รหัสเอกสาร IT_P01
Rev.02

Asiametal
Public Company Limited

นโยบายการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศ

(Information Technology Security Policy)

ประกาศ ณ วันที่ 31 สิงหาคม 2565

ลงชื่อ ..... (ผู้อนุมัติ)
(.....)
ผู้บริหาร

ประวัติการจัดทำ และทบทวนเอกสาร

ครั้งที่	วันที่แก้ไข	รายละเอียด
00	06/11/2560	ออกเอกสารครั้งแรกโดยอ้างอิงให้สอดคล้องกับมาตรฐาน ISO/IEC 270001
01	14/08/2562	เพิ่มเนื้อหาของนโยบายการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศ
02	31/08/2565	เพิ่มเนื้อหาของนโยบายการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศ

สารบัญ

หัวข้อ **หน้า**

1. บทนำ

ปัจจุบันมีการใช้เทคโนโลยีสารสนเทศ (Information Technology - IT) ในธุรกิจของบริษัท เอเซีย เมทัล จำกัด (มหาชน) เพื่อช่วยให้การดำเนินธุรกิจของบริษัทในเครือเป็นไปด้วยความสะดวกรวดเร็วและถูกต้อง มีการจัดเก็บและบริหารจัดการข้อมูลหลายประเภทด้วยระบบเทคโนโลยีสารสนเทศ ไม่ว่าจะเป็นข้อมูลลูกค้า ข้อมูลการจัดจำหน่าย ข้อมูลการให้บริการธุรกิจ ข้อมูลด้านบุคลากร ข้อมูลด้านการบัญชี และข้อมูลที่ใช้งานอื่นๆ ที่เกี่ยวข้อง

การใช้ระบบเทคโนโลยีสารสนเทศดังกล่าว อาจก่อให้เกิดความเสี่ยงหลายประการ ได้แก่ ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลในระบบเทคโนโลยีสารสนเทศในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ (Access Risk), ความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบเทคโนโลยีสารสนเทศ (Integrity Risk), ความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบเทคโนโลยีสารสนเทศได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ (Availability Risk) และความเสี่ยงเกี่ยวกับการมิได้จัดให้มีการบริหารจัดการระบบเทคโนโลยีสารสนเทศและเจ้าหน้าที่เทคโนโลยีสารสนเทศให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ (Infrastructure Risk) ซึ่งความเสี่ยงตามที่กล่าวอาจส่งผลกระทบต่อการดำเนินงานหรือก่อให้เกิดความเสียหายต่อบริษัทและลูกค้าได้

ฝ่ายเทคโนโลยีสารสนเทศ บริษัท เอเซีย เมทัล จำกัด (มหาชน) ผู้ดูแลรับผิดชอบการใช้งานระบบเทคโนโลยีสารสนเทศ ของมาลาคีได้ตระหนักถึงความสำคัญเกี่ยวกับการควบคุมการปฏิบัติงานและความปลอดภัยด้านเทคโนโลยีสารสนเทศ จึงได้จัดทำนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้บริษัทสามารถใช้เทคโนโลยีสารสนเทศในธุรกิจของบริษัทได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือทั้งต่อลูกค้าและผู้ที่เกี่ยวข้อง

2. วัตถุประสงค์

2.1. เพื่อใช้เป็นแนวทางกำหนดมาตรการ วิธีการปฏิบัติงาน และระบบการควบคุมภายในเพื่อควบคุมการปฏิบัติงาน และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

2.2. เพื่อเป็นแนวทางปฏิบัติ ให้การสนับสนุนการดำเนินการ ด้านรักษาความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศของบริษัท เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2554

3. ขอบเขต

นโยบายฉบับนี้ให้บังคับใช้กับพนักงาน ผู้บริหารทุกระดับ ผู้ให้บริการ ที่ปรึกษา และบุคคล/นิติบุคคลที่ปฏิบัติหน้าที่ตามสัญญาจ้างงาน ที่ได้ใช้ทรัพยากร และระบบเทคโนโลยีสารสนเทศของบริษัท ให้มีผลครอบคลุมถึง ข้อมูล และระบบเทคโนโลยีสารสนเทศทั้งปวงของบริษัท แต่ไม่รวมถึงข้อมูลทดสอบ และระบบเครื่องคอมพิวเตอร์อื่นใดที่มิได้เชื่อมโยงกับระบบเทคโนโลยีสารสนเทศของบริษัท

4. คำนิยาม

"บริษัท"	หมายถึง	บริษัท เอเซีย เมทัล จำกัด (มหาชน)
"ระบบเทคโนโลยีสารสนเทศ"	หมายถึง	อุปกรณ์ (Hardware) หรือโปรแกรม (Software) หรือระบบคอมพิวเตอร์ ตลอดจนระบบเครือข่ายที่ใช้งานในบริษัท
"ฝ่ายเทคโนโลยีสารสนเทศ"	หมายถึง	หน่วยงานที่รับผิดชอบดูแลระบบเทคโนโลยีสารสนเทศของบริษัท และให้หมายความรวมถึงสถานที่ปฏิบัติงานของเจ้าหน้าที่เทคโนโลยีสารสนเทศ
"พนักงาน"	หมายถึง	พนักงานของบริษัท ทั้งพนักงานประจำ ลูกจ้างชั่วคราว หรือพนักงานฝึกงาน และให้หมายความรวมถึงบุคคลอื่นที่บริษัทแต่งตั้ง
"เจ้าหน้าที่เทคโนโลยีสารสนเทศ"	หมายถึง	พนักงานของบริษัทที่ปฏิบัติงานในฝ่ายเทคโนโลยีสารสนเทศ
"บุคคลภายนอก"	หมายถึง	บุคคลที่ไม่ใช่พนักงานของบริษัท เช่น ผู้ให้บริการ, ลูกค้า, ผู้ขายสินค้า เป็นต้น
"ผู้ให้บริการ"	หมายถึง	บุคคลภายนอกที่ให้บริการพัฒนาระบบงาน หรือให้บริการบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์อื่น หรือผู้ให้บริการด้านเทคโนโลยี ซึ่งบริษัท เป็นผู้ใช้บริการ
"ข้อมูล"	หมายถึง	สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบข้อมูลอิเล็กทรอนิกส์ หรือคอมพิวเตอร์ หรือเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"ทรัพย์สินสารสนเทศ"	หมายถึง	ทรัพย์สินซึ่งทางบริษัทเป็นเจ้าของ เช่า ว่าจ้างให้พัฒนา พัฒนาขึ้นเอง หรือซื้อ ได้แก่ ข้อมูลสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่างๆ โปรแกรมคอมพิวเตอร์ อุปกรณ์เชื่อมโยงเครือข่าย ระบบอินทราเน็ต ของบริษัท รวมทั้งการเรียกใช้ ส่งข้อมูล และการค้นหาข้อมูลผ่านทางอินเทอร์เน็ต
"หน่วยงานธุรกิจเจ้าของข้อมูล"	หมายถึง	หน่วยงานที่ก่อให้เกิดข้อมูลขึ้นในบริษัท มีความรับผิดชอบในความถูกต้องของข้อมูล และจัดทำข้อมูลให้เป็นปัจจุบันอยู่เสมอ จัดหมวดหมู่ ดูแล และควบคุมให้มีการรักษาความปลอดภัยที่เหมาะสม รวมถึงเป็นผู้พิจารณาอนุมัติการการเข้าถึงข้อมูล การจัดเก็บ และการทำลายข้อมูล ที่ตนเป็นเจ้าของ
"ผู้ดูแลระบบเทคโนโลยีสารสนเทศ"	หมายถึง	พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่ายคอมพิวเตอร์และระบบฐานข้อมูลของบริษัท
"ผู้ดูแลระบบงาน"	หมายถึง	พนักงานของบริษัทที่ปฏิบัติงานในฝ่ายเทคโนโลยีสารสนเทศ และได้รับมอบหมายให้ดูแลระบบงาน หรือโปรแกรมต่างๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัท
"Asset Owner"	หมายถึง	ผู้ที่ได้รับมอบหมายจากผู้บริหารให้ทำหน้าที่ควบคุมการใช้งาน และปกป้อง Asset นั้นๆ อาจกำหนดเป็นหน่วยงาน หรือตำแหน่งงาน ตามความเหมาะสม
"Asset"	หมายถึง	ทรัพย์สิน หรือสิ่งต่างๆ ที่มีความจำเป็นต่อการดำเนินธุรกิจภายในขอบเขตของระบบสารสนเทศ แบ่งออกได้เป็น 5 ประเภท ได้แก่
1. Information Asset	หมายถึง	ข้อมูลต่างๆ เช่น ฐานข้อมูล หนังสือสัญญา คู่มือปฏิบัติงาน เป็นต้น
2. Software Asset	หมายถึง	ซอฟต์แวร์ต่างๆ เช่น OS Database Development tool เป็นต้น
3. Physical Asset	หมายถึง	อุปกรณ์ต่างๆ เช่น Server Network Equipment PC สื่อบันทึกข้อมูล เป็นต้น
4. Personnel Asset	หมายถึง	บุคลากรในตำแหน่งต่างๆ เช่น Developer System Admin เป็นต้น
5. Service Asset	หมายถึง	บริการที่ได้รับต่างๆ เช่น ระบบปรับอากาศ ระบบแสงสว่าง ระบบสื่อสาร บริการซ่อมบำรุง เป็นต้น
"Inventory of Assets"	หมายถึง	บัญชีทรัพย์สิน ใช้สำหรับบันทึกข้อมูลรายละเอียดต่างๆ ของทรัพย์สิน (Asset) แต่ละประเภท

5. นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security Policy)

1) การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดผังโครงสร้างการจัดการเรื่องการดำเนินการ ระบบการควบคุมความปลอดภัย และกำหนดบทบาทหน้าที่ผู้ที่เกี่ยวข้องอย่างชัดเจน จัดให้มีการแบ่งอำนาจหน้าที่ในการปฏิบัติงาน และจัดให้มีระบบการสอบทานการปฏิบัติงานระหว่างเจ้าหน้าที่เทคโนโลยีสารสนเทศ โดยต้องไม่มอบหมายให้เจ้าหน้าที่เทคโนโลยีสารสนเทศ คนใดคนหนึ่งรับผิดชอบการปฏิบัติงานตลอดกระบวนการในลักษณะที่อาจเป็นช่องทางให้ระบบเทคโนโลยีสารสนเทศของบริษัทถูกแก้ไข หรือเปลี่ยนแปลงโดยมิชอบ ยกเว้นกรณีที่มีความจำเป็นต้องมอบหมายให้เจ้าหน้าที่เทคโนโลยีสารสนเทศคนหนึ่งคนใดปฏิบัติงานหลายหน้าที่ควบคู่กัน ให้กำหนดมาตรการหรือวิธีการกำกับดูแลและควบคุมการปฏิบัติงานของเจ้าหน้าที่เทคโนโลยีสารสนเทศรายดังกล่าวให้รอบคอบ และรัดกุมเพียงพอ เช่น กำหนดให้มีบันทึกการปฏิบัติงาน (Log files) ดังกล่าว และมีการตรวจสอบบันทึกอย่างสม่ำเสมอ เป็นต้น

1.1 แนวทางการปฏิบัติ เรื่ององค์กรการรักษาความปลอดภัยข้อมูลสารสนเทศ

ต้องแต่งตั้งคณะทำงานด้านความปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างเป็นทางการ โดยมีหน้าที่ดังนี้

- กำหนดขอบเขต ทบทวน นโยบายรักษาความปลอดภัยข้อมูลสารสนเทศ (6.1.1) (6.1.2)
- ควบคุม ดูแล และให้ความเห็นชอบในวิธีการและกระบวนการด้านการรักษาความปลอดภัยข้อมูลสารสนเทศ และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (6.1.1) (6.1.2) (14.1.1)
- เป็นศูนย์กลางในการจัดการประเด็นต่างๆ ให้คำแนะนำ และประสานงานกับหน่วยงานต่างๆ ทั้งภายในและภายนอก ในเรื่องที่เกี่ยวกับการรักษาความปลอดภัยข้อมูลสารสนเทศ (6.1.2)
- ตรวจสอบการละเมิดการคุกคามความปลอดภัยข้อมูลสารสนเทศ (6.1.2)
- ป้องกัน สืบหาสาเหตุ และเสนอแนวทางการแก้ไขสำหรับเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูลสารสนเทศ (6.1.8)

1.2 แนวทางการปฏิบัติ เรื่องการแบ่งแยกอำนาจหน้าที่

ต้องไม่กำหนดให้บุคคลเดียวกันปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการ และต้องแบ่งแยกหน้าที่ความรับผิดชอบสำหรับงานที่มีความสำคัญมาก เช่น ผู้ดูแลระบบงาน ผู้ดูแลระบบเครือข่าย ผู้พัฒนาระบบ และผู้ใช้งานระบบเป็นต้น (10.1.3) (10.6.1)

อ้างอิง ISO/IEC27001

6.1.1 Management commitment to information security

6.1.2 Information security co-ordination

6.1.8 Independent review of information security

10.1.3 Segregation of duties

10.6.1 Network control

14.1.1 Including information security in the business continuity management process

2) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และการป้องกันความเสียหาย (Physical Security)

ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีระบบรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้เข้าถึงระบบเทคโนโลยีสารสนเทศที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์ และต้องจัดให้มีระบบป้องกันความเสียหายแก่ระบบเทคโนโลยีสารสนเทศจากปัจจัยสภาวะแวดล้อม หรือภัยพิบัติต่าง ๆ

2.1 แนวทางการปฏิบัติ เรื่องการรักษาความปลอดภัยของศูนย์คอมพิวเตอร์

1. ต้องระบุและจำกัดการเข้าออกในบริเวณพื้นที่ศูนย์คอมพิวเตอร์ โดยอนุญาตเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น (9.1.1) (9.1.5)
2. ต้องควบคุมการเข้าออกภายในบริเวณศูนย์คอมพิวเตอร์ โดยใช้การควบคุมแบบอิเล็กทรอนิกส์ (9.1.1)
3. บันทึกและจัดเก็บการเข้าออกบริเวณศูนย์คอมพิวเตอร์ (9.1.1)
4. ต้องแยกห้องประชุม บริเวณรับรอง หรือบริเวณสาธารณะ จากพื้นที่ศูนย์คอมพิวเตอร์ (9.1.1)

2.2 แนวทางการปฏิบัติ เรื่องการป้องกันความเสียหายต่อระบบเทคโนโลยีสารสนเทศ

1. ต้องมีอุปกรณ์การตรวจและป้องกันอัคคีภัย รวมทั้งระบบและอุปกรณ์ป้องกันอื่นๆ เช่น (9.2.1)
   - ระบบสัญญานเตือนภัย
   - เครื่องตรวจจับควัน
   - เครื่องตรวจจับความร้อน
   - ระบบตัดไฟฟ้าอัตโนมัติ
   - ระบบดับเพลิง
   - เครื่องตรวจวัดระดับและควบคุมความชื้น
   - พื้นยกระดับ
2. ต้องติดตั้งอุปกรณ์ไฟฟ้าสำรอง (UPS) รวมทั้งจัดให้มีการทดสอบและบำรุงรักษาอย่างสม่ำเสมอ (9.2.2)

อ้างอิง ISO/IEC27001

9.1.1 Physical security perimeter

9.1.5 Working in secure areas

9.2.1 Equipment siting and protection

9.2.2 Supporting utilities

3) การรักษาความปลอดภัยข้อมูล ระบบเทคโนโลยีสารสนเทศ และระบบเครือข่าย

(Information System and network Security)

ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีมาตรการเพื่อควบคุมพนักงานที่ไม่เกี่ยวข้อง มิให้เข้าถึง ล่วงรู้ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง โดยมิได้รับอนุญาต พร้อมทั้งจัดให้มีมาตรการป้องกันการบุกรุกผ่านระบบเครือข่ายโดยมีวัตถุประสงค์เพื่อป้องกันบุคคล Virus รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึง หรือสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศ โดยมาตรการต้องมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

3.1 แนวทางการปฏิบัติ เรื่องการควบคุมสิทธิในการเข้าใช้ระบบงานและข้อมูลสารสนเทศ

1. ต้องแบ่งแยกหน้าที่ความรับผิดชอบระหว่างผู้ดูแลระบบเทคโนโลยีสารสนเทศ และผู้ดูแลระบบงานออกจากกัน (10.1.3)
2. ผู้ดูแลระบบเทคโนโลยีสารสนเทศ หรือพนักงานปฏิบัติการคอมพิวเตอร์ และผู้ดูแลระบบงาน ต้องไม่มีหน้าที่เกี่ยวข้องในการบันทึกข้อมูลประจำวันเข้าระบบงาน
3. ต้องจัดทำบัญชีรายชื่อผู้ใช้งานระบบ (11.2.1)
4. ต้องมีการกำหนดชื่อผู้ใช้งานระบบ และรหัสผ่าน สำหรับผู้ใช้ระบบงานเป็นรายบุคคล เพื่อให้ทราบการใช้งานระบบของแต่ละบุคคลได้ (11.2.1)
5. ต้องกำหนดรหัสผ่านเข้าสู่ระบบสำหรับระบบงานที่มีข้อมูลสารสนเทศที่เป็นความลับ และไม่อนุญาตให้ใช้ร่วมกับผู้อื่น (11.3.1) (11.2.3)
6. ต้องกำหนดสิทธิในการใช้ระบบและข้อมูลสารสนเทศสำหรับผู้ใช้แต่ละคนตามบทบาท และหน้าที่รับผิดชอบ โดยการกำหนดสิทธิควรคำนึงถึงหัวข้อต่อไปนี้
   - การรักษาความปลอดภัยในแต่ละระบบงาน (11.1.1)
   - ข้อมูลที่เกี่ยวข้องสำหรับแต่ละระบบงาน (11.1.1)
   - นโยบายการเผยแพร่ และการอนุมัติการใช้ข้อมูลสารสนเทศ (11.1.1)
   - ความสอดคล้องของการกำหนดการเข้าถึงข้อมูลสารสนเทศจากช่องทางต่างๆ และนโยบายการจัดหมวดหมู่ข้อมูลสารสนเทศ (11.1.1)
   - กฎหมายและข้อกำหนดต่างๆ ที่เกี่ยวข้อง (11.1.1)
   - มาตรฐานการเข้าถึงข้อมูลสารสนเทศสำหรับการปฏิบัติงานประเภทเดียวกัน (11.1.1)
   - การจัดการสิทธิในการเข้าถึงข้อมูลในระบบที่สามารถเข้าถึงได้หลายช่องทาง (11.1.1)
   - ต้องสอดคล้องกับวัตถุประสงค์ทางธุรกิจ (11.2.1)
7. การกำหนดสิทธิการใช้งานข้อมูลสารสนเทศ ต้องอนุญาตตามความจำเป็นที่ต้องทราบและนำไปใช้ในการปฏิบัติงานเท่านั้น (11.2.1)
8. ต้องกำหนดขั้นตอนการปฏิบัติงานในการกำหนดสิทธิการใช้ข้อมูลสารสนเทศจนกระทั่งถึงกระบวนการเพิกถอนสิทธิการใช้งาน (11.2.1)

9. ต้องตรวจสอบบัญชีรายชื่อ และสอบทานสิทธิของผู้ใช้ในระบบทุกเดือน เช่น การเพิกถอนสิทธิ กรณีพนักงานลาออก ย้ายหน่วยงาน หรือ เปลี่ยนแปลงหน้าที่รับผิดชอบ (11.2.1)

3.2 แนวทางการปฏิบัติ เรื่องการรักษาความปลอดภัยระบบเครือข่าย

1. การเชื่อมต่ออุปกรณ์ การเข้าถึงระบบงานและข้อมูลสารสนเทศ รวมทั้งการใช้ข้อมูลสารสนเทศต่างๆ จากบุคคลภายนอก จะต้องได้รับอนุมัติจากผู้มีอำนาจที่ได้รับการแต่งตั้งจากบริษัท (11.2.1)
2. ต้องจัดทำเอกสารแสดงการเชื่อมต่อเครือข่ายภายนอกทั้งหมด
3. ต้องกำหนดระเบียบวิธีปฏิบัติเพื่อดูแลประสิทธิภาพ และความพร้อมใช้งานของระบบเครือข่าย (11.4.1)
4. ต้องติดตั้งอุปกรณ์ Firewall เพื่อป้องกันการเข้าถึงระบบเครือข่ายภายใน โดยไม่ได้รับอนุญาต (11.4.2)

อ้างอิง ISO/IEC27001

7.2.1 Classification guidelines

10.1.3 Segregation of duties

11.1.1 Access control policy

11.2.1 User registration

11.3.1 Password use

11.4.1 Policy on use of network services

11.4.2 User authentication for external connections

10.6.2 Security of network services

11.2.3 UserPassword management

11.6.1 Information access restriction

11.6.2 Sensitive system isolation

4) การควบคุมการพัฒนา (Development Management) จัดหา หรือแก้ไขเปลี่ยนแปลงระบบงาน (Change Management)

ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีมาตรการควบคุมที่เพียงพอเพื่อให้ระบบเทคโนโลยีสารสนเทศที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลง มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้านความไม่ถูกต้องครบถ้วนของข้อมูล โดยให้มีมาตรการครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้น ซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง รวมถึงต้องสื่อสารการเปลี่ยนแปลงให้พนักงานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง

4.1 แนวทางการปฏิบัติ เรื่องการควบคุมการพัฒนา/จัดหาระบบงาน

1. การปรับปรุงพัฒนาระบบงานด้านธุรกิจ ต้องสอดคล้องกับความต้องการทางธุรกิจ และความต้องการในการรักษาความปลอดภัยข้อมูลสารสนเทศ
2. คณะทำงานที่จัดทำโครงการจะต้องประกอบด้วยตัวแทนจากหน่วยงานผู้ใช้เข้าร่วมด้วย
3. ในกรณีที่จำเป็น ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอก ต้องมีส่วนร่วมในกระบวนการพัฒนา/จัดหาโปรแกรมที่จะนำมาใช้งาน เพื่อให้คำแนะนำเกี่ยวกับการควบคุมภายในของระบบงาน
4. ต้องตรวจสอบความถูกต้องของข้อมูล รวมทั้งเอกสารต้นฉบับก่อนการบันทึกเข้าระบบงาน (12.2.1)
5. ต้องตรวจสอบโปรแกรมก่อนติดตั้งทุกครั้ง เพื่อให้แน่ใจว่าเป็นรุ่นที่ถูกต้องในการปฏิบัติงาน(12.2.2)
6. ต้องไม่ให้ข้อมูลสำหรับการปฏิบัติงานต่อบุคคลภายนอกเพื่อทดสอบระบบงาน ยกเว้นได้รับการอนุมัติจากหน่วยงานธุรกิจเจ้าของข้อมูล โดยไม่ขัดต่อข้อบังคับหรือระเบียบปฏิบัติงาน
7. การตรวจรับระบบงาน จะต้องคำนึงถึงหัวข้อดังต่อไปนี้ (10.3.2)
   - ความสามารถและสมรรถนะของระบบงาน
   - แผนงานหรือวิธีปฏิบัติกรณีเกิดเหตุฉุกเฉิน
   - วิธีทดสอบระบบ
   - ผลกระทบต่อระบบงานและความปลอดภัยข้อมูลสารสนเทศในปัจจุบัน
   - คู่มือปฏิบัติงาน
   - การฝึกอบรมผู้ปฏิบัติงาน
8. ต้องทดสอบระบบงานโดยผู้พัฒนาระบบ และผู้ใช้ระบบ ก่อนนำโปรแกรมเข้าสู่ระบบสำหรับปฏิบัติงานจริง รวมทั้งต้องมีการควบคุมการเปลี่ยนแปลงที่เหมาะสม เพื่อให้แน่ใจว่าสามารถประมวลผลได้อย่างถูกต้องและมีการรักษาความปลอดภัยที่เพียงพอ (12.4.1, 12.5.1)
9. ต้องจัดให้มีระบบการจัดการและควบคุมทรัพยากรในการพัฒนาโปรแกรม ได้แก่ สารบบ (Directory) คลังในการจัดเก็บโปรแกรม ต้นฉบับ (Source Code) โปรแกรมทำงาน (Executable Code) องค์ประกอบอื่นๆ (Component) เป็นต้น และต้องจัดเก็บโปรแกรมต้นฉบับในสถานที่ปลอดภัย (12.4.3)
10. การติดตั้งหรือถอนการติดตั้งระบบปฏิบัติงานจริง (Production System) ต้องได้รับอนุมัติจากผู้มีอำนาจและกระทำโดยพนักงานปฏิบัติงานคอมพิวเตอร์ซึ่งได้รับอนุญาต (12.4.3)

4.2 แนวทางการปฏิบัติ เรื่องการแก้ไขเปลี่ยนแปลงระบบงาน

1. ต้องจัดทำแผนงานสำหรับพัฒนาและบำรุงรักษาโปรแกรมระบบงานทั้งหมด เมื่อมีการเปลี่ยนแปลงที่สำคัญ ต้องได้รับการอนุมัติจากผู้มีอำนาจก่อน
2. ต้องปรับปรุงเอกสารที่เกี่ยวข้องทุกครั้งที่มีการเปลี่ยนแปลงระบบงาน
3. ต้องอนุญาตให้มีการเปลี่ยนแปลงโปรแกรมสำเร็จรูปเฉพาะในกรณีที่จำเป็นเท่านั้น โดยต้องคำนึงถึงหัวข้อต่อไปนี้ (12.5.3)
   - ความเสี่ยงในการเกิดผลกระทบต่อการควบคุมภายใน และกระบวนการปฏิบัติซึ่งกำหนดไว้ในโปรแกรมสำเร็จรูป
   - การขออนุญาตจากเจ้าของผลิตภัณฑ์
   - ความเป็นไปได้ในการปรับปรุงโปรแกรมตามความต้องการให้เป็นมาตรฐาน โดยเจ้าของผลิตภัณฑ์
   - การบำรุงรักษาโปรแกรมสำเร็จรูปในอนาคต

อ้างอิง ISO/IEC27001

10.1.4 Separation of development, test, and operational facilities

10.3.2 System acceptance

10.7.3 Information handling procedures

10.9.3 Publicly available information

11.6.1 Information access restriction

12.1.1 Security requirements analysis and specification

12.2.1 Input data validation

12.2.2 Control of internal processing

12.4.1 Control of operational software

12.4.3 Access control to program source code

12.5.1 Change control procedures

12.5.3 Restrictions on changes to software packages

5) การสำรองข้อมูล ระบบเทคโนโลยีสารสนเทศ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีมาตรการที่เพียงพอเพื่อให้สามารถใช้ข้อมูล และระบบเทคโนโลยีสารสนเทศได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ เพื่อป้องกันปัญหาด้านความไม่เพียงพอต่อการใช้งาน โดยให้มีมาตรการครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลของระบบเทคโนโลยีสารสนเทศ รวมทั้งการทดสอบและการเก็บรักษา จัดทำและการทดสอบแผนฉุกเฉิน

5.1 แนวทางการปฏิบัติ เรื่องการสำรองข้อมูล

1. ต้องจัดทำคู่มือวิธีปฏิบัติสำหรับการเก็บสำรองข้อมูล รวมทั้งสอบทานการปฏิบัติอย่างสม่ำเสมอ (10.5.1)
2. ต้องจัดทำตารางการสำรองข้อมูล ตามขอบเขตงาน ความถี่ รอบระยะเวลาในการสำรองข้อมูล และต้องจัดเก็บบันทึกการสำรองข้อมูล และปรับปรุงให้เป็นปัจจุบัน (10.5.1)
3. ต้องจัดเก็บข้อมูลที่สำรองไว้ในสถานที่ปลอดภัย เช่น จัดเก็บในสถานที่ซึ่งห่างไกลจากองค์กร หรือเก็บในตู้นิรภัยทนไฟ เป็นต้น และ อนุญาตให้บุคคลที่มีอำนาจเท่านั้นสามารถนำข้อมูลสารสนเทศไปใช้ได้ (10.5.1)
4. ต้องจัดเตรียมอุปกรณ์ในการเก็บสำรองข้อมูลให้พร้อมใช้งาน และทดสอบข้อมูลที่เก็บสำรองไว้เป็นประจำ อย่างน้อยปีละครั้ง เพื่อให้มั่นใจว่าสามารถนำกลับมาใช้งานได้กรณีฉุกเฉินและจำเป็น (10.5.1)
5. ต้องจัดทำคู่มือวิธีการปฏิบัติและกระบวนการในการกู้คืนระบบ พร้อมทั้งทดสอบการปฏิบัติงานตามขั้นตอน (14.1.3)

อ้างอิง ISO/IEC27001

10.5.1 Information back-up

14.1.3 Developing and implementing continuity plans including information security

14.1.4 Business continuity planning framework

14.1.5 Testing, maintenance and re-assessing business continuity plan

6) การควบคุมการปฏิบัติงานประจำด้านเทคโนโลยีสารสนเทศ (Computer Operation)

ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีมาตรการที่เพียงพอในการควบคุมการปฏิบัติงานประจำด้านเทคโนโลยีสารสนเทศเพื่อให้ระบบเทคโนโลยีสารสนเทศและการประมวลผลข้อมูลทำงานได้อย่างต่อเนื่อง ถูกต้องครบถ้วนและมีประสิทธิภาพ โดยให้มีมาตรการครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านต่างๆ ซึ่งได้แก่ การติดตามการทำงานของระบบเทคโนโลยีสารสนเทศ การจัดการปัญหา และการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้านความไม่ถูกต้องครบถ้วนของข้อมูลและความไม่เพียงพอต่อการใช้งาน

แนวทางการปฏิบัติ เรื่องการจัดการด้านปฏิบัติการคอมพิวเตอร์

ต้องจัดทำระเบียบวิธีปฏิบัติงานสำหรับงานด้านปฏิบัติการคอมพิวเตอร์ เช่น เอกสารคู่มือการทำงาน (Operation Manual) ของระบบงาน เพื่อเป็นแนวทางสำหรับผู้ดูแลระบบเทคโนโลยีสารสนเทศ (8.1.1) ซึ่งต้องระบุขั้นตอนการปฏิบัติงานโดยละเอียด เช่น

- กระบวนการประมวลผลข้อมูล (Processing) (10.1.1)(12.2.2)
- รายชื่อผู้ติดต่อและวิธีการในกรณีเกิดเหตุการณ์ผิดปกติ หรือขัดข้องทางเทคนิค (10.1.1)

อ้างอิง ISO/IEC27001

10.1.1 Documented operating procedures

12.2.2 Control of internal processing

7) การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

ในกรณีที่มีการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น ฝ่ายเทคโนโลยีสารสนเทศหรือฝ่ายงานเจ้าของโครงการต้องปฏิบัติตามระเบียบของบริษัทที่กำหนดเกี่ยวกับการคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ รวมทั้งต้องควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าผู้ให้บริการได้ปฏิบัติงานเป็นไปตามขอบเขตที่ได้กำหนดไว้ และจัดให้มีมาตรการควบคุม เพื่อให้การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นเป็นไปอย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้

แนวทางการปฏิบัติ เรื่องการควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น

1. การคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ ต้องเป็นไปตามระเบียบปฏิบัติของบริษัท เพื่อใช้เป็นมาตรการควบคุมการใช้บริการจากผู้ให้บริการภายนอก อย่างมีประสิทธิภาพ และน่าเชื่อถือ
2. ในกรณีที่ใช้บริการด้านการพัฒนาระบบ ต้องกำหนดให้ผู้ให้บริการเข้าถึงได้เฉพาะส่วนของระบบที่เตรียมไว้สำหรับพัฒนาและทดสอบ (Development System) หากมีความจำเป็นต้องเข้าถึงระบบปฏิบัติงานจริง (Production System) จะต้องอยู่ในการควบคุมดูแลอย่างใกล้ชิด โดยต้องไม่ขัดต่อข้อบังคับหรือระเบียบปฏิบัติงาน (8.1.5 a)

อ้างอิง ISO/IEC27001

10.1.4 Separation of development, test, and operational facilities

8) การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Compliance)

ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีมาตรการที่เพียงพอในการตรวจสอบ และประเมินระบบเทคโนโลยีสารสนเทศ เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดด้านความมั่นคงปลอดภัยอื่นๆ เพื่อให้เป็นไปตามนโยบาย และมาตรฐานความมั่นคงปลอดภัยของบริษัท โดยมิให้กระบวนการธุรกิจหยุดชะงัก

แนวทางการปฏิบัติ เรื่องการปฏิบัติตามข้อกำหนดทางด้านกฎหมาย

1. ปฏิบัติตามพระราชบัญญัติ พระราชกิจจานุเบกษา และกฎหมายต่างๆ ที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2554
2. ต้องจัดหาเทคโนโลยีเพื่อรองรับการปฏิบัติตามข้อกำหนดทางด้านกฎหมาย เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ

9) การรักษาความปลอดภัยเกี่ยวกับบุคลากร (Personnel Security)

ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีกระบวนการสรรหาบุคลากร เพื่อลดความเสี่ยงจากความผิดพลาดจากการขโมย การปลอมแปลง และการนำไปใช้ในทางที่ไม่เหมาะสมของพนักงาน ผู้ที่ทำสัญญาว่าจ้าง และหน่วยงานภายนอก ให้เข้าใจบทบาทหน้าที่ความรับผิดชอบ อันเกิดจากการปฏิบัติงานกับระบบเทคโนโลยีสารสนเทศ และทรัพยากรอื่นๆ ของบริษัท และให้มีการอบรมพนักงานให้ตระหนักถึงภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้แก่พนักงานเพื่อให้สามารถป้องกันภัย ดังกล่าวได้

แนวทางการปฏิบัติ เรื่องการรักษาความปลอดภัยเกี่ยวกับบุคลากร

1. พนักงานมีหน้าที่รับผิดชอบในการรักษาความปลอดภัย และดูแลความถูกต้องครบถ้วนของข้อมูลสารสนเทศ รวมทั้งปฏิบัติตามนโยบายการรักษาความปลอดภัยข้อมูลสารสนเทศ (8.1.1)
2. พนักงานจะต้องตระหนักถึงการถูกตรวจสอบด้านการรักษาความปลอดภัยข้อมูลสารสนเทศ เป็นสิ่งจำเป็นและพึงปฏิบัติ (15.1.5)
3. พนักงานทุกคนต้องได้รับการอบรมเพื่อให้ตระหนักถึงการรักษาความปลอดภัยข้อมูลสารสนเทศ เพื่อให้เข้าใจถึงภัยคุกคามที่อาจเกิดขึ้นต่อระบบสารสนเทศ (8.2.2)
4. การประพฤติปฏิบัติที่ละเมิดต่อนโยบายการรักษาความปลอดภัยข้อมูลสารสนเทศ ต้องมีบทลงโทษที่ชัดเจน (8.1.3) (8.2.3)

อ้างอิง ISO/IEC27001

6.1.1	8.1.1	Roles and responsibilities
6.1.4	8.1.3	Terms and conditions of employment
6.2.1	8.2.2	Information security awareness, education, and training
6.3.5	8.2.3	Disciplinary process
12.1.5	15.1.5	Prevention of misuse of information processing facilities

10) การบริหารจัดการทรัพย์สิน (Asset Management)

1. ระบุรายละเอียดของ Asset และการเปลี่ยนแปลงที่มี

Asset Owner ระบุรายละเอียดของการเปลี่ยนแปลงของ Asset ที่อยู่ในความรับผิดชอบเมื่อรับทราบว่ามีการเปลี่ยนแปลงต่อ Asset เกิดขึ้น โดยการเปลี่ยนแปลงสามารถจำแนกได้เป็น 3 แบบ คือ

1.1. การเพิ่มเติม Asset

ระบุ Asset ที่มีการเพิ่มเติมรวมถึงรายละเอียดต่างๆ บันทึกข้อมูลลงใน Inventory of Assets สำหรับรายละเอียดของ Asset แต่ละประเภทมีดังนี้

• Information Asset รายละเอียดที่ต้องระบุคือ ชื่อข้อมูล ระดับชั้นความลับ รูปแบบ(กระดาษ ไฟล์) ที่จัดเก็บ การสำรองข้อมูล Asset Owner กฎหมายที่เกี่ยวข้อง สำหรับระดับชั้นความลับให้อ้างอิงตามตารางต่อไปนี้

ชั้นความลับ	คำอธิบาย
Secret	ข้อมูลที่เปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตที่กำหนดไว้เท่านั้น
Confidential	ข้อมูลที่เปิดเผยได้เฉพาะในส่วนงานเดียวกันเท่านั้น
Internal Use Only	ข้อมูลที่เปิดเผยได้ภายในองค์กรเท่านั้น
Public	ข้อมูลที่เปิดเผยสู่สาธารณะได้

• Software Asset รายละเอียดที่ต้องระบุคือ ชื่อและรุ่นของซอฟต์แวร์ ประเภท(Commercial, In-house Developed, Free, Open source) จำนวน License วันที่หมดอายุ บรรจุภัณฑ์ ที่จัดเก็บ เครื่องที่ติดตั้ง Asset Owner กฎหมายที่เกี่ยวข้อง

• Hardware Asset รายละเอียดที่ต้องระบุคือ ชื่ออุปกรณ์ Spec จำนวน สถานที่ติดตั้ง Asset Owner กฎหมายที่เกี่ยวข้อง

• Personnel Asset รายละเอียดที่ต้องระบุคือ ชื่อตำแหน่ง ประเภท(Normal, Temporary, Outsource) จำนวน Asset Owner กฎหมายที่เกี่ยวข้อง

• Service Asset รายละเอียดที่ต้องระบุคือ ลักษณะของบริการ ชื่อผู้ให้บริการ ชื่อผู้ประสานงานและเบอร์ติดต่อ Asset Owner กฎหมายที่เกี่ยวข้อง

1.2. การเปลี่ยนแปลงรายละเอียดของ Asset

ระบุรายละเอียดของ Asset ตามข้อ 1.1 ส่วนที่มีการเปลี่ยนแปลงเกิดขึ้น และปรับปรุงข้อมูลใน Inventory of Assets ให้เป็นปัจจุบัน

1.3. การยกเลิกการใช้งาน Asset

ระบุ Asset ที่ยกเลิกการใช้งาน ปรับปรุงข้อมูลใน Inventory of Assets โดยบันทึกวันที่ยกเลิกการใช้งานลงในช่อง "Remark" ท้าย Asset ที่ต้องการยกเลิก ทำการ Highlight Row เป็นสีเทาเพื่อความชัดเจน ห้ามลบข้อมูลของ Asset ที่ยกเลิกการใช้งานออก

2. กำหนด Group ของ Asset

Asset Owner กำหนดกลุ่มของ Asset เพื่อใช้เป็นข้อมูลสำหรับการประเมินความเสี่ยง โดยพิจารณาจับกลุ่มดังนี้

• เป็น Asset ประเภทเดียวกัน และใช้ในงานใกล้เคียงกัน เช่น กลุ่มของเครื่อง PC ที่ใช้ในแผนกเดียวกัน

• เป็น Asset ต่างประเภทที่ทำงานร่วมกันเช่น กล้อง+ซอฟต์แวร์ควบคุม+เครื่องติดตั้ง รวมเป็นระบบ CCTV

• เป็น Asset ที่ถูกดูแลควบคุมด้วยวิธีเดียวกัน เช่น กลุ่มของคู่มือระบบ อาจมีทั้งคู่มือที่เป็นความลับ และไม่ลับ แต่ได้รับการจัดเก็บ ควบคุมการนำไปใช้งาน เหมือนกัน

Asset เดียวอาจอยู่ในหลายกลุ่ม หรืออาจไม่ถูกจับกลุ่มได้เช่นกัน ขึ้นกับความเหมาะสม และความเสี่ยงที่มีอยู่ บันทึกกลุ่มของ Asset ลงในช่อง Risk Assessment Item

3. กำหนด Value ของ Asset และ Group

Asset Owner ร่วมกับผู้ที่มีส่วนเกี่ยวข้อง เช่น ผู้ใช้งาน ทำการกำหนดหรือปรับปรุง Value ของ Asset โดยประเมินค่าจากผลกระทบหากสูญเสียคุณสมบัติในแต่ละด้านของ Information Security ดังนี้

• ความลับ (Confidentiality) หากข้อมูลถูกเปิดเผยไปสู่ผู้ที่ไม่ได้รับอนุญาต จะเกิดความเสียหายในระดับใด

• ความถูกต้องครบถ้วน (Integrity) หากข้อมูลถูกบิดเบือน แก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต จะเกิดความเสียหายในระดับใด

• ความมีพร้อมใช้ (Availability) หากข้อมูลไม่สามารถใช้งานได้เมื่อต้องการ จะเกิดความเสียหายระดับใด

โดย Value ของ Asset แบ่งเป็น 5 ระดับ ดังตารางต่อไปนี้

	ผลกระทบหากสูญเสีย C,I,A ไป			
Asset Value	จำนวนเงิน (บาท)	ภาพลักษณ์	ชีวิตของผู้เกี่ยวข้อง	ธุรกิจหยุดชะงัก
Very High	มากกว่า 25% ของมูลค่าทรัพย์สินบริษัทรวมกับกำไรต่อปี	ภาพลักษณ์สูญเสียถาวร ลูกค้าหมดความเชื่อถือ	ตายหรือบาดเจ็บจำนวนมาก	มากกว่า 1 สัปดาห์
High	2.5% - 25% ของมูลค่าทรัพย์สินบริษัทรวมกับกำไรต่อปี	ส่งผลกับภาพลักษณ์ขององค์กรค่อนข้างสูง ลูกค้าอาจเลิกใช้บริการ	ตาย, พิการ, บาดเจ็บสาหัสจำนวนไม่มาก หรือบาดเจ็บปานกลางจำนวนมาก	ไม่เกิน 1 สัปดาห์
Medium	0.25% - 2.5% ของมูลค่าทรัพย์สินบริษัทรวมกับกำไรต่อปี	กระทบกับภาพลักษณ์ขององค์กรเล็กน้อย ส่งผลกับความเชื่อมั่นของลูกค้าบ้าง	บาดเจ็บปานกลาง เช่น กระดูกหัก	ไม่เกิน 1 วัน
Low	0.025 - 0.25% ของมูลค่าทรัพย์สินบริษัทรวมกับกำไรต่อปี	ไม่กระทบภาพลักษณ์	บาดเจ็บเล็กน้อย	ไม่เกิน 1 ชั่วโมง
Very Low	น้อยกว่า 0.025% ของมูลค่าทรัพย์สินบริษัทรวมกับกำไรต่อปี	ไม่กระทบภาพลักษณ์	ไม่บาดเจ็บ	หยุดชะงักในระดับที่ไม่มีผลกระทบ

4. ปรับปรุงข้อมูลใน Track changes

Asset Owner ระบุรายละเอียดของการปรับปรุงแก้ไขแต่ละครั้งลงในหน้า "Track Changes" โดยละเอียด และต้องทำการปรับปรุง Version ของ Inventory of Assets ด้วยทุกครั้ง

5. รายงานการเปลี่ยนแปลงต่อผู้อำนวยการสำนักคอมพิวเตอร์

Asset Owner แจ้งการเปลี่ยนแปลงของ Asset ในความรับผิดชอบของตนในส่วนที่มี Value ตั้งแต่ระดับ High ขึ้นไปต่อผู้อำนวยการสำนักคอมพิวเตอร์เพื่อรับทราบ

11) การควบคุมการเข้าถึง (Access Control)

การควบคุมการเข้าถึงระบบ (Access Control) เพื่อเป็นแนวปฏิบัติสำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศได้อย่างเหมาะสม

การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ (Access Control)

1. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน จำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

2. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้สารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

Super User = ALL

DBA User = Tables (Create/Drop/Read/write/Insert/delete), Grant Privilege

Developer = Read /Write ขึ้นกับความจำเป็นของระบบงาน

Operator User = Read (For Backup)

Audit User = Read

3. กำหนดเกณฑ์การระงับสิทธิ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งานที่ได้กำหนดไว้

4. ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย

การควบคุมการเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (ห้อง Server)

เนื่องจากห้องเครื่องคอมพิวเตอร์แม่ข่าย (ห้อง Server)เป็นสถานที่สำหรับจัดเก็บเครื่องแม่ข่ายที่มีการติดตั้งระบบเทคโนโลยีสารสนเทศที่สำคัญของบริษัทฯ อุปกรณ์เครือข่ายหลัก และระบบสำรองไฟ (UPS)

ดังนั้น เพื่อให้การเข้าออกห้อง SERVER เป็นไปด้วยความสะดวก เรียบร้อย มีความปลอดภัยทั้งข้อมูลและอุปกรณ์ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร บริษัทฯ จึงได้กำหนดระบบผ่านเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (ห้อง Server) และได้กำหนดสิทธิ์การเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (ห้อง Server) เฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง

สำหรับเจ้าหน้าที่ ที่มีความจำเป็นต้องเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (ห้อง Server) แต่ไม่ได้รับการกำหนดสิทธิ์ จะต้องแจ้งให้เจ้าหน้าที่ ผู้ดูแลระบบทราบ เพื่อเป็นผู้นำเข้าห้อง SERVER เท่านั้น

อนุมัติสิทธิ์เข้า-ออกและการปฏิบัติงานในห้องเครื่องคอมพิวเตอร์แม่ข่าย (ห้อง Server) สำหรับบุคคลภายนอก **โดยอ้างอิงตามเอกสาร** แบบฟอร์ม FM-IT-27 ใบขออนุญาตเข้าปฏิบัติงานของแผนกเทคโนโลยีสารสนเทศ

12) การเข้ารหัสข้อมูล (Cryptography)

การเข้ารหัสข้อมูลมีจุดประสงค์เพื่อรักษาความลับของข้อมูล ข้อมูลนั้นจะถูกเปิดอ่านโดยบุคคลที่ได้รับอนุญาตเท่านั้น ยมีการตรวจสอบการเข้าสู่ระบบ มีการพิสูจน์ตัวตน คือกระบวนการแสดงหลักฐาน และตรวจสอบความถูกต้องของของบุคคลหรือคอมพิวเตอร์ เพื่อให้ทราบว่าบุคคลหรือคอมพิวเตอร์ที่กล่าวอ้างนั้นเป็นตัวจริงหรือไม่ **โดยอ้างอิงตามเอกสาร**

IT_P03 แผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ (IT Contingency Plan)

ในหน้าที่ 8 ในหัวข้อที่ *10. การตรวจสอบการเข้าสู่ระบบ และ 11. การบริหารการจัดการเกี่ยวกับการกำหนดรหัสผู้ใช้งาน*

13) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

ความมั่นคงปลอดภัย (Security) คือ สถานะที่มีความปลอดภัยไร้กังวล หรืออยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ

ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information System Security) คือการป้องกันข้อมูลสารสนเทศรวมถึงองค์ประกอบอื่นๆ ที่เกี่ยวข้อง เช่น ระบบและฮาร์ดแวร์ที่ใช้ในการจัดเก็บและถ่ายโอนข้อมูลสารสนเทศนั้นให้รอดพ้นจากอันตรายอยู่ในสถานะที่มีความปลอดภัยไร้ความกังวลและความกลัว

การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)
การรักษาความปลอดภัยด้านการสื่อสารถูกพัฒนามาอย่างต่อเนื่อง โดยเฉพาะในช่วงสงครามที่ข้อมูลข่าวสารเป็นปัจจัยสำคัญของชัยชนะ **โดยอ้างอิงตามเอกสาร**

IT_P02 ระเบียบว่าด้วยการใช้งาน ระบบเทคโนโลยีสารสนเทศ สำหรับพนักงาน

IT_P03 แผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ (IT Contingency Plan)

IT_P04 แผนรองรับสถานการณ์ฉุกเฉิน ระบบสารสนเทศ (Information System Contingency Plan)

IT_P05 การบริหารจัดการความเสี่ยงด้านสารสนเทศ

14) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศ ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

1. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ อ้างอิงตามเอกสาร WI-IT-08 แนวปฏิบัติที่สอดคล้องกับการปฏิบัติงาน และ การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
2. การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย
3. การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย ที่สังเกตุพบหรือเกิดความสงสัยในระบบ
4. การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ มีการตัดสินว่าสถานการณ์ นั้นถือเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่
5. การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ เมื่อเกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้
6. การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้วและเตรียมการปูองกันที่จ าเป็นไว้ล่วงหน้า
7. การเก็บรวบรวมหลักฐาน สำหรับอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

15) นโยบายครอบคลุมข้อมูลส่วนบุคคล (Personal Data)

เพื่อเป็นการควบคุมการใช้งานระบบคอมพิวเตอร์และอุปกรณ์อิเลคทรอนิค เพราะคอมพิวเตอร์เป็นส่วนหนึ่งในชีวิตประจำวัน และมีการใช้คอมพิวเตอร์โดยมิชอบ ซึ่งส่งผลเสียต่อบุคคลอื่น นอกจากนี้ยังมีการใช้งานคอมพิวเตอร์ในการเผยแพร่ข้อมูลที่เป็นเท็จหรือลามกอนาจาร ดังนั้นจึงต้องมีมาตรการควบคุมการใช้คอมพิวเตอร์

การกำหนดนโยบาย ระเบียบปฏิบัติ เพื่อให้ผู้ที่ใช้งานระบบคอมพิวเตอร์ได้รู้ถึงกฎหมาย ตาม พ.ร.บ. คอมพิวเตอร์ ฉบับ 25560 และ บทลงโทษตามกฎหมาย เพื่อไม่ให้ผู้ใช้งานในระบบคอมพิเตอร์ กระทำผิดที่ขัดต่อข้อกฎหมายและสามารถนำไปเผยแพร่ต่อบุคคลอื่น เพื่อนำไปใช้ในชีวิตประจำวันได้

รายละเอียด กฎหมาย พ.ร.บ. คอมพิวเตอร์ 2560

อ้างอิง http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF

พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร

ให้ไว้ ณ วันที่ ๒๓ มกราคม พ.ศ. ๒๕๖๐

เป็นปีที่ ๒ ในรัชกาลปัจจุบัน

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร มีพระราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ๒๕๖๐"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้ยกเลิกความในมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่กับออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงและประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้"

มาตรา ๔ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๑๑ แห่งพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิด ความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับ สามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกิน สองแสนบาท

ให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของ ข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ และลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย"

มาตรา ๕ ให้ยกเลิกความในมาตรา ๑๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษา ความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่ สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึง สองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาท ถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่น ถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท" มาตรา ๖ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๒/๑ แห่งพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"มาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตราย แก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่น ถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท"

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

"ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำ ความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำ ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญา ตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำ ความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่ง หรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่าย หรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสาม หรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว"

มาตรา ๘ ให้ยกเลิกความในมาตรา ๑๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย แก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิด ความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิด ความตื่นตระหนกแก่ประชาชน

๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูล คอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได

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

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใด บุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้"

มาตรา ๙ ให้ยกเลิกความในมาตรา ๑๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๕ ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิด ตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิด ตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของ ข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้อง รับโทษ"

มาตรา ๑๐ ให้ยกเลิกความในมาตรา ๑๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็น การติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระท ำไม่มีความผิด ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย"

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

"มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลย มีความผิด ศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณา หรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำ ความผิดนั้น

มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลาย ตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี"

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

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

คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคนหนึ่งต้องเป็น พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับ ตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกัน ตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ต้องหาไม่ได้ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่ นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว"

มาตรา ๑๓ ให้ยกเลิกความในมาตรา ๑๘ และมาตรา ๑๙ แห่งพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มี เหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสอง ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็น หลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มี เหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครอง ของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับ การกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับ ของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับ ดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียด แห่งความผิดและผู้กระทำความผิด

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณา ความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิด หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวน อาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริง ดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่ รีบรวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (๑) (๒) และ (๓) ดำเนินการ ตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงาน

เจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาต จากพนักงานเจ้าหน้าที่ ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดระยะเวลาที่ต้องดำเนินการ ที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการ ตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่ง อย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณา คำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนา บันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของ หรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันที ที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายใน สี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควร เชื่อได้ว่ามีการกระทำความผิด และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครอง ข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัด มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึด หรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มี เขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้ง รวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง" มาตรา ๑๔ ให้ยกเลิกความในมาตรา ๒๐ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๒๐ ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ดังต่อไปนี้ พนักงานเจ้าหน้าที่ โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มี คำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้

(๑) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัตินี้

(๒) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ ในภาค ๒ ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา

(๓) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และเจ้าหน้าที่ตามกฎหมายนั้นหรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพจารณาความอาญาได้ร้องขอ

ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ จะมอบหมายให้พนักงานเจ้าหน้าที่ยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่ง ระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้ ทั้งนี้ ให้นำบทบัญญัติ ว่าด้วยคณะกรรมการที่มีอำนาจดำเนินการพิจารณาทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการ ทางปกครองมาใช้บังคับกับการประชุมของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์โดยอนุโลม

ให้รัฐมนตรีแต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ตามวรรคสองขึ้นคณะหนึ่ง หรือหลายคณะ แต่ละคณะให้มีกรรมการจำนวนเก้าคนซึ่งสามในเก้าคนต้องมาจากผู้แทนภาคเอกชน ด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ หรือด้านอื่นที่เกี่ยวข้อง และให้กรรมการ ได้รับค่าตอบแทนตามหลักเกณฑ์ที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

การดำเนินการของศาลตามวรรคหนึ่งและวรรคสอง ให้นำประมวลกฎหมายวิธีพิจารณาความอาญา มาใช้บังคับโดยอนุโลม ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ตามวรรคหนึ่งหรือวรรคสอง พนักงานเจ้าหน้าที่จะทำการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ นั้นเองหรือจะสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้รัฐมนตรี ประกาศกำหนดหลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือ ลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการให้เป็นไปในแนวทางเดียวกันโดยคำนึงถึงพัฒนาการ ทางเทคโนโลยีที่เปลี่ยนแปลงไป เว้นแต่ศาลจะมีคำสั่งเป็นอย่างอื่น

ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่จะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่จะได้รับ ความเห็นชอบจากรัฐมนตรี หรือพนักงานเจ้าหน้าที่โดยความเห็นชอบของคณะกรรมการกลั่นกรอง ข้อมูลคอมพิวเตอร์จะยื่นคำร้องตามวรรคสองไปก่อนที่รัฐมนตรีจะมอบหมายก็ได้ แต่ทั้งนี้ต้องรายงาน ให้รัฐมนตรีทราบโดยเร็ว"

มาตรา ๑๕ ให้ยกเลิกความในวรรคสองของมาตรา ๒๑ แห่งพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่ง หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง เว้นแต่ เป็นชุดคำสั่งไม่พึงประสงค์ที่อาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ทั้งนี้ รัฐมนตรี อาจประกาศในราชกิจจานุเบกษากำหนดรายชื่อ ลักษณะ หรือรายละเอียดของชุดคำสั่งไม่พึงประสงค์ ซึ่งอาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์ก็ได้"

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

และพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสอง เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มา ตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิด ตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นในกรณีตามมาตรา ๑๘ วรรคสอง หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือกับพนักงานสอบสวนในส่วนที่เกี่ยวกับการปฏิบัติหน้าที่ตามมาตรา ๑๘ วรรคสอง โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสอง ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูล ของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของ ผู้ใช้บริการที่พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อ ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มา ตามพระราชบัญญัตินี้หรือที่พนักงานสอบสวนได้มาตามมาตรา ๑๘ วรรคสอง ให้อ้างและรับฟังเป็น พยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบ ประการอื่น"

มาตรา ๑๗ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใด เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะราย และเฉพาะคราวก็ได้"

มาตรา ๑๘ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๒๘ แห่งพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ อาจได้รับค่าตอบแทนพิเศษ ตามที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

ในการกำหนดให้ได้รับค่าตอบแทนพิเศษต้องคำนึงถึงภาระหน้าที่ ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่หรือมีการสูญเสียผู้ปฏิบัติงานออกจากระบบราชการเป็นจำนวนมาก คุณภาพของงาน และการดำรงตนอยู่ในความยุติธรรมโดยเปรียบเทียบค่าตอบแทนของผู้ปฏิบัติงานอื่น ในกระบวนการยุติธรรมด้วย"

มาตรา ๑๙ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๓๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"มาตรา ๓๑ ค่าใช้จ่ายในเรื่องดังต่อไปนี้ รวมทั้งวิธีการเบิกจ่ายให้เป็นไปตามระเบียบที่รัฐมนตรี กำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

(๑) การสืบสวน การแสวงหาข้อมูล และรวบรวมพยานหลักฐานในคดีความผิดตามพระราชบัญญัตินี้

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

(๓) การดำเนินการอื่นใดอันจำเป็นแก่การป้องกันและปราบปรามการกระทำความผิด ตามพระราชบัญญัตินี้"

มาตรา ๒๐ บรรดาระเบียบหรือประกาศที่ออกตามพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ยังคง ใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติแห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ จนกว่าจะมีระเบียบหรือประกาศที่ต้อง ออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติม โดยพระราชบัญญัตินี้ ใช้บังคับ

การดำเนินการออกระเบียบหรือประกาศตามวรรคหนึ่ง ให้ดำเนินการให้แล้วเสร็จภายในหกสิบวัน นับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีว่าการกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคมรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

มาตรา ๒๑ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการ ตามพระราชบัญญัติน

6. บทลงโทษ

การกระทำใดๆ ที่เข้าข่ายละเมิด หรือฝ่าฝืน หรือการละเว้นไม่ปฏิบัติตามนโยบายฉบับนี้ รวมถึงขั้นตอน หรือวิธีปฏิบัติที่จัดทำขึ้นเพื่อรองรับนโยบายฉบับนี้ ถือว่ามีความผิดทางวินัยและจะถูกลงโทษตามระเบียบของบริษัท