นโยบายรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

วันที่มีผลบังคับใช้ 15 **สิงหาคม** 2561

นโยบายนี้ได้กำหนดเป็นแนวทางเพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมหรือลดโอกาสของความเสี่ยงด้านต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดนโยบาย และการปฏิบัติตามนโยบาย เพื่อการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ ได้อย่างมีประสิทธิภาพ และมีมาตรฐานในระดับเดียวกัน

หมวด 1 ความหมายและคำจำกัดความ

มีวัตถุประสงค์ในการจัดทำเพื่อให้ความหมายในคำจำกัดความในส่วนที่เกี่ยวข้องกับนโยบายเพื่อให้ผู้เกี่ยวข้องได้ทราบและมีความเข้าใจในเนื้อหาตรงกัน

1.1 **สินทรัพย์คอมพิวเตอร์** (Computer Asset) หมายถึง สินทรัพย์ทุกอย่างที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เป็นต้น

1.2 **คอมพิวเตอร์แม่ข่าย** (Server) หมายถึง เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟต์แวร์สำหรับให้บริการแก่เครื่องคอมพิวเตอร์อื่น ๆ หรือ ควบคุมการทำงานในเครือข่าย

1.3 **การเข้าถึงเครือข่ายระยะไกล** (Remote to Network) หมายถึง การที่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์หรือเครือข่ายอื่นผ่านอุปกรณ์สื่อสารหรือสื่อสัญญาณอื่น ๆ อาทิ Modem, VPN IP Router

1.4 **การควบคุมการเข้าถึง** (Access Control) หมายถึง การควบคุมการเข้าถึงหรือใช้งานสินทรัพย์คอมพิวเตอร์ให้เป็นไปตามสิทธิที่กำหนดไว้เท่านั้น

1.5 **เครื่องคอมคอมพิวเตอร์** (Computer) หมายถึง อุปกรณ์ที่ใช้ในการประมวลผลข้อมูลที่ทำงานด้วยระบบอิเล็กทรอนิกส์ โดยทำงานตามคำสั่งผ่านทางซอฟต์แวร์ที่ให้ได้ผลตามที่ต้องการ อาทิ คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์, คอมพิวเตอร์ส่วนบุคคล (Desktop Computer) และคอมพิวเตอร์แบบพกพาได้ (Notebook/Laptop)

1.6 **อุปกรณ์คอมพิวเตอร์** (Computer Accessories) หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ และให้รวมถึงเครื่องคอมพิวเตอร์

1.7 **สื่อสัญญาณ** (Signal /Network link/Lan) หมายถึง สื่อกลางใด ๆ ที่ใช้เชื่อมต่อระหว่างอุปกรณ์คอมพิวเตอร์ อาทิ สายทองแดง สายใยแก้วนำแสง (fiber optic) เครือข่ายไร้สาย (Wi-fi wireless)

1.8 **ฮาร์ดแวร์** (Hardware) หมายถึง อุปกรณ์คอมพิวเตอร์ หรือ ชิ้นส่วนในคอมพิวเตอร์

1.9 **ซอฟต์แวร์** (Software) หมายถึง โปรแกรมที่ใช้เป็นเครื่องมือในการทำงานเช่น Microsoft Office, Adobe Acrobat

1.10 **ซอฟต์แวร์ประยุกต์** (Specialized programs) หมายถึง ซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้กับงานเฉพาะด้านตามความต้องการ เช่น โปรแกรมสำหรับคำนวณทางบัญชี (Winspeed), โปรแกรมคำนวณน้ำหนักตาชั่ง

1.11 **แอพพลิเคชั่น** (Application) หมายถึง โปรแกรมที่ใช้ช่วยเหลือการทำงาน ดาวน์โหลดฟรี (การจะใช้แอพอื่นๆ เพิ่มเติมต้องได้รับ อนุญาตจากทางเจ้าหน้าที่ฝ่ายงานระบบ IT ก่อน) เช่น Line PC

1.12 **ระบบเทคโนโลยีสารสนเทศ** (MIS) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่น อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ระบบงาน และสารสนเทศ

1.13 **สารสนเทศ** (Information system) หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผนและอื่น ๆ

1.14 **ระบบปฏิบัติการ** (Operating System/OS) หมายถึง ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุมการทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) และอุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์)

1.15 **ระบบป้องกันการบุกรุก** (Firewall) หมายถึง ระบบรักษาความปลอดภัยที่ประกอบด้วยกลุ่มอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ ซึ่งทำหน้าที่ป้องกันผู้ไม่ได้รับอนุญาตจากเครือข่ายภายนอกเข้าใช้ระบบ และจำกัดการใช้ของผู้ใช้ภายในให้เป็นไปตามนโยบายที่บริษัทกำหนด

1.16 **ข้อมูล** (Information/Data) หมายถึง ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลได้ด้วยวิธีการทางอิเล็กทรอนิกส์บนอุปกรณ์คอมพิวเตอร์ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

1.17 **ไฟล์** (File) หมายถึง ข้อมูลที่ถูกรวบรวมลงสื่อบันทึกและระบุเป็นหนึ่งหน่วยโดยมีชื่อเฉพาะ เช่น ซอฟต์แวร์ใช้งาน และไฟล์เอกสารต่าง ๆ ที่สร้างขึ้นและใส่ชื่อให้แก่ไฟล์นั้นแล้วเก็บบันทึกลงสื่อบันทึก เป็นต้น

1.18 **ผู้ใช้งาน** (User) หมายถึง เจ้าหน้าที่หรือบุคคลภายนอก ที่มีสิทธิใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

1.19 **ผู้บริหารเครือข่าย** (Network Administrator) หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาเครือข่าย

1.20 **ผู้บริหารคอมพิวเตอร์แม่ข่าย** (Host/Server Administrator) หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาคอมพิวเตอร์แม่ข่าย

1.21 **ผู้บริหารระบบป้องกันการบุกรุก** (Firewall Administrator) หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาป้องกันการบุกรุก

1.22 **บัญชีผู้ใช้งาน** (User Account) หมายถึง บัญชีที่ผู้ใช้งานในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบเทคโนโลยีสารสนเทศ

1.23 **บัญชีผู้บริหารคอมพิวเตอร์แม่ข่าย** (Administrator Account) หมายถึง บัญชีที่ผู้บริหารคอมพิวเตอร์แม่ข่ายใช้ในการบริหารระบบคอมพิวเตอร์แม่ข่าย

1.24 **เอกสารโครงแบบ** (Configuration Document) หมายถึง เอกสารที่แสดงรายละเอียดการกำหนดค่าต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศใช้งานได้ตามความต้องการ

1.25 **ความเสี่ยง** หมายถึง โอกาสของสินทรัพย์คอมพิวเตอร์ในการถูกละเมิดการรักษาความปลอดภัยของระบบ

1.26 **เจ้าหน้าที่** (Staff) หมายถึง พนักงานในบริษัท

1.27 **ส่วนงาน** (Section) หมายถึง แผนกหรือฝ่ายงานตามโครงสร้างของบริษัท

1.28 **ไวรัส** (Virus) หมายถึง ซอฟต์แวร์ที่มีการตั้งใจใส่เข้าไปในระบบโดยไม่ได้รับอนุญาต หรือ เพื่อให้ทำงานตามความประสงค์ของผู้ประสงค์ร้าย ซึ่งมีผลให้คอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศ หรือชุดคำสั่งอื่นได้รับความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

1.29 **สแปม** (Spam) , **มัลแวร์** (Malware) หมายถึง โปรแกรมที่ผู้พัฒนาขึ้นซึ่งปัจจุบันมีอยู่นับพันโปรแกรมโดยพัฒนาโดยวัตถุประสงค์หลากหลาย เช่น แฮคเกอร์ หรือ สามารถจำและบันทึกว่าแป้นคีย์บอร์ดแป้นไหนถูกกดบ้าง เพื่อล้วงความลับในคอมพิวเตอร์ของเครื่องที่ติด เช่น ชื่อผู้ใช้ รหัสผ่าน และอาจจะเป็นข้อมูลส่วนตัวเกี่ยวกับการ Login เข้าระบบ ที่ถูกพิมพ์ผ่านคีย์บอร์ดโดยผู้ใช้งาน โดยส่วนใหญ่ แฮคเกอร์จะส่งโปรแกรม เข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนำไปใช้ในการเจาะระบบ หรือเพื่อโจมตีคอมพิวเตอร์ เซิฟเวอร์ ระบบเครือข่าย ซึ่งเป็นที่รู้จักกันในชื่อการโจมตีเพื่อ "ปฏิเสธการให้บริการ" (Denied of Services) โปรแกรม เป็นต้น

1.30 **หน่วยงานภายนอก** (Outsource) หมายถึง องค์กรซึ่งบริษัท อนุญาตให้มีสิทธิในการเข้าถึงหรือใช้ข้อมูลหรือใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท โดยจะได้รับสิทธิ ตามประเภทการใช้งานและต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทโดยไม่ได้รับอนุญาต

หมวดที่ 2 นโยบายด้านความมั่นคงปลอดภัย (Security Policy)

มีวัตถุประสงค์ในการกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับบริษัท เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และเป็นไปตามมาตรฐานการตรวจสอบจากหน่วยงานภายนอกในด้าน IT General Audit

2.1 เมื่อ นโยบายฉบับนี้มีผลบังคับใช้ ให้หน่วยงานที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ เป็นผู้ทำหน้าที่ในการออกระเบียบปฏิบัติ ข้อกำหนด ข้อบังคับต่าง ๆ ที่จำเป็นเพื่อให้การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ของบริษัทโดยความเห็นชอบของผู้บริหารระดับสูง รวมถึงงานฝ่ายบริหารให้การสนับสนุนในเรื่องนโยบาย งบประมาณ ทรัพยากรและอื่น ๆ ที่จำเป็นเพื่อให้การรักษาความมั่นคงปลอดภัยของ ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์มีการพัฒนาปรับปรุงอย่างต่อเนื่อง

2.2 ต้องจัดให้มีการเผยแพร่นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารเสนเทศและเครือข่ายคอมพิวเตอร์ให้กับเจ้าหน้าที่ ผู้ให้บริการภายนอก และผู้ที่เกี่ยวข้องรับทราบและนำไปปฏิบัติ

2.3 ต้องดำเนินการทบทวน และประเมินนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์อย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญซึ่งมีผลต่อการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัท

หมวดที่ 3 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)

3.1 โครงสร้างทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายในองค์กร (Internal Organization)

มีวัตถุประสงค์ในการจัดทำเพื่อบริหารและกำหนดหน่วยงานในการดูแลระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัท

3.1.1 ผู้บริหารระดับสูง เป็นผู้กำหนดให้มีตัวแทนหรือคณะทำงานจากหน่วยงานต่าง ๆ ภายในบริษัท เพื่อประสานงานหรือร่วมมือในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัท โดยที่ตัวแทนหรือคณะทำงานเหล่านั้น จะต้องมีการกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานทางด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่าย คอมพิวเตอร์ขององค์กรอย่างชัดเจน

3.1.2 ตัวแทนหรือคณะทำงานซึ่งถูกแต่งตั้งโดยผู้บริหารระดับสูง เป็นผู้รับผิดชอบในการบริหารจัดการและควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่าย คอมพิวเตอร์ขององค์กร ตลอดจนทบทวนนโยบายระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยมีการจัดทำขั้นตอนและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ต่าง ๆ และเอกสารที่เกี่ยวข้องในการจัดทำการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

3.1.3 เจ้าหน้าที่ของบริษัทต้องไม่เปิดเผยความลับของบริษัท เว้นแต่จะได้รับอนุญาตให้เปิดเผยจากบริษัท

3.1.4 ต้องกำหนดให้มีการตรวจสอบบริหารจัดการการดำเนินงานและการปฏิบัติที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์โดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อบริษัท

3.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)

มีวัตถุประสงค์ในการจัดทำเพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัทที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้า หรือหน่วยงานภายนอก

3.2.1 ต้องมีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับ หรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

3.2.2 ต้องระบุและบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัท เมื่อมีความจำเป็นต้องให้บุคคลภายนอก หรือผู้มาติดต่อ หน่วยงานตรวจสอบภายนอกเข้าถึงสารสนเทศหรือทรัพย์สิน สารสนเทศของบริษัทก่อนที่จะอนุญาตให้สามารถเข้าถึงได้ต้องระบุ และจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างบริษัทและหน่วยงานภายนอก เมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศของบริษัทก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

หมวดที่ 4 การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)

มีวัตถุประสงค์ในการจัดทำเพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัทที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้า หรือหน่วยงานภายนอก

4.1 ความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

4.1.1 ต้องมีการจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อบริษัทให้ถูกต้องอยู่สม่ำเสมอ รวมทั้งมีการระบุความเป็นเจ้าของในทรัพย์สินต่าง ๆ

4.1.2 ต้องจัดทำกฎระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับการประมวลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น เช่น การขาดความระมัดระวัง การขาดการดูแลและเอาใจใส่

4.1.3 ต้องมีการเก็บรักษาทรัพย์สินที่มีความสำคัญต่อบริษัทอย่างเป็นระเบียบในสถานที่ที่ปลอดภัยและเหมาะสม

4.1.4 การอนุญาตให้ใช้งานทรัพย์สินด้านอุปกรณ์คอมพิวเตอร์ (Computer) มีดังนี้

- ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่บริษัทเป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการปฏิบัติงานตามภารกิจของบริษัท การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่

- เจ้าหน้าที่ ตลอดจนบุคคล และ/หรือนิติบุคคลที่ได้รับว่าจ้างโดยบริษัท จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายความรวมถึงข้อมูล และระบบสารสนเทศของบริษัท

- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ของบริษัทอย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน

- เครื่องคอมพิวเตอร์ลูกข่าย (Client) เครื่องคอมพิวเตอร์พกพา (Laptop/Notebook) และเครื่องคอมพิวเตอร์แม่ข่าย (Server) ทั้งหมดของบริษัทต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการ

- กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบอุปกรณ์คอมพิวเตอร์ของบริษัทที่ได้รับมอบหมาย

- ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายของบริษัทรวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท ก่อนได้รับอนุญาตจากหน่วยงานเทคโนโลยีสารสนเทศ

- เครื่องคอมพิวเตอร์พกพา (Laptop/Notebook) ที่บริษัทจัดสำหรับให้ใช้งาน ที่มีการเก็บข้อมูลลับไว้ต้องได้รับการปกป้อง เทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัท เช่น ต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ

- อุปกรณ์คอมพิวเตอร์ของบริษัท ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และเจ้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด

4.1.5 การอนุญาตให้ใช้สินทรัพย์ด้านซอฟต์แวร์ (Software) มีดังนี้

- ห้ามเจ้าหน้าที่ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัท

- ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัท ทั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมาต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของบริษัท

- ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของบริษัทมีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้

- รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการอนุมัติโดยผู้บริหารระดับสูง เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัทเท่านั้น

4.1.6 การอนุญาตให้ใช้งานอินเทอร์เน็ต (Internet) มีดังนี้

- บริษัทจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการค้นหาข้อมูลความรู้และการติดต่อสื่อสารกับบุคคลภายนอกเพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของบริษัท

- ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัทและบุคคลผู้ที่เกี่ยวข้องกับบริษัทเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

- การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านช่องทาง (Gateway) ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเท่านั้น

- ห้ามใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม (Spam) เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมประสงค์ร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

- ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย

- บริษัทไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ด หรือบล็อก) ของเจ้าหน้าที่ ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

4.1.7 การอนุญาตให้ใช้อีเมล์ (Email) มีดังนี้

- ผู้ใช้งานทั้งหมดของบริษัท ต้องมี E-mail Account เป็นของตนเอง

- เมื่อมี user ใหม่หรือคนออกจะต้องมีการยื่นเอกสาร (Doc no. IT2019-001) ที่เจ้าหน้าที่ฝ่ายไอทีเพื่อการขอใช้ email หรือการยกเลิกการใช้

- E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่านเพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมล์ไปใช้ในทางที่ผิด

- Email Account ทั้งหมด และอีเมล์ทุกฉบับ (รวมถึงอีเมลล์ส่วนตัว) ที่ถูกสร้างและเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท ถือเป็นสินทรัพย์ของบริษัท

- ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือติดต่อสื่อสารกับระบบอีเมล์ของบริษัท

- พื้นที่เก็บอีเมล์บนระบบแม่ข่ายส่วนกลาง (Mail Box Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้เมื่อปริมาณของอีเมล์มากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับ-ส่ง อีเมล์ได้ตามปกติ ผู้ใช้งานควรลบอีเมลล์ที่ไม่สำคัญออก และบริหารพื้นที่จัดเก็บ อย่างมีประสิทธิภาพ

- ขนาดของอีเมล์ไฟล์แนบได้รับการจำกัดไว้ โดยหากอีเมลล์ไฟล์แนบมีขนาดใหญ่เกิดกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายตีกลับแจ้งว่าไม่สามารถส่งอีเมล์ดังกล่าวได้

- ผู้ใช้งานต้องลบ อีเมล์ไม่จำเป็นออกจาก Mailbox ของตนเองอยู่เสมอ เพื่อเป็นการรักษาพื้นที่จัดเก็บอีเมล์ให้เป็นไปตามขนาดที่บริษัทกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงานและอีเมล์ตามที่กฎหมายกำหนดไว้เท่านั้น

- ห้ามใช้ E-mail Account ของบริษัทเพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย เช่น การโฆษณาสิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมินลิขสิทธิ์

- ห้ามใช้ E-mail Account ของบริษัทในการประกาศข้อมูลใด ๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับบริษัท

- ซอฟต์แวร์สำหรับใช้งานอีเมล์ต้องได้รับการตั้งค่าให้อีเมลล์ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงาน ชื่อบริษัทและเบอร์โทรศัพท์ติดต่อ

- ไฟล์เอกสารที่แนบมาพร้อมกับอีเมล์ จะต้องอยู่ในรูปแบบมาตรฐานซึ่งผู้รับสามารถเปิดอ่านได้ด้วยซอฟต์แวร์พื้นฐานบนทุกระบบปฏิบัติการ เช่น PDF, DOC, TXT, XLS, JPG, GIF, PPT เป็นต้น

- ห้ามผู้ใช้งานทำสำเนาข้อความหรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล

- ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนของบริษัท

- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ E-Mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม

- ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่าง อีเมล์ขยะ (Junk mail) หรือโฆษณาสินค้าต่าง ๆ (Spam mail)

- ห้ามผู้ใช้สร้างหรือมีส่วนร่วมใด ๆ กับการส่ง อีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด

- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

- ห้ามผู้ใช้งานส่งอีเมล์ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อบริษัท

- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส หรือสแปมเมลล์

- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับสู่สภาพปกติ

4.1.8 การอนุญาตให้ใช้โทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร มีดังนี้

- ถ้าหากผู้ใช้งานได้รับข้อมูลจากการส่งโทรสารที่ผิดพลาด ตัวอย่างเช่น ส่งโทรสารผิดหมายเลขผิดส่วนงาน เป็นต้น ผู้ใช้ต้องแจ้งให้ผู้ส่งโทรสารนั้นรับทราบ และทำลายเอกสารข้อมูลนั้น

- ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น

- ห้ามสนทนาเกี่ยวกับข้อมูลลับผ่านลำโพงของเครื่องโทรศัพท์ (Speakerphones) หรือผ่านสื่ออิเล็กทรอนิกส์ใด ๆ เช่น โทรศัพท์เปิด speaker phone ในระหว่างการประชุมทางไกล เว้นแต่ผู้เข้าร่วมประชุมทุกหน่วยงานได้รับการพิสูจน์ตัวตนแล้วว่าเป็นผู้ที่เกี่ยวข้อง และมีสิทธิ์รับทราบข้อมูล

- ผู้ที่เกี่ยวข้องตรวจสอบจนมั่นใจแล้วว่า ไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณใกล้เคียงที่อาจได้ยินข้อมูลลับที่สนทนาอยู่

- การประชุมทางไกลถูกจัดขึ้นในบริเวณที่มีความมั่นคงปลอดภัย เช่น ห้องประชุมที่มีผนังและประตูที่เหมาะสม สามารถป้องกันเสียงลอดออกมาได้

- ผู้ใช้งานต้องขออนุญาตจากเจ้าของข้อมูลก่อนทำการถ่ายเอกสารหรือแสกนเอกสารที่มีข้อมูลลับ

4.2 การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Information Classification)

มีวัตถุประสงค์เพื่อบริหารจัดการสารสนเทศของบริษัทเพื่อให้ได้รับการปกป้องในระดับที่เหมาะสม

4.2.1 ต้องทำการจัดหมวดหมู่ การกำหนดลำดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อบริหารจัดการสารสนเทศให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม

4.2.2 เอกสารหรือสิ่งตีพิมพ์ ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความสำคัญ เช่นเอกสารเป็นความที่เป็นเอกสารลับ ให้ถือว่ามีชั้นความสำคัญเช่นเดียวกับเอกสารลับที่เป็นต้นฉบับที่เป็นข้อมูลดิจิตอล หรือสารสนเทศดิจิตอลนั้น

4.2.3 ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูล และอุปกรณ์สินทรัพย์ สารสนเทศ (Asset information Tag) ที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศ

4.2.4 ข้อมูลที่อยู่ในรูปของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย ข้อมูลที่เป็นเอกสารลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น

4.2.5 ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม

4.2.6 ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสาร โดยทันที

4.2.7 เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงให้มีการเปิดเผยข้อมูล

4.2.8 เจ้าหน้าที่ต้องไม่พูดคุยหรือใช้งานข้อมูลลับของบริษัทในพื้นที่สาธารณะ เช่น ลิฟต์ ร้านอาหาร

4.2.9 สื่อข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ เช่น Thump-Drive, CD-ROM, External Hard disk drive ที่มีข้อมูลลับของบริษัทบันทึกอยู่ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

4.2.10 ข้อมูลสำคัญที่เกี่ยวข้องกับการดำเนินงานของบริษัททั้งหมด ทั้งที่มีการเก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลโดยผู้ใช้งานต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาใด ๆ เกิดขึ้น เช่น การติดไวรัส ฮาร์ดดิสก์เสีย

หมวด 5 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

5.1 การสร้างความมั่นคงปลอดภัยให้เจ้าหน้าที่ที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้แก่พนักงานเพื่อให้สามารถป้องกันภัยต่าง ๆ ได้

มีวัตถุประสงค์เพื่อบริหารจัดการเพื่อให้เจ้าหน้าที่ได้ตระหนักถึงภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้กับพนักงานเพื่อให้สามารถป้องกันภัยดังกล่าวได้

5.1.1 เจ้าหน้าที่หรือผู้ใช้งานมีหน้าที่ศึกษาทำความเข้าใจวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัยของระบบสารสนเทศที่บริษัทกำหนด เพื่อนำไปปฏิบัติในการรักษาความปลอดภัย สินทรัพย์คอมพิวเตอร์ในส่วนที่ตนใช้งานหรือดูแลรับผิดชอบ

5.1.2 ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติของบริษัท แต่หากเป็นการละเมิดกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุในแต่ละข้อกฎหมายนั้น ๆ

5.2 การยกเลิกสิทธิ์กับเจ้าหน้าที่ที่มีการยกเลิกการจ้างงาน

มีวัตถุประสงค์เพื่อบริหารจัดการเพื่อให้มีการยกเลิกสิทธิ์กับเจ้าหน้าที่ที่ถูกยกเลิกการจ้างงานหรือหมดสัญญาฯ เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ

5.2.1 เพื่อให้การบริหารจัดการ Login หรือ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด หน่วยงานด้านทรัพยากรบุคคลต้องแจ้งให้หน่วยงานเทคโนโลยีสารสนเทศทราบทันทีเมื่อมีเหตุดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร เจ้าหน้าที่ และลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

เจ้าหน้าที่และลูกจ้างซึ่งพ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวเจ้าหน้าที่ (ถ้ามี) บัตรผ่านเข้า-ออก (ถ้ามี) , คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน

หลังจากมีการยกเลิกหรือเปลี่ยนแปลงตำแหน่งเป็นเจ้าหน้าที่และลูกจ้างแล้ว จะต้องแจ้ง ยกเลิกการเข้าถึงข้อมูลต่าง ๆ ของหน่วยงานและจะแจ้งต่อเจ้าหน้าที่ และลูกจ้างอื่น ๆ , ลูกค้า , บริษัทคู่ค้า, Third Party/ Outsource ที่เกี่ยวข้องให้รับทราบตามเหมาะสม

ทั้งนี้หากการเปลี่ยนแปลงข้างต้นมีผลกับการเปลี่ยนแปลง user ผู้ใช้งาน หรือสิทธิ์การใช้งานในระบบโปรแกรมต่าง ๆ ของบริษัทฯ ต้องยื่นเรื่องตามเอกสาร (Doc no. IT2019-001) เพื่อแจ้งถึงการเปลี่ยนแปลงที่เกิดขึ้นให้เจ้าหน้าที่ฝ่ายไอทีเพื่อทราบและดำเนินการเปลี่ยนแปลงสิทธิ์การใช้งาน หรือ ยกเลิกการใช้งานของผู้ใช้ในระบบงานต่างๆ (user ID) ที่เกี่ยวข้อง

หมวด 6 ความมั่นคงปลอดภัยด้านสถานที่และอุปกรณ์ (Environment and Equipment Security)

6.1 สถานที่จัดเก็บอุปกรณ์คอมพิวเตอร์ และข้อมูลสารสนเทศต้องมีสภาพแวดล้อมที่ปลอดภัยและเหมาะสม

มีวัตถุประสงค์เพื่อบริหารจัดการด้านสถานที่ในการจัดเก็บให้มีความมั่นคงปลอดภัยและเหมาะสม

6.1.1 ต้องจัดสถานที่ หรือพื้นที่สำหรับจัดเก็บอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้อง รวมถึงสารสนเทศสำคัญให้อยู่ในบริเวณที่ตั้งที่มีความมั่นคงปลอดภัยและเหมาะสม และมีผู้รับผิดชอบดูแลด้านสภาพแวดล้อมให้มีความปลอดภัย และควรมีการจัดทำป้ายชี้บ่งสถานที่ที่ไม่อนุญาตให้บุคคลภายนอกเข้าในพื้นที่ที่มีการจัดเก็บอุปกรณ์สำคัญ รวมถึงต้องมีป้ายชี้บ่งถึงเจ้าหน้าที่ที่มีหน้าที่ความรับผิดชอบในการดูแล บริเวณที่จัดเก็บอุปกรณ์ทุกจุดอย่างชัดเจน

6.1.2 ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงานในห้องประชุม หรือในตู้ที่ไม่ได้ล๊อคกุญแจ

6.1.3 เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตน เว้นแต่บุคคลนั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการตามนโยบายคำสั่งอย่างถูกต้องจากหน่วยงานที่รับผิดชอบในการดูแลระบบสารสนเทศของบริษัท

6.1.4 เพื่อประโยชน์ในการรักษาความปลอดภัย ด้านสถานที่ที่ติดตั้งและเก็บรักษาสินทรัพย์คอมพิวเตอร์ ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่าง ๆ เช่น อัคคีภัย ภัยธรรมชาติ หรือภัยจากการโจรกรรม หรืออื่น ๆ ตามโอกาสที่อาจเกิดขึ้น

6.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

มีวัตถุประสงค์เพื่อบริหารจัดการเพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยคุกคามที่อาจเกิดขึ้น

6.2.1 เจ้าหน้าที่หรือผู้ใช้งานต้องจัดวางและป้องกันอุปกรณ์ของบริษัทเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

6.2.2 กำหนดให้มีการจัดเตรียมความพร้อมของอุปกรณ์ป้องกัน และมีการดูแลบำรุงรักษา เพื่อเตรียมความพร้อมของอุปกรณ์ป้องกันให้มีความพร้อมสม่ำเสมอ เช่น อุปกรณ์สำรองไฟ (UPS) โดยเจ้าหน้าที่และผู้ใช้เป็นผู้รับผิดชอบในการตรวจตราเพื่อให้ทดสอบอุปกรณ์ป้องกันเพื่อให้มีความพร้อมในการป้องกัน กรณีเกิดปัญหากระแสไฟฟ้าบกพร่อง อุปกรณ์ป้องกันต้องมีสภาพพร้อมใช้เสมอ หากอุปกรณ์ป้องกันชำรุดบกพร่องต้องแจ้งหน่วยงานที่เกี่ยวข้อง ที่ดูแลระบบให้จัดหาอุปกรณ์ป้องกันสำรองเพื่อเปลี่ยน หรือดำเนินการจัดหาอุปกรณ์ทดแทนหากพบอุปกรณ์ป้องกันชำรุดบกพร่อง

6.2.3 กำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ โดยเจ้าหน้าที่และผู้ใช้ รวมถึงผู้รับผิดชอบในดูแลในพื้นที่มีหน้าที่จัดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

6.2.4 เจ้าหน้าที่หรือผู้ใช้งานต้องทำการประสานงานกับหน่วยงานเทคโนโลยีสารสนเทศในการจัดเตรียมแผนรองรับหากอุปกรณ์คอมพิวเตอร์ได้รับความเสียหายและทดสอบแผนรองรับตามระยะเวลาอันสมควร

6.2.5 เจ้าหน้าที่หรือผู้ใช้งานต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะมีการ บริจาค ทิ้ง หรือส่งอุปกรณ์ดังกล่าวไปซ่อมบำรุงในหน่วยงานภายนอก ทั้งนี้เพื่อป้องกันข้อมูลดังกล่าว

6.2.6 มอบหมายให้เจ้าหน้าที่ในส่วนงานแต่ละหน่วยงานเป็นผู้ดูแลการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และควบคุมการขนย้ายอุปกรณ์คอมพิวเตอร์ เพื่อป้องกันข้อมูลที่จัดเก็บในอุปกรณ์คอมพิวเตอร์รั่วไหลหรือถูกแก้ไข

หมวด 7 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communication and Operation Management)

7.1 การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน

มีวัตถุประสงค์เพื่อให้ใช้ปฏิบัติงานและบริหารจัดการโครงสร้างพื้นฐานด้านสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

7.1.1 ให้หน่วยงานเทคโนโลยีสารสนเทศจัดทำคู่มือและ/หรือขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติ ชี้แจง รวมถึงแจกจ่ายหรือส่งมอบหมายให้เจ้าหน้าที่หรือหน่วยงานในพื้นที่จัดเก็บเป็นผู้ดูแลและรับผิดชอบดำเนินการตามขั้นตอนที่ได้ระบุ

7.1.2 ให้หน่วยงานเทคโนโลยีสารสนเทศมีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ซอฟต์แวร์ ทุกครั้ง ให้มีการสื่อสารบันทึกการเปลี่ยนแปลงทุกครั้ง โดยจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องรับทราบรายละเอียดถึงการเปลี่ยนแปลง ให้เกิดความชัดเจน เพื่อหลีกเลี่ยงการใช้งานสินทรัพย์ผิดวัตถุประสงค์ หรือใช้โดยไม่มีสิทธิ์

7.2 กรณีมีการจัดจ้างผู้ให้บริการภายนอก ให้มีการจัดการผู้ให้บริการภายนอก

มีวัตถุประสงค์เพื่อให้มีและคงไว้ซึ่งระดับการรักษาความปลอดภัยสารสนเทศ และระดับการให้บริการที่เหมาะสมและสอดคล้องกับข้อตกลงการบริการกับหน่วยงานภายนอก (กรณีถ้ามี)

7.2.1 ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการด้านเทคโนโลยีสารสนเทศของหน่วยงานภายนอกโดยต้องประกอบไปด้วยรายละเอียด ดังนี้

- การยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

- ขอบเขต รายละเอียด และระดับการให้บริการ (Service Level Agreement)

- เอกสารต่าง ๆ เกี่ยวกับมาตรการการควบคุมด้าน การรักษาความลับ (Confidentiality), การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

- ข้อตกลงการเชื่อมโยงระบบเครือข่ายของหน่วยงานภายนอก

- ข้อมูลที่หน่วยงานภายนอกสามารถเข้าถึงได้และขั้นตอนและวิธีการร้องขอข้อมูลของบริษัท กรณีต้องการข้อมูลเพิ่มเติม

- สัญญาในการไม่เปิดเผยข้อมูลของบริษัท

- ข้อกำหนดทางด้านกฎหมาย เช่น ความลับส่วนบุคคล (Privacy) และการป้องกันข้อมูล

- ให้หน่วยงานเทคโนโลยีสารสนเทศทบทวนในการบริหารจัดการการเปลี่ยนแปลงในการให้บริการฯ จากผู้ให้บริการภายนอก (กรณีมีการใช้บริการจาก Outsource)

7.3 การควบคุมและป้องกันการใช้งานเครื่องคอมพิวเตอร์รวมถึงอุปกรณ์แบบพกพาผิดวัตถุประสงค์
(Protection against malicious)

มีวัตถุประสงค์เพื่อป้องกันควบคุมและคุ้มครองผู้ใช้งานระบบซอฟต์แวร์ ข้อมูลและอุปกรณ์ ผิดจากวัตถุประสงค์การใช้งานที่กำหนดหรือกิจกรรมที่ไม่ประสงค์

7.3.1 เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แบบพกพา ที่ต้องการใช้งานผ่านระบบเครือข่ายของบริษัท จะต้องได้รับการลงทะเบียนและกำหนดสิทธิ์การใช้งานตามนโยบายความปลอดภัยก่อนได้รับอนุมัติเพื่อให้ใช้งานในระบบ โดยการลงทะเบียนของอุปกรณ์

7.3.2 เครื่องคอมพิวเตอร์ลูกข่าย (Client) และเครื่องคอมพิวเตอร์แบบพกพา (Laptop/Notebook) ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสรุ่นล่าสุดที่ได้รับการอนุมัติจากหน่วยงานเทคโนโลยีสารสนเทศและต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง

7.3.3 ห้ามเจ้าหน้าที่ทำการดาวน์โหลดโปรแกรมหรือฟรีแวร์โดยตรงจากอินเตอร์เน็ต โดยปราศจากการอนุมัติจากหน่วยงานเทคโนโลยีสารสนเทศ หลังจากการอนุมัติแล้วเจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัส ก่อนการใช้งาน

7.3.4 ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมล์ สำเนาจากแฟรชไดฟ์ หรือไฟล์แชร์ต่าง ๆ ต้องได้รับการสแกนหาไวรัส

7.3.5 ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใด ๆ ตัวอย่าง ไวรัส สแปมแวร์ โปรแกรมแฝง เข้าสู่ระบบคอมพิวเตอร์ของบริษัท

7.3.6 ห้ามผู้ใช้ขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้นที่ได้รับอนุญาตให้สามารถรับ-ส่งผ่านระบบเครือข่ายของบริษัทได้ ทั้งนี้ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักและจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสของบริษัทก่อนเปิดใช้งานเสมอ

7.4 การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

มีวัตถุประสงค์เพื่อป้องกันข้อมูลในระบบเครือข่ายและป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของบริษัท

7.4.1 ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย เช่น Modem, Router, Switch Hub และ Wireless Access Point โดยไม่ได้รับอนุญาตเด็ดขาด

7.4.2 กรณีมีการเชื่อมต่อไปยัง เครือข่ายภายนอกเพื่อให้ Outsource หรือผู้ให้บริการแก้ไขปัญหา ทำการแก้ไขปัญหาระบบ ห้ามผู้ใช้งานทำการเชื่อมต่อออกไปยังเครือข่ายภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าในหน่วยงานนั้น หรือ ผู้ใช้ไม่ได้เฝ้าอยู่ในหน้าจอเพื่อมองเห็นกระบวนทำงานหรือการควบคุมการดำเนินการที่ผิดวัตถุประสงค์

7.4.3 หน่วยงานเทคโนโลยีสารสนเทศควรมีการจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของบริษัท และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้

เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของบริษัททั้งทางด้านกายภาพ และทางด้าน Logical และต้องไม่อนุญาติให้หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายบริษัท

7.4.4 ระบบเครือข่ายทั้งหมดของบริษัทที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ควรต้องมีการติดตั้งซอฟต์แวร์พื้นฐานในการตรวจจับและป้องกันไวรัส หรือควรมีการพิจารณาในการจัดหาอุปกรณ์ Firewall เพื่อเป็นอุปกรณ์ป้องกันป้องกันการโจมตีจากผู้ที่เชื่อมต่อที่ประสงค์ร้าย หรือการเชื่อมต่อโดยไม่ได้รับอนุญาต

7.4.5 หน่วยงานเทคโนโลยีสารสนเทศควรมีการจัดทำหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ แนวทางการตรวจสอบถึงความผิดปกติในกรณีต่าง ๆรวมถึงคู่มือการแก้ไขหากพบปัญหาข้อผิดพลาด หรือการละเมิดซึ่งส่งผลกระทบต่อระบบเครือข่ายของบริษัท

7.5 การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media Handling)

มีวัตถุประสงค์เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลแต่ละหน่วยงานควรมีการกำหนดแนวทางการให้สิทธิ์ในการใช้สื่อบันทึกข้อมูล (Thump drive) **หรือ** External Hard disk drive **สำหรับผู้ใช้งานในระบบ**

7.6 การแลกเปลี่ยนข้อมูลสารสนเทศ (Exchange of Information)

มีวัตถุประสงค์เพื่อป้องกันการสูญหายของสารสนเทศและซอฟต์แวร์ รวมทั้งเพื่อป้องกันการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต หรือการนำสารสนเทศไปใช้ในทางที่ไม่เหมาะสม

7.6.1. ให้หน่วยงานเทคโนโลยีสารสนเทศ กำหนดวิธีการจัดเก็บสื่อบันทึกข้อมูล (สารสนเทศ หรือซอฟต์แวร์) ให้มีความมั่นคงปลอดภัย

7.6.2 ให้หน่วยงานเทคโนโลยีสารสนเทศกำหนดวิธีการป้องกันการเข้าถึงข้อมูล อิเล็กทรอนิกส์รวม รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

7.6.3 ให้เจ้าหน้าที่สแกนไวรัสอุปกรณ์ต่อพ่วง เช่น แฟรชไดฟ, external HDD ทุกครั้งที่เสียบใช้งาน โดยโปรแกรมสแกนไวรัสที่อยู่ภายในคอมพิวเตอร์

7.7 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

มีวัตถุประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

7.7.1 ให้หน่วยงานเทคโนโลยีสารสนเทศทำการบันทึกกิจกรรม (Audit Logging) การใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ

7.7.2 ให้หน่วยงานเทคโนโลยีสารสนเทศตรวจสอบการใช้งานสินทรัพย์สารสนเทศ อย่างสม่ำเสมอเพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

7.7.3 ให้หน่วยงานเทคโนโลยีสารสนเทศกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

7.7.4 ให้หน่วยงานเทคโนโลยีสารสนเทศบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and Operator Logs)

7.7.5 ให้หน่วยงานเทคโนโลยีสารสนเทศบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging) ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศวิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร

7.7.6 ให้หน่วยงานเทคโนโลยีสารสนเทศตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในหน่วยงานให้ตรงกัน (Clock Synchronization) โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจช่วงเวลาหากเครื่องคอมพิวเตอร์ของบริษัทถูกบุกรุก

หมวด 8 นโยบายการสำรองข้อมูลและกู้คืนข้อมูล SERVER (Backup and recovery)

8.1 นโยบายการสำรองข้อมูล SERVER (Back-up)

มีวัตถุประสงค์เพื่อเป็นแนวทางในการกำหนดแนวทางการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ เช่น โดนไวรัสโจมตี อุปกรณ์สำรุด หรือไฟฟ้าตก ไฟฟ้ากระชากทำให้ระบบเสียหาย หรือภัยธรรมชาติ อุบัติภัย เป็นต้น

8.1.1 หน่วยงานเทคโนโลยีสารสนเทศต้องทำการสำรองข้อมูล สัปดาห์ละ1 ครั้ง เป็นประจำ

8.1.2 หน่วยงานเทคโนโลยีสารสนเทศต้องมีการควบคุมการเข้าถึงห้องเซิฟเวอร์เพื่อความปลอดภัยของข้อมูล

8.1.3 หน่วยเทคโนโลยีสารสนเทศต้องมีกระบวนการสำรองข้อมูลโดยมีการสำรองข้อมูล 2 สถานที่ คือ 1. ที่ ๆ ข้อมูลอยู่ 2. นอกสถานที่ เพื่อกันเหตุการณ์ภัยต่าง ๆ ที่จะเกิดขึ้น

8.1.4 ต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูล

8.1.5 ต้องลงบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูลต้องได้รับการตรวจสอบเป็นประจำทุกปี

8.1.6 กระบวนการในการเก็บสื่อข้อมูลและสถานที่เก็บข้อมูลสำรอง ต้องได้รับการตรวจสอบอย่างน้อยปีละครั้ง

8.1.7 สื่อที่ใช้เก็บข้อมูลต้องมีป้ายบอกรายละเอียด ซึ่งประกอบด้วยข้อมูลอย่างน้อย ดังต่อไปนี้ ชื่อระบบ,วันสร้าง,ระดับความสำคัญของข้อมูล,รายละเอียดติดต่อผู้ดูแลข้อมูล

8.2 นโยบายการกู้คืน (Recovery)

8.2.1 หน่วยงานเทคโนโลยีสารสนเทศต้องมีการ ทดลองการกู้คืนข้อมูลอยู่เป็นประจำ ทุก ๆ ครึ่งปี

8.2.2 หน่วยงานเทคโนโลยีสารสนเทศต้องมี แผน ฉุกเฉิน สำหรับรองรับการเกิดภัย ต่าง ๆ

8.2.3 หน่วยงานเทคโนโลยีสารสนเทศต้องมี ข้อมูลการ back up อยู่ทั้งในและนอกสถานที่ เพื่อกันเหตุภัย ต่าง ๆ

หมวด 9 การควบคุมการเข้าถึง (Access Control)

9.1 การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

จุดประสงค์เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย

9.1.1 หน่วยงานเทคโนโลยีสารสนเทศต้องจัดทำนโยบายและความต้องการในการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงให้ทำได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

9.1.2 หน่วยงานเทคโนโลยีสารสนเทศต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

9.1.3 ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้หน่วยงานเทคโนโลยีสารสนเทศต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท และเฝ้าระวังการละเมิดความปลอดภัยที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

9.2 การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

จุดประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

9.2.1 การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการ สำหรับการลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในบริษัท เป็นต้น โดยผู้ใช้งานต้องได้รับการทบทวน และพิจารณาอนุมัติตามขั้นตอนของบริษัทอย่างเคร่งครัด

9.2.2 ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบด้วยผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ

9.2.3 หน่วยงานเทคโนโลยีสารสนเทศต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัยอยู่เสมอ หน่วยงานเทคโนโลยีสารสนเทศต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

9.2.4 ให้มีการจัดเก็บบันทึกข้อมูลการเข้าถึงและการใช้งานระบบสารสนเทศแต่ละระบบ (Log Files)

9.3 การรับผิดชอบหน้าที่ของผู้ใช้งาน (User Responsibilities)

จุดประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ สามารถเข้าถึงระบบสารสนเทศได้

9.3.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์ ของแต่ละผู้ใช้งาน

9.3.2 เจ้าหน้าที่ต้องปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศบริษัท การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่านและการจัดการควบคุมการใช้รหัสผ่าน

9.3.3 กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

- ควรได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาและผู้ดูแลระบบงานนั้น ๆ

- ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

- ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 90 วัน เป็นต้น

9.3.4 ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษา User Name และรหัสผ่านของตนเอง รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้ให้มีความมั่นคงปลอดภัยอย่างสม่ำเสมอ

9.3.5 รหัสผ่านต้องมีความมั่นคงปลอดภัยตามที่ได้กำหนดไว้

9.3.6 รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย ห้ามใช้ Account ร่วมกันหรือให้ผู้อื่นเข้าใช้งาน Account ของตนโดยเด็ดขาด ทั้งนี้รวมถึงสมาชิกในครอบครัวเมื่อผู้ใช้งานนำงานกลับไปทำที่บ้านด้วย

9.3.7 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่าน User ID และรหัสผ่านของตนทั้งหมด หากผู้ใช้งานสงสัยว่า User ID หรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อหน่วยงานเทคโนโลยีสารสนเทศและทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที

9.3.8 ผู้จัดการโครงการของระบบใหม่ที่เกิดขึ้นในบริษัทต้องตรวจสอบให้มั่นใจว่าระบบในความดูแลของตนสอดคล้องกับเนื้อหาของนโยบายฉบับนี้ รวมถึงเอกสารสนับสนุนอื่น ๆ ที่เกี่ยวข้องทั้งหมด และต้องประสานงานกับผู้ดูแลระบบให้ทำการควบคุม และปรับแต่งค่าต่าง ๆ ของระบบให้เป็นไปตาม ข้อกำหนดที่เกี่ยวข้องทั้งหมดนี้ก่อนเริ่มนำมาใช้งานจริง

9.3.9 การ Reset Password ต้องผ่านกระบวนการมาตรฐานของบริษัทเท่านั้น เพื่อให้มั่นใจว่าตรงกับ User ที่ต้องการ Reset รหัสผ่านจริง อีกทั้งเจ้าหน้าที่ ที่ดูแลระบบมีสิทธิ์ในการขอข้อมูลและพิสูจน์ตัวตนของผู้ใช้งานตามความเหมาะสม

9.3.10 ในทางกลับกัน ผู้ใช้งานอาจได้รับการร้องขอจากหน่วยงานเทคโนโลยีสารสนเทศให้ทำการเปลี่ยนรหัสผ่านใหม่ ในกรณีที่รหัสผ่านของผู้ใช้งานไม่มีความมั่นคงปลอดภัย สามารถถูกคาดเดา หรือถูกล่วงละเมิดได้ง่าย ทั้งนี้ผู้ใช้งานต้องตรวจสอบความถูกต้องของแหล่งที่มาของคำร้องขอดังกล่าวด้วย เพื่อให้มั่นใจว่าการร้องขอนั้นไม่ได้เป็นการหลอกลวง

9.4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

จุดประสงค์เพื่อควบคุมการใช้บริการบนเครือข่ายของบริษัท

9.4.1 หน่วยงานเทคโนโลยีสารสนเทศต้องจัดทำแนวทาง นโยบายควบคุมการเข้าถึง เครือข่ายและบริการบนเครือข่ายโดยเฉพาะเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

9.4.2 จัดแบ่งต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

9.4.3 หน่วยงานเทคโนโลยีสารสนเทศต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้นหน่วยงานเทคโนโลยีสารสนเทศต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

9.5 การควบคุมการใช้งานระบบปฏิบัติการ (Operating System Access Control)

จุดประสงค์เพื่อป้องกันการใช้งานระบบปฏิบัติการโดยไม่ได้รับอนุญาต

9.5.1 หน่วยงานเทคโนโลยีสารสนเทศต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

9.5.2 หน่วยงานเทคโนโลยีสารสนเทศต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนใช้ต้องทำการแจ้งเจ้าหน้าที่ดูแลระบบ เพื่อขอติดตั้งก่อน

- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน

- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ อาทิ ผู้ใช้งานระบบ

9.5.3 กลุ่มงานเทคโนโลยีสารสนเทศและการสื่อสารต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย เมื่อเครื่องคอมพิวเตอร์ลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลาหนึ่ง อาทิ กลไกการล็อคหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ

9.6 การควบคุมการใช้งานระบบสารสนเทศและสารสนเทศ (Application and Information Access Control)

จุดประสงค์เพื่อป้องกันการใช้งานระบบสารสนเทศและสารสนเทศโดยไม่ได้รับอนุญาต

9.6.1 กลุ่มงานเทคโนโลยีสารสนเทศต้องมีการควบคุมการใช้งานสารสนเทศใน ระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน อาทิ เขียน อ่าน ลบ ได้ กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

9.6.2 บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

9.6.3 บุคคลภายนอกต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของบริษัทอย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท

9.6.4 หน่วยงานเทคโนโลยีสารสนเทศต้องมีการแยกระบบสารสนเทศที่มีความสำคัญ หรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ต ภายในที่ใช้งานในบริษัท เป็นต้น

9.7 การควบคุมการเข้าถึงข้อมูลสารสนเทศ (Information Technology Access Control)

จุดประสงค์เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

9.7.1 สิทธิ์การเข้าถึงไฟล์ข้อมูลสารสนเทศต้องได้รับการควบคุม และได้รับการพิจารณาอนุมัติเท่าที่จำเป็นเท่านั้น เพื่อให้ไฟล์ข้อมูลสารสนเทศได้รับการรักษาความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ รวมทั้งเป็นการแบ่งแยกสิทธิ์ และหน้าที่ของผู้ใช้งาน

9.8 คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถานที่ (Mobile Computing)

จุดประสงค์เพื่อควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทเคลื่อนที่ได้ รวมทั้งการปฏิบัติงานนอกสำนักงานให้เป็นไปอย่างปลอดภัย

9.8.1 ต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Notebook, Palmtops, Laptop) และอุปกรณ์สื่อสารอื่น ๆ อาทิ เมื่อปฏิบัติงานอยู่นอกสถานที่

- ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง

- ต้องใส่รหัสผ่านป้องกันข้อมูลที่สำคัญ

หมวด 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition, Development and Maintenance)

10. 1 **การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ** (Security Requirements of Information Systems)

จุดประสงค์เพื่อการสร้างความปลอดภัยให้กับระบบสารสนเทศ

10.1.1 หน่วยงานเทคโนโลยีสารสนเทศต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจน ในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งาน

10.1.2 หน่วยงานดูแลระบบเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้

- มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย อาทิ การสำรองข้อมูล

- มาตรการปฏิบัติหลังจากเกิดความเสียหาย อาทิ แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล

10. 2 **ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ** (Security in Development and Support Processes)

จุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย

10.2.1 ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว อาทิ

- คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์

- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ

10.2.2 เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

10.2.3 ในการทำสัญญาว่าจ้างการพัฒนาระบบของบริษัทต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบและการกำหนดขอบเขตในการจ้างพัฒนาระบบ

หมวด 11 การสร้าง username & password และกำหนดสิทธิ์สำหรับโปรแกรม ERP (Winspeed)

หน่วยงานเทคโนโลยีสารสนเทศต้องมีแบบฟอร์มเป็นลายลักษณ์อักษร สำหรับ พนักงานใหม่ หรือลาออก หรือย้ายแผนก

11.1 หน่วยงานเทคโนโลยีสารสนเทศต้องจัดให้มีการ กรอกแบบฟอร์ม เพื่อขอ username & password โดยจะต้องมีข้อมูล ดังนี้

11.1.1 ชื่อ-นามสกุล พนักงาน ที่ขอใช้สิทธิ์

11.1.2 ชื่อแผนก ระบุว่า พนักงานใหม่, ลาออก, ย้ายแผนก

11.1.3 โดยระบุ สิทธิ์ที่จะใช้งาน และระบุวันที่ขอใช้

11.1.4 โดยจะต้องมีลายเซ็น ได้รับความยินยอมจาก หัวหน้าแผนกบัญชี และ หน่วยงานเทคโนโลยี

11.1.5 โดยสิทธิ์การเข้าถึงโมดูลสูงสุด เจ้าหน้าที่ดูแลระบบ จะได้รับสิทธิ์นั้นผู้เดียว ในกรณี มีบุคคลท่านอื่นจำเป็นต้องใช้โมดูลเหล่านี้ จะต้องได้รับ ความยินยอมจาก ผู้บริหารสูงสุด

11.2 หน่วยงานเทคโนโลยีสารสนเทศจะต้องมีการ กำหนด password อย่างเข้มงวดเพื่อความปลอดภัย

11.2.1 โดยรหัสจะต้องมีตัวอักษร 8-10 ตัวอักษร

11.2.2 โดยรหัสมีตัวอักษรพิมพ์ใหญ่ขึ้นต้น และ ตามด้วยตัวพิมพ์เล็ก

11.2.3 โดยรหัสจะต้องมี ตัวเลข อยู่ด้วยอย่างน้อย 1 ตัว

11.2.4 โดยจะต้องมีการ reset password ทุก ๆ 90 วัน

11.3 หน่วยงานเทคโนโลยีสารสนเทศจะต้องมีการ ตรวจสอบ user และ สิทธิ์ การใช้งานอยู่เป็นประจำ

11.3.1 โดยจะต้องมีการตรวจสอบ สิทธิ์ และนำไป recheck กับข้อมูลฝ่ายบุคคล ว่าตรงกัน ในทุกๆ 90 วัน

11.4 หน่วยงานเทคโนโลยีสารสนเทศจะต้องมีการจัดทำหลักฐานเป็นลายลักษณ์อักษรในกรณีมีการอัพเดต ฟอร์ม หรือ change program (ERP)

11.4.1 ในกรณีมีการ แก้ไขตัวโปรแกรมหรือเพิ่ม function ต่าง ๆ โดย vender โดยฝ่ายบัญชีจะต้องมีอีเมลล์เป็นลายลักษณ์อักษรส่งถึง vender เพื่อเป็นหลักฐาน

11.4.2 โดยทุกครั้งที่มีการแก้ไขฟอร์ม จะต้องการขออนุมัติจากผู้มีอำนาจ และรวบรวมรายการแก้ไขฟอร์มเพื่อเก็บเป็นหลักฐาน

หมวด 12 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

จุดประสงค์เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ทางด้านการปฏิบัติงานของบริษัทเพื่อป้องกันกระบวนการทางด้านการปฏิบัติงานของบริษัทที่สำคัญอันเป็นผลมาจากการล้มเหลว หรือ หายนะที่มีต่อระบบเทคโนโลยีสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

12.1 กำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัท การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ

12.2 กำหนดให้มีการทดสอบกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัทอย่างสม่ำเสมอ

หมวด 13 การปฏิบัติตามข้อกำหนด (Compliance)

13.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย (Compliance with Legal Requirements)

จุดประสงค์เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติระเบียบข้อบังคับรวมทั้งสัญญาต่าง ๆ

13.1.1 หน่วยงานเทคโนโลยีสารสนเทศต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศของหน่วยงาน

13.1.2 เจ้าหน้าที่ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของ นโยบาย กฎระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ ที่กำหนดขึ้นอย่างเคร่งครัด

โดยมีรายการดังต่อไปนี้เป็นอย่าง

- นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
- พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
- พ.ร.บ. ลิขสิทธิ์

13.1.3 ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัทถือเป็นทรัพย์สินของบริษัท (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้าหรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือ วัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

13.1.4 เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และ ระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ที่กำหนดไว้ตลอดจนการเข้าถึง ทบทวน และตรวจสอบอีเมลล์ของผู้ใช้งานโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตามการตรวจสอบดังกล่าวจะดำเนินการต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใด ๆ ของผู้ใช้เว้นแต่เป็นการเปิดเผยตามคาสั่งศาล ตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น

13.1.5 ห้ามเจ้าหน้าที่ทุกคนใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัท กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม

13.1.6 ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิดต้องปฏิบัติตามข้อกาหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่

13.1.7 ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือ เอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัทโดยเด็ดขาด

13.1.8 เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจหรือพลั้งเผลอ จึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัทเพื่อจุดประสงค์ใด ๆ ก็ตาม โดยที่ไม่ได้รับอนุญาต

13.2 การพิจารณาการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations)

จุดประสงค์เพื่อทำให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมดมีผลกระทบน้อยที่สุดต่อการดำเนินงานของหน่วยงาน

13.2.1 หน่วยงานเทคโนโลยีสารสนเทศต้องวางแผนการตรวจสอบระบบทั้งหมด โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบ และกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด

13.2.2 หน่วยเทคโนโลยีสารสนเทศต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด หรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น

หมวดที่ 14 มาตรการในการป้องกันความเสี่ยงและลดผลกระทบจากภัยคุกคามและปัญหาคุกคามทางไซเบอร์

จุดประสงค์เพื่อจุดประสงค์เพื่อป้องกันความเสี่ยงและลดผลกระทบจากภัยคุกคามและปัญหาคุกคามทางไซเบอร์ ภัยคุกคามและปัญหาคุกคามทางไซเบอร์ ในปัจจุบันที่ปรากฏ เช่น

- Malware – ภัยจากการถูกโจมตีด้วยมัลแวร์ (โปรแกรมไม่พึงประสงค์)
- Web Application Attack - ภัยจากการถูกโจมตีเว็บแอพพลิเคชั่น
- Phishing – ภัยจากการถูกพิชชิ่ง (เป็นเทคนิคในการดึงข้อมูลชั้นที่เป็นความลับ เช่น หมายเลขบัตรเครดิต รหัสผ่าน ชื่อผู้ใช้โดยการ ปลอมแปลงเป็นองค์กรที่ถูกกฎหมาย)
- DDoS (Distributed denial of service) - DoS - ภัยจากการถูกโจมตีเพื่อขัดขวางการทำงานของระบบ DoS - เป็นการโจมตีโดยทุ่มเทข้อมูลใส่เซิร์ฟเวอร์จนโอเวอร์โหลด ทำให้เซิร์ฟเวอร์ล่มหรือช้าลง จนกระทั่งใช้การไม่ได้
- Spam – ภัยจากการได้รับสแปมเมล์
- Botnets – ภัยจากการที่อุปกรณ์ในองค์กรตกเป็นเหยื่อของบอทเน็ต (Email bombing and spamming: โจมตีด้วยอีเมล์จำนวนมหาศาล ทำให้ทรัพยากรของระบบเครือข่ายต้องทำงานหนัก จะส่งข้อความที่ไม่มีความหมายใด ๆ เพื่อต้องการให้อีเมล์ ชื่อบัญชี หรือเมล์เซิร์ฟเวอร์ล่ม Botnets = private internet-connected computers whose security has been compromised by malware and under the attacker's control as a DDoS attack. Spam (Violate) (AUP = the Acceptable Use Policy))
- Ransomware – ภัยจากมัลแวร์เรียกค่าไถ่
- Data Breaches - ภัยจากการที่ข้อมูลขององค์กรรั่วไหล

โดยกำหนดมาตรการในการปกป้องระบบข้อมูลสารสนเทศที่สำคัญ และลดผลกระทบ ดังนี้

14.1 มีการกำหนดนโยบายการมาตรการดำเนินการด้านความปลอดภัยของระบบสารสนเทศเพื่อเป็นแนวทางและมาตรฐานการการป้องกันภัยคุกคามต่าง ๆ ข้างต้นที่อาจเกิดขึ้น

14.2 ติดตั้งอุปกรณ์ Firewall เพื่อป้องกันระบบที่มีความสำคัญ

14.3 การกำหนดการติดตั้งและใช้โปรแกรมลิขสิทธิ์อย่างถูกต้อง ซึ่งโปรแกรมลิขสิทธิ์จะมีระบบการอัพเดตระบบอย่างถูกต้องและสม่ำเสมอเพื่อป้องกันภัยต่าง ๆ ที่เกิดขึ้นกับระบบได้ในระดับหนึ่ง

14.4 การเลือกใช้โปรแกรมการป้องกันไวรัสและสแปมที่ได้มาตรฐานความปลอดภัยโดยมีการติดตั้งให้กับทุก User และได้รับการ Updated สม่ำเสมอ

14.5 การเลือกใช้ผู้ให้บริการ Email Hosting, Web Hosting ที่มีมาตรฐาน เพื่อสามารถให้บริการระบบที่มีมาตรฐานการป้องกันอย่างปลอดภัย

14.6 การกำหนดแนวทางในการจัดการสำรองข้อมูลที่สำคัญขององค์กรอย่างเป็นระบบ รวมถึงความถี่ของระยะเวลาที่ทำการสำรองข้อมูลที่สามารถกู้คืนได้โดยไม่ทำให้เกิดผลกระทบต่อการดำเนินธุรกิจปกติ มีการแยกจัดเก็บฐานข้อมูลที่สำคัญโดยอิสระเพื่อป้องกันภัยคุมคาม อันอาจเกิดขึ้นจากส่งภัยคุมคามผ่านการเชื่อมต่อระบบเครือข่ายมายังฐานข้อมูลที่มีการเชื่อมต่อกับระบบการทำงานหลัก

รายละเอียดเอกสารที่จัดทำและการปรับปรุง

ลำดับ	เลขที่เอกสาร	ว.ด.ป.ที่อนุมัติ	เสนอที่ประชุมคณะกรรมการเพื่ออนุมัติ
1	CS20140802	8 สิงหาคม 2561	ที่ประชุมคณะกรรมการครั้งที่ 4/2561
2	CS20140802(Rev 1)	14 พฤศจิกายน 2561	ที่ประชุมคณะกรรมการครั้งที่ 5/2561
3	CS20140802(Rev 2)	13 พฤศจิกายน 2563	ที่ประชุมคณะกรรมการครั้งที่ 4/2563