคม 2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของคอมพิวเตอร์ลูกข่ายระบบบาทเนต (“ธนาคารแห่งประเทศไทย”,ออนไลน์, 2562)

เพื่อให้ระบบบาทเนตมีมาตรฐานในการกำหนดนโยบายและมาตรการการบริหารจัดการความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001ซึ่งมุ่งเน้นด้านการรักษาและเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร และใช้เป็นแนวทางกำหนดวิธีปฏิบัติในการตรวจสอบและรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการโอนเงินผ่านระบบบาทเนตให้มีความน่าเชื่อถือมีความมั่นคงปลอดภัยและสามารถให้บริการได้อย่างต่อเนื่องเป็นไปตามมาตรฐานสากล มุ่งเน้นการรักษาความมั่นคงปลอดภัยสารสนเทศของ “คอมพิวเตอร์ลูกข่าย” ที่ใช้เชื่อมโยงกับบาทเนตของธปท.จากภัยคุกคามในรูปแบบต่างๆ เพื่อให้ผู้ใช้บริการบาทเนตถือปฏิบัติให้สอดคล้องกับข้อกำหนดตามกฎหมายในปัจจุบันและเป็นไปตามมาตรฐานสากลISO/IEC 27001 สถาบันผู้เกี่ยวข้อง

1.กรมบัญชีกลาง

2.ธนาคารพาณิชย์จดทะเบียนในประเทศ

3.บริษัทเงินทุน

4.บริษัทเงินทุนหลักทรัพย์

5.บริษัทศูนย์รับฝากหลักทรัพย์ (ประเทศไทย) จำกัด

6.บริษัทหลักทรัพย์

7.อื่น ๆ

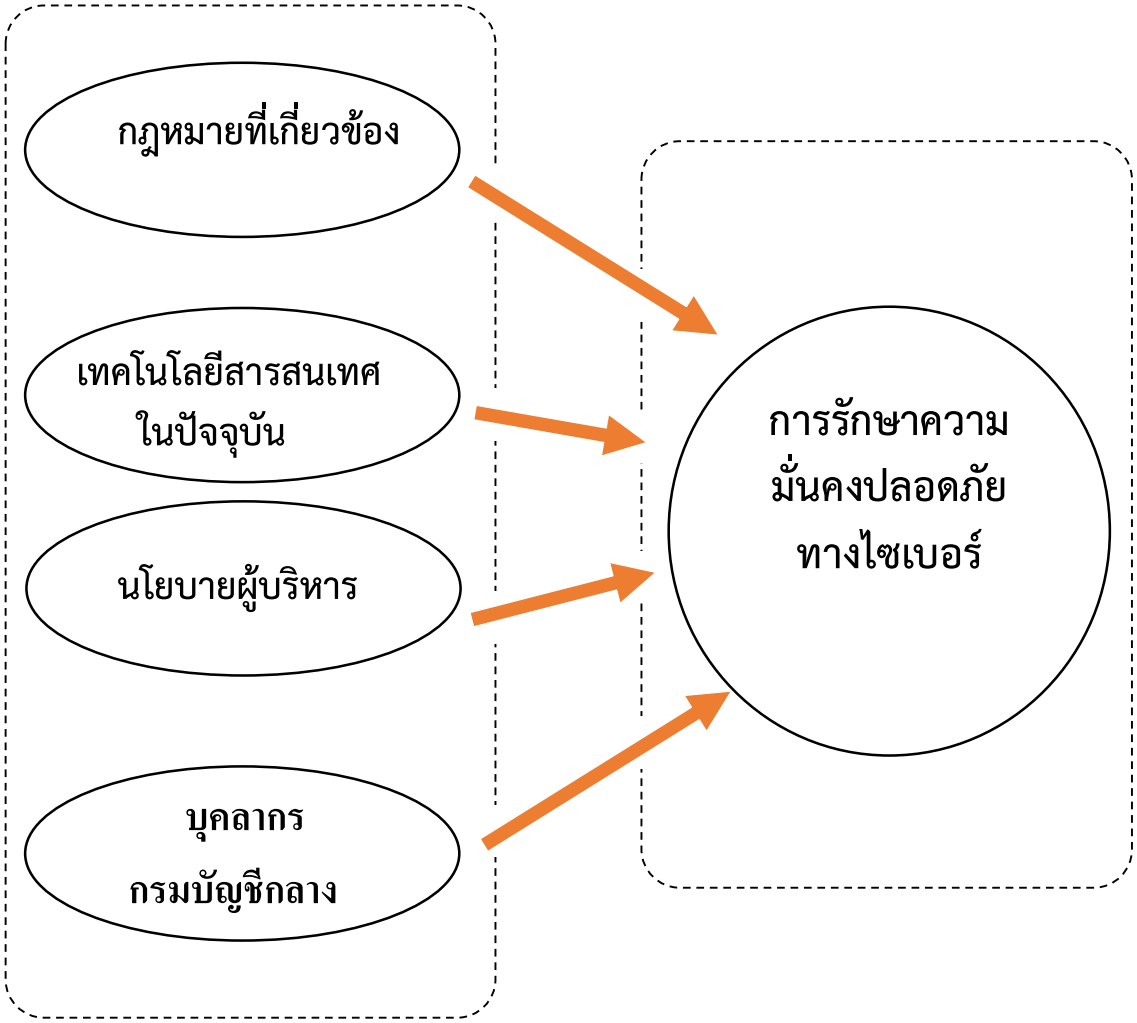
งานวิจัยที่เกี่ยวข้อง

ศิวลีย์ สิริโรจน์บริรักษ์ (ออนไลน์, 2562) ได้ศึกษาเรื่อง “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม มีวัตถุประสงค์เพื่อศึกษานโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ศึกษามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล และเพื่อเสนอแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ของ กห. ให้ได้มาตรฐานระดับสากล โดยการศึกษาครั้งนี้ใช้วิธีการสัมภาษณ์กลุ่มผู้ให้ข้อมูลสำคัญ (Key Informants) และการ ค้นคว้าข้อมูลจากเอกสารทางวิชาการต่าง ๆ ที่มีเนื้อหาเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. และมาตรฐาน การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ผลการศึกษา พบว่า 1) กรอบนโยบายยุทธศาสตร์ และการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวง กลาโหม ได้แก่ พ.ร.บ. ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศและการสื่อสารของ กห. พ.ศ. 2551, นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กห. พ.ศ. 2554, ยุทธศาสตร์ กห. อิเล็กทรอนิกส์ (e-Defence), แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของ กห. ฉบับที่ 3 พ.ศ. 2557 – 2561, การจัดตั้งศูนย์ บัญชาการไซเบอร์ กห. 2) มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO 27001: 2005, มาตรฐาน FIPS PUB 200, มาตรฐาน NIST 800 – 14, มาตรฐาน COBIT, และ มาตรฐาน IT BPM 3) แนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ให้ได้มาตรฐานในระดับสากล เชิงนโยบาย ได้แก่ ส่วนบังคับการ ต้องเปิดอัตรานายทหารสงครามข้อมูลข่าวสาร เพื่อดำเนินการตอบสนองต่อปัญหา/เหตุการณ์บุกรุกระบบของหน่วยขึ้นตรงได้อย่างรวดเร็ว ส่วนนโยบายและแผน ต้องมีการบรรจุข้อกำหนดในกระบวน การจัดซื้อจัดจ้าง อุปกรณ์ฮาร์ดแวร์/ซอฟต์แวร์ เพื่อให้อุปกรณ์ มีความปลอดภัยในระดับสากล ส่วนปฏิบัติการไซเบอร์ จะต้องมีหน่วยปฏิบัติการเชิงรับสงครามข้อมูลข่าวสาร และ หน่วยปฏิบัติการเชิงรุก สงครามข้อมูลข่าวสาร ส่วนวิจัยและ พัฒนาไซเบอร์จะต้องจัดตั้งส่วนงาน Information Warfare System Research เพื่อพัฒนาระบบการรักษาความปลอดภัย ของข้อมูลข่าวสารให้มีประสิทธิภาพมากยิ่งขึ้น และต้องบรรจุ อัตราจเรทหารที่มีความเชี่ยวชาญเฉพาะด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ เพื่อดำเนินการตรวจสอบตามหลักการ ICT Audit เชิงปฏิบัติ ได้แก่ 1) ควรจัดทำหลักสูตร Cyber Training เพื่ออบรมความรู้เกี่ยวกับการใช้งานซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมทั้งการให้ทุน การศึกษาต่อในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่ บุคลากรทุกระดับ 2) ควรมีการจัดการองค์ความรู้ด้านไซเบอร์ (Cyber Knowledge Management: KM) ในหน่วยงาน และ ควรนำ E-Document มาใช้ในการปฏิบัติราชการมากยิ่งขึ้น คำสำคัญ: การรักษาความมั่นคงปลอดภัยไซเบอร์, มาตรฐาน การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (“การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม” ,ออนไลน์, 2562)

กรอบแนวคิดการวิจัย

สรุป จากการทบทวนวรรณกรรมต่าง ๆ ได้แก่ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549, ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550, พระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ,พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560, พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553, ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553, ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553, ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556, ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555, ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559, ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 วันที่ 23 พฤษภาคม 2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของคอมพิวเตอร์ลูกข่ายระบบบาทเนต ดังนั้น กรอบแนวคิดในการวิจัย คือ การร่างนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ของกรมบัญชีกลางพร้อมการบริหารจัดการเพื่อรับมือภัยคุกคามทางไซเบอร์ ในปัจจุบันนั้นยังไม่มีการกำหนดนโยบายและแนวปฏิบัติในการดำเนินการที่เหมาะสม กับเทคโนโลยี บุคลากร ทักษะ ความรู้ และอุปกรณ์ต่างๆ ที่ใช้ในการดำเนินการเพื่อให้ระบบงานของกรมมีความมั่นคงปลอดภัย อาจยังขาดองค์ประกอบที่สำคัญหลายประการและถ้าใช้เป็นแนวทางในการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ของกรมบัญชีกลางดังกล่าวจะเป็นนโยบายที่มีความเหมาะสมกับลักษณะการทำงานของกรมบัญชีกลาง พอที่จะนำไปใช้เป็นกลไกสำคัญในการขับเคลื่อนการปฏิรูปองค์กรให้เป็นหน่วยงานที่มีความน่าเชื่อถือในระบบงานของกรมที่ให้บริการอยู่ในปัจจุบันรวมถึงระบบงานที่จะเกิดขึ้นในอนาคต

แผนภาพที่ 2 - 1 : กรอบแนวคิดในการวิจัย



สรุป

จากการศึกษาข้อระเบียบและกฎหมายที่เกี่ยวข้องพบว่า ในการดำเนินงานต่าง ๆ โดยต้องประเมินความเสี่ยงขององค์กรและหามาตรการควบคุมที่เหมาะสมและต้องสอดคล้องกับกฎระเบียบและข้อบังคับที่เกี่ยวข้องทั้งเป็นกำหนดแนวทางการปรับปรุงให้เหมาะสมกับการรับมือภัยคุกคามที่คาดว่าจะเกิดขึ้น

บทที่ 3
นโยบายการรักษาควบคุมความมั่นคงทางไซเบอร์ของกรมบัญชีกลาง

แนวคิดและหลักการของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศนั้น มีวัตถุประสงค์เพื่อ รักษาระบบสารสนเทศให้คงไว้ซึ่งคุณสมบัติหลัก 3 ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การคงสภาพความถูกต้องและความน่าเชื่อถือของข้อมูล (Integrity) และความพร้อมใช้งาน (Availability)

จากแนวคิดดังกล่าว การศึกษา เรื่อง การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมบัญชีกลาง ได้มีการนำปัจจัยที่เกี่ยวข้องมาวิเคราะห์โดยปัจจัยที่เกี่ยวข้องประกอบด้วย

1. การตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ
2. กฎระเบียบกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ
3. อุปกรณ์เครื่องมือต่าง ๆ
4. บุคลากร
5. แนวปฏิบัติ

โดยเฉพาะอย่างยิ่งด้าน บุคลากร เนื่องจากบุคลากรเป็นตัวบุคคลที่จะดำเนินการในด้านต่าง ๆ ซึ่งถ้าบุคลากรไม่เข้าใจในองค์ประกอบตัวบุคลากรจะเป็นจุดอ่อน ไม่ว่าอุปกรณ์และเทคโนโลยี นโยบาย กฎระเบียบและการปฏิบัติจะเคร่งครัดขนาดไหนก็ตาม

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

ในการศึกษาพฤติกรรมการใช้งานอินเตอร์ผ่านเครือข่ายกรมบัญชีกลางของบุคลากร พบว่ายังคงมีการใช้งานที่ไม่เหมาะสมรวมถึงเข้าเว็บไซต์ที่มีการฝังมัลแวร์ในการโจมตีเครื่องคอมพิวเตอร์ของผู้ใช้งาน และพบว่าผู้ใช้งานได้มีการนำอุปกรณ์พกพาที่ติดมัลแวร์มาใช้กับเครื่องของผู้ใช้งาน และทำให้เครื่องคอมพิวเตอร์เครื่องนั้นติดมัลแวร์ ซึ่งจากพฤติกรรมนี้ของผู้ใช้งานทำให้แสดงว่าผู้ใช้งานยังขาดความรู้ในด้านความมั่นคงปลอดภัยสารสนเทศของกรมบัญชีกลาง ทางศูนย์เทคโนโลยีสารสนเทศได้จัดอบรมให้ความรู้พบว่ามีบุคลากรของกรมบัญชีกลางในหลายหน่วยงานไม่ทราบหรือไม่รู้ว่ามีการจัดอบรมในเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัย และทางศูนย์เทคโนโลยีสารสนเทศได้จัดทำแผนการจัดฝึกอบรมการสร้างการตระหนักรู้ในเรื่องความมั่นคงปลอดภัยสารสนเทศ ให้มีการอบรมให้บุคลากรของกรมบัญชีกลาง อย่างน้อยปีละ 1 ครั้ง พร้อมการปฐมนิเทศให้กับบุคลากรใหม่ของกรมบัญชีกลางรับทราบนโยบายความมั่นคงปลอดภัยก่อนเริ่มปฏิบัติงาน พร้อมทั้งเพิ่มรายวิชาที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัยในการอบรมหลักสูตรข้าราชการบรรจุใหม่ของกรมบัญชีกลาง และได้มีการแจ้งนโยบายความมั่นคงปลอดภัยสารสนเทศ สำหรับผู้ให้บริการภายนอกทราบพร้อมทั้งปฏิบัติตามนโยบายดังกล่าวในการปฏิบัติงานที่กรมบัญชีกลาง

ตารางที่ 3-1 ตารางรายการการสื่อสารนโยบายด้านระบบเทคโนโลยีสารสนเทศการสื่อสาร และการสร้างความตระหนักรู้สำหรับผู้ปฏิบัติงานของกรมบัญชีกลาง

แผนการสื่อสารนโยบายฯ และ Awareness	สำหรับบุคลากรบรรจุในตำแหน่งอื่น	บุคลากรกรมบัญชีกลางส่วนกลาง	บุคลากรส่วนภูมิภาค.	ผู้ให้บริการภายนอกที่ปฏิบัติงานภายในกรม	ผู้ให้บริการภายนอกที่ไม่ได้ปฏิบัติงานภายในกรม.
1.หลักสูตรการพัฒนาศักยภาพข้าราชการบรรจุใหม่ “วิชานโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศรวมทั้งกฎหมายที่เกี่ยวข้องและการป้องกันภัยคุกคาม”	✓	✓			
2.เอกสารสรุปนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารกรมบัญชีกลาง (Security Awareness Policy)		✓	✓	✓	
3. โครงการฝึกอบรมหลักสูตรความรู้เรื่องนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมบัญชีกลาง และการสร้างความตระหนักรู้สำหรับบุคลากร (CGD Information Security Policy And Security Awareness Training)			✓		
4. สรุปรายละเอียดนโยบายความมั่นคงปลอดภัย ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับผู้ให้บริการภายนอก (Information security Policy And Suppler)				✓	✓
5.อบรมนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับผู้ให้บริการภายนอก				✓	

ที่มา : ศูนย์เทคโนโลยีสารสนเทศกรมบัญชีกลาง แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง พ.ศ. 2557 – 2561 (ระยะ 5 ปี) ,2557

1. กฎระเบียบ กฎหมาย พรบ. ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

กรมบัญชีกลางเป็นหน่วยงานกลางที่มีลักษณะงานที่หลากหลายโดยแบ่งได้เป็นงานหลัก 2 ด้าน และ งานสนับสนุน 1 ด้าน คือ

งานหลักที่ 1 การกำกับดูแลทางด้านการเงินและการบัญชีภาครัฐ (Regulator)

งานหลักที่ 2 การให้บริการของกรมบัญชีกลาง (Service Provider)

งานสนับสนุน คืองานที่ช่วยให้งานหลักสามารถดำเนินไปได้อย่างมีประสิทธิภาพ เช่น ด้านงบประมาณ เทคโนโลยีสารสนเทศ เป็นต้น

งานหลักที่ 1 : การกำกับดูแลทางด้านการเงินและการบัญชีภาครัฐ (Regulator) โดยมีงานกำกับดูแลที่อยู่ในแผนงานนี้ ประกอบด้วย 8 ด้าน คือ

ด้านที่ 1 ด้านกฎหมายการคลัง

ด้านที่ 2 ด้านบัญชีภาครัฐ

ด้านที่ 3 ด้านการจัดซื้อจัดจ้างภาครัฐ

ด้านที่ 4 ด้านการตรวจสอบภายใน

ด้านที่ 5 ด้านสวัสดิการรักษาพยาบาลข้าราชการ

ด้านที่ 6 ด้านเงินนอกงบประมาณ

ด้านที่ 7 ด้านลูกจ้าง

ด้านที่ 8 ด้านละเมิดและแพ่ง

งานหลักที่ 2 : การให้บริการของกรมบัญชีกลาง **(Service Provider)** โดยมีงานบริการ ประกอบด้วย 5 ด้าน คือ

ด้านที่ 1 ด้านการเปลี่ยนการบริหารการเงินการคลังภาครัฐด้วยระบบอิเล็กทรอนิกส์ (GFMIS)

ด้านที่ 2 ด้านการพัฒนาและบริหารระบบเศรษฐกิจการคลังส่วนภูมิภาค

ด้านที่ 3 ด้านจ่ายตรงเงินเดือน ค่าจ้างประจำ บำเหน็จบำนาญ

ด้านที่ 4 ด้านพัฒนางานการคลัง

ด้านที่ 5 ด้านการอบรมพัฒนาบุคลากรภาครัฐ

และงานสนับสนุนในเรื่องเทคโนโลยีสารสนเทศ ซึ่งเป็นการให้บริการทั้งหน่วยงานภายในและหน่วยงานภายนอก โดยเฉพาะหน่วยงานภายในมีการใช้งานผ่านระบบเครือข่ายที่ติดตั้งภายในสำนักงานของกรมบัญชีกลางทั่วประเทศโดยเชื่อมโยงเครือข่ายทั้งในส่วนกลาง สำนักงานคลังเขต (9 แห่ง) และสำนักงานคลังจังหวัด (75 แห่ง) เพื่อใช้ปฏิบัติงานด้านต่าง ๆ ที่เป็นภารกิจของกรมบัญชีกลางและงานทั่วไปของกรมบัญชีกลาง ดังนั้นข้อมูลสารสนเทศต่าง ๆ จึงมีความสำคัญและต้องมีการปกป้องทรัพย์สินทางด้านสารสนเทศ

นอกจากนั้น กรมบัญชีกลางให้บริการระบบงานที่สำคัญแก่หน่วยงานภาครัฐ ภาคเอกชน ผู้ค้าภาครัฐ ตลอดจนประชาชนทั่วไป เช่น ระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (*e*-Government Procurement : *e*-GP) ระบบจ่ายตรงเงินเดือนและค่าจ้างประจำ ระบบบำเหน็จบำนาญ ระบบสวัสดิการรักษาพยาบาล ระบบบูรณาการฐานข้อมูลสวัสดิการสังคม ระบบสวัสดิการแห่งรัฐ เป็นต้น ซึ่งระบบเหล่านี้จะมีข้อมูลที่สำคัญไม่ว่าจะเป็นข้อมูลบุคคล และข้อมูลการปฏิบัติงานที่แสดงถึงการดำเนินงานที่โปร่งใสในการปฏิบัติงาน ซึ่งข้อมูลเหล่านี้อยู่ในความคุ้มครองตาม พรบ.ข้อมูลข่าวสารจึงต้องมีการเก็บรักษาที่ปลอดภัยและยากที่ผู้ไม่เกี่ยวข้องจะเข้าถึงข้อมูลเหล่านี้ได้ ซึ่งผู้ใช้งานมีความหลากหลายในด้านวัยวุฒิและคุณวุฒิ โดยผู้ใช้งานมีการใช้งานคอมพิวเตอร์ในหลายรูปแบบจึงเป็นช่องทางที่นำไวรัสและเปิดช่องโหวให้ผู้ไม่เกี่ยวข้องพยายามเข้ามาในระบบงานเพื่อทำให้เกิดความเสียหายและส่งผลกระทบกับระบบเครือข่ายของกรมบัญชีกลางให้มีการใช้งานเกินความเป็นจริงโดยการโจมตีระบบอย่างต่อเนื่อง ทำให้ช่องทางที่มีอยู่ไม่เพียงพอต่อการทำงานปกติผู้ใช้งานที่ใช้ระบบต่าง ๆ ของกรมบัญชีกลางได้รับการตอบสนองที่ช้าและบางครั้งไม่สามารถทำงานได้

จากการให้บริการข้อมูลดังกล่าว สิ่งที่หลีกเลี่ยงไม่ได้และจะต้องถือปฏิบัติตามกฎหมายกฎระเบียบต่าง ๆ ได้แก่

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

1. พระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
3. พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553
4. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
5. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
6. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556
7. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
8. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559

9. ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 วันที่ 23 พฤษภาคม 2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของคอมพิวเตอร์ลูกข่ายระบบบาทเนต

จากการศึกษากฎหมายและกฎระเบียบข้างต้น พบว่ามีหลักการที่ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ โดยเฉพาะการปกป้องข้อมูลและทรัพย์สินที่มาในรูปแบบต่าง ๆ เช่น ความเสี่ยงจากการใช้งานอินเทอร์เน็ต ภัยจากการทำธุรกรรมทางอิเล็กทรอนิกส์ โจรกรรมพาสเวิร์ด การจู่โจมด้วยการส่งโปรแกรมดักจับข้อมูลทางคอมพิวเตอร์ เป็นต้น ซึ่งต้องทำการประเมินเสี่ยงในด้านต่าง ๆ ให้สอดคล้องกับ CIA และหามาตรการควบคุมหรือการจัดการความเสี่ยงทางศูนย์เทคโนโลยีสารสนเทศได้ดำเนินการ

1.1. วิเคราะห์ปัจจัยภายใน

1.1.1 ลักษณะองค์กรของกรมบัญชีกลาง

กรมบัญชีกลาง มีภารกิจเกี่ยวกับการควบคุมดูแลการใช้จ่ายเงินแผ่นดินและของหน่วยงานภาครัฐให้เป็นไปโดยถูกต้อง มีวินัย คุ้มค่า โปร่งใส และสามารถตรวจสอบได้ โดยการวางกรอบหลักเกณฑ์กลาง ให้หน่วยงานภาครัฐถือปฏิบัติ การให้บริการคำแนะนำปรึกษาด้านการเงิน การคลัง การบัญชี การตรวจสอบภายใน การบริหารเงินนอกงบประมาณ และการพัสดุภาครัฐ การดำเนินการเกี่ยวกับ การบริหารเงินคงคลังให้มีใช้จ่ายอย่างเพียงพอ และการเสนอข้อมูลในเชิงนโยบายการคลัง แก่ฝ่ายบริหาร โดยประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อให้เกิดเสถียรภาพทางการคลัง รวมทั้งดำเนินการเกี่ยวกับการประเมินผลการคลังภาครัฐ การกำกับดูแลนโยบายและมาตรฐานค่าตอบแทนสวัสดิการและสิทธิประโยชน์ของบุคลากรภาครัฐ

1.1.2 วิสัยทัศน์ของกรมบัญชีกลาง

กำกับดูแลและบริหารการใช้จ่ายเงินของแผ่นดินให้เกิดประโยชน์สูงสุด

1.1.3 พันธกิจของกรมบัญชีกลาง

กรมบัญชีกลางได้กำหนดพันธกิจของกรมบัญชีกลาง 5 พันธกิจ ดังนี้

1.1.3.1 กำหนดมาตรฐาน หลักเกณฑ์ แนวปฏิบัติด้านกฎหมายการคลัง การบัญชี การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ การตรวจสอบภายใน ค่าตอบแทนและสวัสดิการ เงินนอกงบประมาณ ลูกจ้าง และความรับผิดทางละเมิดของเจ้าหน้าที่ของรัฐ ให้สอดคล้องกับการรักษาวินัยและความยั่งยืนทางการคลัง

1.1.3.2 บริหารเงินสดภาครัฐ บริหารการรับ-จ่ายเงิน ให้เป็นไปอย่างมีประสิทธิภาพโดยใช้ระบบเทคโนโลยีที่ทันสมัย

1.1.3.3 สนับสนุนการบริหารเศรษฐกิจการคลังในส่วนภูมิภาค

1.1.3.4) พัฒนาขีดความสามารถของบุคลากรภาครัฐทางด้านการบริหารการเงินภาครัฐ

1.1.3.5) เป็นศูนย์ข้อมูลสารสนเทศทางการคลัง

1.1.4 ยุทธศาสตร์ของกรมบัญชีกลาง

ตารางที่ 3-2 ยุทธศาสตร์กรมบัญชีกลาง

ยุทธศาสตร์กรมบัญชีกลาง ประกอบด้วย 3 ประเด็นยุทธศาสตร์ ดังนี้:	
ยุทธศาสตร์ที่ 1	การเป็นกลไกหลักของนโยบายการคลังที่ขับเคลื่อนการฟื้นตัวของเศรษฐกิจไทย (Fiscal Stimulus)
ยุทธศาสตร์ที่ 2 :	การปรับภาวะการคลังให้เข้าสู่สมดุล (Fiscal Consolidation)
ยุทธศาสตร์ที่ 3 :	การเสริมสร้างความเข้มแข็งขององค์กร (Strengthen the CGD organization)

ที่มา : ศูนย์เทคโนโลยีสารสนเทศกรมบัญชีกลาง แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง พ.ศ. 2557 – 2561 (ระยะ 5 ปี) ,2557

1.1.5 ยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง

กรมบัญชีกลางได้กำหนดยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง

1.1.5.1 สร้างนวัตกรรมด้าน ICT เพื่อตอบสนองความต้องการในการกำกับดูแลและบริหารการใช้จ่ายเงินของแผนดินอย่างมีประสิทธิภาพและทันสมัย

1.1.5.2 เพิ่มประสิทธิภาพและสนับสนุนให้มีการใช้เทคโนโลยีสารสนเทศและการสื่อสารภายในองค์กรอย่างครบวงจร

1.1.5.3 เพิ่มช่องทางการให้บริการในลักษณะ e-server ผ่านอุปกรณ์สื่อสารเคลื่อนที่ต่าง ๆ (Mobile Devices) ให้กับข้าราชการ ประชาชน และส่วนราชการหรือหน่วยงานที่เกี่ยวข้อง

1.1.5.4 ยกระดับการบริการอิเล็กทรอนิกส์ของกรมบัญชีกลาง โดยการมีส่วนร่วมของผู้เกี่ยวข้องกับภารกิจของกรมบัญชีกลาง ในแนวทาง Smart Service โดยการบริการอิเล็กทรอนิกส์ของกรมฯ หรือ e-CGD Service ภายใต้การให้บริการแบบไร้รอยต่อ/ไร้ตะเข็บรอยต่อ (Seamless) ระหว่างกรมบัญชีกลางกับผู้รับบริการ/ผู้เกี่ยวข้อง (เช่น หน่วยงาน/ส่วนราชการ บุคลากรภาครัฐ ผู้มีสิทธิ์/ผู้อาศัย/ทายาทของบุคลากรภาครัฐ ประชาชนและภาคเอกชน) เพื่อก้าวไปสู่การพัฒนาบริการอิเล็กทรอนิกส์ด้านข้อมูลข่าวสาร เอกสาร และการมีส่วนร่วมของผู้รับบริการ/ผู้เกี่ยวข้อง

1.1.5.5 เพิ่มมูลค่าเพิ่มให้กับระบบสารสนเทศในปัจจุบันของกรมบัญชีกลางอย่างเป็นรูปธรรม เพื่อประโยชน์เชิงการบริหารทุกมิติอย่างครบวงจร

1.1.5.6 เพิ่มประสิทธิภาพการบริหารจัดการภายในและเพิ่มศักยภาพของบุคลากรภายในกรมบัญชีกลาง

1.1.5.7 ปรับปรุงระบบการให้บริการและระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารไปสู่มาตรฐานสากล

1.1.6 ปัจจัยความสำเร็จ

ผลการศึกษาปัจจัยความสำเร็จของกรมบัญชีกลางที่ระบุในแผนแม่บทเทคโนโลยีสารสนเทศ และการสื่อสารของกรมบัญชีกลาง พ.ศ. 2557 – 2561 (ระยะ 5 ปี) พบว่ามีปัจจัยความสำเร็จ แบ่งเป็น 7 ประเด็น ดังนี้

1.1.6.1 มีนโยบายขององค์กรที่ชัดเจน เพียงพอ เพื่อให้ความสามารถวางแผนทางด้านเทคโนโลยีสารสนเทศและการสื่อสารได้อย่างถูกต้อง

1.1.6.2 ผู้บริหารให้ความสำเร็จและให้การสนับสนุนงานด้านเทคโนโลยีสารสนเทศและการสื่อสารและเข้าร่วมดำเนินการอย่างจริงจังในการสนับสนุนและการแก้ไขปัญหาการใช้งานระบบสารสนเทศ

1.1.6.3 ผู้บริหารให้การสนับสนุนอัตรากำลังคน งบประมาณที่เหมาะสมเพียงพอต่อภารกิจ และกำหนดแนวทางการเติบโตในสายอาชีพทางด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่สอดคล้องกับยุทธศาสตร์ของกรมบัญชีกลาง

1.1.6.4 มีการกำหนดยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสารที่สอดคล้องกับยุทธศาสตร์ของกรมฯ

1.1.6.5 จัดทำแผนด้านเทคโนโลยีสารสนเทศและการสื่อสารตามยุทธศาสตร์อย่างเป็นระบบและแบบองค์รวม และศึกษาความเป็นไปได้ (Feasibility Study) ของกิจกรรม ในแผนตามหลักวิชาการ ก่อนการนำไปดำเนินการอย่างจริงจัง (Implementation) และต้องมีการกำหนดเวลาแล้วเสร็จในการดำเนินงาน

1.1.6.6 ด้านบุคลากร

1.1.6.6.1 บุคลากรของศูนย์เทคโนโลยีสารสนเทศต้องได้รับการฝึกอบรมตามหลักวิชาการ อย่างเหมาะสม เพื่อให้มีความรู้ ความสามารถ ความเชี่ยวชาญในการปฏิบัติหน้าที่และงานที่ได้รับผิดชอบอย่างเหมาะสม เพื่อให้ทันต่อการเปลี่ยนแปลงของสภาพแวดล้อมของโลก โดยเฉพาะด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่มีการพัฒนาแบบก้าวกระโดดอย่างต่อเนื่อง และสามารถตอบสนอง ต่อการเปลี่ยนแปลงของสภาพแวดล้อมได้อย่างเป็นระบบและอย่างต่อเนื่อง

1.1.6.6.2 เพื่อศึกษาและกำหนดแนวทางการพัฒนาความรู้ความสามารถ และการจัดทำมาตรฐานการกำหนดตำแหน่งให้ความสามารถก้าวหน้าในสายงานด้านคอมพิวเตอร์และสารสนเทศภาครัฐได้อย่างมั่นคง

1.1.6.6.3 สร้างขวัญและกำลังใจให้กับบุคลากรที่มีความรู้ความสามารถ และความรับผิดชอบต่อหน้าที่

1.1.6.6.4 ปรับโครงสร้างองค์กรของศูนย์เทคโนโลยีสารสนเทศให้มีความยืดหยุ่น สามารถรองรับปริมาณงานตามภารกิจของกรมบัญชีกลาง ที่มีการอัตราขยายตัวอย่างก้าวกระโดดและรวดเร็ว

1.1.6.6.5 การทำงานเป็นทีม

1.1.6.7 นำแผนด้านเทคโนโลยีสารสนเทศและการสื่อสารตามยุทธศาสตร์มาดำเนินการ อย่างเป็นระบบและเป็นรูปธรรม และต้องมีการกำหนดเวลาแล้วเสร็จในการดำเนินงานในแต่ละแผนงาน/โครงการ พร้อมการจัดทำ/จัดหาเครื่องมือในการติดตามประเมินผล การดำเนินงานเพื่อเป็นการสร้างระบบเตือนภัยในการติดตามความก้าวหน้าของกรมบัญชีกลาง

1.1.7 ภารกิจของศูนย์เทคโนโลยีสารสนเทศ

กรมบัญชีกลางได้กำหนดภารกิจของศูนย์เทคโนโลยีสารสนเทศ 5 ภารกิจ ดังนี้

1.1.7.1 จัดทำแผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศของกรมบัญชีกลางให้สอดคล้องกับมาตรฐานกลางและนโยบายของกระทรวง

1.1.7.2 วางและพัฒนาระบบเทคโนโลยีสารสนเทศของกรมบัญชีกลาง

1.1.7.3 บริหารจัดการระบบเทคโนโลยีสารสนเทศของกรมบัญชีกลางตลอดจนสนับสนุนและให้คาปรึกษาแนะนา ระบบเทคโนโลยีสารสนเทศให้แก่หน่วยงานในสังกัดกรมบัญชีกลาง

1.1.7.4 เป็นศูนย์ดำเนินการเกี่ยวกับข้อมูลสารสนเทศกรมบัญชีกลาง

1.1.7.5 ปฏิบัติงานร่วมกันหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

1.1.8 นโยบายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

กรมบัญชีกลางได้ประกาศนโยบายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ 1 ฉบับ คือ นโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง (Information Security Policy)

1.1.9 สภาพปัจจุบันของระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

กรมบัญชีกลางได้เคยรับรองระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) ISO/IEC 27001:2005 ใน 3 ขอบเขต ดังนี้

1.1.9.1 ระบบควบคุมสภาพความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and system environment control system) สำหรับศูนย์ข้อมูลกลาง (Data center) และจุดติดตั้งอุปกรณ์สำรองไฟฟ้า อุปกรณ์กำเนิดไฟฟ้า ครอบคลุมถึง

1.1.9.1.1 การให้บริการพื้นที่สำหรับระบบคอมพิวเตอร์

1.1.9.1.2 การควบคุมการเข้าถึงทางกายภาพ (Access control) ภายในศูนย์ข้อมูลกลาง

1.1.9.1.3 การติดตามผ่านระบบกล้องวงจรปิด (Surveillance)

1.1.9.1.4 การควบคุมสภาพแวดล้อมทางกายภาพ (Environment control)

1.1.9.1.5 การบำรุงรักษาอุปกรณ์ (Hardware maintenance)

1.1.9.1.6 การติดตามโครงสร้างการให้บริการศูนย์ข้อมูลกลางขั้นพื้นฐาน (Data center infrastructure monitoring)

1.1.9.1.7 การบริหารจัดการผู้ให้บริการภายนอก (Third party management)

1.1.9.2 การควบคุมความมั่นคงปลอดภัยทางเครือข่ายคอมพิวเตอร์ (Network infrastructure security control) สำหรับศูนย์ข้อมูลกลาง (Data center) ครอบคลุมถึง

1.1.9.2.1 การควบคุมการเข้าถึงทางเครือข่าย (Network access control system)

1.1.9.2.2 การควบคุมการเชื่อมโยงเครือข่าย (Network connection control)

1.1.9.2.3 การติดตามโครงสร้างการให้บริการเครือข่าย (Network infrastructure monitoring)

1.1.9.2.4 การบริหารจัดการผู้ให้บริการภายนอก (Third party management)

1.1.9.2.5 การป้องกันโปรแกรมไม่ประสงค์ดี (Malicious control)

1.1.9.3 การให้บริการระบบคอมพิวเตอร์แม่ข่าย สำหรับระบบงานจัดซื้อจัดจ้างภาครัฐ ด้วยอิเล็กทรอนิกส์ ครอบคลุมถึง

1.1.9.3.1 การบำรุงดูแลอุปกรณ์คอมพิวเตอร์ (Hardware maintenance)

1.1.9.3.2 การจัดการสมรรถนะระบบ (Capacity management)

1.1.9.3.3 การสำรองข้อมูล (Backup service)

1.1.9.3.4 การบริหารจัดการผู้ให้บริการภายนอก (Third party management)

1.1.9.3.5 การควบคุมการลงทะเบียนผู้ดูแลระบบ (Registering control)

1.1.9.3.6 การบริหารจัดการอุบัติการณ์ (Incident management)

1.1.9.3.7 การควบคุมการใช้งานลิขสิทธิ์ (License management)

1.2 ปัจจัยภายนอก

1.2.1 กฎหมายด้านเทคโนโลยีสารสนเทศ

กรมบัญชีกลาง มีกฎหมายด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง ดังนี้

1.2.1.1 พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537

1.2.1.2 พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558

1.2.1.3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

1.2.1.4 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2561

1.2.1.5 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

1.2.1.6 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1.2.1.7 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

1.2.1.8 พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

1.2.1.9 พระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

1.2.1.10 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

1.2.1.11 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

1.2.1.12 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555

1.2.1.13 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องรายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559

1.2.1.14 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

1.3 การวิเคราะห์ SWOT

จากการสัมภาษณ์คณะทำงานกรมบัญชีกลาง ซึ่งสรุปจุดแข็ง จุดอ่อน โอกาส และอุปสรรค ของระบบเทคโนโลยีสารสนเทศของกรมบัญชีกลาง ดังนี้

1.3.1 จุดแข็ง (Strengths)

จากการศึกษาจุดแข็งของกรมบัญชีกลาง สรุปได้เป็น 2 ประเด็น ดังนี้

1.3.1.1 บุคลากรมีจิตบริการ มีความมุ่งมั่น อดทน และรับผิดชอบในการทำงาน

1.3.1.2 กรมบัญชีกลางมีการบริหารจัดการแบบรวมศูนย์ เชื่อมโยงบูรณาการ

1.3.2 จุดอ่อน (Weaknesses)

จากการศึกษาจุดอ่อนของกรมบัญชีกลาง สรุปได้เป็น 3 ประเด็น ดังนี้

1.3.2.1 ขาดบุคลากรที่มีความรู้ความสามารถ

1.3.2.2 บุคลากรไม่เพียงพอต่อการปฏิบัติงาน

1.3.2.3 อุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศไม่ทันสมัยและไม่เพียงพอ

1.3.3 โอกาส (Opportunities)

จากการศึกษาโอกาสของกรมบัญชีกลาง สรุปได้เป็น 3 ประเด็น ดังนี้

1.3.3.1 นโยบายภาครัฐส่งเสริมการดำเนินงานด้านเทคโนโลยีสารสนเทศของกรมบัญชีกลาง

1.3.3.2 กรมบัญชีกลางได้รับความเชื่อถือในด้านการให้บริการที่ดี

1.3.3.3 หน่วยงานกำกับดูแลของกรมบัญชีกลางให้ความสำคัญในด้านความมั่นคงปลอดภัยสารสนเทศ

1.3.4 อุปสรรค (Threats)

จากการศึกษาอุปสรรคของกรมบัญชีกลาง สรุปได้เป็น 3 ประเด็น ดังนี้

1.3.4.1 การจัดสรรงบประมาณไม่เพียงพอ

1.3.4.2 ความไม่ชัดเจนของหน่วยงานด้านเทคโนโลยีสารสนเทศ

1.3.4.3 การโจมตีด้านไซเบอร์

1.4 การวิเคราะห์สถานภาพความเสี่ยง

จากการวิเคราะห์สถานภาพความเสี่ยงของกรมบัญชีกลางจากการวิเคราะห์ SWOT พบประเด็นที่เกี่ยวข้องทั้งสิ้น 18 ประเด็น คณะทำงานฯ ได้ศึกษาแนวทางตอบสนองต่อความเสี่ยงเบื้องต้น

1.5 ผู้มีส่วนได้ส่วนเสีย

กรมบัญชีกลางมีผู้มีส่วนได้ส่วนเสียแบ่งเป็น 2 กลุ่ม คือ ผู้มีส่วนได้ส่วนเสียภายในองค์กร และ ผู้มีส่วนได้ส่วนเสียภายนอกองค์กร โดยมีรายละเอียดดังนี้

1.5.1 ผู้มีส่วนได้ส่วนเสียภายในองค์กร

1.5.1.1 ผู้บริหาร หมายถึง อธิบดี รองอธิบดี ผู้อานวยการ ผู้เชี่ยวชาญ

15.1.2 เจ้าหน้าที่ หมายถึง ข้าราชการระดับชำนาญการพิเศษลงมา เจ้าหน้าที่ราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว

1.5.2 ผู้มีส่วนได้ส่วนเสียภายนอกองค์กร

1.5.2.1 หน่วยงานกำกับดูแล หมายถึง หน่วยงานกับกำดูแลกรมบัญชีกลางทั้งทางตรงและทางอ้อม เช่น กระทรวงการคลัง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

1.5.2.2 ผู้ใช้บริการ หมายถึง ผู้ใช้บริการของกรมบัญชีกลาง

1.5.2.3 ผู้ให้บริการภายนอก หมายถึง ผู้ที่ส่งมอบผลิตภัณฑ์หรือบริการให้กับกรมบัญชีกลาง

1.6 ศึกษาความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสีย

กรมบัญชีกลางศึกษาความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียภายในและภายนอกองค์กรสรุปได้ดังนี้

1.6.1 ความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียภายในองค์กร

ตารางที่ 3-3 ความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียภายในองค์กร

ผู้มีส่วนได้ส่วนเสียภายในองค์กร	ความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย
1.6.1.1 ผู้บริหาร	1.6.1.1.1 เจ้าหน้าที่มีความตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ 1.6.1.1.2 ระบบสารสนเทศมีความพร้อมใช้งานและตอบสนองต่อเหตุการณ์ ที่อาจจะเกิดขึ้น 1.6.1.1.3 กรมบัญชีกลางผ่านการรับรองมาตรฐาน ISO/IEC 27001 1.6.1.1.4 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศได้รับการทบทวนให้เป็นปัจจุบัน
1.6.1.2 เจ้าหน้าที่	1.6.1.2.1 ระบบสารสนเทศมีความพร้อมใช้งานและตอบสนองต่อเหตุการณ์ที่อาจจะเกิดขึ้น 1.6.1.2.2 ได้รับความรู้ ความตระหนักด้านความมั่นคงปลอดภัย 1.6.1.2.3 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศได้รับการทบทวนให้เป็นปัจจุบัน

ที่มา : ศูนย์เทคโนโลยีสารสนเทศกรมบัญชีกลาง แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง พ.ศ. 2557 – 2561 (ระยะ 5 ปี),2557

1.6.2 ความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียภายนอกองค์กร

ตารางที่ 3-4 ความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียภายนอกองค์กร

ผู้มีส่วนได้ส่วนเสียภายนอกองค์กร	ความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย
1.6.2.1 หน่วยงานกำกับดูแล	1.6.2.1.1 ปฏิบัติตามกฎระเบียบ กฎหมาย ที่เกี่ยวข้อง
1.6.2.2 ผู้ใช้บริการ	1.6.2.2.1 มั่นใจได้ว่าระบบสารสนเทศที่ใช้ของกรมบัญชีกลางมีความพร้อมใช้ 1.6.2.2.2 ใช้บริการที่มีการคำนึงถึงความมั่นคงปลอดภัย และเชื่อถือได้
1.6.2.3 ผู้ให้บริการภายนอก	1.6.2.3.1 ระบบสารสนเทศมีความพร้อมใช้งานและตอบสนองต่อเหตุการณ์ ที่อาจจะเกิดขึ้น

ที่มา : ศูนย์เทคโนโลยีสารสนเทศกรมบัญชีกลาง แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง พ.ศ. 2557 – 2561 (ระยะ 5 ปี),2557

1.7 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

กรมบัญชีกลางตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยสารสนเทศและมุ่งมั่น ที่จะพัฒนาการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง จึงกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของกรมบัญชีกลางไว้ดังนี้

1.7.1 มุ่งมั่นให้กรมบัญชีกลางให้บริการประชาชนอย่างมีมาตรฐาน

1.7.2 มุ่งมั่นที่จะให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและให้บริการได้อย่างต่อเนื่อง

1.7.3 มุ่งมั่นที่จะให้การปฏิบัติงานของเจ้าหน้าที่กรมบัญชีกลางเป็นไปอย่างเป็นระบบ และมีความมั่นคงปลอดภัย

1.7.4 มุ่งมั่นที่จะปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

1.8 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Objectives)

กรมบัญชีกลาง ได้กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อตอบสนอง ต่อความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย โดยมีวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ จำนวน 5 วัตถุประสงค์ ดังนี้

1.8.1 เพื่อขอรับรองมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัย ISO/IEC 27001:2013

1.8.2 เพื่อบริหารจัดการให้ระบบสามารถให้บริการได้ตามเกณฑ์ที่กำหนด

1.8.3 เพื่อทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

1.8.4 เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

1.8.5 เพื่อให้กรมบัญชีกลางสามารถปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้องกับความมั่นคง ปลอดภัยสารสนเทศ

1.9 ขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

จากการศึกษาบริบทองค์กรพบว่า กรมบัญชีกลางให้ความสำคัญเรื่องการให้บริการผ่านระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อให้การบริหารจัดการระบบเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ กรมบัญชีกลางจึงได้พัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐานสากล ISO/IEC 27001:2013 อีกทั้งจากประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต เป็นแรงขับเคลื่อนสำคัญ ทำให้กรมบัญชีกลางกำหนดขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เป็นดังนี้

1.9.1 ศูนย์คอมพิวเตอร์หลักกรมบัญชีกลาง โดยรวมถึง ระบบควบคุมสภาพความมั่นคงปลอดภัย ทางกายภาพและสภาพแวดล้อม (Physical and System Environmental Control System) และ โครงสร้างพื้นฐานการควบคุมความมั่นคงปลอดภัยทางเครือข่าย (Network Security Control Infrastructure)

1.9.2 การให้บริการระบบคอมพิวเตอร์แม่ข่ายของระบบงาน ดังนี้

1.9.2.1 ระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e-Government Procurement: e-GP)

1.9.2.2 ระบบบูรณาการฐานข้อมูลสวัสดิการสังคม (e-Social Welfare)

1.9.2.3 ระบบการชำระเงินแบบอิเล็กทรอนิกส์ (e-payment)

1.9.2.4 ระบบจ่ายตรงเงินเดือนและค่าจ้างประจา

1.9.2.5 ระบบบำเหน็จบำนาญและสวัสดิการรักษาพยาบาล

1.9.2.6 ระบบเว็บไซต์อินเตอร์เน็ตกรมบัญชีกลาง

1.9.3 ชุดคอมพิวเตอร์ลูกข่ายระบบบาทเนต (BATHNET) ของกรมบัญชีกลาง สำหรับการปฏิบัติงานจริงและสำหรับเป็นชุดสำรองที่ใช้เชื่อมโยงกับระบบบาทเนตของธนาคารแห่งประเทศไทย ได้แก่ ระบบคอมพิวเตอร์สำหรับบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (Electronic Financial Services) หรือระบบงานคอมพิวเตอร์อื่นที่เชื่อมโยงเพื่อการรับส่งข้อมูลโดยตรงกับระบบคอมพิวเตอร์แม่ข่ายของธนาคารแห่งประเทศไทย (Host to Host) ครอบคลุมทั้งศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรอง จำนวน 2 แห่ง

จากการศึกษาข้างต้น ทางศูนย์เทคโนโลยีสารสนเทศได้มีการขอรับรองตามมาตรฐาน ISO / IEC 27001 : 2013 กับระบบบาทเนต ระบบจัดซื้อจัดจ้างภาครัฐด้วยวิธีอิเล็กทรอนิกส์ ระบบบูรณาการฐานข้อมูลสวัสดิการสังคม และData Center ของกรมบัญชีกลาง ซึ่งในการขอรับรองในส่วนนี้จะเป็นขั้นพื้นฐานของกฎหมายข้างต้น

2. เทคโนโลยีและอุปกรณ์

กรมบัญชีกลางมีอุปกรณ์และกระบวนการในการดำเนินการที่ช่วยในการควบคุม และได้มีการจัดทำแผนเพื่อของบประมาณในการจัดซื้ออุปกรณ์ที่ทันสมัยเพื่อให้ศูนย์เทคโนโลยีสารสนเทศมีความพร้อมในการเฝ้าระวังและรับมือกับภัยคุกคามที่คาดว่าจะเกิดขึ้น และจากการสังเกตการณ์พบว่าทางศูนย์เทคโนโลยีสารสนเทศได้มีการออกแบบในการเข้าถึงระบบงานไว้หลายชั้น ซึ่งทำให้การเฝ้าระวังและการตอบสนองหรือการปิดกั้นสามารถแยกเป็นส่วนๆ ได้ ทำให้ผลกระทบที่เกิดมีผลกระทบกับระบบงานอื่นน้อยลง แต่ด้วยการที่เทคโนโลยีในปัจจุบันกับลักษณะการโจมตีเปลี่ยนแปลงค่อนข้างเร็ว ทำให้การตอบสนองต่อภัยคุกคามอาจไม่ทันท่วงที

ดังนั้น การบริหารจัดการการเข้าถึงข้อมูลของกรมบัญชีกลาง จะต้องนำเทคโนโลยีที่ทันสมัยและอุปกรณ์ที่มีประสิทธิภาพมาใช้งาน และสิ่งที่สำคัญอีกประการหนึ่งก็คือการออกแบบระบบเครือข่ายเพื่อให้การบริการแบ่งตามกลุ่มการให้บริการด้านระบบงาน เช่น กลุ่ม Web Portal Server, กลุ่ม Application Server และ กลุ่ม Database Server เป็นต้น เพื่อกำหนดนโยบายด้านความปลอดภัย (Policy) ให้มีความปลอดภัยสอดคล้องตามประเภทการให้บริการระบบงานฯ โดยแบ่งเป็นโซนต่าง ๆ ตามประเภทของระบบงาน และระดับความปลอดภัย

3.บุคลากร

ในกรณีของบุคลากรนั้น เป็นที่ยอมรับกันว่าถือเป็นองค์ประกอบหลักที่สำคัญที่สุด โดยบุคลากรในที่นี้อาจหมายรวมถึง กลุ่มคนและบทบาทของบุคคลนั้น ๆ ไม่ว่าจะเป็นคณะกรรมการด้านเทคโนโลยีสารสนเทศในองค์กร เจ้าของข้อมูล นักพัฒนา ผู้ตรวจสอบภายในองค์กร แอดมินดูแลระบบเครือข่าย ไปจนถึงผู้ใช้งานหรือ Endorsers เอง ดังนั้นถ้าผู้ที่เกี่ยวข้องทั้งหมดเข้าใจและปฏิบัติตามกฎเกณฑ์ที่กำหนด ปัญหาต่าง ๆ ที่พบก็จะลดน้อยลง

บุคลากรของกรมบัญชีกลาง ทางด้านศูนย์เทคโนโลยีสารสนเทศมีจำนวนจำกัด และในความรู้ความสามารถของบุคลากรยังมีความรู้ความสามารถที่ยังไม่ครอบคลุมการปฏิบัติงาน ซึ่งทางกรมบัญชีกลาง ได้จัดสนับสนุนให้บุคลากรมีการฝึกอบรม ทั้งส่วนที่เป็นการใช้งานอุปกรณ์ด้านความมั่นคงปลอดภัย และอุปกรณ์สนับสนุน พร้อมทั้งมีความร่วมมือกับผู้ให้บริการภายนอก ในการให้ความรู้และการเฝ้าระวัง เพื่อลดช่องว่างของจำนวนบุคลากรที่มีจำนวนจำกัด โดยบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศจะเป็นกลุ่มงานที่จำเป็นต้องมีความรู้ความสามารถและทักษะในการรับมือกับภัยคุกคามที่เกิดขึ้น

เพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศดำเนินการได้อย่างมีประสิทธิผล กรมบัญชีกลางจึงได้กำหนดโครงสร้างบุคลากรระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยประกอบด้วย

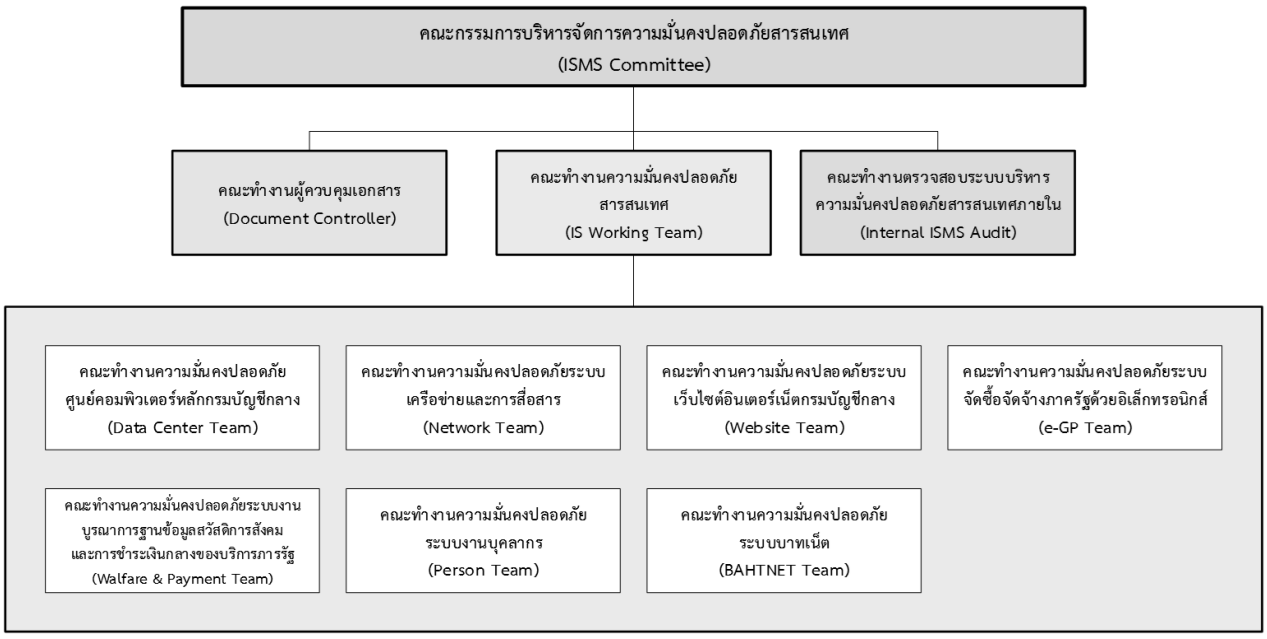
3.1 คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee)

3.2 คณะทำงานตรวจสอบระบบบริหาร ความมั่นคงปลอดภัยสารสนเทศภายใน (Internal ISMS Audit)

3.3 คณะทำงานความมั่นคงปลอดภัยสารสนเทศ (IS Working Team)

3.4 คณะทำงานผู้ควบคุมเอกสาร (Document Controller)

แผนภาพที่ 3-1 โครงสร้างบุคลากรระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ



ทั้งนี้ ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จะดำเนินการกำหนดแนวทางการบริหารจัดการและสั่งการโดยคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) ซึ่งคณะทำงานตรวจสอบระบบบริหาร ความมั่นคงปลอดภัยสารสนเทศภายใน (Internal ISMS Audit) คณะทำงานความมั่นคงปลอดภัยสารสนเทศ (IS Working Team) และคณะทำงานผู้ควบคุมเอกสาร (Document Controller) ต้องนำไปดำเนินการตามแนวทางที่ได้กำหนดขึ้น โดยบทบาทและหน้าที่ของแต่ละคณะมีรายละเอียด ดังนี้

3.1 คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Committee: ISMS Committee)

คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คือ บุคลากรที่ได้รับการแต่งตั้งจากอธิบดีกรมบัญชีกลาง โดยมีรายละเอียดบทบาทหน้าที่ ดังนี้

3.1.1 สนับสนุนการจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ให้มีการดำเนินงานอย่างต่อเนื่องตามมาตรฐานสากล (ISO/IEC 27001)

3.1.2 พิจารณาและสั่งการให้เกิดการดำเนินการปรับปรุงระบบบริหารความมั่นคงปลอดภัยสารสนเทศเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนด

3.1.3 ทบทวนและอนุมัติขอบเขต แผนงาน และนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) วัตถุประสงค์ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Objective) คู่มือและอื่น ๆ ที่จำเป็น

3.1.4 พิจารณาวิธีการบริหารความเสี่ยงและกำหนดระดับความเสี่ยงที่ยอมรับได้ตลอดจนพิจารณาผลการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Assessment) พิจารณาแผนการจัดการความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Treatment Plan)

3.1.5 พิจารณาผลการตรวจสอบที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เช่น ผลการตรวจติดตามภายใน (Internal ISMS Audit) และผลการตรวจสอบโดยผู้ตรวจสอบมาตรฐานสากล (Certification Audit)

3.1.6 พิจารณาและรับรองเกี่ยวกับการดำเนินมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ

3.1.7 สนับสนุนทรัพยากรที่จำเป็นเพื่อให้สามารถดำเนินมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ มาตรการลดความเสี่ยงและบริหารได้ตามกรอบที่กำหนด

3.1.8 แต่งตั้งคณะทำงานเพื่อดำเนินงานตามแผนงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

3.1.9 ติดตามและประเมินผลการดำเนินการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

3.1.10 อนุมัตินโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ ขั้นตอนปฏิบัติ/แนวทางปฏิบัติ (Procedures/Guideline) และเอกสารต่าง ๆ ที่เกี่ยวข้องในการจัดทำและพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)

3.1.11 ดำเนินการในส่วนที่เกี่ยวข้องเพื่อสนับสนุนการดำเนินงานเป็นไปตามมาตรฐานสากล (ISO/IEC 27001)

3.2 คณะทำงานความมั่นคงปลอดภัยสารสนเทศ (IS Working Team)

คณะทำงานความมั่นคงปลอดภัยสารสนเทศ คือ ตัวแทนบุคลากรที่ได้รับการแต่งตั้งจากประธานคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ ที่มีหน้าที่ในการปฏิบัติตามกรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และรายงานผลต่อคณะกรรมการฯ ซึ่งประกอบไปด้วยคณะทำงานย่อย 7 คณะ โดยมีรายละเอียดบทบาทหน้าที่ ดังนี้

3.2.1 คณะทำงานความมั่นคงปลอดภัยศูนย์คอมพิวเตอร์หลักกรมบัญชีกลาง (Data Center Team)

3.2.2 คณะทำงานความมั่นคงปลอดภัยระบบเครือข่ายและการสื่อสาร (Network Team)

3.2.3 คณะทำงานความมั่นคงปลอดภัยระบบเว็บไซต์อินเทอร์เน็ตกรมบัญชีกลาง (Website Team)

3.2.4 คณะทำงานความมั่นคงปลอดภัยระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e-GP Team)

3.2.5 คณะทำงานความมั่นคงปลอดภัยระบบงานบูรณาการฐานข้อมูลสวัสดิการสังคมและการชำระเงินของบริการภาครัฐ (Welfare & Payment Team)

3.2.6 คณะทำงานความมั่นคงปลอดภัยระบบงานบุคลากร (Person Team)

3.2.7 คณะทำงานความมั่นคงปลอดภัยระบบบาทเนต (BAHTNET Team)

คณะทำงานทั้ง 7 คณะ มีอำนาจหน้าที่ดังนี้

3.2.7.1 จัดทำวิธีการปฏิบัติ/วิธีการประเมินความเสี่ยง/วิธีการควบคุม/วิธีการวัดประสิทธิผลการควบคุม

3.2.7.2 จัดเก็บ รวบรวมข้อมูลสารสนเทศ ระบบสารสนเทศ และทรัพย์สินเพื่อประเมินความเสี่ยง

3.2.7.3 ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

3.2.7.4 วิเคราะห์และวางแผนการลดความเสี่ยงที่คาดว่าจะนำมาใช้

3.2.7.5 รายงานผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

3.2.7.6 นำแผนการลดความเสี่ยงและมาตรการควบคุมความมั่นคงปลอดภัยอื่น ๆ มาปฏิบัติ

3.2.7.7 เก็บรวบรวมผลการปฏิบัติ สรุปผลการดำเนินการ และวัดประสิทธิผลของการดำเนินการ

3.2.7.8 จัดเตรียมความพร้อมและให้ความร่วมมือในการตรวจสอบภายใน

3.2.7.9 เข้าร่วมประชุมเพื่อรายงานผลการปฏิบัติ

3.2.7.10 ดำเนินการในส่วนอื่น ๆ ที่เกี่ยวข้องตามนโยบายและคำสั่งของคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee)

3.3 คณะทำงานตรวจสอบระบบบริหารความมั่นคงปลอดภัยสารสนเทศภายใน (Internal ISMS Auditor)

คณะทำงานตรวจสอบระบบบริหารความมั่นคงปลอดภัยสารสนเทศภายใน คือ ตัวแทนบุคลากรที่ได้รับการแต่งตั้งจากประธานคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ ที่มีหน้าที่ในการตรวจสอบ ประเมินและรายงานผลการตรวจสอบการดำเนินงานของผู้เกี่ยวข้องภายในระบบบริหารจัดการความมั่นคงปลอดภัยฯ ต่อคณะกรรมการฯ โดยมีรายละเอียดบทบาทหน้าที่ ดังนี้

3.3.1 จัดทำวิธีการปฏิบัติการตรวจสอบภายในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

3.3.2 วางแผนการตรวจสอบภายในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

3.3.3 ดำเนินการตรวจสอบภายในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

3.3.4 ติดตามผลการตรวจสอบภายในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

3.3.5 รายงานผลการตรวจสอบภายในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

3.3.6 ดำเนินการในส่วนอื่น ๆ ที่เกี่ยวข้องตามนโยบายและคำสั่งของคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee)

3.4 คณะทำงานผู้ควบคุมเอกสาร (Document Controller)

คณะทำงานผู้ควบคุมเอกสาร คือ ตัวแทนบุคลากรที่ได้รับการแต่งตั้งประธานคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ ที่มีหน้าที่ในการควบคุมทะเบียนเอกสารที่เกี่ยวข้องภายในระบบบริหารจัดการความมั่นคงปลอดภัยฯ ประสานงานกับผู้เกี่ยวข้องเพื่อจัดการด้านเอกสาร โดยมีรายละเอียดบทบาทหน้าที่ ดังนี้

3.4.1 จัดทำวิธีการปฏิบัติการควบคุมเอกสาร

3.4.2 ประสานงานกับคณะทำงานเพื่อการขึ้นทะเบียน การขอแก้ไขเอกสาร การแจกจ่าย และการยกเลิกทะเบียนเอกสาร

3.4.3 ดำเนินการในส่วนอื่น ๆ ที่เกี่ยวข้องตามนโยบายและคำสั่งของคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee)

3.5 กรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

การให้บริการจัดการความมั่นคงปลอดภัยสารสนเทศของกรมบัญชีกลาง กำหนดให้ผู้เกี่ยวข้องประกอบด้วย คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ คณะทำงานความมั่นคงปลอดภัยสารสนเทศ คณะทำงานผู้ควบคุมเอกสาร คณะทำงานตรวจสอบระบบบริหารความมั่นคงปลอดภัยสารสนเทศภายใน ต้องดำเนินการตามขั้นตอนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศซึ่งประกอบด้วย

3.5.1 ระยะการวางแผน คือ ระยะที่ใช้ในการเตรียมการ โดยประกอบด้วยกิจกรรมการกำหนด หรือทบทวนขอบเขตการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การกำหนดหรือทบทวนนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การกำหนดขั้นตอนการปฏิบัติการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ การประเมินความเสี่ยงฯ และการพิจารณาแนวทางการตอบสนองความเสี่ยง

3.5.2 ระยะการดำเนินการ คือ ระยะการนำแผนการตอบสนองความเสี่ยง และมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศมาประยุกต์ใช้ โดยเริ่มตั้งแต่การอบรม การควบคุมตามมาตรการที่กำหนดไว้ การกำหนดวิธีการวัดประสิทธิผล และการเตรียมการตรวจสอบภายใน

3.5.3 ระยะการตรวจสอบ คือ ระยะการติดตามและตรวจสอบผลการดำเนินการซึ่งประกอบด้วย การวัดประสิทธิผล การตรวจสอบภายใน การประชุมเพื่อติดตามผล และการสั่งการเพื่อให้เกิดการปรับปรุง

3.5.4 ระยะการแก้ไข คือ ระยะการนำผลที่ได้จากการติดตามและการตรวจสอบมาปรับปรุงหรือแก้ไข ทั้งที่อยู่ในรูปแบบแก้ไขความผิดพลาด (Corrective) และปรับปรุงเพื่อป้องกัน (Preventive) ซึ่งอาศัยหลักการคิดวิเคราะห์และแยกแยะสาเหตุปัญหาก่อนการดำเนินการ

4. แนวปฏิบัติ

เพื่อให้กำหนดนโยบายการควบคุมการใช้งานระบบสารสนเทศให้มีความมั่นคงปลอดภัยและเกิดประสิทธิภาพ กรมบัญชีกลางได้ดำเนินการกำหนดนโยบายตามมาตรฐาน ISO/IEC 27001 สำหรับมาตรฐานการรักษาความมั่นคงปลอดภัย ซึ่งสาระสำคัญของมาตรฐานดังกล่าวประกอบด้วย 11 หัวข้อหลักดังนี้

4.1 นโยบายความมั่นคงปลอดภัย (Security policy)

ประกอบด้วยนโยบายความมั่นคง ปลอดภัยสำหรับสารสนเทศ ซึ่งมีวัตถุประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง โดยผู้บริหารองค์กรจะต้องมีการจัดทำนโยบายที่เป็นลายลักษณ์อักษร รวมถึงการทบทวนนโยบายตามระยะเวลาที่กำหนดหรือมีการเปลี่ยนแปลงที่สำคัญขององค์กร

4.2 โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Internal organization)

โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Internal organization) หมายถึง บทบาทของผู้บริหารองค์กรและหัวหน้างานสารสนเทศ ในด้านต่าง ๆ ดังต่อไปนี้

4.2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

4.2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

4.3 การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

การบริหารจัดการทรัพย์สินขององค์กร (Asset management) หมายถึง บทบาทของหัวหน้างานสารสนเทศและหัวหน้างานพัสดุในด้านต่าง ๆ ดังต่อไปนี้

4.3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจขึ้นได้

4.3.2 การจัดหมวดหมู่สารสนเทศ เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

4.4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security) หมายถึง บทบาทของผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ หัวหน้างานบุคคลและหัวหน้างานที่เกี่ยวข้องในต่าง ๆ ดังต่อไปนี้

4.4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

4.4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบและทำความเข้าใจกับนโยบาย เพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

4.4.3 การสิ้นสุดและการเปลี่ยนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

4.4.4 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security) หมายถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานอาคารในด้านต่าง ๆ ดังต่อไปนี้

4.4.4.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

4.4.4.2 ความมั่นคงปลอดภัยของอุปกรณ์ เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และทำให้กิจกรรมการดำเนินงานต่าง ๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

4.4.5 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management) หมายถึงบทบาทของผู้บริหารองค์กร ผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจ และพนักงานสารสนเทศในด้านต่าง ๆ ดังต่อไปนี้

4.4.5.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

4.4.5.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

4.4.5.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

4.4.5.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

4.4.5.5 การสำรองข้อมูล เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

4.4.5.6 การบริหารจัดการทางด้านความปลอดภัยสำหรับเครือข่ายขององค์กร เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

4.4.5.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ

4.4.5.8 การแลกเปลี่ยนสารสนเทศ เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

4.4.5.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน

4.4.5.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

4.4.6 การควบคุมการเข้าถึง (Access control) หมายถึงบทบาทของผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ ผู้ดูแลระบบและพนักงานในด้านต่าง ๆ ดังต่อไปนี้

4.4.6.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศเพื่อควบคุมการเข้าถึงสารสนเทศ

4.4.6.2 การบริหารจัดการการเข้าถึงของผู้ใช้ เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.4.6.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

4.4.6.4 การควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต

4.4.6.5 การควบคุมการเข้าถึงระบบปฏิบัติการที่ไม่ได้รับอนุญาต

4.4.6.6 การควบคุมการเข้าถึง Application และสารสนเทศที่ไม่ได้รับอนุญาต

4.4.6.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกเพื่อสร้างความมั่นคงปลอดภัยให้กับอุปกรณ์และการปฏิบัติงานที่เกี่ยวข้อง

4.4.7 การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance) หมายถึง บทบาทของหัวหน้างานสารสนเทศ ผู้พัฒนาระบบ และผู้เป็นเจ้าของระบบในด้านต่าง ๆ ดังต่อไปนี้

4.4.7.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศเพื่อให้การจัดหาและพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

4.4.7.2 การประมวลผลสารสนเทศใน Application เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์

4.4.7.3 มาตรการการเข้ารหัสข้อมูลเพื่อรักษาความลับของข้อมูลยืนยันตัวตนของผู้ส่งข้อมล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการทางการเข้ารหัสข้อมูล

4.4.7.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

4.4.7.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุนเพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

4.4.7.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

4.4.8 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management) หมายถึงบทบาทของหัวหน้างานสารสนเทศ หัวหน้างานนิติกร ผู้ดูแลระบบและพนักงานในด้านต่าง ๆ ดังต่อไปนี้

4.4.8.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

4.4.8.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

4.4.9 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management) หมายถึงบทบาทของผู้บริหารสารสนเทศ และหัวหน้างานสารสนเทศ ที่เกี่ยวกับหัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

4.4.10 การปฏิบัติตามข้อกำหนด (Compliance) หมายถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานนิติกร ในด้านต่าง ๆ ดังต่อไปนี้

4.4.10.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ

4.4.10.2 การปฏิบัติตามนโยบาย มาตรฐานความปลอดภัยและข้อกำหนดทางเทคนิค เพื่อให้ระบบเป็นตามนโยบายและมาตรฐานความมั่นคงปลอดภัยตามที่องค์กรกำหนดไว้

4.4.10.3 การตรวจประเมินระบบสารสนเทศ เพื่อตรวจประเมินระบบสารสนเทศให้ได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

สรุป

1. การวิเคราะห์เรื่องการตระหนักรู้ของบุคลากรของกรมบัญชีกลาง

ในการวิเคราะห์ส่วนนี้จะเป็นการรวบรวมข้อมูลโดยการสังเกตการณ์ลักษณะพฤติกรรมการใช้งานเครื่องคอมพิวเตอร์ของบุคลากรกับข้อมูลการจราจรทางคอมพิวเตอร์รวมถึงการติดไวรัสของเครื่องคอมพิวเตอร์ โดยนำข้อมูลที่ได้มาสร้างเหตุการณ์การฝึกอบรมเพื่อสร้างการตระหนักรู้ จากการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศที่ผ่านมา เรื่องการรับรู้เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศได้ผลลัพธ์บุคคลกรที่เข้ารับการอบรมมีความเข้าใจในเรื่องความมั่นคงปลอดภัยที่ดีขึ้นแต่ต้องมีการสร้างรับรู้อย่างต่อเนื่องเพื่อให้บุคลากรมีความเข้าใจกับภัยคุกคามที่เป็นปัจจุบันมากขึ้น

2. วิเคราะห์เทคโนโลยีในปัจจุบันที่เหมาะสมกับกรมบัญชีกลาง

ด้วยเทคโนโลยีด้านความมั่นคงปลอดภัยในปัจจุบันมีการพัฒนาศักยภาพอย่างต่อเนื่องและในศูนย์เทคโนโลยีสารสนเทศได้มีการเตรียมจัดหาอุปกรณ์มีเพิ่มประสิทธิภาพในการเฝ้าระวังและ

รับมือกับภัยคุกคาม แต่ในบางระบบงานโดยเฉพาะระบบงานที่พัฒนาบนเทคโนโลยีเก่ายังคงมีช่องโหว่อยู่ ดังนั้นเพื่อให้การเฝ้าระวังมีประสิทธิภาพมากขึ้นจำเป็นต้องจัดหาอุปกรณ์เพิ่มเติม พร้อมทั้งระบบงานถ้าสามารถปรับปรุงแก้ไขได้ควรต้องมีแผนในการแก้ไข

3. วิเคราะห์นโยบายผู้บริหารที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

จากการที่สัมภาษณ์และสังเกตการณ์การสนับสนุนการดำเนินการในด้านความมั่นคงปลอดภัยสารสนเทศ พบว่าผู้บริหารได้ให้ความสำคับในการดำเนินการให้ระบบงานรวมถึงการให้บริการมีความมั่นคงปลอดภัยสารสนเทศและมีความน่าเชื่อถือ ทำให้ในการดำเนินการกำหนดนโยบายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศได้รับการผลักดันจากผู้บริหาร

4. วิเคราะห์ความตระหนักหรือการรับรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

ในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรกรมบัญชีกลาง ยังมีความเข้าใจในเรื่องความมั่นคงปลอดภัยสารสนเทศ ทำให้ในการจัดอบรมการสร้างความตระหนักรู้ต้องทำอย่างต่อเนื่องและต้องมีตัวอย่างให้ผู้เข้ารับการอบรมมีส่วนร่วม จะทำให้เกิดความเข้าใจมากขึ้นและเกิดความตระหนักรู้ในการใช้เทคโนโลยีสารสนเทศให้ปลอดภัย

5. วิเคราะห์การกำหนดนโยบายความมั่นคงปลอดภัยที่เหมาะสมกับกรมบัญชีกลาง

ในการกำหนดนโยบายความมั่นคงปลอดภัยที่เหมาะสมกับกรมบัญชีกลาง จำเป็นจะต้องให้บุคลากรกรมบัญชีกลางมีส่วนร่วมในการบังคับใช้นโยบายฯ เพราะในการบังคับใช้นโยบายฯ ต้องให้ผู้ถูกบังคับใช้นโยบาย มีความรู้และเข้าใจในวัตถุประสงค์ของนโยบายที่กำหนด

บทสรุปการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ มีปัจจัยสำคัญที่ “ตัวบุคคล” ดังนั้นการเตรียมความพร้อมในการสร้างภูมิคุ้มกันให้ผู้ใช้ระบบสารสนเทศทั่วไป และ การให้ความรู้ด้านภัยคุกคามทางไซเบอร์ จึงเป็นเรื่องจำเป็น และต้องสร้างให้บุคลากรเหล่านั้นมีทักษะในการปฏิบัติงานในองค์กรตลอดจนผู้บริหารทั้งระดับกลางและระดับสูง ได้ตระหนักรู้และสร้างประสบการณ์ในการรับมือกับภัยคุกคามทางไซเบอร์ ปฏิบัติและมีความพร้อมต่อการรับมือกับเหตุการณ์ต่าง ๆ ที่จะเกิดขึ้น นอกจากนี้ กลไก กระบวนการ และเทคนิคในการตรวจจับความผิดปกติในระบบแบบ Real-Time ก็มี ความจำ เป็นเช่นกัน เพราะฉะนั้นเราจึงต้องเตรียมพร้อมกับเหตุการณ์ที่ไม่พึงประสงค์ ตลอดเวลา ก็จะช่วยให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีประสิทธิผล มากขึ้นโดยลำดับ

บทที่ 4
ปฏิรูปนโยบายความมั่นคงปลอดภัยสารสนเทศ

ความเป็นมาและความสำคัญของปัญหา

ความมั่นคงปลอดภัยไซเบอร์ ถือว่ามีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้นการที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีกระบวนการในการดำเนินการ โดยเลือกมาตรฐานสากลแล้วนำมาประยุกต์ใช้ให้เหมาะสมกับองค์กร และต้องสอดคล้องตามกฎหมายต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ยุทธศาสตร์ชาติ จึงนำมาสู่การปฏิรูปนโยบายความมั่นคงสารสนเทศ

กระบวนการในการปฏิรูปนโยบายความมั่นคงปลอดภัยสารสนเทศ

สิ่งสำคัญที่จะต้องดำเนินการก็คือการศึกษาปัจจัยภายในและภายนอกของกรมบัญชีกลางเพื่อวิเคราะห์หาสถานภาพความเสี่ยงและขอบเขตของระบบความมั่นคงปลอดภัยสารสนเทศ รวมทั้งศึกษาความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย เพื่อกำหนดนโยบายและวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

1. ปัจจัยภายใน

ปัจจัยภายในเป็นการศึกษาปัจจัยภายในที่จะมีผลกระทบต่อการปฏิรูปนโยบายความมั่นคงสารสนเทศ

1.1 ลักษณะองค์กรของกรมบัญชีกลาง

กรมบัญชีกลาง มีภารกิจเกี่ยวกับการควบคุมดูแลการใช้จ่ายเงินแผ่นดินและของหน่วยงานภาครัฐให้เป็นไปโดยถูกต้อง มีวินัย คุ้มค่า โปร่งใส และสามารถตรวจสอบได้ โดยการวางกรอบหลักเกณฑ์กลางให้หน่วยงานภาครัฐถือปฏิบัติ การให้บริการคำแนะนำปรึกษาด้านการเงิน การคลัง การบัญชีการตรวจสอบภายใน การบริหารเงินนอกงบประมาณ และการพัสดุภาครัฐ การดำเนินการเกี่ยวกับการบริหารเงินคงคลังให้มีใช้จ่ายอย่างเพียงพอ และการเสนอข้อมูลในเชิงนโยบายการคลังแก่ฝ่ายบริหาร โดยประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อให้เกิดเสถียรภาพทางการคลัง รวมทั้งดำเนินการเกี่ยวกับการประเมินผลการคลังภาครัฐ การกำกับดูแลนโยบายและมาตรฐานค่าตอบแทนสวัสดิการ และสิทธิประโยชน์ของบุคลากรภาครัฐ

1.2 วิสัยทัศน์ของกรมบัญชีกลาง กำกับดูแลและบริหารการใช้จ่ายเงินของแผ่นดินให้เกิดประโยชน์สูงสุด

1.3 พันธกิจของกรมบัญชีกลาง กรมบัญชีกลางได้กำหนดพันธกิจของกรมบัญชีกลาง 5 พันธกิจ ดังนี้

1.3.1 กำหนดมาตรฐาน หลักเกณฑ์ แนวปฏิบัติด้านกฎหมายการคลัง การบัญชี การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ การตรวจสอบภายใน ค่าตอบแทนและ

สวัสดิการ เงินนอกงบประมาณ ลูกจ้าง และความรับผิดทางละเมิดของเจ้าหน้าที่ของรัฐให้สอดคล้องกับการรักษาวินัยและความยั่งยืนทางการคลัง

1.3.2 บริหารเงินสดภาครัฐ บริหารการรับ-จ่ายเงิน ให้เป็นไปอย่างมีประสิทธิภาพโดยใช้ระบบเทคโนโลยีที่ทันสมัย

1.3.3 สนับสนุนการบริหารเศรษฐกิจการคลังในส่วนภูมิภาค

1.3.4 พัฒนาขีดความสามารถของบุคลากรภาครัฐทางด้านการบริหารการเงินภาครัฐ

1.3.5 เป็นศูนย์ข้อมูลสารสนเทศทางการคลัง

1.4 ยุทธศาสตร์ของกรมบัญชีกลาง ยุทธศาสตร์กรมบัญชีกลาง ประกอบด้วย 3 ประเด็นยุทธศาสตร์ ดังนี้

ตารางที่ 4-1 ตารางยุทธศาสตร์กรมบัญชีกลาง

ยุทธศาสตร์ที่ 1 :	การเป็นกลไกหลักของนโยบายการคลังที่ขับเคลื่อนการฟื้นตัวของเศรษฐกิจไทย (Fiscal Stimulus)
ยุทธศาสตร์ที่ 2 :	การปรับภาวะการคลังให้เข้าสู่สมดุล (Fiscal Consolidation)
ยุทธศาสตร์ที่ 3 :	การเสริมสร้างความเข้มแข็งขององค์กร (Strengthen the CGD organization)

ที่มา : ศูนย์เทคโนโลยีสารสนเทศกรมบัญชีกลาง แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง พ.ศ. 2557 – 2561 (ระยะ 5 ปี) ,2557

1.5 ยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง กรมบัญชีกลางได้กำหนดยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง

1.5.1 สร้างนวัตกรรมด้าน ICT เพื่อตอบสนองความต้องการในการกำกับดูแลและบริหารการใช้จ่ายเงินของแผนดินอย่างมีประสิทธิภาพและทันสมัย

1.5.2 เพิ่มประสิทธิภาพและสนับสนุนให้มีการใช้เทคโนโลยีสารสนเทศและการสื่อสารภายในองค์กรอย่างครบวงจร

1.5.3 เพิ่มช่องทางการให้บริการในลักษณะ e-server ผ่านอุปกรณ์สื่อสารเคลื่อนที่ต่าง ๆ (Mobile Devices) ให้กับข้าราชการ ประชาชน และส่วนราชการหรือหน่วยงานที่เกี่ยวข้อง

1.5.4 ยกระดับการบริการอิเล็กทรอนิกส์ของกรมฯ โดยการมีส่วนร่วมของผู้เกี่ยวข้องกับภารกิจของกรมฯ ในแนวทาง Smart Service โดยการบริการอิเล็กทรอนิกส์ของกรมฯ หรือ e-CGD Service ภายใต้การให้บริการแบบไร้รอยต่อ/ไร้ตะเข็บรอยต่อ (Seamless) ระหว่างกรมบัญชีกลางกับผู้รับบริการ/ผู้เกี่ยวข้อง (เช่น หน่วยงาน/ส่วนราชการ บุคลากรภาครัฐ

ผู้มีสิทธิ์/ผู้อาศัย/ทายาทของบุคลากรภาครัฐ ประชาชนและภาคเอกชน) เพื่อก้าวไปสู่การพัฒนาบริการอิเล็กทรอนิกส์ด้านข้อมูลข่าวสาร เอกสาร และการมีส่วนร่วมของผู้รับบริการ/ผู้เกี่ยวข้อง เพิ่มมูลค่าเพิ่มให้กับระบบสารสนเทศในปัจจุบันของกรมบัญชีกลางอย่างเป็นรูปธรรม เพื่อประโยชน์เชิงการบริหารทุกมิติอย่างครบวงจร เพิ่มประสิทธิภาพการบริหารจัดการภายในและเพิ่มศักยภาพของบุคลากรภายในกรมบัญชีกลาง ปรับปรุงระบบการให้บริการและระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารไปสู่มาตรฐานสากล

1.6 นโยบายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ กรมบัญชีกลางได้ประกาศนโยบายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ 1 ฉบับ คือ นโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมบัญชีกลาง (Information Security Policy)

2. ปัจจัยภายนอก

2.1 กฎหมายด้านเทคโนโลยีสารสนเทศ กรมบัญชีกลางมีกฎหมายด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง ดังนี้

2.1.1 พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537

2.1.2 พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558

2.1.3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

2.1.4 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

2.1.5 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

2.1.6 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

2.1.7 พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

2.1.8 พระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

2.1.9 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

2.1.10 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

2.1.11 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556

2.1.12 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555

2.1.13 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องรายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559

2.1.14 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

2.1.15 ประกาศธนาคารแห่งประเทศไทยที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต

2.2 การวิเคราะห์ SWOT จากการสัมภาษณ์คณะทำงานฯ กรมบัญชีกลาง ซึ่งสรุปจุดแข็ง จุดอ่อน โอกาส และอุปสรรค ของระบบเทคโนโลยีสารสนเทศของกรมบัญชีกลาง ดังนี้ (ศูนย์เทคโนโลยีสารสนเทศกรมบัญชีกลาง แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง พ.ศ. 2557 – 2561 (ระยะ 5 ปี) ,2557)

2.2.1 จุดแข็ง (Strengths) จากการศึกษาจุดแข็งของกรมบัญชีกลาง สรุปได้เป็น 2 ประเด็น ดังนี้

ตารางที่ 4-2 ตารางสรุปจุดแข็งของกรมบัญชีกลาง

ลำดับ	รายละเอียด
S1	บุคลากรมีจิตบริการ มีความมุ่งมั่น อดทน และรับผิดชอบในการทำงาน
S2	กรมบัญชีกลางมีการบริหารจัดการแบบรวมศูนย์ เชื่อมโยง บูรณาการ

2.2.2 จุดอ่อน (Weaknesses) จากการศึกษาจุดอ่อนของกรมบัญชีกลาง สรุปได้เป็น 3 ประเด็น ดังนี้

ตารางที่ 4-3 ตารางสรุปจุดอ่อนของกรมบัญชีกลาง

ลำดับ	รายละเอียด
W1	บุคลากรมีความรู้ความสามารถไม่เพียงพอ
W2	บุคลากรไม่เพียงพอต่อการปฏิบัติงาน
W3	อุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศไม่ทันสมัยและไม่เพียงพอ

2.2.3 โอกาส (Opportunities) จากการศึกษาโอกาสของกรมบัญชีกลาง สรุปได้เป็น 3 ประเด็น ดังนี้

ตารางที่ 4-4 ตารางสรุปโอกาสของกรมบัญชีกลาง

ลำดับ	รายละเอียด
O1	นโยบายภาครัฐส่งเสริมการดำเนินงานด้านเทคโนโลยีสารสนเทศของกรมบัญชีกลาง
O2	กรมบัญชีกลางได้รับความเชื่อถือในด้านการให้บริการที่ดี
O3	หน่วยงานกำกับดูแลของกรมบัญชีกลางให้ความสำคัญในด้านความมั่นคงปลอดภัยสารสนเทศ

2.2.4 อุปสรรค (Threats) จากการศึกษาอุปสรรคของกรมบัญชีกลาง สรุปได้เป็น 3 ประเด็น ดังนี้

ตารางที่ 4-5 ตารางสรุปอุปสรรคของกรมบัญชีกลาง

ลำดับ	รายละเอียด
T1	การจัดสรรงบประมาณไม่เพียงพอ
T2	นโยบายภาครัฐทางด้านเทคโนโลยีสารสนเทศ เช่น โครงการสวัสดิการภาครัฐ โดยมีนโยบายให้กรมบัญชีกลางต้องดำเนินการ แต่ไม่มีอัตรากำลังคนเพิ่ม ทำให้กรมบัญชีกลางต้องจัดสรรบุคลากร เพื่อมาทำหน้าที่เพิ่มเติม
T3	การโจมตีด้านไซเบอร์

2.2.5 การวิเคราะห์สถานภาพความเสี่ยง จากการวิเคราะห์สถานภาพความเสี่ยงของกรมบัญชีกลางจากการวิเคราะห์ SWOT พบประเด็นที่เกี่ยวข้องทั้งสิ้น 11 ประเด็น ได้ศึกษาแนวทางตอบสนองต่อความเสี่ยงเบื้องต้นแบ่งเป็น 5 โครงการ ดังตารางที่ 5 โดยมีรายละเอียดความสัมพันธ์ระหว่างโครงการและผลการวิเคราะห์ SWOT

ตารางที่ 4-6 ตารางแสดงชื่อโครงการจากผลการวิเคราะห์สถานภาพความเสี่ยง

ลำดับโครงการ	ชื่อโครงการ
PJ01	จัดทำแผนส่งเสริมสมรรถนะของบุคลากร
PJ02	จัดทำแผนสรรหาทรัพยากรบุคคล
PJ03	โครงการเพิ่มประสิทธิภาพการใช้ระบบเทคโนโลยีสารสนเทศของกรมบัญชีกลาง
PJ04	การสำรวจการปฏิบัติตามกฎหมาย ประกาศด้านเทคโนโลยีสารสนเทศที่กรมบัญชีกลางต้องปฏิบัติตาม
PJ05	จัดทำแผนตอบสนองเมื่อเกิดเหตุการณ์ถูกโจมตีด้านไซเบอร์

ตารางที่ 4-7 ตารางแสดงความสัมพันธ์ระหว่างโครงการและผลการวิเคราะห์ SWOT

ลำดับของ SWOT	รายละเอียด	ลำดับโครงการ	ชื่อโครงการ
S1	บุคลากรมีจิตบริการ มีความมุ่งมั่น อดทน และรับผิดชอบในการทำงาน	-	N/A
S2	กรมบัญชีกลางมีการบริหารจัดการแบบรวมศูนย์ เชื่อมโยงบูรณาการ	-	N/A
W1	บุคลากรมีความรู้ความสามารถไม่เพียงพอ	PJ01	จัดทำแผนส่งเสริมสมรรถนะของบุคลากร
W2	บุคลากรไม่เพียงพอต่อการปฏิบัติงาน	PJ02	จัดทำแผนสรรหาทรัพยากรบุคคล
W3	อุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศไม่ทันสมัยและไม่เพียงพอ	PJ03	โครงการเพิ่มประสิทธิภาพการใช้ระบบเทคโนโลยีสารสนเทศของกรมบัญชีกลาง
O1	นโยบายภาครัฐส่งเสริมการดำเนินงานด้านเทคโนโลยีสารสนเทศของกรมบัญชีกลาง	-	N/A
O2	กรมบัญชีกลางได้รับความเชื่อถือในด้านการให้บริการที่ดี	-	N/A
O3	หน่วยงานกำกับดูแลของกรมบัญชีกลางให้ความสำคัญในด้านความมั่นคงปลอดภัยสารสนเทศ	PJ04	การสำรวจการปฏิบัติตามกฎหมายประกาศด้านเทคโนโลยีสารสนเทศที่กรมบัญชีกลางต้องปฏิบัติตาม
T1	การจัดสรรงบประมาณไม่เพียงพอ	-	N/A

ตารางที่ 4-7 ตารางแสดงความสัมพันธ์ระหว่างโครงการและผลการวิเคราะห์ SWOT (ต่อ)

ลำดับของ SWOT	รายละเอียด	ลำดับโครงการ	ชื่อโครงการ
T2	นโยบายภาครัฐทางด้านเทคโนโลยีสารสนเทศ เช่น โครงการสวัสดิการภาครัฐ โดยมีนโยบายให้กรมบัญชีกลางต้องดำเนินการ แต่ไม่มีอัตรากำลังคนเพิ่ม ทำให้กรมบัญชีกลางต้องจัดสรรบุคลากร เพื่อมาทำหน้าที่เพิ่มเติม	-	N/A
T3	การโจมตีด้านไซเบอร์	PJ05	จัดทำแผนตอบสนองเมื่อเกิดเหตุการณ์ถูกโจมตีด้านไซเบอร์

2.3 ผู้มีส่วนได้ส่วนเสีย กรมบัญชีกลางมีผู้มีส่วนได้ส่วนเสียแบ่งเป็น 2 กลุ่ม คือ ผู้มีส่วนได้ส่วนเสียภายในองค์กร และผู้มีส่วนได้ส่วนเสียภายนอกองค์กร โดยมีรายละเอียดดังนี้

2.3.1 ผู้มีส่วนได้ส่วนเสียภายในองค์กร

ผู้บริหาร หมายถึง อธิบดี ที่ปรึกษา รองอธิบดี ผู้อำนวยการ ผู้เชี่ยวชาญ

เจ้าหน้าที่ หมายถึง ข้าราชการระดับชำนาญการพิเศษลงมา พนักงานราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว

2.3.2 ผู้มีส่วนได้ส่วนเสียภายนอกองค์กร

หน่วยงานกำกับดูแล หมายถึง หน่วยงานกับกำดูแลกรมบัญชีกลางทั้งทางตรงและทางอ้อม เช่น กระทรวงการคลัง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ผู้ใช้บริการ หมายถึง ผู้ใช้บริการของกรมบัญชีกลาง

ผู้ให้บริการภายนอก หมายถึง ผู้ที่ส่งมอบผลิตภัณฑ์หรือบริการให้กับกรมบัญชีกลาง

2.3.3 ศึกษาความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสีย กรมบัญชีกลางศึกษาความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียภายในและภายนอกองค์กรสรุปได้ดังนี้

2.3.3.1 ความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียภายในองค์กร

ตารางที่ 4-8 ตารางความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียภายในองค์กร

ผู้มีส่วนได้ส่วนเสียภายในองค์กร	ความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย
ผู้บริหาร	☐ เจ้าหน้าที่มีความตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ ☐ ระบบสารสนเทศมีความพร้อมใช้งานและตอบสนองต่อเหตุการณ์ที่อาจจะเกิดขึ้น ☐ กรมบัญชีกลางผ่านการรับรองมาตรฐาน ISO/IEC 27001 เพื่อให้มีความน่าเชื่อถือ ☐ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศได้รับการทบทวนให้เป็นปัจจุบัน
เจ้าหน้าที่	☐ ระบบสารสนเทศมีความพร้อมใช้งานและตอบสนองต่อเหตุการณ์ที่อาจจะเกิดขึ้น ☐ ได้รับความรู้ ความตระหนักด้านความมั่นคงปลอดภัย ☐ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศได้รับการทบทวนให้เป็นปัจจุบัน

2.3.3.2 ความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียภายนอกองค์กร

ตารางที่ 4-9 ตารางความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียภายนอกองค์กร

ผู้มีส่วนได้ส่วนเสียภายนอกองค์กร	ความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย
หน่วยงานกำกับดูแล	☐ ปฏิบัติตามกฎระเบียบ กฎหมาย ที่เกี่ยวข้อง
ผู้ใช้บริการ	☐ มั่นใจได้ว่าระบบสารสนเทศที่ใช้ของกรมบัญชีกลางมีความพร้อมใช้ ☐ ใช้บริการที่มีการคำนึงถึงความมั่นคงปลอดภัย และเชื่อถือได้
ผู้ให้บริการภายนอก	☐ ระบบสารสนเทศมีความพร้อมใช้งานและตอบสนองต่อเหตุการณ์ที่อาจจะเกิดขึ้น

3. นโยบายความมั่นคงที่เหมาะสมกับกรมบัญชีกลาง

จากการศึกษาและวิเคราะห์ข้างต้น ทำให้กรมบัญชีกลางสามารถกำหนดนโยบายความมั่นคงปลอดภัยให้กับองค์กรได้อย่างเหมาะสม โดยมุ่งมั่นที่จะพัฒนาการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง จึงกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของกรมบัญชีกลางไว้ดังนี้

3.1 มุ่งมั่นให้กรมบัญชีกลางให้บริการประชาชนอย่างมีมาตรฐาน

3.2 มุ่งมั่นที่จะให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและให้บริการได้อย่างต่อเนื่อง

3.3 มุ่งมั่นที่จะให้การปฏิบัติงานของเจ้าหน้าที่กรมบัญชีกลางเป็นไปอย่างเป็นระบบและมีความมั่นคงปลอดภัย

3.4 มุ่งมั่นที่จะปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

4 สรุปแนวทางในการปฏิรูปนโยบายให้มีความสมบูรณ์และเหมาะสมกับบุคลากรกรมบัญชีกลาง

4.1 ปฏิรูปนโยบายความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ปฏิรูปนโยบายความมั่นคงปลอดภัยสารสนเทศ และเป็นไปตามมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 จึงได้ให้นโยบายในการกำหนดขอบเขตระบบงานที่เป็นระบบงานหลักและมีความสำคัญ โดยเฉพาะทางด้านการเงินของกรมบัญชีกลาง เพื่อขอรับรองระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) ISO/IEC 27001:2005 ใน 3 ขอบเขต ดังนี้

4.1.1 ศูนย์คอมพิวเตอร์หลักกรมบัญชีกลาง โดยรวมถึง ระบบควบคุมสภาพความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and System Environmental Control System) และโครงสร้างพื้นฐานการควบคุมความมั่นคงปลอดภัยทางเครือข่าย (Network Security Control Infrastructure) โดยครอบคลุมถึง

4.1.1.1 การให้บริการพื้นที่สำหรับระบบคอมพิวเตอร์

4.1.1.2 การควบคุมการเข้าถึงทางกายภาพภายในศูนย์ข้อมูลกลาง

4.1.1.3 การติดตามผ่านระบบกล้องวงจรปิด

4.1.1.4 การควบคุมสภาพแวดล้อมทางกายภาพ

4.1.1.5 การบำรุงรักษาระบบและอุปกรณ์

4.1.1.6 การติดตามโครงสร้างการให้บริการศูนย์ข้อมูลกลางขั้นพื้นฐาน

4.1.1.7 การบริหารจัดการสิทธิ

4.1.1.8 การบริหารจัดการผู้ให้บริการภายนอก

4.1.1.9 การควบคุมการเข้าถึงทางเครือข่าย

4.1.1.10 การควบคุมการเชื่อมโยงเครือข่าย

4.1.1.11 การติดตามโครงสร้างการให้บริการเครือข่าย

4.1.1.12 การป้องกันโปรแกรมไม่ประสงค์ดี

4.1.1.13 การเฝ้าระวังระบบและอุปกรณ์

4.1.1.14 การสำรองข้อมูล

4.1.1.15 การควบคุมการเปลี่ยนแปลง

4.1.1.16 การบริหารจัดการอุบัติการณ์

4.1.2 ชุดคอมพิวเตอร์ลูกข่ายระบบบาทเนต (BAHTNET) ของกรมบัญชีกลาง สำหรับการปฏิบัติงานจริงและสำหรับเป็นชุดสำรองที่ใช้เชื่อมโยงกับระบบบาทเนตของธนาคารแห่งประเทศไทย ได้แก่ ระบบคอมพิวเตอร์สำหรับบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (Electronic Financial Services) หรือระบบงานคอมพิวเตอร์อื่นที่เชื่อมโยงเพื่อการรับส่งข้อมูลโดยระบบคอมพิวเตอร์แม่ข่ายของธนาคารแห่งประเทศไทย (Host o Host) ครอบคลุมทั้งศูนย์คอมพิวเตอร์ และพื้นที่ปฏิบัติงานสำรอง

4.1.2.1 การบำรุงดูแลอุปกรณ์คอมพิวเตอร์

4.1.2.2 การจัดการสมรรถนะระบบ

4.1.2.3 การสำรองข้อมูล

4.1.2.4 การบริหารจัดการผู้ให้บริการภายนอก

4.1.2.5.การควบคุมการลงทะเบียนผู้ดูแลระบบ

4.1.2.6 การบริหารจัดการอุบัติการณ์

4.1.2.7 การควบคุมการใช้งานลิขสิทธิ์

4.1.2.8 การควบคุมการเปลี่ยนแปลง

4.1.2.9 การเฝ้าระวังระบบและอุปกรณ์

4.1.3 การให้บริการระบบคอมพิวเตอร์แม่ข่ายของระบบงาน ประกอบด้วยระบบคอมพิวเตอร์แม่ข่ายของระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e-Government Procurement: e-GP) และระบบบูรณาการฐานข้อมูลสวัสดิการสังคม (e-Social Welfare) โดยครอบคลุมถึง

4.1.3.1 การบำรุงดูแลอุปกรณ์คอมพิวเตอร์

4.1.3.2 การจัดการสมรรถนะระบบ

4.1.3.3 การสำรองข้อมูล

4.1.3.4 การบริหารจัดการผู้ให้บริการภายนอก

4.1.3.5 การควบคุมการลงทะเบียนผู้ดูแลระบบ

4.1.3.6 การบริหารจัดการอุบัติการณ์

4.1.3.7 การควบคุมการใช้งานลิขสิทธิ์

4.1.3.8 การควบคุมการเปลี่ยนแปลง

4.1.3.9 การเฝ้าระวังระบบและอุปกรณ์

พร้อมทั้งกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Objectives) เพื่อตอบสนองต่อความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย โดยมีวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ จำนวน 5 วัตถุประสงค์ ดังนี้

วัตถุประสงค์ที่ 1 OBJ01 เพื่อขอรับรองมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัย ISO/IEC 27001:2013

วัตถุประสงค์ที่ 2 OBJ02 เพื่อบริหารจัดการให้ระบบสามารถให้บริการได้ตามเกณฑ์ที่กำหนด

วัตถุประสงค์ที่ 3 OBJ03 เพื่อทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์ที่ 4 OBJ04 เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์ที่ 5 OBJ05 เพื่อให้กรมบัญชีกลางสามารถปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

ตารางที่ 4-10 ตารางสรุปความสัมพันธ์ของความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียกับวัตถุประสงค์และนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

ผู้มีส่วนได้ส่วนเสียภายในองค์กร	ความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย	วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
ความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียภายในองค์กร			
ผู้บริหาร	เจ้าหน้าที่มีความตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ	OBJ04 เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ	มุ่งมั่นที่จะให้การปฏิบัติงานของเจ้าหน้าที่กรมบัญชีกลางเป็นไปอย่างเป็นระบบและมีความมั่นคงปลอดภัย
	ระบบสารสนเทศมีความพร้อมใช้งานและตอบสนองต่อเหตุการณ์ที่อาจจะเกิดขึ้น	OBJ02 เพื่อบริหารจัดการให้ระบบสามารถให้บริการได้ตามเกณฑ์ที่กำหนด	มุ่งมั่นที่จะให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและให้บริการได้อย่างต่อเนื่อง
	กรมบัญชีกลางผ่านการรับรองมาตรฐาน ISO/IEC 27001 เพื่อให้มีความน่าเชื่อถือ	OBJ01 เพื่อขอรับรองมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัย ISO/IEC 27001:2013	มุ่งมั่นให้กรมบัญชีกลางให้บริการประชาชนอย่างมีมาตรฐาน
	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศได้รับการ	OBJ03 เพื่อทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ	มุ่งมั่นที่จะให้การปฏิบัติงานของเจ้าหน้าที่กรมบัญชีกลาง

ตารางที่ 4-10 ตารางสรุปความสัมพันธ์ของความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียกับวัตถุประสงค์และนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (ต่อ)

ผู้มีส่วนได้ส่วนเสียภายในองค์กร	ความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย	วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
	ทบทวน ให้เป็นปัจจุบัน		เป็นไปอย่างเป็นระบบและมีความมั่นคงปลอดภัย
เจ้าหน้าที่	ระบบสารสนเทศมีความพร้อมใช้งานและตอบสนองต่อเหตุการณ์ที่อาจจะเกิดขึ้น	OBJ02 เพื่อบริหารจัดการให้ระบบสามารถให้บริการได้ตามเกณฑ์ที่กำหนด	มุ่งมั่นที่จะให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและให้บริการได้อย่างต่อเนื่อง
	ได้รับความรู้ ความตระหนักด้านความมั่นคงปลอดภัย	OBJ04 เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ	มุ่งมั่นที่จะให้การปฏิบัติงานของเจ้าหน้าที่กรมบัญชีกลางเป็นไปอย่างเป็นระบบและมีความมั่นคงปลอดภัย
	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศได้รับการทบทวน ให้เป็นปัจจุบัน	OBJ03 เพื่อทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ	มุ่งมั่นที่จะให้การปฏิบัติงานของเจ้าหน้าที่กรมบัญชีกลางเป็นไปอย่างเป็นระบบและมีความมั่นคงปลอดภัย
ความต้องการ/ความคาดหวังของผู้มีส่วนได้ส่วนเสียภายนอกองค์กร			
หน่วยงานกำกับดูแล	ปฏิบัติตามกฎระเบียบ กฎหมาย ที่เกี่ยวข้อง	OBJ05 เพื่อให้กรมบัญชีกลางสามารถปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ	มุ่งมั่นที่จะปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ
ผู้ใช้บริการ	มั่นใจได้ว่าระบบสารสนเทศที่ใช้ของกรมบัญชีกลางมีความพร้อมใช้	OBJ02 เพื่อบริหารจัดการให้ระบบสามารถให้บริการได้ตามเกณฑ์ที่กำหนด	มุ่งมั่นที่จะให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและให้บริการได้อย่างต่อเนื่อง
	ใช้บริการที่มีการคำนึงถึงความมั่นคงปลอดภัย และเชื่อถือได้	OBJ01 เพื่อขอรับรองมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัย ISO/IEC 27001:2013	มุ่งมั่นที่จะให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและให้บริการได้อย่างต่อเนื่อง
ผู้ให้บริการภายนอก	ระบบสารสนเทศมีความพร้อมใช้งานและตอบสนองต่อเหตุการณ์ที่อาจจะเกิดขึ้น	OBJ02 เพื่อบริหารจัดการให้ระบบสามารถให้บริการได้ตามเกณฑ์ที่กำหนด	มุ่งมั่นที่จะให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและให้บริการได้อย่างต่อเนื่อง

5. ด้านบุคลากร

บุคลากรปัจจัยที่สำคัญที่สุดในการปฏิรูปนโยบาย และเป็นปัจจัยความสำเร็จควรของกรมบัญชีกลางที่ระบุในแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง และจัดโครงสร้างด้านบุคลากรให้เหมาะสม ดังนี้

5.1 มีนโยบายขององค์กรที่ชัดเจน เพียงพอ เพื่อให้ความสามารถวางแผนทางด้านเทคโนโลยีสารสนเทศและการสื่อสารได้อย่างถูกต้อง

5.2 ผู้บริหารให้ความสำเร็จและให้การสนับสนุนงานด้านเทคโนโลยีสารสนเทศและการสื่อสารและเข้าร่วมดำเนินการอย่างจริงจังในการสนับสนุนและการแก้ไขปัญหาการใช้งานระบบสารสนเทศ

5.3 ผู้บริหารให้การสนับสนุนอัตรากำลังคน งบประมาณที่เหมาะสมเพียงพอต่อภารกิจ และกำหนดแนวทางการเติบโตในสายอาชีพทางด้านเทคโนโลยีสารสนเทศและการสื่อสารที่สอดคล้องกับยุทธศาสตร์ของกรมฯ

5.4 มีการกำหนดยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสารที่สอดคล้องกับยุทธศาสตร์ของกรมฯ

5.5 จัดทำแผนด้านเทคโนโลยีสารสนเทศและการสื่อสารตามยุทธศาสตร์อย่างเป็นระบบและแบบองค์รวม และศึกษาความเป็นไปได้ (Feasibility Study) ของกิจกรรมในแผนตามหลักวิชาการ ก่อนการนำไปดำเนินการอย่างจริงจัง (Implementation) และต้องมีการกำหนดเวลาแล้วเสร็จในการดำเนินงาน

5.6 ด้านบุคลากร

5.6.1 บุคลากรของศูนย์เทคโนโลยีสารสนเทศต้องได้รับการฝึกอบรมตามหลักวิชาการอย่างเหมาะสม เพื่อให้มีความรู้ ความสามารถ ความเชี่ยวชาญในการปฏิบัติหน้าที่และงานที่ได้รับผิดชอบอย่างเหมาะสม เพื่อให้ทันต่อการเปลี่ยนแปลงของสภาพแวดล้อมของโลก โดยเฉพาะด้านเทคโนโลยีสารสนเทศและการสื่อสารที่มีการพัฒนาแบบก้าวกระโดดอย่างต่อเนื่อง และสามารถตอบสนองต่อการเปลี่ยนแปลงของสภาพแวดล้อมได้อย่างเป็นระบบและอย่างต่อเนื่อง

5.6.2 เพื่อศึกษาและกำหนดแนวทางการพัฒนาความรู้ ความสามารถ และการจัดทำมาตรฐานการกำหนดตำแหน่งให้ความสามารถก้าวหน้าในสายงานด้านคอมพิวเตอร์และสารสนเทศภาครัฐได้อย่างมั่นคง

5.6.3 สร้างขวัญและกำลังใจให้กับบุคลากรที่มีความรู้ ความสามารถ และความรับผิดชอบต่อหน้าที่

5.6.4 ปรับโครงสร้างองค์กรของศูนย์เทคโนโลยีสารสนเทศให้มีความยืดหยุ่นสามารถรองรับปริมาณงานตามภารกิจของกรมฯ ที่มีการอัตราขยายตัวอย่างก้าวกระโดดและรวดเร็ว

5.6.5 การทำงานเป็นทีม

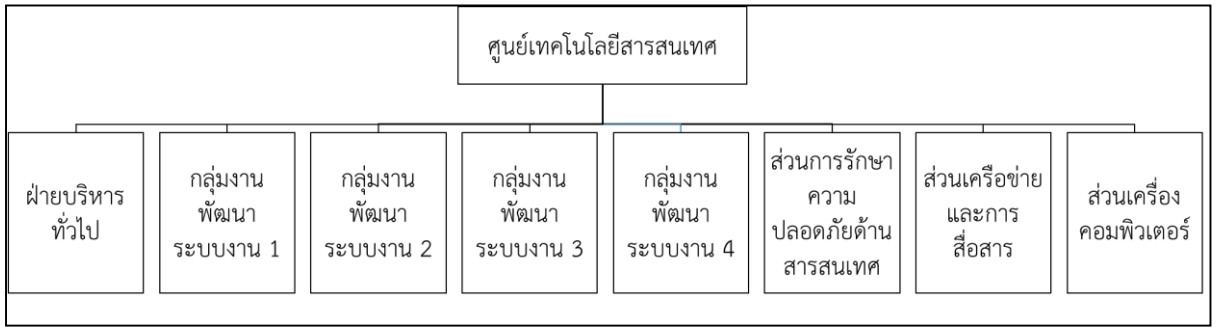
5.7 นำแผนด้านเทคโนโลยีสารสนเทศและการสื่อสารตามยุทธศาสตร์มาดำเนินการอย่างเป็นระบบและเป็นรูปธรรม และต้องมีการกำหนดเวลาแล้วเสร็จในการดำเนินงานในแต่ละแผนงาน/โครงการ พร้อมการจัดทำ/จัดหาเครื่องมือในการติดตามประเมินผลการดำเนินงาน เพื่อเป็นการสร้างระบบเตือนภัยในการติดตามความก้าวหน้าของกรมบัญชีกลาง

แผนภาพที่ 4-1 โครงสร้างกรมบัญชีกลาง

5.8 โครงสร้างของศูนย์เทคโนโลยีสารสนเทศการสื่อสาร

ศูนย์เทคโนโลยีสารสนเทศการสื่อสาร มีการแบ่งโครงสร้างของศูนย์ดังแผนภาพ

แผนภาพที่ 4- 2 โครงสร้างของศูนย์เทคโนโลยีสารสนเทศการสื่อสาร



ที่มา : ศูนย์เทคโนโลยีสารสนเทศกรมบัญชีกลาง แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง พ.ศ. 2557 – 2561 (ระยะ 5 ปี) ,2557

ภารกิจของศูนย์เทคโนโลยีสารสนเทศ กรมบัญชีกลางได้กำหนดภารกิจของศูนย์เทคโนโลยีสารสนเทศ 5 ภารกิจ ดังนี้

5.8.1 จัดทำแผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศของกรมให้สอดคล้องกับมาตรฐานกลางและนโยบายของกระทรวง

5.8.2 วางและพัฒนาระบบเทคโนโลยีสารสนเทศของกรมฯ

5.8.3 บริหารจัดการระบบเทคโนโลยีสารสนเทศของกรมฯ ตลอดจนสนับสนุนและให้คำปรึกษาแนะนำ ระบบเทคโนโลยีสารสนเทศให้แก่หน่วยงานในสังกัดกรมฯ

5.8.4 เป็นศูนย์ดำเนินการเกี่ยวกับข้อมูลสารสนเทศกรมฯ

5.8.5 ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

บทที่ 5
สรุปและข้อเสนอแนะ

สรุป

จากศึกษากฎหมาย กฎระเบียบ วรรณกรรมที่เกี่ยวข้อง บุคลากร อุปกรณ์และเทคโนโลยีที่เกี่ยวข้องกับกรมบัญชีกลาง พบว่าหลายๆ ส่วนต้องมีการปรับปรุงและเพื่อให้การควบคุมนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ ของกรมบัญชีกลาง ได้มีการกำหนดหมวดหมู่ที่เกี่ยวข้องกับการควบคุม ได้นโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมบัญชีกลาง โดยมีข้อกำหนด ดังนี้

1. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

เพื่อกำหนดทิศทางและเป็นกรอบแนวทางการดำเนินงานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง ให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางกฎหมาย และนโยบายฯ ที่เกี่ยวข้อง รวมถึง การกำหนดบทบาท หน้าที่ความรับผิดชอบ แนวทางปฏิบัติ ด้านความมั่นคงปลอดภัย และการควบคุมความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร (Organization of information security)

เพื่อกำหนดบทบาท หน้าที่ความรับผิดชอบในการบริหารและจัดการความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศขององค์กร และลดความเสี่ยง โดยมีการป้องกันการสูญหายหรือการเปลี่ยนแปลงแก้ไขหรือการเข้าถึง ประมวลผล การน้าระบบเทคโนโลยีสารสนเทศและการสื่อสารไปใช้โดยไม่ได้รับอนุญาต หรือไม่เหมาะสม

3. การบริหารจัดการทรัพย์สินสารสนเทศ (Asset management)

เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหาย หรือการน้าไปใช้อย่างผิดวัตถุประสงค์ อันเกิดจากการปฏิบัติหน้าที่ของเจ้าหน้าที่ในองค์กร และบุคคลภายนอกที่เข้าถึงสารสนเทศขององค์กร

3.1 การจัดแบ่งระดับชั้นความลับข้อมูล และการจัดการสารสนเทศ

3.2 ความเป็นส่วนตัวของสารสนเทศ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร

3.3 การปฏิบัติงานของเจ้าหน้าที่ต่อทรัพย์สินขององค์กร

4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human resources security)

เพื่อให้เจ้าหน้าที่ รวมถึงหน่วยงานภายนอก เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตน และตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย ทั้งการก่อนจ้างงาน ระหว่างจ้างงาน และการสิ้นสุดหรือการเปลี่ยนการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับกฎระเบียบขององค์กรและกฎหมาย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment)

4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During Employment)

4.3 การสร้างความมั่นคงปลอดภัยเมื่อสิ้นสุดหรือเปลี่ยนการจ้างงาน (Termination or change of employment)

5. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and environmental security)

เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต รวมถึงป้องกันทรัพย์สินขององค์กร ไม่ให้เกิดความเสียหาย สูญหาย ถูกขโมย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต และป้องกันไม่ให้การดำเนินงานต่าง ๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

5.1 ข้อกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Area)

5.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของอุปกรณ์

6. การบริหารจัดการด้านการสื่อสารและการดาเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (Communications and operations management)

เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย รักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลง ลดความเสี่ยงจากการล้มเหลวของระบบ ป้องกันซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกท้าลาย โดยซอฟต์แวร์ที่ไม่ประสงค์ดี ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการท้างานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการท้าลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต

7. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (Access control)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)

7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)

7.3 หน้าที่ความรับผิดชอบของผู้ใช้ (User responsibilities)

8. การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (Information systems acquisition, development and maintenance)

เพื่อให้การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร ได้พิจารณาถึงประเด็นความมั่นคงปลอดภัยด้านสารสนเทศเป็นองค์ประกอบพื้นฐานที่สำคัญ

8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Security requirements of information systems)

8.2 การประมวลผลสารสนเทศในแอปพลิเคชัน (Correct processing in applications)

8.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic controls)

8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files)

8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in Development and support processes)

8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

9. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Information security incident management)

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ และการสื่อสารขององค์กร ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการ ที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)

9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)

10. การบริหารจัดการด้านการบริการหรือการดาเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง (Business continuity management)

เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานขององค์กร และป้องกันกระบวนการที่สำคัญต่อการดำเนินงานขององค์กรอันเป็นผลมาจากการล้มเหลวหรือหายนะ ที่มีต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

10.1 หัวข้อพื้นฐานสำหรับการบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กร เพื่อให้มีความต่อเนื่อง (Information security aspects of business continuity management)

10.2 ต้องพิจารณาถึงประเด็นด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการการดำเนินงานของหน่วยงาน หรือองค์กรเพื่อให้มีความต่อเนื่อง

11.การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Compliance)

เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุด และมีการแทรกแซงหรือท้าให้หยุดชะงักต่อกระบวนการการดำเนินงานขององค์กรน้อยที่สุด

11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)

11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance)

11.3 การตรวจประเมินระบบเทคโนโลยีสารสนเทศและการสื่อสาร(Information systems audit considerations)

12. การบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอก (Supplier Relationships)

เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่สามารถเข้าถึงได้โดยหน่วยงานภายนอก และเพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของหน่วยงานภายนอก

12.1 ความมั่นคงปลอดภัยด้านสารสนเทศกับความสัมพันธ์กับหน่วยงานภายนอก (Information security in supplier relationships)

12.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

ซึ่งจากทั้ง 12 กลุ่มจะต้องนำมาประยุกต์ใช้ให้เกิดความเหมาะสมและสอดคล้องกับเทคโนโลยีที่กรมมีอยู่พร้อมทั้งการสร้างการรับรู้ให้กับบุคลากรที่เกี่ยวข้องเพื่อให้การบังคับใช้นโยบายที่ประสิทธิภาพ

ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงนโยบาย

นโยบายฯ ที่กำหนดต้องมีการทบทวนให้เป็นปัจจุบันอยู่เสมอ และถ้ามีกฎหมาย กฎระเบียบ ข้อบังคับที่เกี่ยวข้องออกมาใหม่ให้ทบทวนนโยบายให้สอดคล้องกับกฎหมาย นั้น ๆ พร้อมทั้งสื่อสารให้บุคคลากรที่เกี่ยวข้องทั้งหมดรับรู้และปฏิบัติตามนโยบายดังกล่าวพร้อมเตรียมความพร้อมในการจัดหาเครื่องมือและอุปกรณ์มาใช้ให้สอดคล้องกับนโยบายที่กำหนด

2. ข้อเสนอแนะเชิงปฏิบัติ

ควรให้มีหน่วยงานกลางระดับสากลในการเข้ามาตรวจสอบและให้คำรับรองความมั่นคงปลอดภัยทางไซเบอร์ การบริหารจัดการโดยเฉพาะบุคลากรที่มีการเตรียมความพร้อมที่จะควบคุมความมั่นคงปลอดภัยทางไซเบอร์

บรรณานุกรม

“บัญชีแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555”. (ออนไลน์). เข้าถึงได้จาก : https://www.etcommission.go.th/files/law/law_standard_security.pdf, 2562.

“ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550”.(ออนไลน์). เข้าถึงได้จาก : https://www.etda.or.th/files/1/files/06.pdf ,2562.

“ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553”. (ออนไลน์). เข้าถึงได้จาก : https://www.etcommission.go.th/files/law/law_sp1.pdf (ออนไลน์), 2562.

“ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556”. (ออนไลน์).เข้าถึงได้จาก : https://www.etcommission.go.th/files/law/law_sp2.pdf, 2562.

“ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559”.(ออนไลน์). เข้าถึงได้จาก : https://ictlawcenter.etda.or.th/files/law/file/78/e37c4fe15bbaeee06907537bdd4a7795.pdf ,2562.

“ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 วันที่ 23 พฤษภาคม 2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของคอมพิวเตอร์ลูกข่ายระบบบาทเนต”. (ออนไลน์). เข้าถึงได้จาก : https://www.bot.or.th/Thai/PaymentSystems/Payment_Regulation/BN_Regulation/DocLib1/ประกาศ%20สรข%204_2560%20BAHTNET.pdf, 2562

“พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549”. (ออนไลน์). เข้าถึงได้จาก : https://www.etda.or.th/content_files/2/files/decree-defines-rules-procedures-electronic-government-transactions-2549.pdf ,2562.

“พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553”.(ออนไลน์). เข้าถึงได้จาก : http://www.ocpb.go.th/images/Article_File/4rule2553.pdf ,2562.

“พระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550”.(ออนไลน์).เข้าถึงได้จาก : https://www.sme.go.th/upload/mod_download/c771-20-2550-a0001.pdf ,2562.

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560”. (ออนไลน์).เข้าถึงได้จาก : http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF ,2562.

ศิวลีย์ สิริโรจน์บริรักษ์. “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม”. วารสารสถาบันวิชาการป้องกันประเทศ. (ออนไลน์). เข้าถึงได้จาก : https://www.kmutt.ac.th/jif/public_html/article_detail.php?ArticleID=1 59480, 2562.

ศูนย์เทคโนโลยีสารสนเทศกรมบัญชีกลาง. “แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลาง พ.ศ. 2557 – 2561 (ระยะ 5 ปี)” ,2557.

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ .“ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553”.(ออนไลน์).เข้าถึงได้จาก : https://www.etcommission.go.th/files/law/law_dp.pdf, 2562.

ภาคผนวก

ผนวก ก

เรื่อง การสัมภาษณ์ผู้บริหาร (ISO 27001:2013)

1. ทำไมถึงเลือกจัดทำระบบ ISMS ในขอบเขตปัจจุบัน

เนื่องจากกรมบัญชีกลางให้ความสำคัญเรื่องการบริหารจัดการระบบสารสนเทศและทรัพย์สินสารสนเทศ เพื่อให้การบริการผ่านระบบเทคโนโลยีสารสนเทศของกรมฯ มีความมั่นคงปลอดภัย เพื่อให้เกิดความมั่นใจต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร อีกทั้งตอบโจทย์ในเรื่องการปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับในส่วนของผู้กำกับดูแลจากภายนอก เช่น ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต เป็นแรงขับเคลื่อนสำคัญทำให้กรมบัญชีกลาง กำหนดขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อขอการรับรองตามมาตรฐานสากล ISO/IEC 27001:2013 โดยขอบเขตที่ดำเนินการครอบคลุม

1.1 ศูนย์คอมพิวเตอร์หลักกรมบัญชีกลาง โดยรวมถึง ระบบควบคุมสภาพความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and System Environmental Control System) และโครงสร้างพื้นฐานการควบคุมความมั่นคงปลอดภัยทางเครือข่าย (Network Security Control Infrastructure)

1.2 การให้บริการระบบคอมพิวเตอร์แม่ข่ายของระบบงาน ดังนี้

1.2.1 ระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e-Government Procurement: e-GP)

1.2.2 ระบบบูรณาการฐานข้อมูลสวัสดิการสังคม (e-Social Welfare)

1.3 ชุดคอมพิวเตอร์ลูกข่ายระบบบาทเนต (BATHNET) ของกรมบัญชีกลาง สำหรับการปฏิบัติงานจริงและสำหรับเป็นชุดสำรองที่ใช้เชื่อมโยงกับระบบบาทเนตของธนาคารแห่งประเทศไทย ได้แก่ ระบบคอมพิวเตอร์สำหรับบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (Electronic Financial Services) หรือระบบงานคอมพิวเตอร์อื่นที่เชื่อมโยงเพื่อการรับส่งข้อมูลโดยตรงกับระบบคอมพิวเตอร์แม่ข่ายของธนาคารแห่งประเทศไทย (Host to Host) ครอบคลุมทั้งศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรอง จำนวน 2 แห่ง

2. ผู้บริหารคาดหวังอะไรจากระบบ ISMS

จากการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ผู้บริหารมีความคาดหวังดังนี้

2.1 เจ้าหน้าที่มีความตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ

2.2 ระบบสารสนเทศมีความมั่นคงปลอดภัยและให้บริการได้อย่างต่อเนื่อง

2.3 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งใช้เป็นข้อบังคับการทำงาน ได้รับการทบทวนให้เป็นปัจจุบันสอดคล้องกับการเปลี่ยนแปลงของยุคสมัยและความก้าวหน้าของเทคโนโลยี

2.4 กรมบัญชีกลางสามารถให้บริการผู้รับบริการอย่างมีมาตรฐาน การปฏิบัติงานของเจ้าหน้าที่กรมบัญชีกลางเป็นไปอย่างเป็นระบบและมีความมั่นคงปลอดภัย

3. ปัจจุบันได้ตามที่คาดหวังหรือไม่

ปัจจุบันมีการกำหนดแผนงานเพื่อให้การดำเนินงานเป็นไปตามที่คาดหวัง และมีหลายกิจกรรมที่จัดทำขึ้นสำเร็จเรียบร้อยแล้ว เช่น

3.1 การจัดอบรมเพื่อเสริมสร้างความตระหนักให้แก่พนักงาน เพื่อให้เข้าใจความสำคัญในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

3.2 การกำหนดเกณฑ์ความพร้อมใช้ของระบบสารสนเทศ และมีการเฝ้าระวังและรายงานผลให้ทราบอย่างต่อเนื่อง

3.3 มีการทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อปรับปรุงเนื้อหาให้เหมาะสมและเป็นปัจจุบัน

3.4 ในส่วนของการขอการรับรองฯ ปัจจุบันอยู่ระหว่างการตรวจสอบ หากตรวจสอบเสร็จสิ้นและสามารถผ่านการรับรองได้ ก็จะบรรลุความคาดหวังอีกหนึ่งรายการเพิ่มเติม

4. ในฐานะที่เป็นผู้บริหาร ได้สนับสนุนทรัพย์กรตามที่คาดหวังไว้อย่างไร

มีการสนับสนุนทรัพยากร ดังนี้

4.1. ด้านทีมบุคลาการ แต่งตั้งคณะทำงานเพื่อจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ แต่งตั้งนายทะเบียน เพื่อช่วยควบคุมเอกสารต่างๆ ที่จัดทำและใช้ประกอบการทำงาน แต่งตั้งคณะผู้ตรวจสอบเพื่อสอบทานผลการทำงาน

4.2 ด้านงบประมาณ ก็มีการสนับสนุนงบประมาณ ในการจัดทำแผนเพื่อบริหารจัดการความเสี่ยง เพื่อลดความเสี่ยงในประเด็นต่างๆ ที่พบ เช่น ระบบบาทเนต มีการอนุมัติ แผนจัดหาเครื่องสำรองไฟฟ้าสำหรับเครื่องคอมพิวเตอร์ลูกข่าย (BN-RTP-2561-012), แผนจัดหาอุปกรณ์ Firewall สารองเพื่อทดแทนเมื่อเกิดปัญหา สาหรับระบบ BAHTNET (BN-RTP-2561-021), แผนจัดหาอุปกรณ์ Switch สำรองเพื่อทดแทนเมื่อเกิดปัญหา สาหรับระบบ BAHTNET (BN-RTP-2561-023) เป็นต้น

4.3 การจัดประชุม Committee เพื่อให้ผู้บริหารสามารถติดตามผลการดำเนินอย่างได้อย่างต่อเนื่อง หากมีปัญหาในส่วนใด ผู้บริหารสามารถให้การสนับสนุนและให้แนวทางในการแก้ไขปัญหาได้อย่างทันถ่วงที

5. มีการติดตามประสิทธิภาพ ประสิทธิผลของระบบ ISMS อย่างไร

มีการจัดประชุม Committee เพื่อให้คณะทำงานฯ ได้รายงานสถานะกิจกรรมต่างๆ ของระบบ ISMS อย่างต่อเนื่อง เดือนละ 1 ครั้ง

6. ความถี่ในการทำ Management Review เป็นอย่างไร?

จัดประชุม เดือนละ 1 ครั้ง

7. ในมุมมองผู้บริหารมีจุดใดที่ต้องการให้ปรับปรุงบ้าง

จากการดำเนินงานที่ผ่านมา กิจกรรมต่างๆ โดยภาพรวมยังไม่น่ากังวล อาจจะมีบางเรื่องที่ต้องเสริมจากเดิมที่ทำอยู่ เช่น การสื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจความสำคัญของการทำระบบ ISMS เพื่อให้บุคลากรมีความเข้าใจและทราบบทบาทหน้าที่ของตนเองมากยิ่งขึ้น

8. เท่าที่ผ่านมาในมุมมองผู้บริหารอะไรที่เป็นความเสี่ยงกับขอบเขตระบบ ISMS

สิ่งที่อาจเป็นความเสี่ยงภายในขอบเขตระบบ ISMS เช่น

- การจัดสรรงบประมาณไม่เพียงพอ

- บุคลากรไม่เพียงพอต่อการปฏิบัติงาน นโยบายภาครัฐทางด้านเทคโนโลยีสารสนเทศ เช่น โครงการสวัสดิการภาครัฐ โดยมีนโยบายให้กรมบัญชีกลางต้องดาเนินการ แต่ไม่มีอัตรากาลังคนเพิ่ม ทำให้กรมบัญชีกลางต้องจัดสรรบุคลากร เพื่อมาทำหน้าที่เพิ่มเติม

- บุคลากรมีความรู้ความสามารถไม่เพียงพอ

- อุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศไม่ทันสมัยและไม่เพียงพอ ซึ่งจากปัจจัยที่อาจเป็นความเสี่ยงดังกล่าว ก็มีการจัดทำแผนเพื่อบริหารจัดการ เช่น จัดทำแผนส่งเสริมสมรรถนะของบุคลากร, จัดทำแผนสรรหาทรัพยากรบุคคล, โครงการเพิ่มประสิทธิภาพการใช้ระบบเทคโนโลยีสารสนเทศของกรมบัญชีกลาง เป็นต้น

9. เท่าที่ผ่านมามี Incident ร้ายแรงกับขอบเขตระบบ ISMS หรือไม่ เป็น Case ที่เป็น Security Incident หรือไม่

เท่าที่ผ่านยังไม่พบ Incident ร้ายแรงกับขอบเขตระบบ ISMS แต่อย่างใด

10. Management Review ครั้งล่าสุด มีประเด็นอะไรที่กังวลหรือไม่

- หากมีประเด็นที่กังวล สามารถแจ้งได้ตามความเป็นจริง หรือ **หากไม่พบเป็นประเด็นที่กังวล** สามารถตอบได้ตามแนวทาง ดังนี้ การประชุมครั้งล่าสุดที่ผ่านมา มีการรายงานสถานะของแผนการดำเนินงานต่างๆ ซึ่งปัจจุบันยังไม่พบประเด็นที่น่ากังวล

11. มีแผนที่จะขยายขอบเขตไปยังส่วนอื่นหรือไม่?

ทางกรมบัญชีกลางมีการวางแผนที่จะขยายขอบเขตการรับรองไปยังระบบอื่นๆ อาทิเช่น

11.1 ระบบการชำระเงินกลางภาครัฐแบบอิเล็กทรอนิกส์ (e-payment)

11.2 ระบบจ่ายตรงเงินเดือนและค่าจ้างประจา (e-payroll)

11.3 ระบบบาเหน็จบำนาญและสวัสดิการรักษาพยาบาล (e-Pension)

11.4 ระบบเว็บไซต์อินเตอร์เน็ตกรมบัญชีกลาง (Internet Website)

ซึ่งปัจจุบันได้ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของระบบดังกล่าว และกำหนดแผนเพื่อจัดการความเสี่ยงแล้ว หากในอนาคตมีการขยายขอบเขตไปยังระบบงานดังกล่าวก็สามารถทำได้โดยง่าย

ประวัติย่อผู้วิจัย

ชื่อ นายเกียรติณรงค์ วงศ์น้อย

วัน เดือน ปีเกิด 1 มกราคม 2508

การศึกษา

ปริญญาตรี บัญชีบัณฑิต มหาวิทยาลัยธรรมศาสตร์
ปริญญาโท วิทยาศาสตรมหาบัณฑิต (คอมพิวเตอร์) จุฬาลงกรณ์มหาวิทยาลัย
ปริญญาโท การจัดการภาครัฐและเอกชนมหาบัณฑิต สถาบันบัณฑิตพัฒนบริหารศาตร์

ประวัติการทำงาน

1 ต.ค. 2560	ที่ปรึกษาด้านเทคโนโลยีสารสนเทศและการสื่อสาร รักษาการในตำแหน่งที่ปรึกษาด้านพัฒนาระบบบริหารการคลัง
26 ส.ค. 2557	ที่ปรึกษาด้านเทคโนโลยีสารสนเทศและการสื่อสาร
11 ธ.ค. 2551	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

ตำแหน่งปัจจุบัน ที่ปรึกษาด้านพัฒนาระบบบริหารการคลัง

สรุปย่อ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

เรื่อง การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมบัญชีกลาง

ผู้วิจัย นายเกียรติณรงค์ วงศ์น้อย หลักสูตร วปอ. รุ่นที่ 61

ตำแหน่ง ที่ปรึกษาด้านพัฒนาระบบการเงินการคลัง

ความเป็นมาและความสำคัญของปัญหา

กรมบัญชีกลางทำหน้าที่ทั้งการเป็นผู้ให้บริการ (Service Provider) และการกำกับดูแลทางด้านการเงินและบัญชีภาครัฐ (Regulator) รวมถึงสนับสนุนการบริหารเศรษฐกิจการเงินการคลังของจังหวัด กรมบัญชีกลางมีพันธกิจที่สำคัญในการกำหนดมาตรฐาน หลักเกณฑ์ แนวปฏิบัติด้านการคลังและการบัญชี การตรวจสอบภายในและการพัสดุภาครัฐ สนับสนุนการบริหารเศรษฐกิจการคลังในส่วนภูมิภาค เป็นศูนย์ข้อมูลสารสนเทศการคลัง และพัฒนาขีดความสามารถของบุคลากรภาครัฐทางการเงิน การคลัง การบัญชี การตรวจสอบภายในและการพัสดุภาครัฐ ปัจจุบันกรมบัญชีกลางได้พัฒนาเทคโนโลยีสารสนเทศมาช่วยงานกิจกรรมภารกิจของกรมบัญชีกลาง เช่น ระบบจ่ายตรงเงินเดือนและค่าจ้างประจำ ระบบจัดซื้อจัดจ้างภาครัฐด้วยวิธีอิเล็กทรอนิกส์ ระบบบำเหน็จบำนาญและสวัสดิการค่ารักษาพยาบาล ระบบบูรณาการฐานข้อมูลสวัสดิการภาครัฐ เป็นต้น ซึ่งมีข้อมูลที่สำคัญและเป็นข้อมูลส่วนบุคคล เช่น ประวัติข้าราชการและประวัติรับราชการ รวมทั้งการจ่ายเงินเดือน ข้อมูลการเข้ารับการรักษาพยาบาลของข้าราชการและบุคคลในครอบครัวที่มีสิทธิ ข้อมูลผู้มีรายได้น้อยที่ลงทะเบียนขอรับบัตรสวัสดิการแห่งรัฐและการจ่ายเงินสวัสดิการด้วยบัตร ข้อมูลการจ่ายเงินสวัสดิการแห่งรัฐประเภทอื่น เช่นเงินอุดหนุนเพื่อการเลี้ยงดูเด็กแรกเกิด เงินช่วยเหลือเยียวยาผู้ได้รับผลกระทบจากสถานการณ์ความไม่สงบในจังหวัดชายแดนภาคใต้ เบี้ยคนพิการกรุงเทพมหานคร เบี้ยยังชีพผู้สูงอายุของเมืองพัทยา ค่าป่วยการอาสาสมัครประจำหมู่บ้าน (อสม.) เงินเดือนทหารกองประจำการ (ทหารเกณฑ์) และเงินสวัสดิการอื่น ๆ ที่จ่ายโดยภาครัฐ พร้อมกันนี้ในปัจจุบันมีภัยคุกคามทางไซเบอร์ (Cyber threat) ที่เป็นปัญหาในหลายประเทศ ซึ่งทางกรมบัญชีกลางได้ตระหนักถึงภัยคุกคามที่คาดว่าอาจเกิดขึ้นกับกรมบัญชีกลางได้ในอนาคต ดังนั้นกรมบัญชีกลางทบทวนกระบวนการหรือการกระทำทั้งหมดที่เกี่ยวข้องกับระบบของกรมบัญชีกลาง เพื่อประเมินความเสี่ยง และดำเนินการทำให้องค์กรปราศจากความเสี่ยง โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA 3 ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

จึงกล่าวได้ว่าความมั่นคงปลอดภัยไซเบอร์ ถือว่ามีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้นการที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมี

กระบวนการในการดำเนินการ โดยเลือกมาตรฐานสากลแล้วนำมาประยุกต์ใช้ให้เหมาะสมกับองค์กร และต้องสอดคล้องตามกฎหมายต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ยุทธศาสตร์ชาติ จากเหตุผลข้างต้น จึงนำมาสู่การศึกษาเรื่อง “การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกรมบัญชีกลาง”

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษานโยบาย ยุทธศาสตร์ และการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมบัญชีกลาง
2. เพื่อศึกษามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล
3. เพื่อเสนอแนวทางในการพัฒนามาตรฐาน การรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมบัญชีกลาง
4. เพื่อวิเคราะห์สถานการณ์ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ขอบเขตของการวิจัย

การวิจัยเรื่อง “การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ของกรมบัญชีกลาง” ประกอบด้วยขอบเขตของการศึกษา ดังนี้

1. ขอบเขตด้านเนื้อหา

การวิจัยครั้งนี้จะดำเนินการการทบทวนวรรณกรรมที่เกี่ยวข้องกับกฎหมาย กฎระเบียบเกี่ยวข้องกับเทคโนโลยีสารสนเทศ ตอลดจนนโยบายขององค์กร

2. ขอบเขตด้านทักษะและความรู้ของบุคลากร

การวิจัยครั้งนี้จะดำเนินการด้านการให้ความรู้ด้านความมั่นคงปลอดภัยให้กับบุคลากรของกรม และสร้างความตระหนักและการรับรู้เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของกรม เพื่อวัดประสิทธิภาพในการดำเนินการด้านความมั่นคงปลอดทางไซเบอร์ และจัดหลักสูตรฝึกอบรมให้บุคลากรมีความรู้ ทักษะในการดำเนินการทางด้านความมั่นคงปลอดภัยทางไซเบอร์

3. ขอบเขตด้านเทคโนโลยีสารสนเทศ

การวิจัยครั้งนี้จะดำเนินการด้านความมั่นคงปลอดภัยของศูนย์เทคโนโลยีสารสนเทศ เพื่อจัดหาหรือเตรียมการให้เหมาะสม และเพิ่มขีดความสามารถในการดำเนินการรับมือกับภัยคุกคามทางไซเบอร์

4. ขอบเขตด้านเวลา

การวิจัยครั้งนี้จะดำเนินการรวบรวมข้อมูลทั้งข้อมูลปฐมภูมิและข้อมูลทุติยภูมิในห้วงเวลาตั้งแต่เดือนตุลาคม 2561 – กันยายน 2562

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีการดำเนินการดังนี้

1. การรวบรวมข้อมูล

1.1 ข้อมูลทุติยภูมิ รวบรวมข้อมูลเรื่องแนวคิด ทฤษฎี รวมถึงวรรณกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เว็บไซต์ที่เกี่ยวข้อง

1.2 ข้อมูลปฐมภูมิ โดยรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึกจากผู้ให้ข้อมูลสำคัญ

2. การจัดระเบียบข้อมูล

เมื่อรวบรวมข้อมูลทั้งข้อมูลปฐมภูมิและข้อมูลทุติยภูมิดังที่กล่าวแล้ว หลังจากนั้นจะนำข้อมูลมาจัดระเบียบและตรวจสอบ (Validity) ของข้อมูลตามขั้นตอนการวิจัยเชิงคุณภาพ เพื่อที่จะเตรียมข้อมูลไว้สำหรับการวิเคราะห์ข้อมูลในขั้นตอนต่อไป

3. การวิเคราะห์ข้อมูล และการสังเคราะห์ข้อมูล

จะดำเนินการวิเคราะห์ข้อมูลโดยวิธีการวิเคราะห์เนื้อหา (Context Analysis) โดยวิเคราะห์เนื้อหาของข้อมูล เพื่อเชื่อมความสัมพันธ์ระหว่างส่วนประกอบต่าง ๆ ของข้อมูล และนำข้อมูลที่ได้มาสังเคราะห์ เพื่อสรุปเป็นตัวแบบในการกำหนดนโยบายด้านความมั่นคงไซเบอร์ ของกรมบัญชีกลาง

ผลการวิจัย

กรมบัญชีกลางทำหน้าที่ทั้งการเป็นผู้ให้บริการ (Service Provider) และการกำกับดูแลทางด้านการเงินและบัญชีภาครัฐ (Regulator) มีภารกิจเกี่ยวกับการควบคุมดูแลการใช้จ่ายเงินของแผ่นดินและหน่วยงานภาครัฐ ให้เป็นไปโดยถูกต้อง มีวินัย คุ้มค่า โปร่งใส และสามารถตรวจสอบได้ ปัจจุบันกรมบัญชีกลางได้พัฒนาเทคโนโลยีสารสนเทศมาช่วยงาน กิจกรรม ภารกิจของกรมบัญชีกลาง เช่น ระบบจ่ายตรงเงินเดือนและค่าจ้างประจำ ระบบจัดซื้อจัดจ้างภาครัฐด้วยวิธีอิเล็กทรอนิกส์ ระบบบำเหน็จบำนาญและสวัสดิการค่ารักษาพยาบาล ระบบบูรณาการฐานข้อมูลสวัสดิการภาครัฐ ระบบรับชำระเงินกลางของบริการภาครัฐ เป็นต้น โดยระบบงานต่าง ๆ ของกรมบัญชีกลางเป็นระบบที่ให้บริการภาครัฐที่สำคัญ และมีข้อมูลที่สำคัญทั้งที่เป็นข้อมูลส่วนบุคคลและข้อมูลที่เป็นความลับมากมาย ซึ่งเป็นเป้าหมายของผู้ไม่หวังดีในการที่พยายามเข้าถึงข้อมูลดังกล่าวโดยให้ใช้เทคโนโลยีทางไซเบอร์ในการเข้าถึงระบบงาน พร้อมกันนี้ในปัจจุบันมีภัยคุกคามทางไซเบอร์ (Cyber threat) ที่เป็นปัญหาในหลายประเทศ ซึ่งทางกรมบัญชีกลางได้ตระหนักถึงภัยคุกคามที่คาดว่าอาจเกิดขึ้นกับกรมบัญชีกลางได้ในอนาคต ดังนั้น กรมบัญชีกลางทบทวนกระบวนการหรือการกระทำทั้งหมดที่เกี่ยวข้องกับระบบงานของกรมบัญชีกลาง เพื่อประเมินความเสี่ยง ดำเนินการทำให้องค์กรปราศจากความเสี่ยง รวมถึงการรับมือกับภัยคุกคามที่จะเกิดขึ้น โดยคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล ประกอบด้วย การรักษาความลับของข้อมูล การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ ของข้อมูลและความพร้อมใช้งานของข้อมูล โดยการศึกษาได้มีการนำกฎหมาย

ที่เกี่ยวข้องกับสารสนเทศ ซึ่งจากการศึกษาดังกล่าวได้พัฒนานโยบายการรักษาควบคุมความมั่นคงทางไซเบอร์ ของกรมบัญชีกลาง โดยมีรายละเอียดแบ่งเป็นแต่ละกลุ่มดังนี้ 1) การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ เพื่อกำหนดทิศทางและเป็นกรอบแนวทางการดำเนินงานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมบัญชีกลางให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางกฎหมาย และนโยบายฯ ที่เกี่ยวข้อง รวมถึง การกำหนดบทบาท หน้าที่ความรับผิดชอบ แนวทางปฏิบัติ ด้านความมั่นคงปลอดภัย และการควบคุมความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร 2) การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร (Organization of information security) เพื่อกำหนดบทบาท หน้าที่ความรับผิดชอบในการบริหารและจัดการความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศขององค์กร และลดความเสี่ยงโดยมีการป้องกันการสูญหายหรือการเปลี่ยนแปลงแก้ไขหรือการเข้าถึง ประมวลผล การน้าระบบเทคโนโลยีสารสนเทศและการสื่อสารไปใช้โดยไม่ได้รับอนุญาต หรือไม่เหมาะสม 3) การบริหารจัดการทรัพย์สินสารสนเทศ (Asset management) เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหาย หรือการน้าไปใช้อย่างผิดวัตถุประสงค์ อันเกิดจากการปฏิบัติหน้าที่ของเจ้าหน้าในองค์กร และบุคคลภายนอกที่เข้าถึงสารสนเทศขององค์กร 4) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human resources security) เพื่อให้เจ้าหน้าที่ รวมถึงหน่วยงานภายนอก เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตน และตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย ทั้งการก่อนจ้างงาน ระหว่างจ้างงาน และการสิ้นสุดหรือการเปลี่ยนการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับกฎระเบียบขององค์กรและกฎหมาย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่ 5)การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and environmental security) เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต รวมถึงป้องกันทรัพย์สินขององค์กร ไม่ให้เกิดความเสียหาย สูญหาย ถูกขโมย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต และป้องกันไม่ให้การดำเนินงานต่าง ๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก 6) การบริหารจัดการด้านการสื่อสารและการดาเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (Communications and operations management) เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย รักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลง ลดความเสี่ยงจากการล้มเหลวของระบบ ป้องกันซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกท้าลาย โดยซอฟต์แวร์ที่ไม่ประสงค์ดี ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการท้างานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต 7) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (Access control) เพื่อควบคุมการ

เข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร 8) การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (Information systems acquisition, development and maintenance) เพื่อให้การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร ได้พิจารณาถึงประเด็นความมั่นคงปลอดภัยด้านสารสนเทศเป็นองค์ประกอบพื้นฐานที่สำคัญ 9) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Information security incident management) เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร 10) การบริหารจัดการด้านการบริการหรือการดาเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง (Business continuity management) เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานขององค์กร และป้องกันกระบวนการที่สำคัญต่อการดำเนินงานขององค์กรอันเป็นผลมาจากการล้มเหลวหรือหายนะ ที่มีต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม 11) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Compliance) เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุด และมีการแทรกแซงหรือท้าให้หยุดชะงักต่อกระบวนการการดำเนินงานขององค์กรน้อยที่สุด 12) การบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอก (Supplier Relationships) เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่สามารถเข้าถึงได้โดยหน่วยงานภายนอก และเพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของหน่วยงานภายนอก ซึ่งจากทั้ง 12 กลุ่มจะต้องนำมาประยุกต์ใช้ให้เกิดความเหมาะสมและสอดคล้องกับเทคโนโลยีที่กรมมีอยู่พร้อมทั้งการสร้างการรับรู้ให้กับบุคลากรที่เกี่ยวข้องเพื่อให้การบังคับใช้นโยบายที่ประสิทธิภาพ

ข้อเสนอแนะ

นโยบายฯ ที่กำหนดต้องมีการทบทวนให้เป็นปัจจุบันอยู่เสมอ และถ้ามีกฎหมาย กฎระเบียบ ข้อบังคับที่เกี่ยวข้องออกมาใหม่ให้ทบทวนนโยบายให้สอดคล้องกับกฎหมายนั้น ๆ พร้อมทั้งสื่อสารให้บุคคลากรที่เกี่ยวข้องทั้งหมดรับรู้และปฏิบัติตามนโยบายดังกล่าว พร้อมเตรียมความพร้อมในการจัดหาเครื่องมือและอุปกรณ์มาใช้ให้สอดคล้องกับนโยบายที่กำหนด