# นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. **วัตถุประสงค์ (Objectives)**

เพื่อรักษาซึ่งความมั่นคงปลอดภัยของข้อมูลอันประกอบไปด้วย การรักษาความลับของข้อมูล (Confidential) การรักษาความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ของบริษัท ทิพย กรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน) ให้มีความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของบริษัทฯ ได้อย่างต่อเนื่องและมีประสิทธิภาพ ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศ รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัทฯ

2. **การบังคับใช้ (Enforcement)**

นโยบายฉบับนี้มีผลบังคับใช้กับ บริษัททิพย กรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน) และบริษัทย่อย รวมถึงผู้บริหาร พนักงาน และผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

3. **นิยาม (Define)**

**บริษัทฯ** หมายถึง บริษัท ทิพย กรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน)

**พนักงาน** หมายถึง ทรัพยากรด้านบุคลากรของบริษัทฯ

**ผู้ให้บริการภายนอก** หมายถึง นิติบุคคลหรือตัวแทนนิติบุคคลที่ปฏิบัติงานให้กับบริษัทฯ โดยมีการว่าจ้างตามระเบียบบริษัทฯ ซึ่งมีระยะเวลาปฏิบัติงานตามช่วงเวลาที่ได้มีการตกลงกันตามสัญญา

**ทรัพย์สินด้านสารสนเทศ** หมายถึง ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด

**ระบบสารสนเทศ** หมายถึง ระบบที่มีการนำฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร แนวปฏิบัติ และข้อมูล ซึ่งทำงานประสานกันเพื่อจัดเตรียมสารสนเทศให้กับบริษัทฯ

**สารสนเทศ** หมายถึง ข้อมูลต่างๆ ที่ได้ผ่านการเปลี่ยนแปลง ประมวลผล หรือวิเคราะห์สรุปผลด้วยวิธีการต่างๆ แล้วเก็บรวบรวมไว้ เพื่อนำมาใช้ประโยชน์ตามต้องการ การประมวลผลเป็นการนำข้อมูลจากแหล่งต่างๆ ที่เก็บรวบรวมไว้มาผ่านกระบวนการต่างๆ เพื่อแปรสภาพข้อมูลให้เป็นระบบที่อยู่ในรูปแบบที่ต้องการและนำไปใช้งานกับธุรกิจของบริษัทฯ

## 4. การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance)

การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ มีวัตถุประสงค์เพื่อทำให้แน่ใจว่าบริษัทฯ สามารถบรรลุเป้าหมายที่กำหนดไว้ โดยนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุน และสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้งานได้อย่างมีประสิทธิภาพ การบริหารจัดการด้านเทคโนโลยีสารสนเทศที่ดีนั้นต้องมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากร และข้อมูลที่มีประสิทธิภาพเพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมายของบริษัทฯ และการบริหารความเสี่ยงที่เหมาะสม รวมทั้งมีการรายงานและติดตามการดำเนินงาน เพื่อให้มั่นใจว่า เทคโนโลยีที่บริษัทฯ นำมาใช้งาน สามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจ และสร้างศักยภาพในการแข่งขันให้กับบริษัทฯ ได้อย่างถูกต้องและเหมาะสม

## 5. นโยบาย

บริษัทฯ กำหนดนโยบายเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศในประเด็นสำคัญดังต่อไปนี้

### 5.1. การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

5.1.1. บริษัทฯ ได้กำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและทำการสื่อสารนโยบายดังกล่าว เพื่อสร้างความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง และให้มีการทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ

### 5.2. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

5.2.1 การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ บริษัทฯ จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือบริหารจัดการความเสี่ยงที่มีอยู่ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ทั้งความเสี่ยงด้านกายภาพและด้านสภาพแวดล้อม

5.2.2 ความเสี่ยงการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต ซึ่งได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์เครือข่ายและอุปกรณ์อื่น ต้องมีการควบคุมการเข้าถึงและควบคุมการใช้งานเฉพาะผู้ได้รับอนุญาตเท่านั้น

5.2.3 ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของบริษัทฯ เพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัยหรือไม่

ประสงค์ดี เช่น การดาวน์โหลดโปรแกรมจากภายนอกมาติดตั้ง ซึ่งอาจจะมีมัลแวร์ หรือไวรัสคอมพิวเตอร์ หรือมีช่องโหว่เชื่อมต่อเครือข่ายภายนอก เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน

5.2.4 ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ ต้องมีการตรวจสอบและเฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต โดยมีการจัดทำระบบป้องกันการเข้าถึงและการโจมตีจากภายนอกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงานใช้งาน เช่น ระบบป้องกันการเข้าออกใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ การกรองข้อมูลรับส่งอีเมล เป็นต้น

5.2.5 ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิการใช้งานและการเข้าถึงระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายต่างๆ และข้อมูล ให้เป็นไปตามสิทธิที่พึงมี เพื่อป้องกันการเข้าแก้ไขหรือเปลี่ยนแปลงข้อมูลที่เกิดขึ้นจากการจัดการสิทธิที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลเกินกว่าหน้าที่ และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้

5.2.6 ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉินที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้งสถานการณ์อื่น เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น

5.2.7 ความเสี่ยงด้านบริหารจัดการที่เกิดขึ้นจากแนวนโยบายที่ทำการใช้งานอยู่อาจไม่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

**5.3 การบริหารจัดการทรัพย์สิน (Asset Management)**

5.3.1 ทรัพย์สินด้านสารสนเทศ ต้องมีการจัดทำบัญชีทรัพย์สิน โดยผู้เป็นเจ้าของข้อมูลนั้นต้องร่วมจัดทำทะเบียนรายการทรัพย์สินด้านสารสนเทศรวมถึงต้องจัดทำและจัดการป้ายชื่อ สำหรับปิดฉลากเอกสารข้อมูลของอุปกรณ์ทรัพย์สินด้านสารสนเทศ

5.3.2 บริษัทฯ ต้องกำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันทรัพย์สินด้านสารสนเทศให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม เอกสารหรือสิ่งตีพิมพ์ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับ ซึ่งมีการกำหนดชั้นความลับไว้ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับข้อมูลนั้น

5.3.3 การใช้งานทรัพย์สินที่เหมาะสม ต้องมีการจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรเพื่อป้องกันความเสียหายต่อทรัพย์สินด้านสารสนเทศ

**5.4 ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)**

5.4.1 พนักงานและผู้ให้บริการภายนอกต้องตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง และเพื่อป้องกันผลประโยชน์ของบริษัทฯ ซึ่งเป็นส่วนหนึ่งของกระบวนการสิ้นสุดหรือเปลี่ยนการจ้างงาน

5.4.2 ต้องมีการกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับผู้ใช้งาน หรือที่ว่าจ้างหน่วยงานภายนอกมาปฏิบัติงาน รวมทั้งกำหนดมาตรการป้องกันและดูแลรักษาความปลอดภัยสำหรับสารสนเทศของบริษัทฯ

5.4.3 ต้องมีการตรวจสอบคุณสมบัติของผู้สมัครเข้าทำงานทุกกรณีโดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา หรือบริษัทฯ ที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และต้องสร้างความตระหนักเรื่องความมั่นคงปลอดภัยเบื้องต้นให้พนักงานเข้าใหม่พร้อมทั้งจัดให้พนักงานมีการลงนามไม่เปิดเผยความลับของบริษัทฯ ในฝ่ายหรือส่วนงานที่สามารถเข้าถึงข้อมูลอ่อนไหวของบริษัทฯ

5.4.4 ต้องกำหนดให้ผู้ใช้งานที่ได้รับการว่าจ้างต้องปฏิบัติตามมาตรการความมั่นคงปลอดภัยให้สอดคล้องกับนโยบายของบริษัทฯ ที่กำหนดไว้

5.4.5 จัดอบรมให้ความรู้แก่ผู้ใช้งานทุกคนเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและสารสนเทศ ต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากร ถ้ามีการเปลี่ยนแปลงทางด้านความมั่นคงปลอดภัยต้องแจ้งให้พนักงานทราบ

5.4.6 ต้องมีการกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และแนวปฏิบัติของบริษัทฯ หากเป็นการละเมิดข้อกฎหมายบทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำ และเป็นไปตามระเบียบของบริษัทฯ

5.4.7 หากมีการแต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงตำแหน่งใดๆ ฝ่ายทรัพยากรบุคคลและบริหารองค์กรต้องแจ้งให้ผู้รับการว่าจ้างทราบ และผู้รับการว่าจ้าง

ต้องปฏิบัติตามเงื่อนไขในสัญญาจ้างจนกว่าจะสิ้นสุดการว่าจ้าง และพนักงานซึ่งพ้นตำแหน่งจากการจ้างงานไม่ว่ากรณีใด ต้องคืนทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศ เช่น กุญแจ บัตรประจำตัวพนักงาน อุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่างๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงานซึ่งฝ่ายเทคโนโลยีสารสนเทศต้องถอดถอนสิทธิการเข้าใช้งานดังกล่าวด้วย

**5.5 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)**

5.5.1 พนักงาน ผู้ให้บริการภายนอกต้องปฏิบัติตามแนวทางเกี่ยวกับความมั่นคงปลอดภัยด้านสถานที่และสภาพแวดล้อมที่บริษัทฯ กำหนด เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบงานสารสนเทศของบริษัทฯ รวมทั้งป้องกันการหยุดชะงักต่อการดำเนินงานของบริษัทฯ

5.5.2 ต้องมีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ และต้องจัดให้มีการป้องกันภัยคุกคามต่างๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อความไม่สงบ เป็นต้น รวมถึงการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัยต้องมีการจัดการป้องกันที่เพียงพอ

5.5.3 ในการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอกต้องมีบริเวณเฉพาะที่จัดไว้ต่างหาก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศของบริษัทฯโดยไม่ได้รับอนุญาต

5.5.4 พนักงานต้องป้องกันอุปกรณ์ของสำนักงาน เพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

5.5.5 ทรัพย์สินด้านสารสนเทศจะต้องอยู่ในพื้นที่ที่เหมาะสมมีความปลอดภัย มีการจำแนกพื้นที่ในการใช้งานระบบสารสนเทศอย่างเหมาะสม มีการแยกศูนย์คอมพิวเตอร์ออกจากสถานที่ทำงานทั่วไปและกั้นเป็นห้องต่างหาก มีการควบคุมการเข้า-ออกพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยให้เข้า-ออกได้เฉพาะผู้ที่มีหน้าที่รับผิดชอบและผู้ที่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

5.5.6 ต้องมีระบบไฟฟ้าสำรองสำหรับอุปกรณ์ที่มีความสำคัญ เพื่อให้สามารถทำงานได้ตลอดเวลาและต้องมีการตรวจสอบระบบไฟฟ้าสำรอง เพื่อเป็นการลดความเสียหายที่อาจจะเกิดขึ้น

5.5.7 การเดินสายเคเบิลต่างๆ ต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการเดินสายนั้นต้องติดป้ายกำกับให้รู้ต้นทางปลายทางของสาย

5.5.8 ต้องบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอหรือตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

5.5.9 ต้องมีมาตรการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น

5.5.10 พนักงานต้องมีการตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญที่อยู่ในอุปกรณ์ดังกล่าวได้ถูกลบทิ้งหรือถูกบันทึกทับก่อนที่จะนำอุปกรณ์ดังกล่าวทิ้งไป โดยต้องเป็นไปตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด

5.5.11 ต้องมีขั้นตอนปฏิบัติสำหรับการจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

5.5.12 ต้องมีการกำหนดมาตรการการป้องกันเอกสารในระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

5.5.13 ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

## 5.6 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

5.6.1 พนักงาน ผู้ให้บริการภายนอก ต้องปฏิบัติตามแนวทางเกี่ยวกับความมั่นคงปลอดภัยด้านบริการที่ได้รับจากผู้ให้บริการที่บริษัทฯ กำหนด เพื่อให้มีการป้องกันทรัพย์สินของบริษัทฯ ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก และเพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

5.6.2 ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการโดยหน่วยงานภายนอก เช่น มีการยอมรับนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ และขอบเขต รายละเอียด ระดับการให้บริการ ต้องได้รับการตรวจสอบจากฝ่ายกฎหมาย รวมถึงสัญญาในการไม่เปิดเผยข้อมูลของบริษัทฯ เป็นต้น

5.6.3 หน่วยงานภายนอกหรือบุคคลภายนอกอื่นๆ ที่ได้รับอนุญาตในการเข้าถึงระบบสารสนเทศของบริษัทฯ ต้องยอมรับและปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ

5.6.4 บริษัทฯ จะประเมินความเสี่ยงในการเข้าถึงระบบสารสนเทศ หรือที่มีผลกระทบต่อบริษัทฯ ของหน่วยงานภายนอกหรือบุคคลภายนอกอื่นๆ ถ้าจำเป็นต้องมีการเปิดเผยข้อมูลนั้นออกไป หน่วยงานภายนอกหรือบุคคลภายนอกนั้นต้องเซ็นสัญญาว่าจะไม่เปิดเผยความลับของบริษัทฯ

5.6.5 ต้องตรวจสอบการให้บริการหรือสัญญาที่ทำกับหน่วยงานภายนอกและบุคคลภายนอกที่เข้ามาให้บริการกับบริษัทฯ โดยมีการทบทวนอย่างสม่ำเสมอตามความจำเป็น รวมถึงต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เช่น เมื่อมีการปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การเปลี่ยนเทคโนโลยีใหม่ เป็นต้น

**5.7 การควบคุมการเข้าถึง (Access Control)**

5.7.1 ต้องกำหนดให้มีขั้นตอนสำหรับการลงทะเบียนต่างๆ เพื่อให้มีสิทธิและควบคุมสิทธิในการเข้าถึงสารสนเทศและระบบสารสนเทศของบริษัทฯ ตามความจำเป็น รวมถึงขั้นตอนการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกหรือเปลี่ยนแปลงตำแหน่ง เป็นต้น รวมถึงต้องมีกระบวนการจัดการรหัสผ่านสำหรับผู้ใช้งาน เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานตามความเหมาะสมหรือที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย

5.7.2 ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษาบัญชีผู้ใช้งาน และรหัสผ่านของตนให้มีความมั่นคงปลอดภัยเพียงพอ

5.7.3 พนักงานต้องมีวิธีป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล เช่น แจ้งหัวหน้าหน่วยงาน หรือเจ้าหน้าที่รักษาความปลอดภัยทุกครั้งที่พบเห็น รวมถึงมีนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัยหรือพบเห็นได้ง่าย

5.7.4 ต้องจัดทำแนวทางการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมว่าบริการใดอนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้

5.7.5 การเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัทฯ จะกระทำได้เมื่อได้รับอนุมัติโดยหัวหน้าหน่วยงานและหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ โดยสามารถใช้ได้เฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น และต้องถูกจำกัดการเข้าถึงให้เฉพาะผู้ที่ได้รับอนุญาต หรือผู้ที่มีความจำเป็นต้องใช้ข้อมูลนั้น และต้องได้รับความยินยอมจากเจ้าของข้อมูล

5.7.6 การเข้าถึงระบบสารสนเทศใดๆ ต้องได้รับการพิสูจน์ตัวตนทุกครั้งเมื่อเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัทฯ สิทธิในการเข้าถึงต้องถูกทบทวนสิทธิอย่างน้อยปีละ 1 ครั้ง

5.7.7 การเปลี่ยนแปลงระบบสารสนเทศ /ระบบเน็ตเวิร์ค หรือแอพพลิเคชั่นใดๆ จะต้องได้รับการตรวจสอบและอนุญาตจากเจ้าของข้อมูล รวมถึงได้รับอนุมัติจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

5.7.8 ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ โดยมาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

5.7.9 ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

5.7.10 ต้องจำกัดและควบคุมการใช้โปรแกรมยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เช่น จำกัดการใช้งานโปรแกรมดังกล่าวให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เป็นต้น และต้องกำหนดวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ เพื่อเครื่องคอมพิวเตอร์นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง รวมถึงต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูงด้วย

5.7.11 ต้องมีการแยกระบบที่มีความสำคัญสูงไว้ในบริเวณแยกต่างหากสำหรับระบบงานนี้โดยเฉพาะ และต้องมีการกำหนดนโยบาย แผนงาน และขั้นตอนการปฏิบัติสำหรับผู้ใช้งานที่จำเป็นต้องปฏิบัติงานของบริษัทฯ จากภายนอกสำนักงาน

5.7.12 การเข้าถึงแอพพลิเคชั่นใดๆ ต้องถูกควบคุมและจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตหรือได้รับมอบหมายให้มีสิทธิ เช่น ผู้ดูแลระบบ เป็นต้น รวมถึง

การใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ต้องอนุญาตเฉพาะผู้ที่มีสิทธิตามจำนวนที่ซื้อเท่านั้น

5.7.13 การควบคุมการเข้าถึงเครือข่าย ต้องกำหนดสิทธิในการเข้าถึงเครือข่ายให้ผู้ที่จะเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเตอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยของบริษัทฯ ที่จัดสรรไว้ และออกแบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

5.7.14 การควบคุมการเข้าถึงระบบปฏิบัติการ ต้องกำหนดสิทธิให้ผู้ที่จะเข้าใช้งานและต้องพิสูจน์ตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าใช้งาน ต้องระงับการใช้งานเมื่อผู้ใช้ไม่ใช้งานอย่างต่อเนื่องตามระยะเวลาที่กำหนด เพื่อจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศ (Session Time-out) การควบคุมการเข้าถึงคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารแบบพกพา (Mobile Computing and Communications) บริษัทฯ มีนโยบายให้ผู้ใช้งานใช้อุปกรณ์สื่อสารแบบพกพาเฉพาะที่เป็นของบริษัทฯ ในการเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัทฯ หากมีความจำเป็นต้องใช้อุปกรณ์สื่อสารแบบพกพาส่วนตัวในการเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัทฯ ต้องขออนุญาตเป็นการเฉพาะ และอุปกรณ์สื่อสารแบบพกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัทฯ ต้องเป็นอุปกรณ์สื่อสารแบบพกพาที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัย หรือที่ละเมิดลิขสิทธิ์ตามนโยบายที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด

5.7.15 ต้องมีการแบ่งแยกระบบเครือข่ายตามกลุ่มที่ให้บริการ เช่น โซนภายในบริษัทฯ โซนภายนอกบริษัทฯ เป็นต้น เพื่อให้สามารถป้องกันการบุกรุกได้อย่างเป็นระบบ

## 5.8 การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

5.8.1 พนักงาน ผู้ให้บริการภายนอกต้องปฏิบัติตามนโยบายการพัฒนาระบบอย่างมั่นคงปลอดภัย เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบ ตลอดจนวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย

5.8.2 ผู้พัฒนาและผู้เป็นเจ้าของระบบต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบที่จัดหาหรือพัฒนาขึ้นมาใช้งาน โดยการประเมินความเสี่ยงและระบุข้อกำหนดด้านความมั่นคงปลอดภัยเพื่อลดความเสี่ยงนั้น

5.8.3 เพื่อป้องกันความผิดพลาดของข้อมูลสารสนเทศ การสูญหายของข้อมูลสารสนเทศหรือการใช้งานสารสนเทศผิดวัตถุประสงค์ ผู้พัฒนาระบบต้องมีการกำหนดขั้นตอนการตรวจสอบความถูกต้องของข้อมูลที่นำเข้าระบบข้อมูลที่อยู่ในระหว่างการประมวลผล และข้อมูลที่นำออกจากระบบเพื่อเป็นการทบทวนว่าข้อมูลสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและสมบูรณ์

## 5.9 การเข้ารหัสข้อมูล (Cryptography)

5.9.1 ต้องกำหนดให้มีการควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้ในบริษัทฯ และต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานของบริษัทฯ

## 5.10 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

5.10.1 ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทฯ เช่น จุดอ่อนใดๆ ให้แก่ผู้บังคับบัญชา หรือฝ่ายเทคโนโลยีสารสนเทศทันทีที่พบหรือสงสัยว่ามีสิ่งผิดปกติเกิดขึ้นและต้องกำหนดหน้าที่และความรับผิดชอบเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน โดยต้องมีการบันทึกเหตุการณ์ พิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดขึ้นจากความเสียหาย

5.10.2 ต้องเก็บรวบรวมหลักฐานตามกฎหรือหลักเกณฑ์เพื่อใช้สำหรับอ้างอิงในกระบวนการของศาลหรือกระบวนการอื่นที่เกี่ยวข้อง

## 5.11 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

5.11.1 พนักงาน ผู้ให้บริการภายนอกต้องปฏิบัติตามแนวทางเกี่ยวกับความมั่นคงปลอดภัยด้านการสื่อสารที่บริษัทฯ กำหนด เพื่อให้มีการป้องกันสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ และเพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในบริษัทฯ หรือถ่ายโอนกับหน่วยงานภายนอก

5.11.2 ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน เช่น ขั้นตอนการกู้คืนระบบ ขั้นตอนการบำรุงรักษาและดูแลระบบ เป็นต้น และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานเมื่อมีการเปลี่ยนแปลงขั้นตอนหรือผู้รับผิดชอบ และต้องทบทวนอย่างน้อยปีละ 1 ครั้ง และต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบคอมพิวเตอร์ ระบบเครือข่าย คอมพิวเตอร์แม่ข่าย ฮาร์ดแวร์ และซอฟต์แวร์

5.11.3 ต้องมีการแบ่งหน้าที่ความรับผิดชอบของผู้ดูแลระบบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต

5.11.4 ต้องมีการแยกระบบสำหรับการพัฒนาและทดสอบแยกออกจากระบบงานจริง เพื่อป้องกันการเข้าถึงข้อมูลหรือเปลี่ยนแปลงต่อระบบงานที่ให้บริการจริงจากผู้ที่ไม่ได้รับอนุญาต และต้องติดตามสภาพการใช้งาน การวิเคราะห์ขีดความสามารถของทรัพยากรสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

5.11.5 การยอมรับระบบใหม่ต้องจัดให้มีเกณฑ์ในการยอมรับ และจัดให้มีการทดสอบระบบใหม่ก่อนที่จะตรวจรับระบบนั้นอย่างเป็นลายลักษณ์อักษร

**5.12 ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)**

5.12.1 พนักงาน ผู้ให้บริการภายนอกที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามแนวทางการบริหารจัดการความต่อเนื่องของระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของบริษัทฯ สามารถให้บริการได้อย่างต่อเนื่อง และเพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ

5.12.2 ต้องจัดลำดับความสำคัญของกระบวนการสร้างความต่อเนื่องทางธุรกิจ ระบุเหตุการณ์ที่ทำให้กระบวนการทางธุรกิจหยุดชะงัก ความเป็นไปได้ และผลกระทบที่จะเกิดขึ้น และแผนบริหารความต่อเนื่องทางธุรกิจจะจัดทำขึ้นสำหรับระบบงานที่มีความสำคัญ

5.12.3 แผนบริหารความต่อเนื่องทางธุรกิจทั้งหมดจะได้รับการทดสอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเมื่อเกิดเหตุฉุกเฉิน แผนที่นำมาทดสอบสามารถใช้งานได้จริง

5.12.4 ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

5.12.5 จัดทำระบบสำรองข้อมูลของระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของบริษัทฯ สามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของผู้ดูแลระบบในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมในกรณีฉุกเฉินหรือในกรณีที่ไม่สามารถดำเนินการได้อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง และแผนบริหารความต่อเนื่องทางธุรกิจดังกล่าวต้องถูกทบทวนและปรับปรุงหากมีความจำเป็น

## 5.13 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

5.13.1 บริษัทฯ และฝ่ายเทคโนโลยีสารสนเทศจะต้องใช้ซอฟต์แวร์ที่มีกระบวนการในการจัดการ และป้องกันโปรแกรมไม่ประสงค์ดี และพนักงานทุกคนต้องให้ความร่วมมือปฏิบัติตามนโยบายดังกล่าว รวมทั้งไม่ติดตั้งซอฟต์แวร์เอง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ทำงานแทน

5.13.2 พนักงาน ผู้ให้บริการต้องปฏิบัติตามแนวทางเกี่ยวกับความมั่นคงปลอดภัยด้านการปฏิบัติงาน เพื่อให้การปฏิบัติงานกับสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบงานสารสนเทศของบริษัทฯ เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย ได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี ได้รับการป้องกันการสูญหายของข้อมูล เพื่อให้ระบบงานสารสนเทศมีการบันทึกเหตุการณ์ และจัดทำหลักฐาน มีการทำงานที่ถูกต้อง และมีการป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค และเพื่อลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบให้บริการ

## 5.14 ความสอดคล้อง (Compliance)

5.14.1 พนักงาน ผู้ให้บริการภายนอกต้องปฏิบัติตามกฎหมาย มาตรฐาน และข้อบังคับ เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้างที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และเพื่อให้มี

การปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

- นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
- พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537
- พระราชบัญญัติเครื่องหมายการค้า พ.ศ. 2534
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- และ / หรือ พระราชบัญญัติ ที่เกี่ยวข้อง

5.14.2 ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบสารสนเทศของบริษัทฯ ถือเป็นทรัพย์สินของบริษัทฯ ยกเว้นข้อมูลที่เป็นทรัพย์สินของลูกค้าหรือบุคคลภายนอก ซอฟต์แวร์ หรือวัสดุอื่นๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตรหรือลิขสิทธิ์ของบุคคลภายนอก

5.14.3 ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและแนวปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ รวมถึงต้องมีมาตรการป้องกันข้อมูลส่วนตัวตามที่ระบุไว้ในกฎหมาย แนวปฏิบัติ และสัญญาที่เกี่ยวข้อง

5.14.4 ต้องกำหนดให้มีการป้องกันสารสนเทศ ระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่าย ไม่ให้ใช้งานไปในทางที่ผิดหรือโดยไม่มีสิทธิ และต้องกำหนดให้ใช้มาตรการเข้ารหัสข้อมูล โดยให้ยึดถือตามหรือสอดคล้องกับข้อตกลงทางกฎหมาย

5.14.5 การทบทวน ตรวจสอบการใช้งานระบบทุกระบบเป็นสิทธิที่บริษัทฯ สามารถกระทำได้หากบริษัทฯ เห็นว่าจำเป็น โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

5.14.6 ต้องมีการตรวจสอบระบบว่ามีความมั่นคงปลอดภัยเพียงพอหรือไม่โดยใช้ซอฟต์แวร์ค้นหาช่องโหว่ และทดสอบการโจมตีระบบเพื่อตรวจข้อบกพร่องของระบบด้วย

5.14.7 ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ และต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ ไม่ให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด โดยกำหนดให้มีการแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบระบบสารสนเทศ

## 6. การลงโทษ

หากพบการกระทำความผิดฝ่าฝืนนโยบายฉบับนี้ บริษัทฯ จะพิจารณาลงโทษทางวินัยตามข้อบังคับเกี่ยวกับการทำงาน และ/หรืออาจมีการดำเนินคดีทางกฎหมาย

## 7. ข้อยกเว้น

หากพนักงาน หรือผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ไม่สามารถปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ หรือแนวทางที่บริษัทฯ กำหนดไว้ได้ ให้ชี้แจงเหตุผล และทำหนังสือขออนุญาตให้ผู้มีอำนาจอนุมัติเป็นกรณีไป ซึ่งข้อยกเว้นนั้นต้องมีระบบรักษาความปลอดภัยที่เหมาะสมมาทดแทนด้วย