แนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ตามวิธีการแบบปลอดภัย ในระดับเคร่งครัด กรมอนามัย

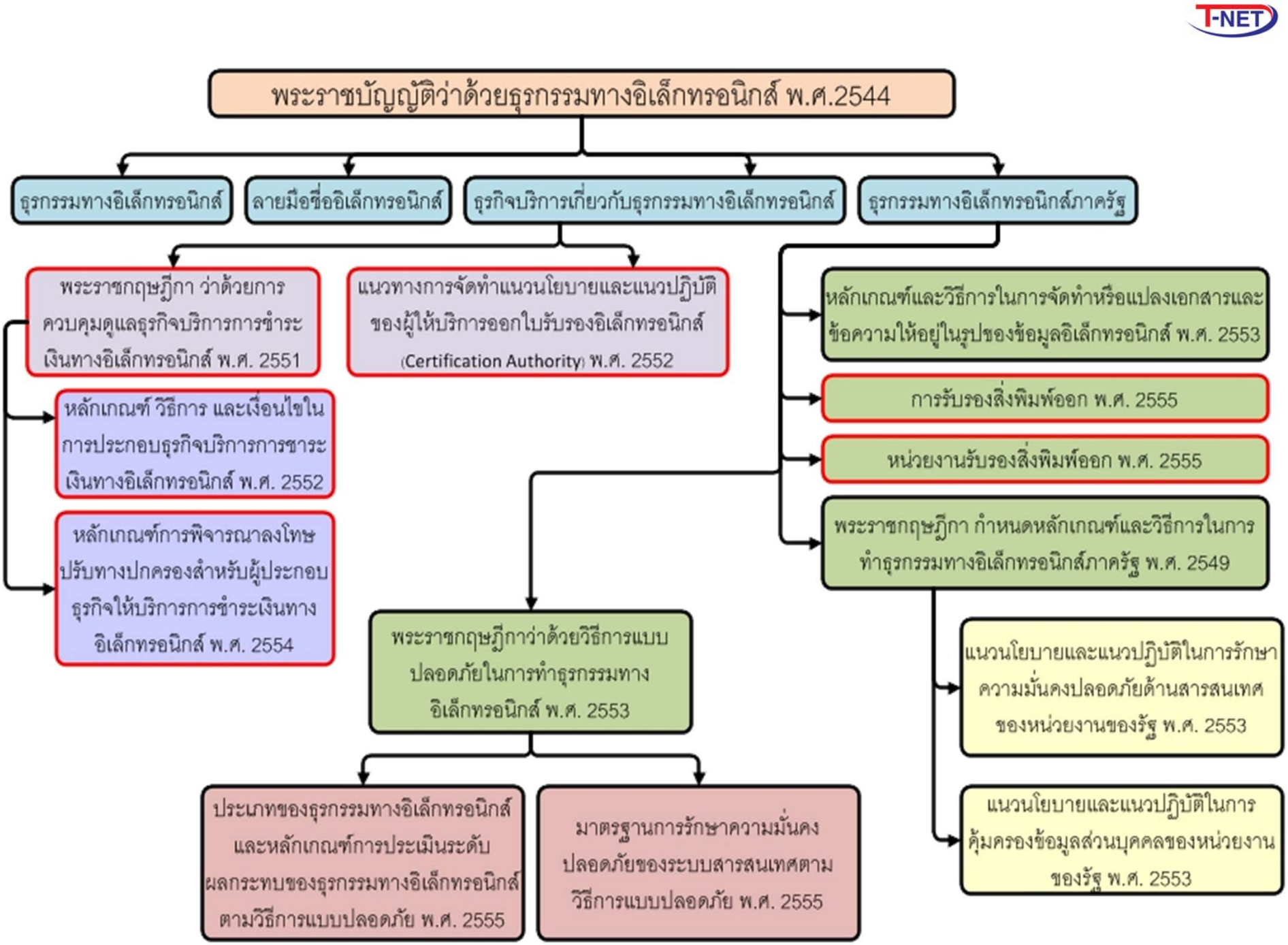
Founded by NECTEC

กฎหมายด้านไอซีทีที่เกี่ยวข้อง

2

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560


พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544
ธุรกรรมทางอิเล็กทรอนิกส์
ลายมือชื่ออิเล็กทรอนิกส์
ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์
ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
พระราชกฤษฎีกา ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551
แนวทางการจัดทำแนวนโยบายและแนวปฏิบัติของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. 2552
หลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2552
หลักเกณฑ์การพิจารณาลงโทษปรับทางปกครองสำหรับผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2554
หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553
การรับรองสิ่งพิมพ์ออก พ.ศ. 2555
หน่วยงานรับรองสิ่งพิมพ์ออก พ.ศ. 2555
พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553
แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555
มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

4

สาระสำคัญ

- ธุรกรรมทางอิเล็กทรอนิกส์
- ลายมือชื่ออิเล็กทรอนิกส์
- ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์
- ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

5

ธุรกรรมทางอิเล็กทรอนิกส์

ธุรกรรมทางอิเล็กทรอนิกส์ หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

- การรับรองรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการรับ การส่งผ่านสื่ออิเล็กทรอนิกส์ สามารถใช้เป็นหนังสือ หรือหลักฐาน
- การรับรองลายมือชื่ออันเป็นการใช้วิธีการใดก็ได้ในการระบุตัวบุคคล เพื่อแสดงว่าเจ้าของลายมือชื่อรับรองข้อความในรูปของข้อมูลอิเล็กทรอนิกส์ว่าเป็นของตน
- ข้อความที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์เหล่านั้นต้องสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลงด้วย
- ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความและสามารถ
- แสดงข้อความนั้นในภายหลังได้ ศาลรับฟังข้อมูลอิเล็กทรอนิกส์เป็น
- พยานหลักฐานเกี่ยวกับการชั่งน้ำหนักพยาน

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

6

ลายมือชื่ออิเล็กทรอนิกส์

ข้อมูล
อิเล็กทรอนิกส์

+

อักษร, อักขระ, ตัวเลข,
เสียง, สัญลักษณ์

ลายมือชื่อ
อิเล็กทรอนิกส์

เพื่อระบุตัวบุคคล

- รับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์กับข้อมูลอิเล็กทรอนิกส์ได้

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

7

ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

"ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์" เป็นคำที่มีความหมายกว้าง ไม่จำกัดเพียงการให้บริการเกี่ยวกับใบรับรอง (Certificate Service Provider) เท่านั้น แต่ยังหมายความรวมถึงบริการต่างๆ ที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งหมด เช่น การให้บริการเกี่ยวกับระบบการรักษาความปลอดภัย การให้บริการเกี่ยวกับการรับฝากข้อมูล การให้บริการเกี่ยวกับการชำระเงิน เป็นต้น

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

8

พรบ. ฉบับนี้อนุญาตให้ประชาชนสามารถประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ได้โดยอิสระ เว้นแต่การประกอบธุรกิจนั้นอาจส่งผลกระทบต่อความมั่นคงของรัฐหรืออาจสร้างความเสียหายต่อสาธารณะ ก็จะต้องมีการแจ้งให้ทราบ ขึ้นทะเบียน หรือได้รับใบอนุญาต ก่อนประกอบกิจการ ได้แก่

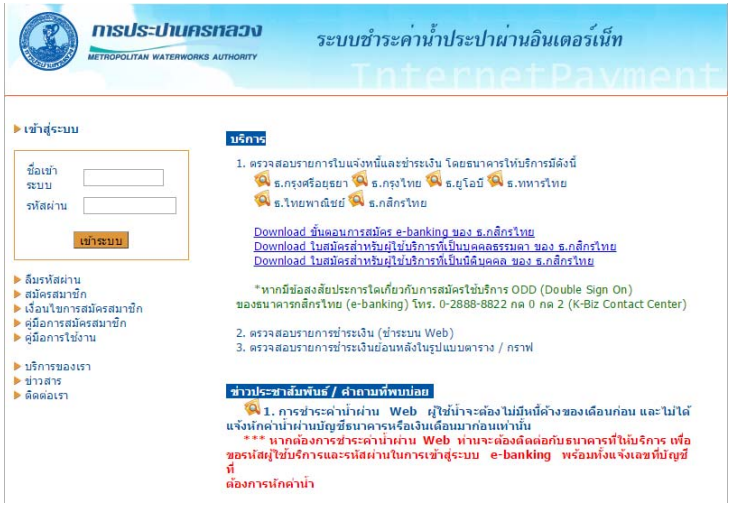
- การให้บริการเครือข่ายบัตรเครดิต (Credit Card Network)
- การให้บริการเครือข่ายอีดีซี (EDC Network)
- การให้บริการสวิตช์ชิ่งในการชำระเงินการให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้าและหรือรับบริการ
- การให้บริการหักบัญชี (Clearing)
- การให้บริการชำระดุล (Settlement)
- ให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใดหรือผ่านทางเครือข่าย
- การให้บริการรับชำระเงินแทน

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

9

ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

การดำเนินการใดๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ที่กำหนดโดยพระราชกฤษฎีกา ให้ปฏิบัติตาม พ.ร.บ. นี้และให้ถือว่ามีผลโดยชอบด้วยกฎหมาย



หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553

ข้อกำหนดวิธีปฏิบัติในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

- ผู้จัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ต้องมีการตรวจสอบ จัดทำหรือแปลงเอกสารและข้อความตามข้อกำหนดโดยพิจารณาความครบถ้วนของข้อความทั้งหมด มาตรฐานขั้นต่ำสำหรับความละเอียดภาพ การตั้งชื่อไฟล์ข้อมูลอิเล็กทรอนิกส์ที่สื่อถึงเนื้อหาของข้อมูลเพื่อสืบค้นได้

- ผู้จัดทำหรือแปลงต้องมีการตรวจสอบและการรับรองคุณภาพกระบวนการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ตลอดจนมีการบันทึกการดำเนินการไว้เป็นหลักฐานและมีการกำหนดตัวบุคคลผู้รับผิดชอบที่เป็นผู้จัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ผู้ตรวจสอบคุณภาพของข้อมูลอิเล็กทรอนิกส์ที่ผ่านการจัดทำหรือแปลง ผู้ตรวจสอบและรับรองกระบวนการจัดทำหรือแปลง และผู้ตรวจสอบและรับรองความถูกต้องและครบถ้วนของเมตาดาตา (Meta data)

- การกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ด้วยวิธีการที่เชื่อถือได้ เช่น การลงทะเบียนผู้ใช้งาน การบริหารจัดการสิทธิของผู้ใช้งาน การทบทวนสิทธิ การใช้รหัสผ่าน เป็นต้น

พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ซึ่งต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

- แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
- แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556
- แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
- แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 (แก้คำผิด)

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

13

- หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร และจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

- ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยดังนี้

  - ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)
  - ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย
  - การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ
  - การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เช่น การใช้งานรหัสผ่าน การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์
  - การควบคุมการเข้าถึงเครือข่าย (network access control)
  - การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

➢ ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยดังนี้

- มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) เช่น ควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

- หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง

- หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง และตรวจสอบโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor)

- หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

- หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่า ข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556

ยกเลิกข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ในข้อ

หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

และกำหนดใหม่เป็น

หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น

แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

- ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยมีสาระสำคัญ เช่น การจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้มีขอบเขตจำกัด และใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม และให้เจ้าของข้อมูลทราบหรือได้รับความยินยอมจากเจ้าของข้อมูลตามแต่กร, การระบุวัตถุประสงค์ในการเก็บรวบรวม, การมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม เป็นต้น

- ให้หน่วยงานของรัฐจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการประกอบด้วย

  - ข้อมูลเบื้องต้น เช่น ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด, รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคล
  - การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล
  - การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น
  - การรวมข้อมูลจากที่มาหลายๆ แห่ง ให้ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลถึงเจตนารมณ์การรวมข้อมูลดังกล่าวด้วย

แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

- การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

- การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ ให้ระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลถึงสิทธิของผู้ใช้บริการ

- การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

- การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์จัดให้มีวิธีการรักษาความมั่นคง*ปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้ให้เหมาะสมกับการรักษาความลับของข้อมูลส่วนบุคคล

โดยจัดให้มีวิธีการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้ให้เหมาะสมกับการรักษาความลับของข้อมูลส่วนบุคคล

- การติดต่อกับเว็บไซต์ เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับหน่วยงานของรัฐ ต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย

* คือ แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 (แก้คำผิด)

แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

- สำหรับหน่วยงานของรัฐที่ได้รับทรัสต์มาร์คจากหน่วยงานหรือองค์กรอื่นที่ทำหน้าที่ออกทรัสต์มาร์ค (Trust Mark) ให้หน่วยงานของรัฐนั้นแสดงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากหน่วยงานหรือองค์กรที่ออกหรือรับรองทรัสต์มาร์คดังกล่าวต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ทรัสต์มาร์ค (Trust Mark) หมายถึง เครื่องหมายที่รับรองว่าหน่วยงานดังกล่าวมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งออกโดยหน่วยงานหรือองค์กรที่จัดตั้งโดยชอบด้วยกฎหมายเพื่อทำหน้าที่ในการตรวจสอบและรับรองการออกทรัสต์มาร์คให้กับผู้ขอรับการรับรอง

- ให้หน่วยงานของรัฐกำหนดชื่อเรียกนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ให้ชัดเจน และในกรณีที่มีการปรับปรุงนโยบาย ให้ระบุวัน เวลา และปี ซึ่งจะมีการปรับปรุงหรือเปลี่ยนแปลงนโยบายดังกล่าวไว้ด้วย

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

- วิธีการแบบปลอดภัย หมายความว่า วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

- วิธีการแบบปลอดภัยมี 3 ระดับ ดังต่อไปนี้

    1. ระดับเคร่งครัด
    2. ระดับกลาง
    3. ระดับพื้นฐาน

- วิธีการแบบปลอดภัยใช้สำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ ดังต่อไปนี้

    1. ธุรกรรมทางอิเล็กทรอนิกส์ซึ่งมีผลกระทบต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน

    2. ธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

- ต้องมีการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่คณะกรรมการประกาศสำหรับวิธีการแบบปลอดภัยในแต่ละระดับ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

- ในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้ ผู้กระทำต้องคำนึงถึงหลักการพื้นฐานของการรักษาความลับ การรักษาความครบถ้วน และการรักษาสภาพพร้อมใช้งาน รวมทั้งต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานหรือองค์กรนั้นด้วย

- คณะกรรมการพิจารณาทบทวนหลักเกณฑ์เกี่ยวกับวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้และประกาศที่ออกตามพระราชกฤษฎีกานี้ รวมทั้งกฎหมายอื่นที่เกี่ยวข้อง อย่างน้อยทุกรอบระยะเวลา 2 ปีนับแต่วันที่พระราชกฤษฎีกานี้ใช้บังคับ ทั้งนี้ โดยพิจารณาถึงความเหมาะสมและความสอดคล้องกับเทคโนโลยีที่ได้มีการพัฒนาหรือเปลี่ยนแปลงไป

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555

- ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด มีดังต่อไปนี้

1. ธุรกรรมทางอิเล็กทรอนิกส์ด้านการชำระเงินทางอิเล็กทรอนิกส์ตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551

2. ธุรกรรมทางอิเล็กทรอนิกส์ด้านการเงินของธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

3. ธุรกรรมทางอิเล็กทรอนิกส์ด้านประกันภัยตามกฎหมายว่าด้วยประกันชีวิตและประกันวินาศภัย

4. ธุรกรรมทางอิเล็กทรอนิกส์ด้านหลักทรัพย์ของผู้ประกอบธุรกิจหลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์

5. ธุรกรรมทางอิเล็กทรอนิกส์ที่จัดเก็บ รวบรวม และให้บริการข้อมูลของบุคคลหรือทรัพย์สินหรือทะเบียนต่าง ๆ ที่เป็นเอกสารมหาชนหรือที่เป็นข้อมูลสาธารณะ

6. ธุรกรรมทางอิเล็กทรอนิกส์ในการให้บริการด้านสาธารณูปโภคและบริการสาธารณะที่ต้องดำเนินการอย่างต่อเนื่องตลอดเวลา

ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555

- การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ จะต้องประเมินผลกระทบในด้านต่อไปนี้ด้วย

1. ผลกระทบด้านมูลค่าความเสียหายทางการเงิน แบ่งเป็น 3 ระดับ โดยคำนวณจากความเสียหายที่จะเกิดขึ้นในหนึ่งวันและคำนวณความเสียหายโดยตรงเท่านั้น

มูลค่าความเสียหายทางการเงิน	ระดับผลกระทบ
≤1,000,000 บาท	ต่ำ
1,000,000 – 100,000,000 บาท	กลาง
>100,000,000 บาท	สูง

ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555

2. ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัย แบ่งเป็น 3 ระดับ โดยคำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบใน 1 วัน

จำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัย	ระดับ ผลกระทบ
ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิตร่างกายหรืออนามัย	ต่ำ
มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่ 1 - 1,000 คน	กลาง
มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย >1,000 คน หรือต่อชีวิตตั้งแต่ 1 คน	สูง

ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555

3. ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นใดนอกจากข้อ 2 แบ่งเป็น 3 ระดับ โดยคำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบใน 1 วันและคำนวณความเสียหายโดยตรงเท่านั้น

จำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบ	ระดับผลกระทบ
≤10,000 คน	ต่ำ
10,000 – 100,000 คน	กลาง
>100,000 คน	สูง

4. ผลกระทบด้านความมั่นคงของรัฐ แบ่งเป็น 2 ระดับ

ผลกระทบด้านความมั่นคงของรัฐ	ระดับผลกระทบ
ไม่มีผลกระทบ	ต่ำ
มีผลกระทบ	สูง

ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555

- การเลือกใช้ระดับของวิธีการแบบปลอดภัย ให้พิจารณาจากผลประเมินที่เป็นผลกระทบดังต่อไปนี้

ผลประเมินที่เป็นผลกระทบ	ระดับของวิธีการแบบปลอดภัย
ระดับสูงด้านหนึ่งด้านใด	เคร่งครัด
ระดับกลางอย่างน้อย 2 ด้านขึ้นไป	กลาง
นอกเหนือจากข้างต้น	พื้นฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

- กรณีที่จะต้องปฏิบัติให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน ให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่กำหนด

- มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นมาตรการสำหรับใช้ในการควบคุมให้ระบบสารสนเทศมีความมั่นคงปลอดภัย ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและสารสนเทศในระบบนั้น โดยการทำธุรกรรมทางอิเล็กทรอนิกส์ด้วยระบบสารสนเทศต้องดำเนินการตามมาตรการที่เกี่ยวข้อง และต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน ทั้งนี้มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ แบ่งออกเป็น 11 ข้อ ได้แก่

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

1. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

- กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติและผลักดันโดยผู้บริหารระดับสูง และมีการประกาศนโยบายให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน

- การวางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ

2. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

- ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใดๆ

- กำหนดสัญญาการรักษาข้อมูลที่เป็นความลับที่สอดคล้องกับสถานการณ์และความต้องการของหน่วยงานในการปกป้องข้อมูลสารสนเทศ

- มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

3. การบริหารจัดการทรัพย์สินสารสนเทศ

- การเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง
- การกำหนดบุคคลผู้มีหน้าที่ดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศไว้ชัดเจน
- การจำแนกประเภทของข้อมูลสารสนเทศ โดยจำแนกตามมูลค่าของข้อมูล ข้อกำหนดทางกฎหมาย ระดับชั้นความลับและความสำคัญต่อหน่วยงาน

4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

- กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของพนักงานหรือหน่วยงานหรือบุคคลภายนอกที่ว่าจ้าง โดยให้สอดคล้องกับความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่หน่วยงานประกาศใช้
- กำหนดให้มีขั้นตอนการลงโทษพนักงานที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในหน่วยงาน
- กำหนดหน้าที่ความรับผิดชอบในการยุติการจ้าง หรือการเปลี่ยนแปลงสถานะการจ้างให้ชัดเจน และมอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

5. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

- มีการป้องกันขอบเขตพื้นที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้ง จัดเก็บ หรือใช้งาน ระบบสารสนเทศและข้อมูลสารสนเทศ
- มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยจากภายนอก ภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ
- มีป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting utilities)

6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

- มีการจัดทำ ปรับปรุง และดูแลเอกสารขั้นตอนการปฏิบัติงานที่อยู่ในสภาพพร้อมใช้งาน เพื่อให้พนักงานสามารถนำไปปฏิบัติได้
- มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่างจ้างปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ
- ติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

7. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

- จัดให้มีนโยบายควบคุมการเข้าถึง โดยจัดทำเป็นเอกสารและมีการติดตามทบทวน
- จัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้อย่างเป็นทางการเพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าใช้งานระบบสารสนเทศใดๆ ของหน่วยงาน
- กำหนดสิทธิในการเข้าถึงระดับสูง ให้ทำอย่างจำกัดและอยู่ภายใต้การควบคุม
- จำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงและข้อกำหนดการใช้งานแอพพลิเคชั่นเพื่อการดำเนินงาน

8. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

- จัดทำข้อกำหนดขั้นต่ำของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศไว้ด้วย
- ดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์
- จำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

9. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

- การรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดผ่านช่องทางการบริหารจัดการที่เหมาะสมโดยเร็วที่สุด

10. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

- กำหนดแผนเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ หลังเกิดเหตุการณ์ที่ทำให้ การดำเนินงานหยุดชะงัก เพื่อให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานตามระดับที่กำหนดไว้ ภายในระยะเวลาที่กำหนดไว้

- ทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

11. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

- มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องตามกฎหมายและข้อกำหนดตามสัญญาต่างๆ ของหน่วยงาน โดยต้องจัดทำเป็นเอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- ป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์
- พนักงานของหน่วยงานต้องดูแลให้งานที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่อยู่ในขอบเขตความรับผิดชอบได้ดำเนินการไปโดยสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

คำนิยาม ม.๓

- ระบบคอมพิวเตอร์
- ข้อมูลคอมพิวเตอร์
- ข้อมูลจราจรทางคอมพิวเตอร์
- ผู้ให้บริการ
- ผู้ใช้บริการ
- พนักงานเจ้าหน้าที่
- รัฐมนตรี

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

กระทำต่อคอมพิวเตอร์

- **ม.๕**: การเข้าถึงระบบคอมฯ
- **ม.๖**: การล่วงรู้มาตรการการป้องกันการเข้าถึง
- **ม.๗**: การเข้าถึงข้อมูลคอมฯ
- **ม.๘**: การดักรับข้อมูลคอมฯ
- **ม.๙**: การรบกวนข้อมูลคอมฯ
- **ม.๑๐**: การรบกวนระบบคอมฯ
- **ม.๑๓**: การจำหน่าย/ เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด

ม.๑๒ บทหนัก

ใช้คอมพิวเตอร์กระทำความผิด

- **ม.๑๑**: Spam mail
- **ม.๑๔**: การปลอมแปลงข้อมูลคอมพิวเตอร์/ เผยแพร่เนื้อหาอันไม่เหมาะสม
- **ม.๑๕**: ความรับผิดของผู้ให้บริการ
- **ม.๑๖**: การเผยแพร่ภาพจากการตัดต่อ/ดัดแปลง

มีผลบังคับใช้ภายหลังประกาศใช้ ๓๐ วัน (ม.๒)

กระทำความผิดนอกราชอาณาจักร ต้องรับโทษภายในราชอาณาจักร์ (ม.๑๗)

การรับฟังพยานหลักฐานที่ได้มาตาม พ.ร.บ. ฉบับนี้ (ม. ๒๕)

หมวด ๒ พนักงานเจ้าหน้าที่

พนักงานเจ้าหน้าที่

อำนาจหน้าที่ (ม.๑๘): (๑) มีหนังสือ/เรียกเพื่อให้ถ้อยคำ/เอกสาร (๒) เรียกข้อมูลจราจร (๓) สั่งให้ส่งมอบข้อมูลที่อยู่ในครอบครอง (๔) ทำสำเนาข้อมูล (๕) สั่งให้ส่งมอบข้อมูล/อุปกรณ์ (๖) ตรวจสอบ/เข้าถึง (๗) ถอดรหัสลับ (๘) ยึด/อายัดระบบ

ข้อจำกัด/การตรวจสอบการใช้อำนาจ (ม.๑๙): ยื่นคำร้องต่อศาลในการใช้อำนาจตาม ม.๑๘ (๔)-(๘) , ส่งสำเนาบันทึกรายละเอียดให้แก่ศาลภายใน ๔๘ ชม., ยึด/อายัดห้ามเกิน ๓๐ วัน ขอขยายได้อีก ๖๐ วัน (ม.๑๘(๘))

การ block เว็บไซต์ (ม.๒๐)

พนักงานเจ้าหน้าที่โดยความเห็นชอบของรมว.ทก.ยื่นคำร้องต่อศาล

ความรับผิดของพนักงานเจ้าหน้าที่: (ม.๒๑ ถึง มาตรา ๒๔)

พยานหลักฐานที่ได้มาโดยมิชอบ อ้างและรับฟังมิได้ (ม.๒๕)

การแต่งตั้ง/กำหนดคุณสมบัติพนักงานเจ้าหน้าที่/การประสานงาน (ม.๒๘-๒๙)

ผู้ให้บริการ

ม.๒๖: เก็บข้อมูลจราจร ๙๐ วันไม่เกิน ๑ ปี

ม.๒๗: ไม่ปฏิบัติตามคำสั่งพนักงานเจ้าหน้าที่หรือคำสั่งศาล ระวางโทษปรับ

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

35

มาตรา ๕	การเข้าถึงระบบคอมพิวเตอร์
มาตรา ๖	การล่วงรู้มาตรการป้องกันการเข้าถึง
มาตรา ๗	การเข้าถึงข้อมูลคอมพิวเตอร์
มาตรา ๘	การดักข้อมูลคอมพิวเตอร์โดยมิชอบ
มาตรา ๙	การรบกวนข้อมูลคอมพิวเตอร์
มาตรา ๑๐	การรบกวนระบบคอมพิวเตอร์
มาตรา ๑๑	สแปมเมล์ (Spam Mail)
มาตรา ๑๒	การกระทำความผิดต่อความมั่นคง
มาตรา ๑๓	การจำหน่าย/เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด
มาตรา ๑๔	การปลอมแปลงข้อมูลคอมพิวเตอร์/เผยแพร่เนื้อหาอันไม่เหมาะสม
มาตรา ๑๕	ความรับผิดของผู้ให้บริการ
มาตรา ๑๖	การเผยแพร่ภาพจากการตัดต่อ/ดัดแปลง

พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

มาตราที่	เรื่อง	สิ่งที่แก้ไข
๑	ชื่อ พรบ.	พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐”
๒	กำหนดการบังคับใช้	พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศ ในราชกิจจานุเบกษาเป็นต้นไป
๔, ๑๒, ๑๔, ๑๕, ๑๖ ๑๘ ๑๙ ๒๐ ๒๒ ๒๓ ๒๔ ๒๕	-	ยกเลิกและใช้ข้อความใหม่
๑๑	สแปมเมล์	เพิ่มข้อความเป็นวรรคสองและวรรคสาม
๑๒/๑	บทหนักกรณีกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐	เพิ่มเป็นมาตราใหม่
๑๓	การจำหน่าย/เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด	เพิ่มข้อความเป็นวรรคสอง วรรคสาม วรรคสี่ และวรรคห้า
๑๖/๑, ๑๖/๒	คำสั่งศาลกรณีกระทำความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖	เพิ่มเป็นมาตราใหม่

พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

มาตราที่	เรื่อง	สิ่งที่แก้ไข
๑๗/๑	อำนาจของคณะกรรมการเปรียบเทียบ	เพิ่มเป็นมาตราใหม่
๒๑	ความรับผิดของพนักงานเจ้าหน้าที่	ยกเลิกความในวรรคสองและใช้ข้อความใหม่
๒๖	การเก็บข้อมูลจราจร	ยกเลิกความในวรรคหนึ่งและใช้ข้อความใหม่
๒๘	การแต่งตั้ง/กำหนดคุณสมบัติพนักงานเจ้าหน้าที่/การประสานงาน	เพิ่มข้อความเป็นวรรคสองและวรรคสาม
๓๑	ค่าใช้จ่ายและวิธีการเบิกจ่ายในการดำเนินการใดๆ	เพิ่มเป็นมาตราใหม่