บริษัท เอ็ม วิชั่น จำกัด (มหาชน)
M Vision Public Company Limited
11/1 ซ. รามคำแหง 121 ถ. รามคำแหง แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
11/1 Ramkhamhaeng 121 Ramkhamhaeng Rd. Huamark, Bangkapi Bangkok 10240
Tel. 02-735-1201,02,04 Fax : 0-2735-2719

บริษัท เอ็ม วิชั่น จำกัด (มหาชน)

นโยบาย

การรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริษัท เอ็ม วิชั่น จำกัด (มหาชน)
M Vision Public Company Limited
11/1 ซ. รามคำแหง 121 ถ. รามคำแหง แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
11/1 Ramkhamhaeng 121 Ramkhamhaeng Rd. Huamark, Bangkapi Bangkok 10240
Tel. 02-735-1201,02,04 Fax : 0-2735-2719

บทนำ

การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้เพื่อให้การดำเนินการใด ๆด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้และในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศถือเป็นสิ่งสำคัญที่ต้องปฏิบัติอย่างต่อเนื่องและจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือจากทุกฝ่ายนอกจากนั้นยังต้องมีการตรวจสอบอย่างสม่ำเสมอเพื่อปรับปรุงให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็วเพื่อให้ระบบสารสนเทศของบริษัทเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องซึ่งอาจส่งผลให้ถูกคุกคามจากภัยต่าง ๆ

ดังนั้น บริษัท เอ็ม วิชั่น จำกัด (มหาชน) จึงได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขึ้น เพื่อเผยแพร่ให้พนักงานผู้ใช้งาน เจ้าหน้าที่ รวมถึงบุคคลภายนอกได้รับทราบ และขอความร่วมมือในการปฏิบัติตามอย่างเคร่งครัดต่อไป

บริษัท เอ็ม วิชั่น จำกัด (มหาชน)
M Vision Public Company Limited
11/1 ซ. รามคำแหง 121 ถ. รามคำแหง แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
11/1 Ramkhamhaeng 121 Ramkhamhaeng Rd. Huamark, Bangkapi Bangkok 10240
Tel. 02-735-1201,02,04 Fax : 0-2735-2719

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์

2) เพื่อให้มีนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทและเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

3) เพื่อกำหนดแนวทางและวิธีการปฏิบัติสำหรับพนักงาน ผู้ใช้งาน เจ้าหน้าที่ บุคคลภายนอก หรือบุคคลที่ปฏิบัติงานให้กับบริษัท

4) เพื่อให้พนักงานทุกคนได้ตระหนักและเข้าใจในบทบาทหน้าที่ของตน ร่วมกันดูแลรักษา และใช้ระบบเทคโนโลยีสารสนเทศให้เกิดประโยชน์สูงสุดต่อบริษัท

5) เพื่อลดความเสี่ยงและเตรียมความพร้อมเมื่อเกิดเหตุการณ์ฉุกเฉิน

6) เพื่อให้เกิดความมั่นใจในระบบสารสนเทศทั้งภายในและภายนอกองค์กร

2. ความหมายของคำจำกัดความ

1) “ทรัพย์สินคอมพิวเตอร์” หมายถึง ทรัพย์สินทุกอย่างที่เกี่ยวกับการใช้งานระบบคอมพิวเตอร์เช่น ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เป็นต้น

2) “ระบบเครือข่าย” (Network System) หมายถึงระบบเครือข่ายคอมพิวเตอร์ของบริษัท

3) “ระบบคอมพิวเตอร์แม่ข่าย” (Server) หมายถึง เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน เช่น จัดเก็บข้อมูล หรือซอฟต์แวร์สำหรับให้บริการแก่เครื่องคอมพิวเตอร์ หรือควบคุมการทำงานเครือข่าย

4) “การเข้าถึงเครือข่ายจากระยะไกล” หมายถึง การที่เครื่องคอมพิวเตอร์หรือระบบเครือข่าย เชื่อมต่อเข้ากับระบบคอมพิวเตอร์ หรือเครือข่ายอื่น ผ่านอุปกรณ์สื่อสารหรือสัญญาณอื่น ๆ เช่น Firewall VPN

5) “การควบคุมการเข้าถึง” (Access Control) หมายถึง การควบคุมการเข้าถึงหรือใช้งานทรัพย์สินคอมพิวเตอร์ให้เป็นไปตามสิทธิ์ที่กำหนดไว้เท่านั้น

6) “คอมพิวเตอร์” หมายถึง อุปกรณ์ที่ใช้ในการประมวลผลข้อมูลที่ทำงานด้วยระบบอิเล็กทรอนิกส์ โดยทำงานตามคำสั่งผ่านซอฟต์แวร์ให้ได้ผลตามที่ต้องการ เช่น คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) และคอมพิวเตอร์แบบพกพา (Notebook)

7) “อุปกรณ์คอมพิวเตอร์” หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์ เพื่อสนับสนุนให้เครื่องเครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ และให้รวมถึงเครื่องคอมพิวเตอร์

8) “สื่อสัญญาณ” หมายถึง สื่อกลางใด ๆ ที่ใช้เชื่อมต่อระหว่างอุปกรณ์คอมพิวเตอร์ เช่น สายทองแดง สายใยแก้วนำแสง เครือข่ายไร้สาย Wi-fiเป็นต้น

9) “ฮาร์ดแวร์” หมายถึง อุปกรณ์คอมพิวเตอร์

10) “ซอฟต์แวร์” หมายถึง ชุดคำสั่งให้คอมพิวเตอร์ทำงานตามต้องการ

11) “ซอฟต์แวร์ระบบ” หมายถึง ซอฟต์แวร์ที่ควบคุมการทำงานของอุปกรณ์คอมพิวเตอร์ เช่น ระบบปฏิบัติการ

12) “ซอฟต์แวร์ประยุกต์” หมายถึง ซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้งานเฉพาะด้านตามความต้องการ เช่น ซอฟต์แวร์สำหรับพิมพ์เอกสาร ซอฟต์แวร์สำหรับการคำนวนทางบัญชีเป็นต้น

13) “ระบบเทคโนโลยีสารสนเทศ” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างระบบสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและการควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่น อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ระบบงาน และสารสนเทศเป็นต้น

14) “สารสนเทศ” หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือ ภาพกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

15) “ระบบงาน” หมายถึง การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงาน เพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ เช่น ระบบจัดเก็บ เอกสารต่าง ๆ หรือระบบบัญชี เป็นต้น

16) “ระบบปฏิบัติการ” (Operating System) หมายถึง ซอฟต์แวร์ควบคุมการทำงานของ เครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ได้แก่ การ์ดหน่วยความจำ การควบคุม การทำงานของอุปกรณ์ การป้อนข้อมูล แป้นพิมพ์ เมาส์อุปกรณ์แสดงผล จอภาพ เครื่องพิมพ์

17) “การป้องการบุกรุก” (Firewall) หมายถึงระบบรักษาความปลอดภัยที่ประกอบด้วย กลุ่มอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ซึ่งทำหน้าที่ป้องกันผู้ไม่ได้รับอนุญาตจากเครือข่ายภายนอกเข้าใช้ระบบ และจำกัดการใช้งานของผู้ใช้ภายในให้เป็นไปการนโยบายที่บริษัทได้กำหนดไว้

18) “ข้อมูล” หมายถึง ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์สร้าง สั่ง รับ เก็บรักษา หรือประมวลผล ได้ด้วยวิธีการทางอิเล็กทรอนิกส์บนอุปกรณ์คอมพิวเตอร์ และให้หมายถึงความรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

19) “ไฟล์” (File) หมายถึง ข้อมูลที่ถูกรวบรวมลงสื่อบันทึกและระบุเป็นหนึ่งหน่วยโดยมีชื่อเฉพาะ เช่น ซอฟต์แวร์ใช้งานและไฟล์เอกสารต่าง ๆ ที่สร้างขึ้นและใส่ชื่อให้แก่ไฟล์นั้นแล้วเก็บบันทึกลงสื่อบันทึกเป็นต้น

20) “ผู้ใช้งาน” (User) หมายถึง เจ้าหน้าที่หรือบุคคลภายนอกที่มีสิทธิ์ใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

21) “ผู้บริหารเครือข่าย” (Network Administrator) หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบในการดูและบำรุงรักษาเครือข่าย

22) “ผู้บริหารคอมพิวเตอร์แม่ข่าย” (Host/Server Administrator) หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลบำรุงรักษาคอมพิวเตอร์แม่ข่าย หรือ Host/Server

23) “ผู้บริหารระบบป้องกันการบุกรุก” (Firewall Administrator) หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลบำรุงรักษาป้องกันการบุกรุก

24) “บัญชีผู้ใช้งาน” (User Name) หมายถึง บัญชีที่ผู้ที่ใช้งานในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบเทคโนโลยีสารสนเทศ

25) “บัญชีผู้บริหารคอมพิวเตอร์แม่ข่าย” (Administrator Account) หมายถึง บัญชีผู้บริหารคอมพิวเตอร์แม่ข่ายใช้ในการบริหารระบบคอมพิวเตอร์แม่ข่าย

26) “บัญชีผู้ใช้ระบบอีเมล์” (Email Account) หมายถึง บัญชีที่ผู้ใช้งานสามารถเข้าถึงระบบอีเมล์ของบริษัท

27) “เอกสารโครงแบบ” (Configuration Document) หมายถึง เอกสารที่แสดงรายละเอียดการกำหนดค่าต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศใช้งานได้ตามความต้องการ

28) “ความเสี่ยง”หมายถึงโอกาสของทรัพย์สินคอมพิวเตอร์ในการถูกละเมิดการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

29) “เหตุการณ์ผิดปรกติ”(Incident) หมายถึงเหตุการณ์ใด ๆที่มีผลกระทบต่อการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

30) “เจ้าหน้าที่” หมายถึง พนักงานของบริษัท

31) “ส่วนงาน” หมายถึง ฝ่ายงานตามโครงสร้างบริษัท

32) “โปรแกรมประสงค์ร้าย” หมายถึง ฮาร์ดแวร์ หรือซอฟต์แวร์ที่มีถูกใส่เข้าไปในระบบโดยไม่ได้รับอนุญาต เพื่อให้ทำงานตามความประสงค์ของผู้ประสงค์ร้าย ซึ่งมีผลให้คอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศ หรือ ชุดคำสั่งอื่นได้รับความเสียหายถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

33) “หน่วยงานภายนอก”หมายถึงองค์กรซึ่งบริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูลหรือใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทโดยจะได้รับสิทธิ์ตามประเภทการใช้งานและต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทโดยไม่ได้รับอนุญาตเมื่อนโยบายฉบับนี้มีผลบังคับใช้ให้แผนกเทคโนโลยีสารสนเทศเป็นผู้ทำหน้าที่ในการออกระเบียบปฏิบัติ ข้อกำหนด ข้อบังคับต่าง ๆ ที่จำเป็นเพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทโดยความเห็นชอบจากผู้บริหารระดับสูง และคณะผู้บริหารให้การสนับสนุนในเรื่องนโยบายงบประมาณ ทรัพยากรและอื่น ๆ ที่จำเป็นเพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ มีการพัฒนาและปรับปรุงอย่างต่อเนื่องซึ่งจะต้องจัดให้มีการเผยแพร่นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ให้กับพนักงาน ผู้ใช้งาน เจ้าหน้าที่ บุคคลภายนอก หรือบุคคลที่ปฏิบัติงานให้กับบริษัททราบและนำไปปฏิบัติ ต้องดำเนินการทบทวนและประเมินนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญซึ่งมีผลต่อการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของบริษัท

3. โครงสร้างทางด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศในองค์กร

3.1. โครงสร้างทางด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศภายในองค์กร

1) ผู้บริหารระดับสูงเป็นผู้กำหนดให้มีตัวแทนหรือคณะทำงานจากหน่วยงานต่าง ๆภายในบริษัทเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศของบริษัทโดยที่ตัวแทนหรือคณะทำงานนี้ จะต้องมีการกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทอย่างชัดเจน
2) ตัวแทนหรือคณะทำงานซึ่งถูกแต่งตั้งโดยผู้บริหารระดับสูง เป็นผู้รับผิดชอบในการบริหารจัดการและควบคุมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทตลอดจนทบทวนนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ จัดทำขั้นตอนและแนวทางปฏิบัติด้านการรักษาความมั่นคง
3) ปลอดภัยของระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ และเอกสารที่เกี่ยวข้องในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์
4) เจ้าหน้าที่ต้องไม่เปิดเผยความลับของบริษัทเว้นแต่จะได้รับการอนุญาตให้เปิดเผยจากบริษัทและต้องกำหนดให้มีการตรวจสอบการดำเนินงานและการปฏิบัติที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อบริษัท

3.2. โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้า หรือหน่วยงานภายนอก

1) ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงระบบสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่อนุญาตให้สามารถเข้าถึงระบบหรือข้อมูลได้
2) ต้องระบุและบังคับใช้ข้อกำหนดทางความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทเมื่อมีความจำเป็นต้องให้บุคคลภายนอก หรือหน่วยงานภายนอก หรือผู้ใช้บริการเข้าถึงระบบสารสนเทศหรือทรัพย์สินสารสนเทศของบริษัทก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

4. การบริหารจัดการทรัพย์สินขององค์กร

4.1 ความรับผิดชอบต่อทรัพย์สิน

ต้องมีการจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อบริษัทให้ถูกต้องอยู่สม่ำเสมอ รวมทั้งต้องจัดทำกฎระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานระบบเทคโนโลยีสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับการประมวลระบบสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้นอันเกิดจากการขาดความระมัดระวังการขาดการดูแลเอาใจใส่ ต้องการเก็บรักษาทรัพย์สินที่มีความสำคัญต่อบริษัทอย่างเป็นระเบียบในสถานที่ปลอดภัยให้เหมาะสม

บริษัท เอ็ม วิชั่น จำกัด (มหาชน)
M Vision Public Company Limited
11/1 ซ. รามคำแหง 121 ถ. รามคำแหง แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
11/1 Ramkhamhaeng 121 Ramkhamhaeng Rd. Huamark, Bangkapi Bangkok 10240
Tel. 02-735-1201,02,04 Fax : 0-2735-2719

1) การอนุญาตให้ใช้งานทรัพย์สินด้านอุปกรณ์คอมพิวเตอร์มีดังนี้

- ☐ ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่บริษัทเป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการปฏิบัติงานตามภารกิจของบริษัท การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้นอนุญาตให้สามารถใช้ได้ในขอบเขตตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่รับผิดชอบของเจ้าหน้าที่
- ☐ เจ้าหน้าที่ หรือบุคคลที่ได้รับว่าจ้างโดยบริษัท จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้รับมอบไว้ให้ใช้งาน รวมทั้ง สอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และถูกต้อง โดยหมายความรวมถึงข้อมูล และระบบเทคโนโลยีสารสนเทศของบริษัท
- ☐ ผู้ใช้งานต้องรับผิดชอบในใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ของบริษัทอย่างระมัดระวัง และให้การปกป้องเสมือนเป็นทรัพย์สินของตนเอง
- ☐ เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดของบริษัทต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้ง เมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Server หรือ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง
- ☐ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบอุปกรณ์คอมพิวเตอร์ของบริษัทตามที่ได้รับมอบหมาย
- ☐ ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวเข้ากับระบบเครือข่ายของบริษัทและต้องไม่ติดตั้ง ซอฟต์แวร์ใดๆ ลงในเครื่องคอมพิวเตอร์ของบริษัทก่อนได้รับอนุญาตจากแผนกเทคโนโลยีสารสนเทศ
- ☐ เครื่องคอมพิวเตอร์พกพาของผู้ใช้งาน ที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัท เช่นการติดตั้ง ซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ
- ☐ เครื่องคอมพิวเตอร์ส่วนตัวของผู้ใช้งาน ที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัท เช่นการติดตั้ง ซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ
- ☐ อุปกรณ์คอมพิวเตอร์ของบริษัทต้องไม่ถูกดัดแปลงหรือติดตั้งอุปกรณ์เพิ่มเติมใดๆก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้นๆ และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ บนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด

2) การอนุญาตให้ใช้งานทรัพย์สินด้านซอฟต์แวร์มีดังนี้

- ☐ ห้ามเจ้าหน้าที่ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัท
- ☐ ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัททั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมาต้องได้รับการตรวจสอบควบคุม หรืออนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

☐ ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไปต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของบริษัทมีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้

☐ รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสารและได้รับการอนุมัติโดยผู้บริหารระดับสูงเพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านั้นมีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัทเท่านั้น

3) การอนุมัติให้ใช้งานอินเทอร์เน็ตมีดังนี้

- บริษัทจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงานและอำนวยความสะดวกแก่เจ้าหน้าที่ในการค้นหาข้อมูลความรู้และการติดต่อสื่อสารกับบุคคลภายนอกเพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของบริษัท
- ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัทและบุคคลอื่นที่เกี่ยวข้องกับบริษัทเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีทางกฎหมาย
- การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านช่องทาง (Gateway) ที่ได้รับอนุญาตหรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้บริษัทขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม
- ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป็อบอัพ หรือเข้าสู่เว็บไซต์ใดๆ ที่โฆษณาโดยเชิงสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต
- ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
- บริษัทไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ด,บล็อก หรือสื่อโซเชียลมีเดียต่าง ๆ) ของเจ้าหน้าที่ ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

4) การอนุญาตให้ใช้งานอีเมล์มีดังนี้

- ผู้ใช้งานอีเมล์ของบริษัท ต้องมี E-Mail Account เป็นของตัวเอง
- E-Mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมล์ไปใช้ในทางที่ผิด
- E-Mail Accountที่มีวัตถุประสงค์พิเศษ อาจได้รับการสร้างขึ้นเพื่อเป็น E-Mail Account กลางของส่วนงาน และ/หรือเพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่า 1 คนขึ้นไป โดยต้องมีผู้ใช้งาน 1 คนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นผู้ดูแล E-Mail Account นั้น
- E-Mail Account ทั้งหมด และอีเมล์ทุกฉบับ (รวมถึงอีเมล์ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท ถือเป็นทรัพย์สินของบริษัท

- ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือติดต่อสื่อสารกับระบบอีเมล์ของบริษัท
- พื้นที่เก็บอีเมล์บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้เมื่อปริมาณของอีเมล์มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ และถ้าหากปริมาณของอีเมล์มากเกินกว่า พื้นที่จัดเก็บแล้วผู้ใช้งานจะไม่สามารถรับ-ส่งอีเมล์ได้ตามปกติอีกต่อไป
- ผู้ใช้งานต้องลบอีเมล์ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล์ให้เป็นไปตามขนาดที่บริษัทกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงาน และอีเมล์ตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้ Email Account ของบริษัทเพื่อกระทำการใดๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมายเช่น เช่นเพื่อโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี และการเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์การเผยแพร่ภาพลามกอนาจารเป็นต้น
- ห้ามใช้ Email Account ของบริษัท ในการประกาศข้อมูลใดๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก สื่อต่างๆ เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานของบริษัท
- การใช้งานอีเมล์ต้องได้รับการตั้งค่าให้อีเมล์ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งออกเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงาน ชื่อบริษัทและเบอร์โทรศัพท์ติดต่อ
- ห้ามผู้ใช้งานทำสำเนาข้อความหรือสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่น ก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนของบริษัท
- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นในอีเมล์ อีเมล์ หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ E-Mail Account ของตนโดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ เช่น อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้าต่างๆ (Spam Mail)
- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่งอีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งต่ออีเมล์ที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาทกล่าวร้ายทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศหรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรมหรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมล์ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียแก่บริษัท
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง

- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

5) การอนุญาตให้ใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร มีดังนี้

- ถ้าหากผู้ใช้งานได้รับข้อมูลจาการส่งโทรสารที่ผิดพลาด เช่น ส่งโทรสารผิดหมายเลข ผิดส่วนงานเป็นต้น ผู้ใช้งานต้องแจ้งให้ผู้ส่งสารนั้นรับทราบ และทำลาย เอกสารข้อมูลนั้น ๆ
- ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น

4.2 จัดการทรัพย์สินสารสนเทศ

1) ต้องจัดให้มีวิธีการจัดทำและจัดการป้อนชื่อสำหรับปิดฉลากเอกสารข้อมูล และอุปกรณ์ทรัพย์สิน สารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศ
2) ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น
3) ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่เก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่า 1 คนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม
4) ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน
5) ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่อง โทรสาร เครื่องถ่ายเอกสาร โดยทันที
6) เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล
7) เจ้าหน้าที่ต้องไม่พูดคุย หรือใช้งานข้อมูลลับของบริษัทในพื้นที่สาธารณะ เช่นลิฟท์ ร้านอาหาร
8) สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ เช่นPDA Thumb-drive CD-Romต่างๆ ที่มีข้อมูลลับของบริษัทบันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง ข้อมูลสำคัญที่เกี่ยวข้องกับการดำเนินงานของบริษัททั้งหมด ทั้งที่มีการเก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลโดยผู้ใช้งานต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาใดๆ เกิดขึ้น เช่น การติดไวรัส ฮาร์ดดิสก์เสีย เป็นต้น

5. ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร

5.1 การสร้างความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากรก่อนการทำงาน

หน่วยงานภายนอกที่ได้รับการว่าจ้างตามสัญญาการจ้างงานต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทอย่างเคร่งครัด

5.2 การสร้างความมั่นคงปลอดภัยขณะเป็นพนักงาน

1) พนักงานผู้ใช้งานเจ้าหน้าที่ที่มีหน้าที่ศึกษาทำความเข้าใจวิธีปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศที่บริษัทกำหนดเพื่อนำไปปฏิบัติในการรักษาความปลอดภัยทรัพย์สินคอมพิวเตอร์ในส่วนที่ตนใช้งานหรือดูแลรับผิดชอบ
2) ต้องจัดอบรมให้ความรู้แก่เจ้าหน้าที่และลูกจ้างเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศของบริษัทด้วย เจ้าหน้าที่และลูกจ้างใหม่ทุกคนต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานก่อน หรืออย่างน้อยภายใน 30 วันนับจากเข้าทำงานในหน่วยงาน
3) ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติของบริษัท แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุไว้ ในแต่ละข้อกฎหมายนั้น ๆ

5.3 การยกเลิกการจ้างงาน

เพื่อให้การบริหารจัดการ Login หรือ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ฝ่ายทรัพยากรบุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีเมื่อมีเหตุดังนี้

1) การว่าจ้างงาน
2) การเปลี่ยนแปลงสภาพการว่าจ้างงาน
3) การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร เจ้าหน้าที่ และลูกจ้าง
4) การโยกย้ายหน่วยงาน
5) การพักงาน การลงโทษทางวินัย หรือการระงับการปฏิบัติหน้าที่

เจ้าหน้าที่และลูกจ้างซึ่งพ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้าออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่างๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน

หลังจากมีการยกเลิกหรือเปลี่ยนแปลงตำแหน่งการเป็นเจ้าหน้าที่และลูกจ้างแล้ว จะต้องแจ้งยกเลิกการเข้าถึงข้อมูลต่างๆ ของหน่วยงานและจะแจ้งต่อเจ้าหน้าที่และลูกจ้างอื่น ๆ ลูกค้า บริษัทคู่ค้า ที่เกี่ยวข้อง ให้รับทราบตามความเหมาะสม

6. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

6.1. บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

1) ให้แผนกเทคโนโลยีสารสนเทศเป็นผู้กำหนดรายละเอียดของสถานที่ อุปกรณ์ ป้องกัน ความเสียหายและการควบคุมการเข้าออกในเขตรักษาความปลอดภัยให้เหมาะสมกับสถานที่หรือพื้นที่ที่ต้องรักษาความปลอดภัยที่เหมาะสม
2) ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัยและอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้นหากมีบุคคลอื่นใดที่ไม่ใช่เจ้าหน้าที่ในฝ่ายเทคโนโลยีสารสนเทศขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้าต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตหรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราวทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชนหรือบัตรประจำตัวอื่นที่ราชการออกให้โดยฝ่ายเทคโนโลยีสารสนเทศจะต้องจดบันทึกบุคคล และการขอเข้าออกไว้เป็นหลักฐาน(ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่)และต้องมีการบันทึกข้อมูลการเข้าออกศูนย์คอมพิวเตอร์ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน
3) ต้องไม่ยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาดเว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงานและพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต
4) ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับสำนักงาน ห้องทำงานและเครื่องมือต่างๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมากสำนักงานหรือห้องทำงานจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว ประตูหน้าต่างของสำนักงานหรือห้องต้องใส่กุญแจเสมอเมื่อไม่มีคนอยู่
5) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุมหรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด
6) ข้อมูลสื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะ โดยไม่ได้รับการทำลายอย่างเหมาะสม
7) เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาดเว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการและเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

เพื่อประโยชน์ในการรักษาความปลอดภัยสถานที่ติดตั้งและเก็บรักษาทรัพย์สินคอมพิวเตอร์ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ อัคคีภัย ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆทั้งที่เกิดจากมนุษย์และธรรมชาติพร้อมทั้งให้ทดสอบระบบรักษาความปลอดภัยภายในเขตรักษาความปลอดภัยอย่างน้อยปีละ 1 ครั้ง จัดอบรมและชักซ้อมเจ้าหน้าที่ที่ปฏิบัติงานภายในเขตรักษาความปลอดภัยตามระยะเวลาอันสมควร เพื่อให้สามารถใช้งานอุปกรณ์รักษาความปลอดภัยได้อย่างถูกต้องและเหมาะสมให้แผนกเทคโนโลยีสารสนเทศรับผิดชอบในการบำรุงรักษาสถานที่อุปกรณ์ป้องกันความเสียหายและอุปกรณ์ป้องกันภัยต่างๆ ภายในเขตรักษาความปลอดภัยตามระยะเวลาอันสมควรให้แผนกเทคโนโลยีสารสนเทศจำกัดพื้นที่การเข้าถึงของบุคคลภายนอกที่อาจเข้ามาในพื้นที่ได้

6.2 ความมั่นคงปลอดภัยของอุปกรณ์

1) เจ้าหน้าที่หรือผู้ใช้งานต้องจัดวางและป้องกันอุปกรณ์ของบริษัทเพื่อลดความเสี่ยงจากภัยคุกคามทางสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต
2) กำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆอย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน
3) เจ้าหน้าที่หรือผู้ใช้งานต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ หรือส่งอุปกรณ์ดังกล่าวไปซ่อมบำรุงทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวมอบหมายให้เจ้าหน้าที่ในส่วนงานดูแลการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และควบคุมการขนย้ายอุปกรณ์คอมพิวเตอร์เพื่อป้องกันข้อมูลที่จัดเก็บในอุปกรณ์คอมพิวเตอร์รั่วไหลหรือถูกแก้ไข

7. การบริหารจัดการด้านสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

7.1 การกำหนดหน้าที่รับผิดชอบ และวิธีการปฏิบัติงาน

1) ให้ฝ่ายเทคโนโลยีสารสนเทศจัดทำคู่มือและ/ขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน เช่น ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติ และเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ
2) เมื่อฝ่ายเทคโนโลยีสารสนเทศมีการจัดการเปลี่ยนแปลงระบบเครือข่ายระบบคอมพิวเตอร์อุปกรณ์ ซอฟต์แวร์ทุกครั้งให้ฝ่ายเทคโนโลยีสารสนเทศบันทึกการเปลี่ยนแปลงทุกครั้ง โดยจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบรายละเอียดการเปลี่ยนแปลงให้ฝ่ายเทคโนโลยีสารสนเทศกำหนดหน้าที่รับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศและเครือข่ายให้เกิดความชัดเจน เพื่อหลีกเลี่ยงการใช้งานทรัพย์สินผิดวัตถุประสงค์ หรือโดยไม่มีสิทธิ์

7.2 การจัดการผู้ให้บริการภายนอก

ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการด้านเทคโนโลยีสารสนเทศของหน่วยงานภายนอกโดยต้องประกอบไปด้วยรายละเอียดดังนี้

1) การยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท
2) ขอบเขต รายละเอียด และระดับการให้บริการ
3) เอกสารต่างๆ เกี่ยวกับมาตรการควบคุมที่ใช้ทั้งด้านกายภาพและด้าน Logical
4) เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศได้ทั้ง 3 ด้าน คือ การรักษาความลับ การรักษาความถูกต้องเชื่อถือได้ และการรักษาความพร้อมที่จะให้บริการ
5) ข้อตกลงการเชื่อมโยงระบบเครือข่ายของหน่วยงานภายนอก (Guest)
6) ข้อมูลที่หน่วยงานภายนอกสามารถเข้าถึงได้และขั้นตอนและวิธีการร้องขอข้อมูลของบริษัทกรณีต้องการข้อมูลเพิ่มเติม
7) สัญญาในการไม่เปิดเผยข้อมูลของบริษัท
8) การยืมหรือการร้องขอให้อุปกรณ์ของบริษัท
9) ข้อกำหนดทางด้านกฎหมาย เช่น ความลับส่วนบุคคล และการป้องกันข้อมูล
10) ให้ฝ่ายเทคโนโลยีสารสนเทศทบทวนและตรวจสอบบริการจากผู้ให้บริการภายนอกตามข้อตกลงที่กำหนด
11) ให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบให้การบริหารจัดการเปลี่ยนแปลงในการให้บริการจากผู้ให้บริการภายนอก

7.3 การวางแผนและการยอมรับระบบสารสนเทศ

1) ฝ่ายเทคโนโลยีสารสนเทศต้องมีการติดตามสภาพการใช้งานและวิเคราะห์ขีดความสามารถทรัพยากรปัจจุบันอย่างสม่ำเสมอตามความเหมาะสมของทรัพยากรชนิดต่าง ๆโดยปฏิบัติตามเอกสารคู่มือจัดการขีดความสามารถ(Management Capabilities)
2) ฝ่ายเทคโนโลยีสารสนเทศต้องมีการวางแผนจัดการขีดความสามารถของระบบอย่างน้อยปีละ 1 ครั้ง โดยพิจารณาจากความต้องการใช้งานทรัพยากรสารสนเทศในอนาคต เช่น ความต้องการใน 1 ปีที่จะถึง เช่น CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่มีความจุมากขึ้น สภาพการใช้งานทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี
3) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่น ๆ ก่อนการใช้งาน รวมทั้งต้องทำการทดสอบก่อนที่จะตรวจรับระบบ

7.4 การควบคุม และป้องกันการใช้งานระบบ และอุปกรณ์เคลื่อนที่ผิดวัตถุประสงค์

1) เครื่องคอมพิวเตอร์ลูกข่าย และคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสรุ่นล่าสุดที่ได้รับการอนุมัติจากฝ่ายเทคโนโลยีสารสนเทศ และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง โดยปฏิบัติตามเอกสารคู่มือการจัดการควบคุมซอฟต์แวร์ไม่ประสงค์ดี
2) เครื่องคอมพิวเตอร์แม่ขายที่ให้บริการการป้องกันไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุดอยู่สม่ำเสมอ เครื่องให้บริการเครื่องตั้งโต๊ะเครื่องคอมพิวเตอร์พกพาทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส
3) ห้ามเจ้าหน้าที่ทำการ Download Software ฟรีแวร์โดยตรงจากอินเตอร์เน็ต โดยปราศจากการอนุมัติจากฝ่ายเทคโนโลยีสารสนเทศหลังจากการอนุมัติแล้วเจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัสก่อนการใช้งาน
4) ห้ามผู้ใช้งานสร้าง เก็บ หรือ เผยแพร่โปรแกรมมุ่งร้ายใด ๆ เช่น ไวรัส อีเมล์บอมบ์ เข้าสู่ระบบคอมพิวเตอร์ของบริษัท
5) ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส ไฟล์ที่เกี่ยวข้อง กับการทำงานเท่านั้นที่ได้รับอนุญาตให้สามารถรับ ส่ง ผ่านระบบเครือข่ายของบริษัทได้ ทั้งนี้ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้นนอกนี้ ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสของบริษัทก่อนเปิดใช้งาน

7.5 นโยบายการสำรองข้อมูล

1) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดความถี่ในการสำรองข้อมูลโดยขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูลหรือระบบโดยปฏิบัติตามเอกสารคู่มือการจัดทำการสำรองข้อมูลสารสนเทศ
2) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพสามรถใช้งานได้ตลอดเวลา
3) ฝ่ายเทคโนโลยีสารสนเทศต้องมีการควบคุมการเข้าถึงทางกายภาพของสถานที่ที่เก็บข้อมูลสำรองสื่อเก็บข้อมูลต้องต้องได้รับการป้องกัน
4) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูลและการเรียกคืนข้อมูลในแต่ละครั้ง ข้อมูลสำรองต้องได้รับการทดสอบเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้คืนกลับมาใช้งานได้อย่างสมบูรณ์
5) ฝ่ายเทคโนโลยีสารสนเทศต้องบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูลต้องได้รับการตรวจสอบเป็นประจำทุกปี

7.6 การรักษาความปลอดภัยระบบเครือข่าย

1) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดหน้าที่รับผิดชอบ รวมทั้ง วิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิดนั้นๆ
2) ฝ่ายเทคโนโลยีสารสนเทศต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่นๆ ที่เกี่ยวข้องทราบกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่ายที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของบริษัทด้วย
3) ระบบเครือข่ายทั้งหมดของบริษัทที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย
4) ฝ่ายเทคโนโลยีสารสนเทศต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของบริษัท และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องที่กำหนดไว้เท่านั้น
5) ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของบริษัทโดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ
6) ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัทโดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องได้รับการอนุมัติอย่างเหมาะสมก่อนทุกครั้ง (Guest)
7) ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย เช่น Router Switch Hub Wireless Access Point โดยไม่ได้รับอนุญาตโดยเด็ดขาด
8) ห้ามผู้ใช้งานที่อยู่ในระบบเครือข่ายของบริษัททำการเชื่อมต่อออกไปยังเครือข่ายภายนอกผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในบริษัทโดยเด็ดขาด

7.7 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย

1) ให้ฝ่ายเทคโนโลยีสารสนเทศ ต้องทำการบันทึกข้อมูลจราจรของผู้ใช้งาน (Traffic Logging) การใช้งานของผู้ใช้งานการปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงความปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ
2) ให้ฝ่ายเทคโนโลยีสารสนเทศตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่
3) ให้ฝ่ายเทคโนโลยีสารสนเทศบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator And Operator logs)
4) ให้หน่วยงานบันทึกเหตุการณ์ข้อผิดพลาด (Incident Logging) ต่างๆ ที่เกี่ยวกับการใช้งานระบบสารสนเทศวิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร

5) ให้ฝ่ายเทคโนโลยีสารสนเทศ ตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในหน่วยงานให้ตรงกับ (Clock Synchronization) โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ของบริษัทถูกบุกรุก

8. การควบคุมการเข้าถึง

8.1 การควบคุมการเข้าถึงระบบสารสนเทศ

1) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำนโยบายการใช้งานคอมพิวเตอร์และระบบเครือข่ายเพื่อควบคุมการเข้าถึงให้ทำได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
2) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศ ให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
3) ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้แผนกเทคโนโลยีสารสนเทศต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทและเฝ้าระวังการละเมิดความมั่นคงปลอดภัยที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

8.2. การจัดการการเข้าถึงระบบของผู้ใช้งาน

1) ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิ์แยกตามหน้าที่รับผิดชอบด้วย
2) ผู้ใช้งานต้องได้รับการพิสูจน์ตัวตนทุกครั้งเมื่อทำการlog-onเข้าสู่ระบบสารสนเทศฝ่ายเทคโนโลยีสารสนเทศต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัยอยู่เสมอ
3) ฝ่ายเทคโนโลยีสารสนเทศต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ (เช่นอย่างน้อง 1 ครั้ง ในรอบ 3 เดือน เป็นต้น)
4) ให้มีการเก็บบันทึกข้อมูลการเข้าถึงและการใช้งานระบบสารสนเทศแต่ละระบบ (Log File) เป็นระยะเวลาอย่างน้อย 90 วัน

8.3. การรับผิดชอบหน้าที่ของผู้ใช้งาน

1) ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิ์แยกตามหน้าที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในเอกสารกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศของบริษัทและการจัดการควบคุมการใช้รหัสผ่าน
2) เจ้าหน้าที่ต้องปฏิบัติตามการควบคุมการเข้าถึงระบบสารสนเทศของบริษัท การกำหนดการเปลี่ยนแปลง และการยกเลิกรหัสผ่านและการจัดการควบคุมการใช้รหัสผ่านกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

- ควรได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาและผู้ดูแลระบบงานนั้นๆ
- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานควรเปลี่ยนรหัสผ่านทุก 3 เดือนเป็นต้น
- ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแลรักษา User Name และรหัสผ่านของตนเองรวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้ให้มีความมั่นคงปลอดภัยอย่างสม่ำเสมอ
- ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่กระทำผ่าน User Name และรหัสผ่านของตนทั้งหมด หากผู้ใช้งานสงสัยว่า User Name หรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อฝ่ายเทคโนโลยีสารสนเทศและทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที
- การ Reset รหัสผ่าน ต้องผ่านกระบวนการมาตรฐานของบริษัทเท่านั้น เพื่อให้มั่นใจว่าตรงกับ User ที่ต้องการ reset รหัสผ่านจริง อีกทั้ง เจ้าหน้าที่ที่ดูแลระบบมีสิทธิ์ในการขอข้อมูลและพิสูจน์ตัวตนของผู้ใช้งานตามความเหมาะสม

8.4. การควบคุมการเข้าถึงระบบเครือข่าย

1) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำนโยบายการใช้งานคอมพิวเตอร์และระบบเครือข่ายโดยเฉพาะเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต
2) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดแบ่งระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งานแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น (Internal zone / External zone / DMZ Guest-Zone)เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ
3) หน่วยงานต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายใน และเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
4) ฝ่ายเทคโนโลยีสารสนเทศต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

8.5. การควบคุมการใช้งานระบบปฏิบัติการ

1) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดกระบวนการในการเข้าถึงให้มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการจะปฏิเสธการใช้งานหากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง เป็นต้น
2) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานระบบรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบได้
3) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีระบบควบคุมการดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

8.6. การควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

1) ต้องมีการควบคุมการใช้งานระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่นเขียน อ่าน ลบ ได้ กำหนดกลุ่มของผู้ใช้งานที่สามารถใช้งานได้ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน
2) บัญชีผู้ใช้งานที่มีสิทธิ์เข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น root หรือ administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงาน
3) บุคคลภายนอกต้องแสดงความยินยอมปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทอย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท

8.7. การควบคุมการเข้าถึงข้อมูลสารสนเทศ

สิทธิ์การเข้าถึงข้อมูลด้านสารสนเทศต้องได้รับการควบคุม และได้รับการพิจารณาอนุมัติเท่าที่จำเป็นเท่านั้น เพื่อให้ข้อมูลสารสนเทศได้รับการรักษาความมั่นคงปลอดภัยอย่างมีประสิทธิภาพรวมทั้งเป็นการแบ่งแยกสิทธิ์และหน้าที่ของผู้ใช้งาน

8.8. คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถานที่

ต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์พกพา (Notebook Laptop) และอุปกรณ์สื่อสารอื่นๆ เช่นเมื่อปฏิบัติติงานอยู่นอกสถานที่

- ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง
- ต้องใส่รหัสผ่านป้องกันข้อมูลที่สำคัญ

9. การจัดหา การพัฒนา และการบำรุงรักษาระบบเทคโนโลยีสารสนเทศ

9.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

1) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้ หรือซื้อมาใช้งาน
2) หน่วยงานดูแลระบบเทคโนโลยีสารสนเทศจะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้
    - มาตรการปฏิบัติติก่อนที่จะเกิดความเสียหาย เช่นการสำรองข้อมูล ระบบเครือข่ายสำรอง
    - มาตรการปฏิบัติติหลังจากเกิดความเสียหาย เช่นแผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล

9.2 **ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ**

1) ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ลงในเครื่องที่ใช้งานหรือเครื่องที่ให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการตรวจสอบการใช้งานมาเป็นอย่างดีว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่แล้ว
2) ข้อมูลจริงที่จะนำไปทดสอบระบบจะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้นก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที
3) ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริงหรือให้บริการ

9.3 **ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ**

ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่ เช่น

- คำขอแก้ไขต้องมาจากผู้มีสิทธิ์
- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
- เมื่อแก้ไขเสร็จต้องมีการตรวจรับจากผู้ขอ

เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่างๆ ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ในการทำสัญญาว่าจ้างพัฒนาระบบของบริษัทต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

10.1 กำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัทการบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ

10.2 กำหนดให้มีกระบวนการทดสอบกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัทอย่างสม่ำเสมอ

11. การปฏิบัติตามข้อกำหนด

11.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย

1) แผนกเทคโนโลยีสารสนเทศต้องมีการศึกษาและกำหนดนโยบาย กฎระเบียบข้อบังคับกฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทเจ้าหน้าที่ทุกคนต้องรับทราบ ทำความเข้าใจและปฏิบัติตามนโยบาย กฎระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด โดยต้องมีรายการอย่างน้อยดังต่อไปนี้
   - นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
   - พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
   - พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
   - พ.ร.บ. กำหนดหลักเกณฑ์และวิธีการในการทางธุรการรมทางอิเล็กทรอนิกส์ภาครัฐ
   - พ.ร.บ. ลิขสิทธิ์

2) ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัทถือเป็นทรัพย์สินของบริษัท ทั้งนี้บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้ เป็นหลักฐานในการสืบสวนความผิดต่างๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า
3) เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทบริษัทขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ระบบคอมพิวเตอร์และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่างๆกำหนดไว้ตลอดจนการเข้าถึงทบทวน และตรวจสอบอีเมล์ของผู้ใช้งานโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้าอย่างไรก็ตามการตรวจสอบดังกล่าวจะดำเนินการต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใด ๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งศาล ตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น
4) ห้ามเจ้าหน้าที่ทุกคนใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัท กระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม
5) ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งาน ซอฟต์แวร์อย่างเคร่งครัด รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่
6) ห้ามผู้ใช้งานทำการใช้งานทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือ เอกสารใดๆ ที่เป็นการละเมิด ลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศขอบบริษัทโดยเด็ดขาด

11.2. **พิจารณาการตรวจสอบระบบเทคโนโลยีสารสนเทศ**

1) ฝ่ายเทคโนโลยีสารสนเทศต้องวางแผนการตรวจสอบระบบทั้งหมด โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบและกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด
2) หน่วยงานเทคโนโลยีสารสนเทศต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบไม่ให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด หรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น