คำสั่งบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

ที่ รบ.20/2564

เรื่อง การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อเป็นการกำหนดทิศทาง หลักการ ตลอดจนขอบเขตและวิธีการในการดำเนินการที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงการป้องกันสารสนเทศให้ปลอดภัยจากภัยคุกคามที่ก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) และสอดคล้องกับมาตรฐานสากล ISO/IEC 27001:2013 รวมทั้งครอบคลุมสาระสำคัญในกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติระบบการชำระเงิน พศ.2560 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 ทั้งนี้เพื่อให้เป็นไปด้วยความเรียบร้อยและสอดคล้องกับสภาพการณ์ปัจจุบัน

อาศัยอำนาจตามความในข้อ 2.1 ของคำสั่งคณะกรรมการบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ที่ 3/2564 เรื่อง มอบอำนาจให้กรรมการผู้จัดการใหญ่ปฏิบัติการแทนคณะกรรมการบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ประกอบกับคำสั่งคณะกรรมการบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ที่ 2/2564 เรื่อง แต่งตั้งรักษาการกรรมการผู้จัดการใหญ่ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) จึงกำหนดนโยบาย และหลักเกณฑ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามที่แนบท้ายคำสั่งนี้

1. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
2. มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
3. ขั้นตอนปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
[1]4. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ 2 พฤศจิกายน 2564

นาวาอากาศเอก สมศักดิ์ ขาวสุวรรณ์

(สมศักดิ์ ขาวสุวรรณ์)

กรรมการบริษัทโทรคมนาคมแห่งชาติ จำกัด (มหาชน)

รักษาการกรรมการผู้จัดการใหญ่

[1]เพิ่มเติมโดย คำสั่ง บมจ.โทรคมนาคมแห่งชาติ ที่ รบ.1/2566 ใช้บังคับตั้งแต่วันที่ 6 มกราคม 2566

ตามแนบท้ายคำสั่ง

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) หรือในลำดับต่อไปใช้คำว่า “บริษัท” ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศว่าเป็นปัจจัยสำคัญในการดำเนินธุรกิจให้ประสบความสำเร็จภายใต้การบริหารจัดการที่ดี ดังนั้นเพื่อเป็นการกำหนดทิศทาง หลักการ ตลอดจนขอบเขตและวิธีการในการดำเนินการที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงการป้องกันสารสนเทศให้ปลอดภัยจากภัยคุกคามที่ก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) อีกทั้งเพื่อให้มีความสอดคล้องกับมาตรฐานสากล ISO/IEC 27001:2013 (Annex A) และมาตรฐานสากล ISO/IEC 27002:2013 รวมทั้งครอบคลุมสาระสำคัญในกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับที่แก้ไขเพิ่มเติม พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับที่แก้ไขเพิ่มเติม จึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศซึ่งประกอบด้วย 14 ข้อนโยบาย

ข้อนโยบาย

1. นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy)

วัตถุประสงค์ (Objective)

เพื่อให้การดำเนินการในการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทเป็นไปอย่างสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

ถ้อยแถลงนโยบาย (Policy Statements)

1.1 การกำหนดทิศทางการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Management Directions for Information Security)

เพื่อให้มั่นใจว่านโยบายและมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้รับการปรับปรุงเมื่อมีการเปลี่ยนสภาพแวดล้อมในการดำเนินการของบริษัท เช่น การเปลี่ยนแปลงโครงสร้างบริษัท การเปลี่ยนแปลงธุรกิจ กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และมีการควบคุมการขอยกเว้นไม่ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.1.1 นโยบายสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Policies for Information Security)

1.1.2 การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

(Review of the Policies for Information Security)

1.1.3 การขอยกเว้นไม่ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Exception to Information Security Standards)

มาตรฐานอ้างอิง (Standard References)

ST-01 มาตรฐานเรื่อง นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy Standard)

2. โครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (Organization of Information Security)

วัตถุประสงค์ (Objective)

เพื่อบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ

ถ้อยแถลงนโยบาย (Policy Statements)

2.1 การกำหนดโครงสร้างการบริหารความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท (Internal Organization)

เพื่อให้มีการกำหนดกรอบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท ตั้งแต่เริ่มดำเนินการ และการควบคุมให้ปฏิบัติตาม เพื่อให้การดำเนินการความมั่นคงปลอดภัยด้านสารสนเทศภายในบริษัทเป็นไปตามกรอบที่กำหนด

2.1.1 บทบาทและหน้าที่ความรับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Roles and Responsibilities)

2.1.2 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties)

2.1.3 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานภายนอก (Contact with Authorities)

2.1.4 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with Special Interest Groups)

2.1.5 ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการบริหารจัดการโครงการ (Information Security in Project Management)

2.2 การป้องกันอุปกรณ์คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานจากภายนอกสำนักงาน (Mobile Devices and Teleworking)

เพื่อให้มีการรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากภายนอกสำนักงานและการป้องกัน

การใช้งานของอุปกรณ์คอมพิวเตอร์ประเภทพกพา

2.2.1 นโยบายสำหรับอุปกรณ์คอมพิวเตอร์ประเภทพกพา (Mobile Device Policy)

2.2.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

มาตรฐานอ้างอิง (Standard References)

ST-02 มาตรฐานเรื่อง โครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (Organization of Information Security Standard)

3. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

วัตถุประสงค์ (Objective)

เพื่อให้พนักงาน ลูกจ้าง นักศึกษาฝึกงาน หน่วยงานภายนอก และบุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัท เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบ ทั้งก่อน ระหว่าง สิ้นสุด หรือเปลี่ยนแปลงการจ้างงาน ตลอดจนตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง การใช้งานสารสนเทศและระบบสารสนเทศผิดวัตถุประสงค์ และความผิดพลาดในการปฏิบัติหน้าที่

ถ้อยแถลงนโยบาย (Policy Statements)

3.1 การสร้างความมั่นคงปลอดภัยก่อนการว่าจ้าง (Prior to Employment)

เพื่อให้พนักงาน ลูกจ้าง นักศึกษาฝึกงาน หน่วยงานภายนอก และบุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัท เข้าใจถึงบทบาท และหน้าที่ความรับผิดชอบของตนเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทก่อนเริ่มปฏิบัติงาน

3.1.1 การตรวจสอบคุณสมบัติของผู้รับจ้าง (Screening)

3.1.2 การระบุเงื่อนไขการว่าจ้าง (Terms and Conditions of Employment)

3.2 การสร้างความมั่นคงปลอดภัยในระหว่างการว่าจ้าง (During Employment)

เพื่อให้พนักงาน ลูกจ้าง นักศึกษาฝึกงาน หน่วยงานภายนอก และบุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัท ได้เข้าใจในหน้าที่ความรับผิดชอบ ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนได้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบาย มาตรฐาน และขั้นตอนปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

3.2.1 การกำหนดหน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management

Responsibilities)

3.2.2 การสร้างความตระหนัก การให้ความรู้และการอบรมความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness, Education and Training)

3.2.3 กระบวนการทางวินัย (Disciplinary Process)

3.3 การสร้างความมั่นคงปลอดภัยเมื่อสิ้นสุดหรือเปลี่ยนแปลงการว่าจ้าง (Termination and Change of Employment)

เพื่อให้พนักงาน ลูกจ้าง นักศึกษาฝึกงาน หน่วยงานภายนอก และบุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัท ได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการว่าจ้างหรือมีการเปลี่ยนแปลงการว่าจ้าง หรือสิ้นสุดระยะเวลาฝึกงาน

3.3.1 การกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการว่าจ้าง (Termination or Change of Employment Responsibilities)

มาตรฐานอ้างอิง (Standard References)

ST-03 มาตรฐานเรื่อง ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security Standard)

4. การบริหารจัดการทรัพย์สินของบริษัท (Asset Management)

วัตถุประสงค์ (Objective)

เพื่อกำหนดระดับของการป้องกันสารสนเทศของบริษัทอย่างเหมาะสม เพื่อป้องกันทรัพย์สินจากความเสียหายที่อาจเกิดขึ้นได้

ถ้อยแถลงนโยบาย (Policy Statements)

4.1 การกำหนดหน้าที่ความรับผิดชอบต่อทรัพย์สินของบริษัท (Responsibility for Assets)

เพื่อป้องกันทรัพย์สินของบริษัทจากความเสียหายที่อาจขึ้นได้

4.1.1 การจัดทำทะเบียนทรัพย์สินของบริษัท (Inventory of Assets)

4.1.2 การระบุส่วนงานที่เป็นเจ้าของทรัพย์สิน (Ownership of Assets)

4.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable Use of Assets)

4.1.4 การคืนทรัพย์สินของบริษัท (Return of Assets)

4.2 การจัดชั้นสารสนเทศตามระดับความมั่นคงปลอดภัยของสารสนเทศ

(Information Classification)

เพื่อกำหนดระดับของการป้องกันสารสนเทศของบริษัทอย่างเหมาะสม

4.2.1 เกณฑ์การจัดชั้นสารสนเทศตามระดับความมั่นคงปลอดภัย (Classification of Information)

4.2.2 การจัดทำป้ายชื่อ (Labeling of Information)

4.2.3 การจัดการทรัพย์สินตามที่ได้กำหนดไว้ (Handling of Assets)

4.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)

เพื่อให้มีการป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และเพื่อควบคุมการเปลี่ยนแปลง การขนย้าย การลบหรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

4.3.1 การบริหารจัดการสื่อบันทึกข้อมูลที่พกพาได้ (Management of Removable Media)

4.3.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

4.3.3 การขนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

มาตรฐานอ้างอิง (Standard References)

ST-04 มาตรฐานเรื่อง การบริหารจัดการทรัพย์สินของบริษัท (Asset Management Standard)

5. การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์ (Objective)

เพื่อควบคุมและป้องกันการเข้าถึง การเปิดเผย และการแก้ไขสารสนเทศและระบบสารสนเทศของบริษัท โดยมิได้รับอนุญาต

ถ้อยแถลงนโยบาย (Policy Statements)

5.1 การควบคุมการเข้าถึงให้เป็นไปตามความต้องการทางธุรกิจ (Business Requirements of Access Control)

เพื่อให้มีการจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

5.1.1 นโยบายการควบคุมการเข้าถึง (Access Control Policy)

5.1.2 การควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Services)

5.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อให้มีการควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต

5.2.1 การลงทะเบียนและการเพิกถอนทะเบียนผู้ใช้งาน (User Registration and De- Registration)

5.2.2 การบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

5.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of Privileged Access Right)

5.2.4 การบริหารจัดการข้อมูลสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of Users)

5.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

5.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึงของผู้ใช้งาน (Removal or Adjustment of Access Rights)

5.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลสำหรับการพิสูจน์ตัวตน

5.3.1 การป้องกันข้อมูลสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Use of Secret Authentication Information)

5.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

เพื่อให้มีการป้องกันการเข้าถึงระบบและแอปพลิเคชันโดยไม่ได้รับอนุญาต

5.4.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

5.4.2 ขั้นตอนปฏิบัติสำหรับการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure Log-on Procedures)

5.4.3 ระบบบริหารจัดการรหัสผ่าน (Password Management System)

5.4.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of Privileged Utility Programs)

5.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access Control to Program Source Code)

มาตรฐานอ้างอิง (Standard References)

ST-05 มาตรฐานเรื่อง การควบคุมการเข้าถึง (Access Control Standard)

6. การเข้ารหัสข้อมูล (Cryptography)

วัตถุประสงค์ (Objective)

เพื่อให้แน่ใจว่า มีความเหมาะสมในการใช้งานและมีประสิทธิภาพในการเข้ารหัสลับ ในการรักษาไว้ซึ่ง ความลับ ความครบถ้วนสมบูรณ์ของข้อมูล รวมถึงความถูกต้องและความน่าเชื่อถือ

ถ้อยแถลงนโยบาย (Policy Statements)

6.1 การควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)

เพื่อให้มีการควบคุม กำหนด เทคนิควิธี ในการเข้ารหัสลับ รวมถึงการบริหารจัดการกุญแจ อย่างถูกต้อง เหมาะสมและมีประสิทธิภาพ เพื่อรักษาไว้ซึ่ง ความลับ ความครบถ้วนถูกต้อง และความพร้อมใช้

6.1.1 นโยบายการใช้งานการควบคุมการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

6.1.2 การบริหารจัดการกุญแจ (Key Management)

มาตรฐานอ้างอิง (Standard References)

ST-06 มาตรฐานเรื่อง การเข้ารหัสข้อมูล (Cryptography Standard)

7. ความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์ (Objective)

เพื่อป้องกันการเข้าถึงทางกายภาพโดยมิได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินของบริษัท อีกทั้งเพื่อป้องกันทรัพย์สินของบริษัท จากการสูญหาย เสียหาย ถูกขโมย หรือสารสนเทศถูกเปิดเผยโดยมิได้รับอนุญาต และป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมการดำเนินงาน

ถ้อยแถลงนโยบาย (Policy Statements)

7.1 การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

เพื่อให้มีการป้องกันการเข้าถึงพื้นที่ทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหายและการก่อกวนหรือแทรกแซงต่ออาคารสถานที่และสารสนเทศของบริษัท

7.1.1 การจัดทำขอบเขตหรือบริเวณโดยรอบพื้นที่ควบคุม (Physical Security Perimeter)

7.1.2 การควบคุมการเข้า-ออกทางกายภาพ (Physical Entry Controls)

7.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและทรัพย์สินอื่นๆ (Securing Office, Room and Facilities)

7.1.4 การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against External and Environmental Threats)

7.1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

7.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Delivery and Loading Areas)

7.2 การสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์ (Equipment)

เพื่อป้องกันทรัพย์สินของบริษัท จากการสูญหาย เสียหาย ถูกขโมย หรือสารสนเทศถูกเปิดเผยโดยมิได้รับอนุญาต และป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมการดำเนินงาน

7.2.1 การจัดวางและป้องกันอุปกรณ์ (Equipment Siting and Protection)

7.2.2 การบริหารจัดการอุปกรณ์สนับสนุนการประมวลผลสารสนเทศ (Supporting Utilities)

7.2.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

7.2.4 การบำรุงรักษาและซ่อมบำรุงอุปกรณ์ (Equipment Maintenance)

7.2.5 การนำทรัพย์สินของบริษัทออกนอกสำนักงาน (Removal of Assets)

7.2.6 การป้องกันอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of Equipment and Assets Off- Premises)

7.2.7 การควบคุมการกำจัดอุปกรณ์และการนำกลับมาใช้งาน (Secure Disposal or Re-Use of Equipment)

7.2.8 การป้องกันอุปกรณ์ขณะที่ไม่มีผู้ใช้งาน (Unattended User Equipment)

7.2.9 นโยบายควบคุมการละทิ้งทรัพย์สิน (Clear Desk and Clear Screen Policy)

มาตรฐานอ้างอิง (Standard References)

ST-07 มาตรฐานเรื่อง ความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security Standard)

8. ความมั่นคงปลอดภัยด้านการปฏิบัติการ (Operations Security)

วัตถุประสงค์ (Objective)

เพื่อให้การดำเนินงานด้านปฏิบัติการด้านสารสนเทศเป็นไปอย่างถูกต้องและรักษาไว้ซึ่งความมั่นคงปลอดภัยด้านสารสนเทศ

ถ้อยแถลงนโยบาย (Policy Statements)

8.1 การกำหนดขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities)

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

8.1.1 การจัดทำคู่มือการปฏิบัติงาน (Documented Operating Procedures)

8.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

8.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

8.1.4 การแยกสภาพแวดล้อมสำหรับการพัฒนาและการทดสอบ ออกจากระบบที่ให้บริการจริง (Separation of Development, Testing and Operational Environments)

8.2 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection from Malware)

เพื่อป้องกันความเสียหายต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี โดยให้มีการบริหารจัดการ ควบคุม และวางแผนการป้องกันไม่ให้ใช้โปรแกรมที่มิได้รับอนุญาตรวมถึงให้มีการสร้างความรู้ความเข้าใจในการใช้งาน

8.2.1 มาตรการป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against Malware)

8.3 การสำรองข้อมูล (Backup)

เพื่อให้มีการป้องกันการสูญหายของข้อมูล

8.3.1 การสำรองข้อมูลสารสนเทศ (Information Backup)

8.4 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานและการเฝ้าระวัง (Logging and Monitoring)

เพื่อให้มีการบันทึกเหตุการณ์ต่างๆ ที่เกี่ยวข้อง กับการใช้งาน รวมทั้งเหตุการณ์ ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดและเพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ มิได้รับอนุญาต

8.4.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งาน (Event Logging)

8.4.2 การป้องกันข้อมูลเหตุการณ์ (Protection of Log Information)

8.4.3 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานของผู้ดูแลระบบและเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and Operator Logs)

8.4.4 การตั้งเวลาของอุปกรณ์ให้ตรงกัน (Clock Synchronization)

8.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Control of Operational Software)

เพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ในระบบที่ให้บริการ เพื่อลดความเสี่ยงที่จะทำให้ระบบที่ให้บริการจริงเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้

8.5.1 การติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of Software on Operational Systems)

8.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

เพื่อให้มีการป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

8.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

8.6.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

8.7 การตรวจประเมินระบบสารสนเทศ (Information Systems Audit Considerations)

เพื่อให้การตรวจสอบระบบสารสนเทศ ได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อการดำเนินงานทางธุรกิจน้อยที่สุด

8.7.1 การควบคุมการตรวจประเมินระบบสารสนเทศ (Information Systems Audit Controls)

มาตรฐานอ้างอิง (Standard References)

ST-08 มาตรฐานเรื่อง ความมั่นคงปลอดภัยด้านการปฏิบัติการ (Operations Security Standard)

9. ความมั่นคงปลอดภัยด้านการสื่อสารข้อมูล (Communications Security)

วัตถุประสงค์ (Objective)

เพื่อให้การบริหารจัดการด้านการสื่อสารข้อมูลเป็นไปอย่างถูกต้องและรักษาไว้ซึ่งความมั่นคงปลอดภัยด้านสารสนเทศ

ถ้อยแถลงนโยบาย (Policy Statements)

9.1 **การบริหารจัดการความมั่นคงปลอดภัยสำหรับเครือข่าย** (Network Security Management)

เพื่อให้มีการป้องกันสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ

9.1.1 การกำหนดมาตรการทางเครือข่าย (Network Controls)

9.1.2 การรักษาความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)

9.1.3 การแบ่งแยกเครือข่าย (Segregation in Networks)

9.2 **การรับส่งสารสนเทศ** (Information Transfer)

เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการรับส่งภายในบริษัท และที่มีการรับส่งกับหน่วยงานภายนอก

9.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการรับส่งสารสนเทศ (Information Transfer Policies and Procedures)

9.2.2 ข้อตกลงสำหรับการรับส่งสารสนเทศ (Agreements on Information Transfer)

9.2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)

9.2.4 ข้อตกลงหรือสัญญาการรักษาความลับหรือการไม่เปิดเผยความลับของบริษัท (Confidentiality or Non-Disclosure Agreements)

มาตรฐานอ้างอิง (Standard References)

ST-09 มาตรฐานเรื่อง ความมั่นคงปลอดภัยด้านการสื่อสารข้อมูล (Communications Security Standard)

10. **การจัดหา พัฒนา และการบำรุงรักษาระบบ** (System Acquisition, Development and Maintenance)

วัตถุประสงค์ (Objective)

เพื่อให้มีความมั่นคงปลอดภัยด้านสารสนเทศ ในกระบวนการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ

ถ้อยแถลงนโยบาย (Policy Statements)

10.1 **การระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ** (Security Requirements of Information Systems)

เพื่อให้การรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นหนึ่งในองค์ประกอบที่สำคัญในวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับระบบที่มีการให้บริการบนเครือข่ายสาธารณะด้วย

10.1.1 การวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Requirements Analysis and Specification)

10.1.2 การรักษาความมั่นคงปลอดภัยสำหรับระบบที่มีการให้บริการบนเครือข่ายสาธารณะ (Securing Application Services on Public Networks)

10.1.3 การป้องกันข้อมูลที่ใช้ในการทำธุรกรรมของระบบ (Protecting Application Services Transactions)

10.2 การรักษาความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาและกระบวนการสนับสนุน (Security in Development and Support Processes)

เพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตลอดวงจรชีวิตการพัฒนาระบบ เริ่มจากการกำหนดนโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัยสำหรับระบบที่มีการให้บริการบนเครือข่ายสาธารณะ การควบคุมการเปลี่ยนแปลงแอปพลิเคชันและสารสนเทศที่เกี่ยวข้อง เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้ รวมถึงการสอบทานผลกระทบต่อแอปพลิชันหลังจากการเปลี่ยนแปลง

10.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy)

10.2.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures)

10.2.3 การสอบทานผลกระทบต่อแอปพลิเคชันหลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications after Operating Platform Changes)

10.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูปที่มาจากผู้ผลิต (Restrictions on Changes to Software Packages)

10.2.5 การกำหนดหลักการพื้นฐานสำหรับวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles)

10.2.6 การสร้างสภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure Development Environment)

10.2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced Development)

10.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing)

10.2.9 การทดสอบเพื่อตรวจรับระบบ (System Acceptance Testing)

10.3 การสร้างความมั่นคงปลอดภัยสำหรับข้อมูลทดสอบ (Test Data)

เพื่อการสร้างความมั่นคงปลอดภัยสำหรับข้อมูลทดสอบ (Test Data)

10.3.1 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of Test Data)

มาตรฐานอ้างอิง (Standard References)

ST-10 มาตรฐานเรื่อง การจัดหา พัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance Standard)

11. ความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก (Supplier Relationships)

วัตถุประสงค์ (Objective)

เพื่อบริหารจัดการความมั่นคงปลอดภัยที่เกี่ยวข้องกับผู้ให้บริการภายนอก รวมทั้งความมั่นคงปลอดภัยของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัทจากการถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับผู้ให้บริการภายนอก

ถ้อยแถลงนโยบาย (Policy Statements)

11.1 ความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับการสร้างความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationship)

เพื่อให้มั่นใจว่ามีการป้องกันทรัพย์สินของบริษัทที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

11.1.1 นโยบายความมั่นคงปลอดภัยด้านสารสนเทศสำหรับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

11.1.2 การระบุข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

11.1.3 ห่วงโซ่อุปทานการให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสารของผู้ให้บริการภายนอก (Information and Communication Technology Supply Chain)

11.2 การบริหารจัดการการให้บริการจากผู้ให้บริการภายนอก (Supplier Service Delivery Management)

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

11.2.1 การเฝ้าระวังและสอบทานการให้บริการจากผู้ให้บริการภายนอก (Monitoring and Review of Supplier Services)

11.2.2 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการจากผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

มาตรฐานอ้างอิง (Standard References)

ST-11 มาตรฐานเรื่อง ความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก (Supplier Relationships Standard)

12. การบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์ (Objective)

เพื่อให้มีการรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

ถ้อยแถลงนโยบาย (Policy Statements)

12.1 การบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศและการปรับปรุง (Management of Information Security Incidents and Improvements)

เพื่อให้มีการรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

12.1.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

12.1.2 การรายงานเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ (Reporting Information Security Events)

12.1.3 การรายงานจุดอ่อนความมั่นคงปลอดภัยด้านสารสนเทศ (Reporting Information Security Weaknesses)

12.1.4 การประเมินและตัดสินใจต่อเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ (Assessment of and Decision on Information Security Events)

12.1.5 การตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ (Response to Information Security Incidents)

12.1.6 การเรียนรู้จากเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ (Learning from

Information Security Incidents)

12.1.7 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

มาตรฐานอ้างอิง (Standard References)

ST-12 มาตรฐานเรื่อง การบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Incident Management Standard)

13. ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการบริหารความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์ (Objective)

เพื่อบริหารความต่อเนื่องทางธุรกิจของบริษัท เมื่อเกิดเหตุการณ์ล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ

ถ้อยแถลงนโยบาย (Policy Statements)

13.1 การสร้างความต่อเนื่องสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Continuity)

เพื่อลดหรือป้องกันการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจอันเป็นผลมาจากภัยคุกคาม ความล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่กำหนด

13.1.1 การวางแผนสร้างความต่อเนื่องสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Planning Information Security Continuity)

13.1.2 การปฏิบัติการเพื่อสร้างความต่อเนื่องสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Implementing Information Security Continuity)

13.1.3 การตรวจสอบ การสอบทาน และการประเมินความต่อเนื่องสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Verify, Review and Evaluate Information Security Continuity)

13.2 การจัดเตรียมอุปกรณ์ประมวลผลสารสนเทศที่จำเป็น (Redundancies)

เพื่อให้จัดเตรียมอุปกรณ์ประมวลผลสารสนเทศที่จำเป็นให้พร้อมใช้งาน

13.2.1 การเตรียมอุปกรณ์ประมวลผลสารสนเทศที่จำเป็นให้พร้อมใช้งาน (Availability of

Information Processing Facilities)

มาตรฐานอ้างอิง (Standard References)

ST-13 มาตรฐานเรื่อง ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการบริหารความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management Standard)

14. การปฏิบัติตามข้อกำหนด (Compliance)

วัตถุประสงค์ (Objective)

เพื่อป้องกันการละเมิดข้อกำหนดที่มีผลทางกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท และเพื่อให้การปฏิบัติของพนักงาน ลูกจ้าง หน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัท และนักศึกษาฝึกงานเป็นไปตามนโยบายและมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท อีกทั้งเพื่อให้การตรวจสอบระบบสารสนเทศและเครือข่ายได้ประสิทธิภาพสูงสุดโดยมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

ถ้อยแถลงนโยบาย (Policy Statements)

14.1 การปฏิบัติตามข้อกำหนดที่มีผลทางกฎหมายและสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดที่มีผลทางกฎหมายที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

14.1.1 การระบุข้อกำหนดที่มีผลทางกฎหมายและสัญญาจ้าง (Identification of Applicable Legislation and Contractual Requirements)

14.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual Property Rights)

14.1.3 การป้องกันข้อมูลที่จำเป็นต้องจัดเก็บตามข้อกำหนดที่มีผลทางกฎหมาย (Protection of Records)

14.1.4 การป้องกันสิทธิและข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information)

14.1.5 การควบคุมการเข้ารหัสข้อมูลให้เป็นไปตามข้อกำหนด (Regulation of Cryptographic Controls)

14.2 **การสอบทานด้านความมั่นคงปลอดภัยด้านสารสนเทศ** (Information Security Reviews)

เพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบาย มาตรฐานและขั้นตอนปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และมาตรฐานทางเทคนิคด้านความมั่นคงปลอดภัยของบริษัท

14.2.1 การสอบทานด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างอิสระ (Independent Review of Information Security)

14.2.2 การตรวจสอบการปฏิบัติตามนโยบายและมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Compliance with Security Policies and Standards)

14.2.3 การสอบทานการปฏิบัติตามข้อกำหนดทางเทคนิค (Technical Compliance Review)

มาตรฐานอ้างอิง (Standard References)

ST-14 มาตรฐานเรื่อง การปฏิบัติตามข้อกำหนด (Compliance Standard)

คำนิยาม

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้ใน นโยบาย มาตรฐาน และขั้นตอนปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

ศัพท์	ความหมาย
การรักษาความมั่นคงปลอดภัยไซเบอร์/สารสนเทศ	มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์/สารสนเทศ ทั้งจากภายในและภายนอกอันกระทบต่อความมั่นคงทางธุรกิจของบริษัท
การเข้าถึง (Access)	ความสามารถในการเข้าไป รวมถึงความพยายามในการเข้าไป อันอาจทำให้สามารถอ่าน ทำ สร้าง คัดลอก แก้ไข ปรับปรุงเปลี่ยนแปลง ทั้งโดยการเข้าถึงด้วยวิธีการทางตรรกะและวิธีการทางกายภาพ
การปฏิบัติงานประจำจากภายนอกสำนักงาน (Teleworking)	การปฏิบัติงานจากบ้าน (Work at Home) หรือสถานที่ภายนอกบริษัทที่บริษัทอนุญาตให้ใช้ทำงานประจำ
การประมวลผลข้อมูล	การดำเนินการใดๆ ซึ่งกระทำต่อข้อมูลไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก การจัดระบบ การเก็บรักษา การใช้ การเปิดเผย การเปลี่ยนแปลง หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อมใช้งาน หรือการผสมเข้าด้วยกัน การลบ การทำลาย
กรรมการผู้จัดการใหญ่	ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO)
ข้อกำหนดที่มีผลทางกฎหมาย (Legal Requirements)	พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ ที่บริษัทต้องปฏิบัติตาม
ข้อมูล (Data)	ข้อมูลดิบ ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ และข้อมูลที่อยู่ในรูปแบบเอกสาร
ข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
คณะผู้ประสานงาน (Coordinator Group)	บุคคลหรือส่วนงานที่ได้รับการแต่งตั้งโดยบริษัทให้มีหน้าที่รับผิดชอบในการประสานงานในเรื่องหนึ่งๆ มีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย กับผู้ร้องขอข้อมูลรวมถึงพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
ความมั่นคงปลอดภัยสารสนเทศ (Information security)	การคงไว้ซึ่งความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้ของข้อมูล นอกจากนั้นแล้วยังหมายรวมถึงคุณสมบัติอื่นๆ เช่น การแสดงตัวตนที่ถูกต้อง (เช่น การแสดงตัวตนของผู้ใช้งานก่อนเข้าใช้ระบบงาน เป็นต้น) การรับผิดชอบต่อกิจกรรมหรืองานต่างๆ ที่ตนปฏิบัติ การไม่ปฏิเสธความรับผิดชอบ และความเชื่อถือได้ (เช่น ของระบบเทคโนโลยีสารสนเทศต่างๆ เป็นต้น)

ศัพท์	ความหมาย
ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล	การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ
เครือข่าย (Network)	โครงข่ายระบบสารสนเทศที่เชื่อมโยงอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และ อุปกรณ์โทรคมนาคม ซึ่งทำให้สามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้
จุดอ่อนที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Weakness)	จุดบกพร่อง หรือความอ่อนแอต่อภัยคุกคามซึ่งผู้ไม่ประสงค์ดีอาจใช้ประโยชน์เพื่อกระทำการใดๆต่อทรัพย์สิน อันอาจจะนำไปสู่ผลเสียต่อการดำเนินธุรกิจ และการรักษาความปลอดภัยด้านสารสนเทศ เช่น • ข้อบกพร่องในแอปพลิเคชัน • ช่องโหว่ทางเทคนิคในระบบปฏิบัติการ • การเปิด Network Protocol และ IP Service Port ที่ไม่ได้ใช้งานทางธุรกิจของบริษัท • การไม่ Lock หน้าจอ หรือ การไม่ Log Off ออกจากระบบ เมื่อไม่ได้ใช้งานเป็นระยะเวลานาน เป็นต้น
เจ้าของข้อมูลส่วนบุคคล	บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล เป็นต้นว่า ลูกค้าหรือผู้ใช้บริการ คู่ค้า ผู้เข้าเยี่ยมชมเว็บไซต์หรือ Mobile Application ของบริษัท ผู้บริหารหรือพนักงานของบริษัทรวมถึงบุคคลใดที่มีนิติสัมพันธ์เกี่ยวข้องกับ บริษัท
ซอฟต์แวร์ (Software)	โปรแกรมคอมพิวเตอร์ประเภทใดๆ เช่น ระบบปฏิบัติการ โปรแกรมประเภทยูทิลิตี้ แอปพลิเคชัน เป็นต้น
ซอร์สโค้ด (Source Code)	ไฟล์ซึ่งประกอบด้วยชุดคำสั่งที่สามารถสั่งการให้เครื่องคอมพิวเตอร์ทำงานตามที่ต้องการได้ โดยทั่วไปชุดคำสั่งเหล่านี้จะอยู่ในรูปแบบหรือภาษาที่สามารถอ่านและทำความเข้าใจได้โดยมนุษย์ ไฟล์ชุดคำสั่งนี้จะถูกแปลงโดยโปรแกรมแปลภาษา เช่น Compiler, Interpreter หรือ Assembler ไปเป็นโค้ดที่เครื่องคอมพิวเตอร์สามารถตีความและสั่งการให้เครื่องทำงานตามที่ตีความนั้น โดยปกติมนุษย์จะไม่สามารถอ่านและทำความเข้าใจโค้ดประเภทนี้ได้
ไซเบอร์ (Cyber)	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป
ทรัพย์สิน (Assets)	หมายถึงวัตถุทั้งที่มีรูปร่างและไม่มีรูปร่าง ที่มีมูลค่าต่อบริษัทและเกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศที่บริษัทเป็นเจ้าของ จัดซื้อ เช่า ว่าจ้าง หรือพัฒนา ลิขสิทธิ์ สิทธิบัตร ทั้งนี้ทรัพย์สินดังกล่าวสามารถแบ่งตามประเภทได้ดังนี้ (1) สารสนเทศ (Information) หมายถึง เอกสาร รายงาน ข้อมูลที่เกิดจากคอมพิวเตอร์และไซเบอร์ เช่น ฐานข้อมูล ไฟล์ข้อมูล ซอร์สโค้ด (Source Code) สัญญา เอกสาร/คู่มือระบบ ข้อมูลการวิจัย คู่มือผู้ใช้งาน ทรัพยากรในการฝึกอบรม ขั้นตอนการปฏิบัติงานหรือสนับสนุน แผนสร้างความต่อเนื่องให้กับธุรกิจ แผนการกู้คืนสภาพ ข้อมูลการตรวจสอบ (Audit Trails) ประวัติการตรวจสอบ ข้อมูลสำรองที่นำออกจาก

ศัพท์	ความหมาย
	ระบบ (Archived Data) และสารสนเทศที่สำคัญอื่นๆ เป็นต้น (2) ทรัพย์สินทางซอฟต์แวร์ (Software Assets) เช่น ลิขสิทธิ์ สิทธิบัตร โปรแกรมประยุกต์ โปรแกรมระบบ เครื่องมือสำหรับพัฒนา และโปรแกรมยูทิลิตี้สำหรับระบบ เป็นต้น (3) ทรัพย์สินทางกายภาพของอุปกรณ์ประมวลผลสารสนเทศ (Physical Assets) เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสาร อุปกรณ์ให้บริการโทรคมนาคม หรืออุปกรณ์โทรคมนาคม สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ และอุปกรณ์สนับสนุนการประมวลผลสารสนเทศ เป็นต้น (4) บริการ (Services) ซึ่งแบ่งได้เป็น 3 ประเภทย่อย ได้แก่ (4.1) บริการพื้นฐาน เพื่อสนับสนุนระบบสารสนเทศเช่น ระบบระบายความชื้น ระบบปรับอากาศ ระบบปรับอุณหภูมิ ระบบกระแสไฟฟ้า เป็นต้น (4.2) บริการด้านการสื่อสารและโทรคมนาคม เช่น บริการโทรศัพท์ประจำที่ (Fixed Line) บริการโทรศัพท์เคลื่อนที่ (Mobile) บริการสายสัญญาณเช่า (Leased Line) บริการเชื่อมต่ออินเทอร์เน็ต บริการศูนย์ข้อมูล (Data Center) บริการลูกค้า (เช่น บริการรับชำระเงิน บริการ Call Center) เป็นต้น (4.3) บริการด้านสารสนเทศ เช่น บริการให้คำปรึกษาด้านเทคโนโลยีสารสนเทศ บริการการติดตั้งและอิมพลีเมนท์ระบบสารสนเทศ การใช้งานแอปพลิเคชันจาก Application Service Provider (ASP) การใช้งาน Cloud Computing Service เป็นต้น (5) บุคลากร (People) รวมถึงคุณวุฒิ ความสามารถและประสบการณ์ของบุคลากร
ธุรกรรมอิเล็กทรอนิกส์ (Online Transactions)	การใช้บริการจากระบบงานโดยผู้ใช้งานเพื่อทำธุรกรรมหรือทำกิจกรรมต่างๆ ตามที่ต้องการ โดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน เช่น ธุรกรรมการเงินกับธนาคาร สั่งซื้อสินค้า จองตั๋วเครื่องบิน ประมูลสินค้า เป็นต้น
บริการเครือข่าย (Network Services)	บริการที่ได้รับจากเครือข่ายซึ่งเอื้ออำนวยหรือเป็นประโยชน์ต่อการทำงานในลักษณะใดลักษณะหนึ่ง เช่น บริการที่ได้รับที่ทำให้ผู้ใช้งานสามารถแลกเปลี่ยนข้อมูลซึ่งกันและกันได้ เป็นต้น
บริษัท	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
บุคคล	บุคคลธรรมดา
โปรแกรมที่ไม่ประสงค์ดี (Malware Code)	โปรแกรมหรือส่วนของรหัสทางคอมพิวเตอร์ รวมถึงโปรแกรมที่ติดตั้งโดยไม่ได้รับอนุญาตและมีจุดประสงค์ที่จะทำลายหรือรบกวนการทำงานของระบบสารสนเทศหรือสารสนเทศ รวมทั้งลักลอบส่งข้อมูลออกจากเครื่องคอมพิวเตอร์ ซึ่งก่อให้เกิดปัญหาต่อระบบสารสนเทศหรือสารสนเทศ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) แอดแวร์ (Adware) สปายแวร์ (Spyware) เป็นต้น
โปรแกรมยูทิลิตี้สำหรับระบบ (System Utilities)	โปรแกรมเพื่อใช้สำหรับงานบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของระบบคอมพิวเตอร์เฉพาะทาง เช่น Registry Editor และ Administrative Tools บนระบบปฏิบัติการ MS Windows เป็นต้น

ศัพท์	ความหมาย
ผู้ใช้งาน (User)	พนักงาน ลูกจ้าง ลูกค้า หน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัทและนักศึกษาฝึกงาน ที่ได้รับสิทธิเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัท
ผู้ควบคุมข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ดูแลระบบ (Administrator)	ผู้ที่มีหน้าที่รับผิดชอบหรือได้รับมอบหมายให้ดูแล ควบคุม ตรวจสอบ เฝ้าระวัง และรักษาความพร้อมใช้งานของระบบ
ผู้บริหารระดับสูง	ผู้บริหารของบริษัท ตั้งแต่ระดับผู้ช่วยกรรมการผู้จัดการใหญ่ขึ้นไป
ผู้ประมวลผลข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
พนักงานและลูกจ้าง (Employee)	พนักงานและลูกจ้างตามที่นิยามไว้ในระเบียบบริษัทว่าด้วยการบริหารงานบุคคล ตัวอย่างเช่น ● พนักงานประจำ ● พนักงานตามสัญญาจ้างที่มีกำหนดระยะเวลาแน่นอน ● ลูกจ้างตามสัญญาจ้างที่มีกำหนดระยะเวลาแน่นอน เป็นต้น
พอร์ต (Ports)	ช่องสัญญาณบนอุปกรณ์เครือข่าย (Physical port) เช่น บนสวิทช์ เร้าเตอร์ โดยทั่วไปช่องสัญญาณนี้สามารถใช้ในการติดต่อสื่อสารข้อมูลกับเครือข่าย คอมพิวเตอร์ และอุปกรณ์เครือข่ายต่างๆ โดยทั่วไปอุปกรณ์เครือข่ายจะมีช่องสัญญาณดังกล่าวจำนวนหนึ่ง นอกจากนั้นแล้วพอร์ตยังหมายถึงบริการต่างๆ บนเครื่องคอมพิวเตอร์ให้บริการ (Service port) โดยทั่วไปบริการเหล่านี้จะได้รับการกำหนดหมายเลขเป็นหมายเลขมาตรฐาน เช่น พอร์ต 80 หมายถึงบริการเว็บซึ่งบริการข้อมูลต่างๆ บนเว็บหนึ่ง พอร์ต 25 หมายถึงบริการรับส่งอีเมล์บนอินเทอร์เน็ต พอร์ต 53 หมายถึงบริการค้นหาไอพีแอดเดรสของเครื่องหรืออุปกรณ์คอมพิวเตอร์ต่างๆ เป็นต้น
พาณิชย์อิเล็กทรอนิกส์ (E-commerce)	การดำเนินการพาณิชย์ที่ใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน เป็นสื่อกลางในการดำเนินการ เช่น การชำระเงิน การซื้อขาย การประมูล การโฆษณาผ่านสื่ออิเล็กทรอนิกส์ เป็นต้น ทั้งนี้ให้หมายรวมถึงการเผยแพร่สารสนเทศในระบบสารสนเทศที่เข้าถึงได้โดยสาธารณะ (Publicly Available System) เช่น Web Site ที่สามารถเข้าถึงได้โดยบุคคลทั่วไป ตู้ Kiosk ป้ายอิเล็กทรอนิกส์ เป็นต้น รูปแบบในการทำธุรกรรม • ระหว่างธุรกิจกับธุรกิจ (Business to Business: B2B) • ระหว่างธุรกิจกับผู้บริโภค (Business to Consumer: B2C) • ระหว่างธุรกิจกับภาครัฐบาล (Business to Government: B2G) • ระหว่างผู้บริโภคกับผู้บริโภค (Consumer to Consumer: C2C) • ระหว่างภาครัฐบาลกับธุรกิจ (Government to Business: G2B)

ศัพท์	ความหมาย
	• ระหว่างภาครัฐบาลกับผู้บริโภค (Government to Consumer: G2C) • ระหว่างภาครัฐบาลกับภาครัฐบาล (Government to Government: G2G)
ภัยคุกคาม (Threat)	ภัยหรือเหตุการณ์ที่เกิดขึ้นที่ไม่พึงประสงค์ ซึ่งอาจส่งผลให้เกิดความเสียหายต่อระบบหรือองค์กร รวมถึงภัยคุกคามทางไซเบอร์
ภัยคุกคามทางไซเบอร์	การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง
ระดับการให้บริการ (Service Level)	ระดับเป้าหมายของการให้บริการที่องค์กรคาดหวัง เช่น เป้าหมายของการให้บริการเครือข่ายอาจถูกกำหนดว่าเครือข่ายต้องสามารถให้บริการได้อย่างต่อเนื่องร้อยละ 98 ของระยะเวลาตลอดทั้งปี กล่าวอีกนัยหนึ่งคือเครือข่ายเกิดการหยุดชะงักได้ไม่เกินร้อยละ 2 ต่อปี เป็นต้น
ระบบงาน (Application Systems)	ระบบสารสนเทศเพื่อให้บริการต่างๆ ซึ่งทำงานอยู่บนอุปกรณ์คอมพิวเตอร์ อุปกรณ์โทรคมนาคม เช่น ระบบงานอีเมล์ ระบบงานบุคคล ระบบงานบัญชี ระบบลงทะเบียนการเข้าใช้งานอินเทอร์เน็ต ระบบเครือข่ายสื่อสารคอมพิวเตอร์เชื่อมโยงหน่วยงานภาครัฐ ระบบให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority: CA) เป็นต้น
ระบบสารสนเทศ (Information System)	ระบบงาน เครือข่าย ชุดของอุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ซึ่งใช้ในการจัดเก็บ ประมวลผลและส่งผ่านข้อมูลคอมพิวเตอร์ รวมถึง ชุดของอุปกรณ์โทรคมนาคม
ลิขสิทธิ์ (Copyright)	สิทธิแต่ผู้เดียวที่จะทำการใดๆ ตามพระราชบัญญัติ ลิขสิทธิ์ พ.ศ. 2537 เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น
ศูนย์การสื่อสาร (Communication Centres)	ตึกหรืออาคารซึ่งเป็นสถานที่จัดเก็บและเป็นที่ตั้งของอุปกรณ์ให้บริการโทรคมนาคมต่างๆ หรือเป็นที่ตั้งของระบบควบคุมอุปกรณ์ให้บริการโทรคมนาคมต่างๆ เช่น อาคารชุมสาย หรือเป็นที่ตั้งของระบบควบคุมอุปกรณ์ให้บริการโทรคมนาคมต่างๆ เป็นต้น
ศูนย์คอมพิวเตอร์ (Data Center)	สถานที่ที่ออกแบบและก่อสร้างให้มีความมั่นคงปลอดภัยสูง โดยสร้างขึ้นด้วยโครงสร้างพื้นฐาน (Infrastructure) เพื่อให้ความคุ้มครองข้อมูล และระบบงานที่จำเป็นในการดำเนินธุรกิจ และการให้บริการดูแลระบบคอมพิวเตอร์ของลูกค้า เช่น ระบบเซิร์ฟเวอร์หลัก ระบบเครือข่ายหลัก และระบบฐานข้อมูลหลัก เพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ และทำงานได้อย่างต่อเนื่องตลอดเวลา
ส่วนงานที่รับผิดชอบด้านบริหารทรัพยากรบุคคล	ส่วนงานที่รับผิดชอบอย่างหนึ่งอย่างใด ดังนี้ • การวิเคราะห์งาน การบริหารกำลังคน การจัดทำคำบรรยายลักษณะงาน การประเมินค่างาน การจัดทำกรอบอัตรากำลัง การจ้างงาน การสรรหาและคัดเลือก • การวิเคราะห์ และดำเนินการในงานปฏิบัติการงานบุคคล ซึ่งรวมถึงงานที่เกี่ยวกับการเกษียณอายุของพนักงาน

ศัพท์	ความหมาย
ส่วนงานที่รับผิดชอบระบบสารสนเทศ	ส่วนงานที่มีหน้าที่รับผิดชอบในการดูแลระบบหรือให้บริการระบบสารสนเทศ และดูแลระบบหรือให้บริการโทรคมนาคม ของบริษัท
ส่วนงานที่รับผิดชอบเรื่องการรวบรวม จัดเก็บ และจัดส่งเอกสารสำคัญ รวมถึงหลักฐาน ตามกฎหรือหลักเกณฑ์สำหรับการเก็บรวบรวมหลักฐานอ้างอิงในกระบวนการทางกฎหมายที่เกี่ยวข้อง	ส่วนงานที่รับผิดชอบ ดังนี้ • รวบรวม จัดเก็บ และจัดส่งเอกสารสำคัญ รวมถึงหลักฐาน ตามกฎหรือหลักเกณฑ์สำหรับการเก็บรวบรวมหลักฐานอ้างอิงในกระบวนการทางกฎหมายที่เกี่ยวข้อง
ส่วนงานที่ว่าจ้าง	ส่วนงานหรือตัวแทนของบริษัทที่ได้รับมอบหมายให้ดำเนินการว่าจ้างพนักงาน ลูกจ้าง หรือหน่วยงานภายนอก
ส่วนงานภายในของบริษัทที่รับผิดชอบในการตรวจสอบ	ส่วนงานที่รับผิดชอบอย่างหนึ่งอย่างใด ดังนี้ • ดำเนินงานตรวจสอบ ให้สอดคล้องกับนโยบาย เป้าหมาย กลยุทธ์ และแผนธุรกิจรวมของบริษัท เพื่อให้บรรลุวัตถุประสงค์ของบริษัท • ดำเนินงานตรวจประเมินระบบสารสนเทศ
สื่อบันทึกข้อมูลที่พกพาได้ (Removable Media)	สื่อบันทึกข้อมูลที่พกพาหรือเคลื่อนย้ายได้ (Removable Media) ที่บันทึกสารสนเทศของบริษัท เช่น เทปสำรองข้อมูล CD DVD ฮาร์ดดิสก์สำหรับติดตั้งภายนอก (External Hard disk) Flash Drive และเอกสาร (Printed Media) เป็นต้น
สิทธิของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
หน่วยงานภายนอก (Third Party)	หน่วยงานหรือบุคคลภายนอกที่ดำเนินธุรกิจหรือให้บริการกับบริษัท ตัวอย่างหน่วยงานหรือบุคคลภายนอก • บริษัทในเครือของบริษัท (Subsidiary) • บริษัทคู่ค้า (Business Partner) • ผู้รับจ้างปฏิบัติงานให้กับบริษัท (Outsource) • ผู้รับจ้างพัฒนาระบบงานหรือจัดหาวัสดุอุปกรณ์ต่างๆ (Supplier) • ผู้รับสัมปทาน (Concessionaire) • ผู้ให้บริการต่างๆ (Service Provider) • ที่ปรึกษา (Consultant) วิทยากร (Instructor)

ศัพท์	ความหมาย
	• เจ้าหน้าที่ของหน่วยงานต่างๆ เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม บริษัท ทริส คอร์ปอเรชั่น จำกัด (TRIS) สำนักงานคณะกรรมการ นโยบายรัฐวิสาหกิจ (สคร.) และสำนักงานตำรวจแห่งชาติ เป็นต้น
ห้องคอมพิวเตอร์ (Computer Room)	ห้องภายในอาคารซึ่งเป็นสถานที่จัดเก็บและเป็นที่ตั้งของเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์สนับสนุนการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย
ห้องอุปกรณ์โทรคมนาคม (Telecommunications Equipment Room)	ห้องภายในตึกหรืออาคารหนึ่งซึ่งเป็นสถานที่จัดเก็บและเป็นที่ตั้งของอุปกรณ์ให้บริการโทรคมนาคมต่างๆ เช่น ห้องโทรคมนาคม
หัวหน้าคณะทำงาน/ โครงการ	บุคคลที่มีหน้าที่รับผิดชอบในการวางแผน การดำเนินการ การจัดการโครงการ ให้เป็นไปตามเป้าหมายที่วางไว้
เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Event)	การเกิดขึ้นของสถานะของระบบสารสนเทศ หรือเครือข่าย ซึ่งแสดงถึงความเป็นไปได้ของการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หรือความล้มเหลวของการป้องกันด้านสารสนเทศ หรือการเกิดขึ้นของเหตุการณ์ผิดปกติที่อาจเกี่ยวข้องกับการรักษาความปลอดภัยด้านสารสนเทศ หรือการดำเนินการใดๆ ที่เป็นการไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เช่น • มีการแจ้งเตือนจาก IDS (Intrusion Detection System) หรือ IPS (Intrusion Protection System) • มีการแจ้งเตือนจากซอฟต์แวร์หรืออุปกรณ์สำหรับตรวจจับและกำจัดโปรแกรมที่ไม่ประสงค์ดี • การโจมตีผ่านทางเครือข่าย • พบไฟล์คอมพิวเตอร์ที่มีชื่อผิดปกติ • ได้รับจดหมายอิเล็กทรอนิกส์มากผิดปกติ • มีปริมาณการใช้งานเครือข่ายมากผิดปกติ • ปริมาณข้อมูลที่วิ่งผ่านเครือข่ายมากผิดปกติ • เผยแพร่ข้อความซึ่งขัดต่อกฎหมาย
เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใดๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์
เหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Incident)	เหตุการณ์ หรือลำดับของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Event) ซึ่งมีความเป็นไปได้สูงที่จะส่งผลเสียต่อการดำเนินธุรกิจ และการรักษาความปลอดภัยด้านสารสนเทศ เช่น • การแพร่กระจายของไวรัสคอมพิวเตอร์ • การดักจับข้อมูลทางเครือข่ายโดยมิได้รับอนุญาต

ศัพท์	ความหมาย
	• การถูกโจมตีทางเครือข่ายโดยผู้ไม่ประสงค์ดีทำให้ระบบเครือข่ายไม่สามารถให้บริการได้ • การเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยผู้ที่ไม่ได้รับอนุญาต • การสูญเสียข้อมูลสำคัญ • การใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ เป็นต้น
อุปกรณ์ให้บริการโทรคมนาคม หรืออุปกรณ์โทรคมนาคม (Telecommunications Facilities)	เครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร สายสื่อสาร สายเคเบิล หรืออุปกรณ์ไฟฟ้าอื่นๆ สำหรับให้บริการด้านโทรคมนาคม
อุปกรณ์คอมพิวเตอร์ (Computer Equipment)	เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง ส่วนประกอบต่างๆทางกายภาพของเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น Printer, Modem, Hard Disk, Disk Drive, Memory Card, Sound Card, Mouse, Keyboard, RAM, CPU และ Network Card เป็นต้น
อุปกรณ์คอมพิวเตอร์ประเภทพกพา (Mobile Device)	อุปกรณ์คอมพิวเตอร์ ที่สะดวกในการพกพา เช่น คอมพิวเตอร์โน้ตบุ๊ค (Laptop), Netbook, Tablet, Personal Digital Assistant (PDA) หรือ Smart Phone เป็นต้น
อุปกรณ์เครือข่าย (Network Equipment)	ฮับ (Hub), อุปกรณ์สวิตซ์ (Switch), อุปกรณ์จัดเส้นทาง (Router), อุปกรณ์เชื่อมต่อวงแลน (Bridge), อุปกรณ์เชื่อมต่อเครือข่ายต่างประเภทเข้าด้วยกัน (Gateway) และอุปกรณ์เครือข่ายอื่นๆ ที่เกี่ยวข้อง เช่น สายสัญญาณ (Cable), Modem, Network Card, Wireless Card, Access Point เป็นต้น
อุปกรณ์ประมวลผลสารสนเทศ (Information Processing Facilities)	ระบบสารสนเทศ อุปกรณ์สนับสนุนการประมวลผลสารสนเทศ บริการพื้นฐานเพื่อสนับสนุนระบบสารสนเทศ บริการด้านการสื่อสารและโทรคมนาคม และสถานที่ตั้งทางกายภาพของระบบสารสนเทศ
อุปกรณ์สนับสนุนการประมวลผลสารสนเทศ (Supporting Utilities)	อุปกรณ์และระบบที่ช่วยสนับสนุนการทำงานของอุปกรณ์ประมวลผลสารสนเทศ เช่น ระบบไฟฟ้า ระบบปรับอากาศ ระบบดับเพลิง ระบบควบคุมอุณหภูมิและความชื้น เป็นต้น
อุปกรณ์สำนักงาน (Office Automation)	อุปกรณ์อิเล็กทรอนิกส์ที่ใช้อำนวยความสะดวกในการดำเนินงานภายในสำนักงาน เช่น เครื่องโทรสาร และเครื่องถ่ายเอกสาร เป็นต้น
อุปกรณ์สื่อสาร (Communication Equipment)	อุปกรณ์ที่สามารถทำให้สื่อสารถึงกันได้ เช่น โทรศัพท์ วิทยุสื่อสาร เป็นต้น
แอปพลิเคชัน (Application)	โปรแกรมคอมพิวเตอร์หรือกลุ่มของโปรแกรมซึ่งทำหน้าที่เพื่อจุดประสงค์อย่างใดอย่างหนึ่ง เช่น เวิร์ดโปรเซสเซอร์ สเปรดชีต ระบบฐานข้อมูล และโปรแกรมที่พัฒนาเพื่อสนับสนุนงานทางธุรกิจ เป็นต้น