นโยบายในการรักษาความมั่งคงปลอดภัยด้านสารสนเทศ
บริษัท กรุงไทยคาร์เร้นท์ แอนด์ ลีส จำกัด (มหาชน)

บริษัท กรุงไทยคาร์เร้นท์ แอนด์ ลีส จำกัด (มหาชน)
นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. บทนำ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท กรุงไทยคาร์เร้นท์ แอนด์ ลีส จำกัด (มหาชน) (บริษัท) ฉบับนี้ จัดทำขึ้นเพื่อให้ระบบสารสนเทศของบริษัทมีการควบคุมภายในที่ดี มีความมั่นคงปลอดภัย ถูกต้อง เชื่อถือได้ สามารถดำเนินงานได้อย่างต่อเนื่อง และสามารถป้องกันรักษาสารสนเทศที่เป็นความลับของบริษัท ทั้งที่เป็นข้อมูลของบริษัท และข้อมูลส่วนบุคคลอื่นๆ

2. วัตถุประสงค์

2.1 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของบริษัท สามารถดำเนินงานได้อย่างมีประสิทธิภาพ ประสิทธิผล และวัตถุประสงค์ที่กำหนดไว้

2.2 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคง ปลอดภัยในการใช้งานด้านสารสนเทศของบริษัท

2.3 เพื่อป้องกันไม่ให้ระบบสารสนเทศ และสารสนเทศของบริษัท ถูกบุกรุก เปลี่ยนแปลง ขโมย ทำลาย หรือกระทำอื่นๆ ที่อาจสร้างความเสียหายต่อบริษัท

2.4 เพื่อสร้างความมั่นใจให้กับบุคคลภายนอกที่เป็นคู่ค้า หรือผู้มีส่วนได้เสียต่างๆ ว่าข้อมูลส่วนบุคคลจะได้รับการปกป้องตามมาตรฐานความปลอดภัยของบริษัท

2.5 เพื่อเผยแพร่ให้ผู้ใช้งาน และบุคคลภายนอก ซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูล หรือระบบสารสนเทศ ได้รับทราบและถือปฏิบัติอย่างเคร่งครัด

3. ขอบเขต

นโยบายฉบับนี้ใช้กับบริษัท กรุงไทยคาร์เร้นท์ แอนด์ ลีส จำกัด (มหาชน) และบุคคลภายนอก ("ผู้ใช้งาน") ที่ได้รับอนุญาตให้ใช้ระบบเครือข่าย คอมพิวเตอร์แม่ข่าย ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ คอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสารแบบพกพา หรืออุปกรณ์สื่อสารโทรคมนาคม เพื่อเข้าถึงสารสนเทศของบริษัท

4. ความหมาย และคำจำกัดความ

"**บริษัท**" หมายถึง บริษัท กรุงไทยคาร์เร้นท์ แอนด์ ลีส จำกัด (มหาชน) (บริษัท)

"**ผู้ใช้งาน**" หมายถึง กรรมการ/พนักงาน หรือผู้ที่ได้รับอนุญาตให้ใช้ระบบคอมพิวเตอร์ระบบเครือข่ายของบริษัท

"**เจ้าของข้อมูล**" หมายถึง ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเสียหาย

"**ทรัพย์สินด้านสารสนเทศ**" ได้แก่ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด

"**ระบบสารสนเทศ**" หมายถึง ระบบที่มีการนำเอา ฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร แนวปฏิบัติ และข้อมูลซึ่งทำงานประสานกัน เพื่อจัดเตรียมสารสนเทศที่จำเป็นให้กับบริษัท

"**สารสนเทศ**" หมายถึง ข้อมูลต่าง ๆ ที่ได้ผ่านการเปลี่ยนแปลงประมวลหรือวิเคราะห์สรุปผลด้วยวิธีการต่าง ๆ แล้วเก็บรวบรวมไว้ เพื่อนำมาใช้ประโยชน์ตามต้องการ การประมวลผล เป็นการนำข้อมูลจากแหล่งต่าง ๆ ที่เก็บรวบรวมไว้ผ่านกระบวนการต่าง ๆ เพื่อแปรสภาพข้อมูลให้เป็นระบบที่อยู่ในรูปแบบที่ต้องการ

"**บุคคลภายนอก**" หมายถึง บุคคล นิติบุคคล ซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูลหรือระบบสารสนเทศ โดยได้รับสิทธิ์ตามประเภทการใช้งาน และต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทโดยไม่ได้รับอนุญาต

"**ผู้รับการว่าจ้าง**" หมายถึง บุคคล บริษัท หรือหน่วยงานภายนอก ซึ่งได้รับการว่าจ้างจากบริษัทให้ทำงานให้ในช่วงระยะเวลาหนึ่ง หรือทำงานในฐานะเป็นผู้ใช้งานของบริษัท ซึ่งรวมถึงลูกจ้างชั่วคราว โดยทั่วไปการว่าจ้างจะมีการทำสัญญาจ้างเพื่อควบคุมให้ผู้รับจ้างปฏิบัติตามเงื่อนไข หรือข้อตกลงการจ้างงานนั้น

5. หน้าที่ความรับผิดชอบ

5.1 หน้าที่ของกรรมการผู้จัดการ

กำหนดกลยุทธ์ในภาพรวม ควบคุมการปฏิบัติงานในบริษัท และอนุมัตินโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

5.2 หน้าที่ของผู้บริหารระดับสูงทางด้านการรักษาความมั่นคงปลอดภัยให้กับโครงสร้างเครือข่าย และความปลอดภัยของข้อมูลสารสนเทศ

5.2.1 กำหนดเป้าหมาย นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท โดยกำหนดให้เป็นไปในทิศทางเดียวกันกับนโยบายยุทธศาสตร์ของบริษัท

5.2.2 ร่างนโยบาย และระเบียบในการดำเนินการดำเนินนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

5.2.3 จัดการพัฒนานโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ Policy, Standard Procedure และ Guideline เพื่อให้บริษัทได้มาซึ่งการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability)

5.2.4 จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่าง ๆ ที่อาจเกิดขึ้นกับระบบ รวมทั้งวางแผนบริหารความต่อเนื่องของธุรกิจ เพื่อกู้ระบบงานฉุกเฉิน

5.2.5 บริหารความเสี่ยง และวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหา กระทบกับการดำเนินธุรกิจของบริษัท

5.2.6 นำเสนอผู้บริหารระดับสูง เช่น ประธานเจ้าหน้าที่บริหาร (CEO) เรื่องแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง

5.2.7 เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ ๆ ทางด้านการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศอย่างสม่ำเสมอ

5.3 หน้าที่ของผู้ใช้งาน

5.3.1 ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทโดยเคร่งครัด

5.3.2 ให้ความร่วมมือกับบริษัท อย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์ และข้อมูลสารสนเทศของบริษัท สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของบริษัท ให้มีความปลอดภัย

5.3.3 รายงานต่อบริษัททันที เมื่อพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรม สารสนเทศ รวมถึงระบบสารสนเทศที่อาจสร้างความเสียหายต่อบริษัท

5.4 หน้าที่ของหัวหน้าหน่วยงาน

5.4.1 ชี้แจงและส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และตักเตือนลงโทษทางวินัยกรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

5.4.2 ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้งจัดหา และพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท

5.4.3 ดูแลทรัพยากรด้านสารสนเทศของบริษัท ให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

5.5 หน้าที่ของเจ้าของข้อมูลและสารสนเทศ

5.5.1 จัดให้มีการจัดทำเอกสาร มาตรการและขั้นตอนควบคุมการเข้าถึงข้อมูล ให้เป็นไปตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

5.5.2 ดูแลให้พนักงานปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของบริษัท

5.5.3 ควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศ และระบบคอมพิวเตอร์ภายใต้หน้าที่และความรับผิดชอบ

5.5.4 รายงานเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ

5.5.5 แจ้งส่วนงานเทคโนโลยีสารสนเทศเพื่อกำหนดสิทธิ์ เพิ่มลบเปลี่ยนแปลงสิทธิ์ เมื่อมีการเปลี่ยนแปลงอำนาจหน้าที่ตำแหน่งงาน หรือโอนย้ายร่วมถึงกรณีลาออก ไล่ออก โดยทันที

5.6 หน้าที่ของเจ้าหน้าที่สารสนเทศ (ไอทีและระบบงาน)

ก. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

5.6.1 กำหนดให้เจ้าหน้าที่สารสนเทศ (แผนกไอทีและระบบงาน) จัดทำขั้นตอน หรือระเบียบปฏิบัติในการปฏิบัติงานประจำในด้านต่าง ๆ ที่สำคัญเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ไอที เช่น ขั้นตอนการเปิด – ปิดระบบงาน ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพการทำงาน และตารางเวลาในการปฏิบัติงาน เป็นต้น และต้องปรับปรุงขั้นตอนหรือระเบียบปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

5.6.2 การเฝ้าติดตามการทำงานของระบบคอมพิวเตอร์ เพื่อให้ส่วนงานสารสนเทศ (แผนกไอทีและระบบงาน) ติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญสามารถทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เช่น การตรวจสอบระบบเครือข่าย การทำงานของเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น และควรบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้อยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

5.6.3 การจัดการปัญหา ควรกำหนดรายชื่อหน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน รวมถึงเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องเพื่อใช้ติดต่อในกรณีที่เกิดปัญหา และควรมีระบบการจัดเก็บบันทึกปัญหาและเหตุการณ์ผิดปกติที่เกิดขึ้น และรายงานให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหาและตรวจสอบถึงหาสาเหตุที่เกิดขึ้นรวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาต่อไป

ข. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย

5.6.4 บริหารจัดการข้อมูลและควบคุมการเข้าถึงข้อมูล กำหนดวิธีปฏิบัติในการจัดเก็บข้อมูลและควบคุมการเข้าถึงเข้ามูลตามประเภทผู้มีอำนาจแต่ละระดับชั้น ทั้งการเข้าถึงโดยตรงและการเข้าถึงระบบงาน รวมถึงวิธีการทำลายข้อมูลในแต่ละระดับชั้น

5.6.5 บริหารจัดการและตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย (Server) จัดทำระเบียบปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย หากพบการใช้งานหรือเปลี่ยนแปลงค่า (Parameter) ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข และรายงานผู้บังคับบัญชาทันที

5.6.6 การป้องกันไวรัสคอมพิวเตอร์และโปรแกรมไม่พึงประสงค์ ส่วนงานสารสนเทศโดยแผนกไอทีและระบบงานต้องติดตั้งโปรแกรมป้องกันไวรัสที่มีประสิทธิภาพในเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ โดยที่ผู้ใช้งานต้องไม่ยุติหรือปิดบริการซอฟต์แวร์ป้องกันไวรัสบนเครื่องที่ใช้งาน รวมทั้งควรแจ้งแผนกไอทีและระบบงานทันทีในกรณีที่พบว่าไวรัส

5.6.7 การเก็บบันทึกการทำงานเพื่อการตรวจสอบ (Audit Log) ดำเนินการตั้งเวลาในเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้ตรงกับเวลาอ้างอิงสากล รวมทั้งจัดให้มีระบบเก็บบันทึกการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งานในระบบต่าง ๆ (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบ และจำกัดสิทธิการเข้าถึงระบบงานบันทึกเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ค. การควบคุมและพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์

5.6.8 ผู้ร้องขอ ผู้ใช้งานที่เกี่ยวข้อง และส่วนงานเทคโนโลยีและสารสนเทศ (แผนกไอทีและระบบงาน) ต้องมีส่วนร่วมในการทดสอบ เพื่อให้ตรงกับความต้องการก่อนที่จะโอนย้ายไปยังระบบงานจริง

5.6.9 ผู้ร้องขอ ผู้ใช้งานที่เกี่ยวข้อง และส่วนงานเทคโนโลยีและสารสนเทศ (แผนกไอทีและระบบงาน) ต้องทำการตรวจสอบการโอนย้ายระบบงานให้ถูกต้อง ครบถ้วน

5.6.10 ส่วนงานเทคโนโลยีและสารสนเทศ (แผนกไอทีและระบบงาน) ต้องจัดให้การเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่ผ่านมา และต้องมีปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้าง ข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม เป็นต้น และต้องจัดเก็บเอกสารทั้งหมดในที่ปลอดภัยและสะดวกต่อการใช้งาน

5.6.11 ส่วนงานสารสนเทศ ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานกรณี Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้ ทั้งนี้ให้ครบคลุมทั้ง Executable Program และ Source Program (ถ้ามี)

5.6.12 ผู้ร้องขอ ผู้ใช้งานที่เกี่ยวข้องและเจ้าหน้าที่ส่วนงานสารสนเทศร่วมกันทบทวนระบบงานใหม่ หลังจากใช้งานไปได้ระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ และประมวลผลได้อย่างถูกต้องตามความต้องการของผู้ใช้งาน

5.6.13 ผู้ใช้งานและเจ้าหน้าที่ส่วนงานและสารสนเทศ ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้ทราบอย่างทั่วถึง เพื่อสามารถใช้งานได้อย่างถูกต้อง ครบถ้วน

5.7 **หน้าที่ของหน่วยงานตรวจสอบภายใน** (Internal Audit)

ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ ตามความจำเป็น

6. นโยบาย

บริษัทกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในประเด็นสำคัญ ดังต่อไปนี้

6.1 **การบริหารจัดการทรัพย์สินของบริษัท**

6.1.1 ทรัพย์สินด้านสารสนเทศ ได้แก่ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด ต้องมีการจัดทำบัญชีทรัพย์สิน เจ้าหน้าที่สารสนเทศเป็นผู้จัดทำ บัญชีฮาร์ดแวร์ และซอฟต์แวร์ แอพพลิเคชันและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลของอุปกรณ์ทรัพย์สินด้านสารสนเทศ

6.1.2 บริษัทต้องกำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันทรัพย์สินด้านสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม เอกสารหรือสื่อตีพิมพ์ หรือที่ทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่า มีชั้นความลับเดียวกันกับต้นฉบับข้อมูลนั้น

6.1.3 การใช้งานทรัพย์สินที่เหมาะสม ต้องมีการจัดทำกฎระเบียบ หรือหลักเกณฑ์เป็นลายลักษณ์อักษรเพื่อป้องกันความเสียหายต่อทรัพย์สินด้านสารสนเทศ

6.2 **ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร**

6.2.1 ต้องมีการกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับผู้ใช้งาน หรือที่ว่าจ้างหน่วยงานภายนอกมาปฏิบัติงาน รวมทั้งกำหนดมาตรการป้องกันและดูแลรักษาความปลอดภัยสำหรับสารสนเทศของบริษัท

6.2.2 แผนกบุคคลต้องมีระบบตรวจสอบคุณสมบัติของผู้สมัครเข้าทำงานที่ต้องสรรหา (โดยเฉพาะตำแหน่งงานสำคัญที่สามารถเข้าถึงข้อมูลชั้นความลับ) ควรกำหนดเงื่อนไขการจ้างงานรวมทั้งจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานและบริษัทว่าจะไม่เปิดเผยความลับของบริษัท โดยการลงนามเป็นส่วนหนึ่งของการจ้างงาน และต้องผ่านการอบรมเรื่องความปลอดภัยสารสนเทศ มีจิตสำนึก สามารถสร้างความตระหนักให้พนักงานผู้ใช้งานระบบได้ ต้องกำหนดให้ผู้ใช้งานที่ได้รับว่าจ้างต้องปฏิบัติตามมาตรการความมั่นคงปลอดภัยที่ได้จัดตั้งกับนโยบายของบริษัทที่กำหนดไว้

6.2.3 ต้องกำหนดให้ผู้ใช้งานที่ได้รับว่าจ้างต้องปฏิบัติตามมาตรการความมั่นคงปลอดภัยให้สอดคล้องกับนโยบายบริษัทที่กำหนดไว้

6.2.4 จัดอบรมให้ความรู้แก่ผู้ใช้งานทุกคนเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ละสารสนเทศ อย่างน้อง 1 ครั้ง ต้องมีการลงนามและเก็บรวมรวมไว้ในแฟ้มประวัติของบุคคลากร ถ้ามีการเปลี่ยนแปลง / เพิ่มเติมระบบใหม่ ต้องประกาศให้พนักงานทราบ

6.2.5 ต้องมีการกำหนดบทลงโทษทางวินัยสำหรับผู้ฝ่าฝืนนโยบาย กฎ และแนวปฏิบัติของบริษัท หากมการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำ และเป็นไปตามระเบียบบริษัท

6.2.6 หากมีการแต่งตั้ง โยกย้าย ปลด หรือเปลี่ยนแปลงตำแหน่งใดๆ แผนกบุคคลต้องแจ้งให้ผู้ว่าจ้างทราบ และผู้รับการว่าจ้างต้องปฏิบัติตามเงื่อนไขในสัญญาจ้าง จนกว่าจะสิ้นสุดการว่าจ้าง และพนักงานซึ่งพ้นตำแหน่งจากการจ้างงานไม่ว่ากรณีใด ต้องคืนทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศ สารสนเทศ เช่น กุญแจ อุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่างๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน ซึ่งส่วนงานเทคโนโลยีสารสนเทศต้องถอดสิทธิ์การเข้าใช้งานดังกล่าวด้วย

6.3 **ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม**

6.3.1 ต้องมีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อห้องทำงานและทรัพย์สินอื่น ๆ จัดให้มีการป้องกันภัยคุกคามต่าง ๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อความไม่สงบ เป็นต้น รวมถึงการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย ต้องมีการจัดการป้องกันที่เพียงพอ

6.3.2 ในการส่งมอบผลิตภัณฑ์ให้บุคคลภายนอก ต้องมีบริเวณเฉพาะที่จัดไว้ต่างหาก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศของบริษัทโดยไม่ได้รับอนุญาต

6.3.3 พนักงานต้องป้องกันอุปกรณ์ของสำนักงาน เพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อม และอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

6.3.4 ทรัพย์สินด้านสารสนเทศจะต้องอยู่ในพื้นที่ที่เหมาะสมรวมความปลอดภัย มีการควบคุมการเข้า –ออกพื้นที่ได้เฉพาะผู้ที่มีหน้าที่รับผิดชอบและผู้ที่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

6.3.5 มีระบบไฟฟ้าสำรองเพื่อให้สามารถทำงานได้อย่างเพียงพอ และต้องมีการตรวจสอบระบบไฟฟ้าสำรองอย่างน้อยปีละ 2 ครั้ง เพื่อเป็นการลดความเสียหายที่อาจจะเกิดขึ้น รวมถึงอุปกรณ์สำคัญ เช่น อุปกรณ์ Network, อุปกรณ์ความปลอดภัย Card Reader หรือ Finger Scan, คอมพิวเตอร์ เครื่องพิมพ์ของผู้ใช้ที่สำคัญ (Key User) เช่น ผู้ใช้ระบบบัญชี รับ-จ่ายเงิน, คีย์ Sales Order หรือผู้ใช้ที่หากใช้งานระบบไม่ได้จะมีผลเสียหายต่อธุรกิจ

6.3.6 การเดินสายเคเบิลต่าง ๆ ต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการเดินสายนั้นต้องติดป้ายกำกับให้รู้ต้นทางปลายทางของสาย

6.3.7 ต้องบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่าย อย่างสม่ำเสมอ

6.3.8 ต้องมีมาตรการป้องกันอุปกรณ์ต่าง ๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น

6.3.9 พนักงานต้องมีการตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูล เพื่อดูว่าข้อมูลสำคัญที่อยู่ในอุปกรณ์ดังกล่าว ได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะนำอุปกรณ์ดังกล่าวทิ้งไป โดยต้องเป็นไปตามที่ส่วนงานเทคโนโลยีสารสนเทศกำหนด

6.3.10 ต้องมีขั้นตอนปฏิบัติสำหรับการจัดการสื่อบันทึกข้อมูลสามารถเคลื่อนย้ายได้

6.3.11 ต้องมีการกำหนดมาตรการการป้องกันเอกสารระบบ จากการเข้าถึงโดยไม่ได้รับอนุญาต

6.3.12 ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

6.3.13 ต้องมีมาตรการ การกำจัดสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร เช่น การเผา ตัด หั่น หรือทำลายสื่อบันทึกข้อมูลที่มีข้อมูลสำคัญในนั้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยกำหนดให้มีบุคลากรผู้ทำหน้าที่ในการสอดส่องและดูแลการกำจัดหรือทำลายสื่อบันทึกข้อมูล การทำลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูล จะต้องได้รับการอนุมัติจากเจ้าของข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม

6.4 **การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของบริษัท**

6.4.1 ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน เช่น ขั้นตอนการกู้คืนระบบ ขั้นตอนการบำรุงรักษา และดูแลระบบ เป็นต้น โดยปรับปรุงคู่มือขั้นตอนการปฏิบัติงานเมื่อมีการเปลี่ยนแปลงขั้นตอน หรือผู้รับผิดชอบ และต้องทบทวนอย่างน้อยปีละ 1 ครั้ง และต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบคอมพิวเตอร์ ระบบเครือข่าย คอมพิวเตอร์แม่ข่าย ฮาร์ดแวร์และซอฟต์แวร์

6.4.2 ต้องมีการแบ่งหน้าที่ความรับผิดชอบของผู้ดูแลระบบเพื่อลดโอกาสในการเปลี่ยนแปลง หรือแก้ไขโดยไม่ได้รับอนุญาต

6.4.3 ต้องมีการแยกระบบสำหรับพัฒนาและทดสอบแยกออกจากระบบงานจริง เพื่อป้องกันการเข้าถึงข้อมูลหรือเปลี่ยนแปลงต่อระบบงาน ที่ให้บริการจริงจากผู้ที่ไม่ได้รับอนุญาต และต้องติดตามสภาพการใช้งาน การวิเคราะห์ขีดความสามารถของทรัพยากรสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

6.4.4 การยอมรับระบบใหม่ ต้องจัดให้มีเกณฑ์ในการยอมรับ และจัดให้มีการทดสอบระบบใหม่ก่อนที่จะตรวจรับระบบนั้นอย่างเป็นลายลักษณ์อักษร

6.5 **การบริหารจัดการการให้บริการของหน่วยงานภายนอก**

6.5.1 ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการโดยหน่วยงานภายนอก เช่น มีการยอมรับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท และขอบเขตรายละเอียดระดับการให้บริการ ต้องได้รับการตรวจสอบจากฝ่ายกฎหมายของบริษัท รวมถึงสัญญาในการไม่เปิดเผยข้อมูลของบริษัท เป็นต้น

6.5.2 หน่วยงานภายนอก หรือบุคคลภายนอกอื่นๆ ที่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศของบริษัท ต้องยอมรับและปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

6.5.3 บริษัทจะประเมินความเสี่ยงในการเข้าถึงระบบสารสนเทศ หรือที่มีผลกระทบต่อบริษัทของหน่วยงานภายนอก หรือบุคคลภายนอกอื่น ๆ ถ้าจำเป็นต้องมีการเปิดเผยข้อมูลนั้นออกไป หน่วยงานภายนอกหรือบุคคลภายนอกนั้นต้องเซ็นสัญญาว่าจะไม่เปิดเผยความลับของบริษัท

6.5.4 ต้องตรวจสอบการให้บริการหรือสัญญาที่ทำกับหน่วยงานภายนอก และบุคคลภายนอกที่เข้ามาให้บริการกับบริษัท โดยมีการทบทวนอย่างสม่ำเสมอตามความจำเป็น รวมถึงต้องกำหนดให้มีการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เช่น เมื่อมีการปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การเปลี่ยนแปลงเทคโนโลยีใหม่ เป็นต้น

6.6 **การบริหารจัดการด้านความมั่นคงปลอดภัยด้านเครือข่าย**

6.6.1 ต้องกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และกำหนดสิทธิ์ผู้ที่ใช้งานผ่านเครือข่ายโดยอนุญาตเฉพาะผู้ที่มีสิทธิ์เท่านั้น

6.6.2 พนักงานต้องมีช่องทางภายนอกเข้าสู่ระบบเครือข่ายภายในเช่น การเข้าถึงเครือข่ายระยะไกลผ่านคอมพิวเตอร์โน้ตบุ๊ก รวมถึงไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวกับการให้บริการเครือข่ายโดยไม่ได้รับอนุญาต

6.7 **การแลกเปลี่ยนสารสนเทศ**

6.7.1 ต้องกำหนดนโยบาย แนวปฏิบัติ และมาตรการเพื่อป้องกันปัญหาของการรับส่งข้อมูลสารสนเทศภายใน (Intranet) บริษัท ภายในกลุ่มบริษัท และหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิดอย่างเป็นลายลักษณ์อักษร เช่น การส่งข้อความทางอิเล็กทรอนิกส์ เป็นต้น

6.7.2 ต้องมีมาตรการตรวจทานก่อนส่งข้อมูลสารสนเทศออกสู่สาธารณะ โดยมีการประเมินความเสี่ยงและกำหนดมาตรการลดความเสี่ยงก่อนนำข้อมูลไปเผยแพร่

6.8 **การตรวจสอบการเข้าใช้งานระบบ**

6.8.1 ต้องกำหนดให้มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ และกิจกรรมการใช้งานของผู้ใช้งานอย่างสม่ำเสมอ และต้องมีมาตรการป้องกันข้อมูลที่บันทึกที่เกี่ยวข้องกับการใช้งานสารสนเทศไม่ให้มีการเปลี่ยนแปลงหรือแก้ไขได้ไม่ได้รับอนุญาต รวมถึงต้องบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบนั้น ๆ ด้วย

6.8.2 ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดที่เกี่ยวข้อง วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร และต้องตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องของบริษัทถูกบุกรุก

6.8.3 การเข้าถึงและการใช้งานระบบสารสนเทศของพนักงาน และต้องถูกสอบทานและทบทวนตามรอบระยะเวลาที่กำหนดไว้จากส่วนงานตรวจสอบภายในโดยส่วนงานตรวจสอบภายในมีสิทธิ์ที่จะสอดส่องดูแลการกระทำใดๆ ที่ผู้ตรวจสอบสงสัยว่ามีการฝ่าฝืนนโยบายดังกล่าว

6.9 **การควบคุมการเข้าถึง**

6.9.1 ให้เจ้าของระบบงานกำหนดสิทธิ์ในการเข้าถึงข้อมูลและระบบงานให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์ในระดับเฉพาะที่จำเป็นแก่การปฏิบัติหน้าที่ รวมทั้งต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษรและต้องมีการทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอรวมถึงกรณียกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนแปลงตำแหน่ง

6.9.2 ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษาบัญชีผู้ใช้งานและรหัสผ่านของตนให้มีความมั่นคงปลอดภัยเพียงพอ

6.9.3 พนักงานต้องมีวิธีป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล เช่น แจ้งหัวหน้าหน่วยงานทุกครั้งที่พบเห็น รวมถึงมีนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย หรือพบเห็นได้ง่าย

6.9.4 ต้องจัดทำนโยบายการใช้งานเครือข่าย ซึ่งจะต้องครอบคลุมว่าบริการใดอนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้

6.9.5 การเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัทจะกระทำได้เมื่อได้รับอนุมัติโดยหัวหน้าหน่วยงาน และหัวหน้าส่วนงานเทคโนโลยีสารสนเทศ สามารถใช้ได้เฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น และต้องถูกจำกัดการเข้าถึง ให้เฉพาะผู้ที่ได้รับอนุญาต หรือผู้ที่มีความจำเป็นต้องใช้ข้อมูลนั้น และต้องได้รับความยินยอมจากเจ้าของข้อมูลเป็นลายลักษณ์อักษรก่อน

6.9.6 การเข้าถึงระบบสารสนเทศใด ๆ ต้องได้รับการพิสูจน์ตัวตนทุกครั้งเมื่อเข้าถึงระบบสารสนเทศ และสารสนเทศของบริษัท สิทธิ์ในการเข้าถึงต้องถูกทบทวนสิทธิ์อย่างน้อยปีละ 1 ครั้ง

6.9.7 การเปลี่ยนแปลงระบบสารสนเทศ / ระบบเน็ตเวิร์ค หรือแอพพลิเคชั่นใดๆ จะต้องได้รับการตรวจสอบ และอนุญาตจากเจ้าของข้อมูล รวมถึงได้รับอนุมัติจากหัวหน้าส่วนงานเทคโนโลยีสารสนเทศ

6.9.8 ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบ โดยมาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพ และการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

6.9.9 ต้องจัดให้มีระบบ หรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านทุก 3 เดือน หรือ ตามระยะเวลาที่กำหนด

6.9.10 ต้องจำกัดและควบคุมการใช้โปรแกรมยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เช่น จำกัดการใช้งานโปรแกรมดังกล่าวให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เป็นต้น และต้องกำหนดวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์เมื่อคอมพิวเตอร์นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง รวมถึงต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูงด้วย

6.9.11 ต้องมีการแยกระบบที่มีความสำคัญสูงไว้ในบริเวณแยกต่างหาก สำหรับระบบงานนี้โดยเฉพาะ และต้องมีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับผู้ใช้งานที่จำเป็นต้องปฏิบัติงานของบริษัทจากภายนอกสำนักงาน

6.9.12 การเข้าถึงแอพพลิเคชันใด ๆ ต้องถูกควบคุมและจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตหรือได้รับมอบหมายให้มีสิทธิ์ เช่น ผู้ดูแลระบบ เป็นต้น รวมถึงการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ ต้องอนุญาตเฉพาะผู้ที่มีสิทธิ์ตามจำนวนที่ซื้อเท่านั้น

6.9.13 การควบคุมการเข้าถึงเครือข่าย ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่ายให้ผู้ที่จะเข้าใช้งานต้องกำหนดให้เส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ สำหรับใช้งานอินเตอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยของบริษัทจัดสรรไว้และออกแบบโครงสร้างโดยแบ่งโซน (Zone) การใช้งาน เพื่อทำให้การควบคุมและการป้องกันภัยคุกคามอย่างเป็นระบบ และมีประสิทธิภาพ

6.9.14 การควบคุมการเข้าถึงระบบปฏิบัติการ ต้องกำหนดสิทธิ์ให้ผู้ที่จะเข้าใช้งาน และต้องพิสูจน์ตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าใช้งาน ต้องระงับการใช้งานเมื่อผู้ใช้ไม่ใช้งานอย่างต่อเนื่องตามระยะเวลาที่กำหนด เพื่อจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศ (Session Time-out)

6.9.15 ต้องมีการแบ่งแยกระบบเครือข่ายตามกลุ่มที่ให้บริการ เช่น โซนภายในบริษัท โซนภายนอกบริษัท เป็นต้น เพื่อให้สามารถป้องกันการบุกรุกได้อย่างเป็นระบบ

6.10 **นโยบายการจัดชั้นความลับของสารสนเทศ** (Information Classification Policy)

การกำหนดเกณฑ์ในการจัดลำดับชั้นของข้อมูล เพื่อให้ข้อมูลได้ถูกจัดลำดับชั้น และได้รับการป้องกันอย่างเหมาะสม ตามแนวทางการจัดการข้อมูลในแต่ละลำดับชั้น นอกจากนี้ นโยบายยังได้กำหนดถึงบทบาทของเจ้าของข้อมูลและผู้ดูแลข้อมูลที่ เกี่ยวข้องกับการจัดลำดับชั้นของข้อมูล เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสม โดยสอดคล้องกับความสำคัญของ สารสนเทศนั้นที่มีต่อองค์กร

ข้อมูลสารสนเทศต้องมีการจัดชั้นความลับ โดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหว หากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต คณะกรรมการความมั่นคงปลอดภัยไซเบอร์และ สารสนเทศได้จัดทำเอกสารแสดงชั้นความลับสารสนเทศ เพื่อให้หน่วยงานต่าง ๆ มาลงทะเบียนเอกสารต่าง ๆ ตามลำดับชั้นที่กำหนดไว้ ดังนี้

ชั้นที่ 1 ข้อมูลเปิดเผยได้ (Public)

ข้อมูลที่บุคคลภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย

ชั้นที่ 2 ข้อมูลใช้ภายในองค์กรเท่านั้น (Internal)

เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้พนักงานทุกคนภายในองค์กรทราบได้ หรือหากต้องการ เปิดเผยต่อบุคคลภายนอกองค์กรสามารถกระทำได้ก็ต่อเมื่อเป็นบุคคลที่มีรายชื่ออยู่ในทะเบียนผู้รับสิทธิ์รับข้อมูล

ชั้นที่ 3 ข้อมูลเฉพาะกลุ่ม (Restricted)

เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้พนักงานทุกคนทราบ ข้อมูลประเภทนี้จะถูกกำหนดให้ผู้ ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานได้ทราบเท่านั้น และเป็นการใช้งานตามสิทธิ์ความจำเป็นที่ควรทราบ เพื่อให้เพียงพอต่อการปฏิบัติงาน ไม่ว่าจะเป็นการจำากัดสิทธิ์ให้พนักงานภาย ในองค์กรของกลุ่มธุรกิจ (HUB), ฝ่าย, แผนก, กลุ่มผู้ที่เกี่ยวข้อง หรือหากต้องการเปิดเผยต่อบุคคลภายนอกองค์กรก็สามารถกระทำได้ ก็ต่อเมื่อเป็นบุคคลที่มี รายชื่ออยู่ในทะเบียนผู้รับสิทธิ์การได้รับข้อมูล

ชั้นที่ 4 ข้อมูลลับ (Confidential)

เป็นข้อมูลที่มีผลทางธุรกิจของบริษัท เป็นข้อมูลซึ่งใช้งานโดยผู้ใช้บางกลุ่มขององค์กรเท่านั้น (ส่วนใหญ่เป็นผู้บริหาร) ไม่สามารถเปิดเผยให้พนักงานทุกคนหรือบุคคลภายนอกองค์กรทราบ ข้อมูลประเภทนี้จำเป็นต้องถูกเข้ารหัสและการ เข้าถึงต้องเป็นบุคคลที่มีรายชื่ออยู่ในทะเบียนผู้รับสิทธิ์การได้รับข้อมูลเท่านั้น หากต้องการเปิดเผยต่อบุคคลภายนอก องค์กรสามารถกระทำได้ก็ต่อเมื่อเป็นบุคคลที่มีรายชื่ออยู่ในทะเบียนผู้รับสิทธิ์การได้รับข้อมูลและต้องได้รับการอนุมัติ เพื่อนำไปใช้จากผู้บริหารเท่านั้น

ชั้นที่ 5 ข้อมูลส่วนบุคคล (Personal)

เป็นข้อมูลที่สามารถระบุถึงตัวตนของเจ้าของข้อมูล (Personal Identifiable Information) หรือเชื่อมโยงไปยังบุคคลนั้นได้ทั้งทางตรงและทางอ้อม ให้ใช้ภายในองค์กร ก็ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้นแล้ว ไม่สามารถเปิดเผยต่อบุคคลภายนอกก่อนได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้นๆ แล้ว

6.11 **การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ**

6.11.1 ผู้พัฒนาและผู้เป็นเจ้าของระบบต้องกำหนดความต้องการด้านความมั่นคงปลอดภัย สำหรับระบบที่จัดหาหรือพัฒนาขึ้นมาใช้งาน โดยการประเมินความเสี่ยงและระบุข้อกำหนดด้านความมั่นคงปลอดภัยเพื่อลดความเสี่ยงนั้น

6.11.2 เพื่อป้องกันความผิดพลาดของสารสนเทศ การสูญหายของสารสนเทศ หรือการใช้งานสารสนเทศผิดวัตถุประสงค์ ต้องมีการตรวจสอบข้อมูลที่เจ้าผู้พัฒนาระบบต้องกำหนดกลไกว่าข้อมูลนำเข้านั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป ต้องมีการตรวจสอบข้อมูลที่อยู่ระหว่างการประมวลผล ซึ่งผู้พัฒนาระบบต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ ในการตรวจสอบความถูกต้องและการตรวจสอบข้อมูลนำออก ซึ่งผู้พัฒนาระบบ และเจ้าของระบบต้องกำหนดกลไกเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม

6.12 **มาตรการการเข้ารหัสข้อมูล**

ต้องกำหนดนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และมีผลบังคับใช้ในบริษัท และต้องกำหนดให้มีการบริหารการจัดการสำหรับกุญแจที่ใช้ในการเข้า หรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้ จะใช้ร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดไว้ในมาตรฐานของบริษัท

6.13 **การสร้างความมั่นคงปลอดภัยในโค้ดของระบบที่ให้บริการ**

6.13.1 ต้องกำหนดมาตรการควบคุมการติดตั้งซอฟต์แวร์ใหม่ซอฟต์แวร์ไลบารี่ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งาน โดยก่อนติดตั้งจะต้องผ่านการตรวจสอบว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

6.13.2 ผู้พัฒนาระบบต้องหลีกเลี่ยงการใช้ข้อมูลจริงในการทดสอบระบบ หากจำเป็นต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน และผู้พัฒนาระบบต้องควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริง และควรเป็น Source Code ไว้ในที่ๆ ปลอดภัย

6.13.3 ต้องกำหนดขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง และตรวจสอบเมื่อระบบปฏิบัติการถูกแก้ไขหรือเปลี่ยนแปลง เพื่อให้มั่นใจว่าแอพพลิเคชันที่ทำงานอยู่นั้นทำงานผิดปกติหรือเกิดปัญหาขึ้นหรือไม่ รวมทั้งไม่แก้ไขเปลี่ยนแปลงซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นให้แก้ไขตามความจำเป็นเท่านั้น

6.13.4 ต้องป้องกันการรั่วไหลของสารสนเทศ หรือลดโอกาสที่จะทำให้การสารสนเทศเกิดการรั่วไหลออกไป และต้องกำหนดมาตรการควบคุมและตรวจสอบการว่าจ้างให้พัฒนาระบบต้องกมีความชัดเจน รวมถึงการรับรองคุณภาพระบบ และกำหนดขอบเขตในการว่าจ้างด้วย

6.13.5 เพื่อลดคามเสี่ยงจากการโจมตี โดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่ ต้องมีการติดตามข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ อย่างสม่ำเสมอ

6.14 **การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท**

6.14.1 ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท เช่น จุดอ่อนใด ๆ ให้แก่ผู้บังคับบัญชา หรือส่วนงานเทคโนโลยีสารสนเทศทันทีที่พบหรือสงสัยว่ามีสิ่งผิดปกติเกิดขึ้น และต้องกำหนดหน้าที่และความรับผิดชอบเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน โดยต้องมีการบันทึกเหตุการณ์ พิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดขึ้นจากความเสียหาย

6.14.2 ต้องเก็บรวบรวมหลักฐานตามกฎหมายหรือหลักเกณฑ์ เพื่อใช้สำหรับอ้างอิงในกระบวนการศาลหรือกฎหมายที่เกี่ยวข้องกับการดำเนินนโยบายธุรกิจที่กำหนดไว้

6.15 **การบริหารความต่อเนื่องในการดำเนินงานของบริษัท**

6.15.1 ต้องจัดลำดับความสำคัญของกระบวนการสร้างความต่อเนื่องทางธุรกิจ ระบุเหตุการณ์ที่ทำให้กระบวนการทางธุรกิจหยุดชะงัก ความเป็นไปได้และผลกระทบที่จะเกิดขึ้น และแผนบริหารความต่อเนื่องทางธุรกิจจะจัดทำขึ้นสำหรับระบบงานที่มีความสำคัญ

6.15.2 แผนบริหารความต่อเนื่องทางธุรกิจทั้งหมดจะได้รับการทดสอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเมื่อเกิดเหตุฉุกเฉิน แผนที่นำมาทดสอบสามารถใช้งานได้จริง

6.15.3 ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

6.15.4 จัดทำระบบสำรองข้อมูลของระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของบริษัทสามารถให้บริการได้อย่างต่อเนื่อง และมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของผู้ดูแลระบบในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมในระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง และแผนบริหารความต่อเนื่องทางธุรกิจดังกล่าวต้องถูกทบทวนและปรับปรุงหากมีความจำเป็น

6.16 **การป้องกันโปรแกรมไม่ประสงค์ดี**

บริษัทและส่วนงานเทคโนโลยีสารสนเทศจะต้องใช้ซอฟต์แวร์ที่มีการบวนการในการจัดการ และป้องกันโปรแกรมไม่ประสงค์ดี และพนักงานทุกคนต้องให้ความร่วมมือปฏิบัติตามนโยบายดังกล่าว รวมทั้งไม่ติดตั้งซอฟต์แวร์เอง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ทำงานแทน

6.17 **การปฏิบัติตามข้อกำหนด**

6.17.1 ผู้ใช้งานทุกคนมีหน้าที่ต้องทำความเข้าใจ และปฏิบัติตามนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด ทั้งนี้รวมถึงแต่ไม่จำกัดเฉพาะ

- นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ 2560
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
- พ.ร.บ. ลิขสิทธิ์
- พ.ร.บ. เครื่องหมายการค้า

6.17.2 ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบสารสนเทศของบริษัท ถือเป็นทรัพย์สินของบริษัท ยกเว้นข้อมูลที่เป็นทรัพย์สินของลูกค้าหรือบุคคลภายนอก ซอฟต์แวร์หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิในทรัพย์สินหรือสิทธิบัตรของบุคคลภายนอก

6.17.3 ต้องกำหนดให้มีการป้องกันข้อมูล ที่เกี่ยวกับข้อกำหนดทางกฎหมายและแนวปฏิบัติข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ รวมถึงต้องมีมาตรการป้องกันข้อมูลส่วนตัวตามที่ระบุไว้ในกฎหมาย แนวปฏิบัติและสัญญาที่เกี่ยวข้อง

6.17.4 ต้องกำหนดให้มีการป้องกัน สารสนเทศ ระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่าย ไม่ให้ใช้งานไปในทางที่ผิดหรือโดยไม่มีสิทธิ์ และต้องกำหนดให้ใช้มาตรการเข้ารหัสข้อมูลโดยให้ยึดถือตามหรือสอดคล้องกับข้อตกลงทางกฎหมาย

6.17.5 การทบทวน ตรวจสอบการใช้งานระบบทุกระบบเป็นสิทธิ์ที่บริษัทสามารถกระทำได้ หากบริษัทเห็นว่าจำเป็นโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

6.17.6 ต้องมีการตรวจสอบระบบว่ามีความมั่นคงปลอดภัยเพียงพอหรือไม่ โดยใช้ซอฟต์แวร์ค้นหาช่องโหว่ และทดสอบการโจมตีระบบเพื่อตรวจข้อบกพร่องของระบบด้วย

6.17.7 ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ และต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ ไม่ให้นำซอฟต์แวร์ไปใช้ในทางที่ผิด โดยกำหนดให้มีการแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบระบบสารสนเทศ

7. **การแจกจ่ายเอกสารนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**

เอกสารนโยบายฉบับนี้ จะจัดให้ผู้ใช้งานทุกคนได้อ่าน และทำความเข้าใจ

บทลงโทษ

ผู้ใช้งานคนใดที่ฝ่าฝืนนโยบายฉบับนี้ บริษัทพิจารณาลงโทษทางวินัยตามระเบียบการบริหารงานบุคคล รวมทั้งอาจมีความรับผิดทั้งทางอาญาและทางแพ่ง

การทบทวนนโยบาย

หัวหน้าส่วนงานเทคโนโลยีสารสนเทศ ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำ อย่างน้อยปีละ 1 ครั้ง และต้องเสนอให้ประธานกรรมการบริหารอนุมัติ หากมีการเปลี่ยนแปลง

ทั้งนี้ให้มีผลตั้งแต่วันที่ 30 เมษายน พ.ศ. 2568

(นายพิเทพ จันทร์เสรีกุล)

ประธานกรรมการบริษัท

บริษัท กรุงไทยคาร์เร้นท์ แอนด์ ลีส จำกัด (มหาชน)