บริษัท พีเอ็มซี เลเบิล แมททีเรียลส์ จำกัด (มหาชน)

นโยบายด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศ

บันทึกการแก้ไข

ครั้งที่	วันที่	รายละเอียดการแก้ไข	เหตุผล	อนุมัติโดย
00	25 ก.พ.65	จัดทำครั้งแรก	-	BOD.2/2565
01	7 เม.ย. 66	แก้ไข ชื่อบริษัทจากบริษัท จำกัด เป็นบริษัทมหาชน และ Vision and Mission ซึ่งได้ปรับแก้ไขใหม่ (BOD 6/2565	แปรสภาพเป็นบริษัทมหาชน	BOD. 2/2566
02				

สารบัญ

นโยบายด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศ

นโยบายด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท พีเอ็มซี เลเบิล แมททีเรียลส์ จำกัด (มหาชน) (“บริษัทฯ”) ฉบับนี้ จัดทำขึ้นเพื่อให้ระบบสารสนเทศของบริษัทฯ และบริษัทในเครือมีการควบคุมภายในที่ดี มีความมั่นคงปลอดภัยถูกต้องเชื่อถือได้ สามารถดำเนินงานได้อย่างต่อเนื่อง และสามารถป้องกันรักษาสารสนเทศที่เป็นความลับของบริษัทฯ และบริษัทในเครือ ทั้งที่เป็นข้อมูลของบริษัทฯ บริษัทในเครือ และข้อมูลส่วนบุคคลอื่น ๆ

1. วัตถุประสงค์

1. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของบริษัทฯ และบริษัทในเครือ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผลและตรงตามวัตถุประสงค์ที่กำหนดไว้
2. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท และบริษัทในเครือ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของบริษัทฯ และบริษัทในเครือ
3. เพื่อป้องกันไม่ให้ระบบสารสนเทศ และสารสนเทศของบริษัทฯ และบริษัทในเครือ ถูกบุกรุก เปลี่ยนแปลง ขโมย ทำลาย หรือการกระทำอื่น ๆ ที่อาจสร้างความเสียหายต่อบริษัท
4. เพื่อสร้างความมั่นใจให้กับบุคคลภายนอกที่เป็นคู่ค้า หรือผู้มีส่วนได้เสียต่าง ๆ ว่าข้อมูลส่วนบุคคลจะได้รับการปกป้องตามมาตรฐานความปลอดภัยของบริษัทฯ
5. เพื่อเผยแพร่ให้ผู้ใช้งาน และบุคคลภายนอก ซึ่งบริษัทฯ หรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิในการเข้าถึงข้อมูลหรือระบบสารสนเทศได้รับทราบและถือปฏิบัติอย่างเคร่งครัด

2. ขอบเขต

นโยบายฉบับนี้ใช้กับบริษัทฯ และบริษัทในเครือ ตลอดจนกรรมการ พนักงาน เจ้าหน้าที่ ที่ได้รับอนุญาตให้ใช้ระบบเครือข่ายคอมพิวเตอร์ แม่ข่าย ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ คอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสารแบบพกพา หรืออุปกรณ์สื่อสารโทรคมนาคม เพื่อเข้าถึงสารสนเทศของบริษัทฯ และบริษัทในเครือ

3. หน้าที่ความรับผิดชอบ

3.1. หน้าที่ของประธานเจ้าหน้าที่บริหาร

- กำหนดกลยุทธ์ในภาพรวม ควบคุมการปฏิบัติงานในบริษัท ให้สอดคล้องกับนโยบายด้านความปลอดภัยสารสนเทศของบริษัทฯ

3.2. หน้าที่ของหัวหน้าส่วนงานเทคโนโลยีสารสนเทศ

- ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้งจัดหา และพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัทฯ
- ดูแลทรัพยาการด้านสารสนเทศของบริษัทฯ ให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

3.3. หน้าที่ของผู้บริหารระดับสูงทางด้านการรักษาความมั่นคงปลอดภัยให้กับโครงสร้างเครือข่ายและความปลอดภัยของข้อมูลสารสนเทศ

- กำหนดเป้าหมาย นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ของบริษัทฯ
- จัดการพัฒนานโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้บริษัทได้มาซึ่งการรักษาความลับของข้อมูล การรักษาความถูกต้องของข้อมูล และเสถียรภาพความมั่นคงของระบบ
- จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่าง ๆ ที่อาจเกิดขึ้นกับระบบ รวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจเพื่อกู้ระบบยามฉุกเฉิน
- มีการบริหารความเสี่ยง และการวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหาที่กระทบกับการดำเนินธุรกิจของบริษัทฯ
- นำเสนอผู้บริหารระดับสูง เช่น ประธานเจ้าหน้าที่บริหาร ประธานฝ่ายสารสนเทศ เรื่องแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง
- เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ๆ ทางด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ

3.4. หน้าที่ของผู้ใช้งาน

- ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ โดยเคร่งครัด
- ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์ และข้อมูลสารสนเทศของบริษัทฯ สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของบริษัทฯ ให้มีความปลอดภัย
- รายงานต่อบริษัททันที เมื่อพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรม สารสนเทศ รวมถึงระบบสารสนเทศ ที่อาจสร้างความเสียหายต่อบริษัท

3.5. หน้าที่ของหัวหน้าหน่วยงาน

- ชี้แจงและส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายด้านความปลอดภัยสารสนเทศ และตักเตือนลงโทษทางวินัยกรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

3.6. หน้าที่ของเจ้าหน้าที่รักษาความปลอดภัย

- ร่างนโยบาย และระเบียบในการดำเนินการด้านนโยบายด้านความปลอดภัยสารสนเทศ

3.7. หน้าที่ของเจ้าของข้อมูลและสารสนเทศ

- จัดให้มีการจัดทำเอกสาร มาตรการและขั้นตอนควบคุมการเข้าถึงข้อมูล ให้เป็นไปตามนโยบายด้านความปลอดภัยสารสนเทศของบริษัทฯ
- ดูแลให้พนักงานปฏิบัติตามนโยบายด้านความปลอดภัยสารสนเทศของบริษัทฯ
- ควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศ และระบบคอมพิวเตอร์ภายใต้หน้าที่และความรับผิดชอบ
- รายงานเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศ

- แจ้งส่วนงานเทคโนโลยีสารสนเทศเพื่อลบหรือเปลี่ยนแปลงสิทธิเมื่อมีการเปลี่ยนแปลงพนักงาน อำนาจหน้าที่ หรือมีการโอนย้าย

3.8. หน้าที่ของหน่วยงานตรวจสอบภายใน

- ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศตามความจำเป็น

4. นโยบาย

บริษัทฯ กำหนดนโยบายด้านความปลอดภัยสารสนเทศในประเด็นสำคัญ ดังต่อไปนี้

4.1. การบริหารจัดการทรัพย์สินของบริษัทฯ

1. ทรัพย์สินด้านสารสนเทศ ได้แก่ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด ต้องมีการจัดทำบัญชีทรัพย์สิน หน่วยงานแอดมินเป็นผู้จัดทำบัญชีฮาร์ดแวร์ ส่วนงานเทคโนโลยีสารสนเทศจัดทำบัญชีซอฟต์แวร์ แอพพลิเคชั่นและข้อมูล โดยผู้เป็นเจ้าของข้อมูลนั้นต้องร่วมจัดทำทะเบียนรายการทรัพย์สินด้านสารสนเทศ รวมถึงต้องจัดทำและจัดการป้ายชื่อ สำหรับปิดฉลากเอกสารข้อมูลของอุปกรณ์ทรัพย์สินด้านสารสนเทศ
2. บริษัทต้องกำหนดลำดับชั้นความลับ และกำหนดระดับความสำคัญของเอกสารเพื่อป้องกันทรัพย์สินด้านสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม ทั้งนี้ เอกสารหรือสิ่งตีพิมพ์ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดลำดับชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับข้อมูลนั้น
3. การใช้งานทรัพย์สินที่เหมาะสม ต้องมีการจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรเพื่อป้องกันความเสียหายต่อทรัพย์สินด้านสารสนเทศ

4.2. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

1. ต้องมีการกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับผู้ใช้งาน หรือที่ว่าจ้างหน่วยงานภายนอกมาปฏิบัติงาน รวมทั้งกำหนดมาตรการป้องกันและดูแลรักษาความปลอดภัยสำหรับสารสนเทศของบริษัทฯ
2. ต้องมีการตรวจสอบคุณสมบัติของผู้สมัครเข้าทำงานทุกกรณีโดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา หรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และต้องสร้างความตระหนักเรื่องความมั่นคงปลอดภัยเบื้องต้นให้พนักงานเข้าใหม่ พร้อมทั้งจัดให้พนักงานมีการลงนามไม่เปิดเผยความลับของบริษัทฯ
3. ต้องกำหนดให้ผู้ใช้งานที่ได้รับการว่าจ้างต้องปฏิบัติตามมาตรการความมั่นคงปลอดภัยให้สอดคล้องกับนโยบายของบริษัทฯ ที่กำหนดไว้
4. จัดอบรมให้ความรู้แก่ผู้ใช้งานทุกคนเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และสารสนเทศ ต้องมีการลงนามและเก็บ

รวบรวมไว้ในแฟ้มประวัติของบุคลากร ถ้ามีการเปลี่ยนแปลงทางด้านความมั่นคงปลอดภัยต้องแจ้งให้พนักงานทราบ

5. ต้องมีการกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎและแนวปฏิบัติของบริษัทฯ หากเป็นการละเมิดข้อกฎหมายบทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำและเป็นไปตามระเบียบบริษัท
6. หากมีการแต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงตำแหน่งใดๆ แผนกทรัพยากรบุคคลต้องแจ้งให้ผู้รับการว่าจ้างทราบ และผู้รับการว่าจ้างต้องปฏิบัติตามเงื่อนไขในสัญญาจ้างจนกว่าจะสิ้นสุดการว่าจ้าง และพนักงานซึ่งพ้นตำแหน่งจากการจ้างงานไม่ว่ากรณีใดต้องคืนทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศ เช่น กุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออกสำนักงาน คอมพิวเตอร์ อุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้ แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน ซึ่งส่วนงานเทคโนโลยีสารสนเทศต้องถอดถอนสิทธิการเข้าใช้งานดังกล่าวด้วย

4.3. ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

1. ต้องมีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงาน ห้องทำงาน และทรัพย์สินอื่น ๆ และต้องจัดให้มีการป้องกันภัยคุกคามต่างๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อความไม่สงบ เป็นต้น รวมถึงการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัยต้องมีการจัดการป้องกันที่เพียงพอ
2. ในการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอกต้องมีบริเวณเฉพาะที่จัดไว้ต่างหากเพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศของบริษัทฯ โดยไม่ได้รับอนุญาต
3. พนักงานต้องป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต
4. ทรัพย์สินด้านสารสนเทศจะต้องอยู่ในพื้นที่ที่เหมาะสมมีความปลอดภัย มีการจำแนกพื้นที่ในการใช้งานระบบสารสนเทศอย่างเหมาะสม มีการแยกศูนย์คอมพิวเตอร์ออกจากสถานที่ทำงานทั่วไปและกั้นเป็นห้องต่างหาก มีการควบคุมการเข้า-ออกพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยให้เข้า-ออกได้เฉพาะผู้ที่มีหน้าที่รับผิดชอบและผู้ที่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร โดยแสดงบัตรประชาชนหรือบัตรที่ราชการออกให้
5. มีระบบไฟฟ้าสำรองเพื่อให้สามารถทำงานได้ตลอดเวลาและต้องมีการตรวจสอบระบบไฟฟ้าสำรองอย่างน้อยปีละ 2 ครั้ง เพื่อเป็นการลดความเสียหายที่อาจจะเกิดขึ้น
6. การเดินสายเคเบิลต่างๆ ต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการเดินสายนั้นต้องติดป้ายกำกับให้รู้ต้นทางปลายทางของสาย
7. ต้องบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่าย อย่างสม่ำเสมอ หรือตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต
8. ต้องมีมาตรการป้องกันอุปกรณ์ต่าง ๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น
9. พนักงานต้องมีการตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญที่อยู่ในอุปกรณ์ดังกล่าวได้ถูกลบทิ้งหรือถูกบันทึกทับก่อนที่จะนำอุปกรณ์ดังกล่าวทิ้งไปโดยต้องเป็นไปตามที่ส่วนงานเทคโนโลยีสารสนเทศกำหนด
10. ต้องมีขั้นตอนปฏิบัติสำหรับการจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

11. ต้องมีการกำหนดมาตรการการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่รับอนุญาต
12. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
13. ต้องมีมาตรการการกำจัดสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร เช่น การเผา ตัด หั่น หรือทำลายสื่อบันทึกข้อมูลที่มีข้อมูลสำคัญในนั้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยกำหนดให้มีบุคลากรผู้ทำหน้าที่ในการสอดส่องและดูแลการกำจัดหรือการทำลายสื่อบันทึกข้อมูล (ทั้งทำลายเองหรือจ้างบริษัทรับทำลายเป็นผู้ทำลายสื่อบันทึกข้อมูลเหล่านั้น) การทำลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูล จะต้องได้รับการอนุมัติจากเจ้าของข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม

4.4. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของบริษัทฯ

1. ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน เช่น ขั้นตอนการกู้คืนระบบ ขั้นตอนการบำรุงรักษาและดูแลระบบ เป็นต้น และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานเมื่อมีการเปลี่ยนแปลงขั้นตอนหรือผู้รับผิดชอบ และต้องทบทวนอย่างน้อยปีละ 1 ครั้ง และต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์แม่ข่าย ฮาร์ดแวร์และซอฟแวร์
2. ต้องมีการแบ่งหน้าที่ความรับผิดชอบของผู้ดูแลระบบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต
3. ต้องมีการแยกระบบสำหรับการพัฒนาและทดสอบแยกออกจากระบบงานจริง เพื่อป้องกันการเข้าถึงข้อมูลหรือเปลี่ยนแปลงต่อระบบงานที่ให้บริการจริงจากผู้ที่ไม่ได้รับอนุญาต และต้องติดตามสภาพการใช้งาน การวิเคราะห์ขีดความสามารถของทรัพยากรสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
4. การยอมรับระบบใหม่ต้องจัดให้มีเกณฑ์ในการยอมรับ และจัดให้มีการทดสอบระบบใหม่ก่อนที่จะตรวจรับระบบนั้นอย่างเป็นลายลักษณ์อักษร

4.5. การบริการจัดการการให้บริการของหน่วยงานภายนอก

1. ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการโดยหน่วยงานภายนอก เช่น มีการยอมรับนโยบายด้านความปลอดภัยสารสนเทศของบริษัทฯ และขอบเขตรายละเอียด ระดับการให้บริการ ต้องได้รับการตรวจสอบจากฝ่ายกฎหมายของบริษัทฯ รวมถึงสัญญาในการไม่เปิดเผยข้อมูลของบริษัทฯ เป็นต้น
2. หน่วยงานภายนอกหรือบุคคลภายนอกอื่นๆ ที่ได้รับอนุญาตในการเข้าถึง ระบบสารสนเทศของบริษัทฯ ต้องยอมรับและปฏิบัติตามนโยบายด้านความปลอดภัยสารสนเทศของบริษัทฯ
3. บริษัทจะประเมินความเสี่ยงในการเข้าถึงระบบสารสนเทศ หรือที่มีผลกระทบต่อบริษัท ของหน่วยงานภายนอกหรือบุคคลภายนอกอื่น ๆ ถ้าจำเป็นต้องมีการเปิดเผยข้อมูลนั้นออกไป หน่วยงานภายนอกหรือบุคคลภายนอกนั้นต้องลงนามสัญญาว่าจะไม่เปิดเผยความลับของบริษัทฯ
4. ต้องตรวจสอบการให้บริการหรือสัญญาที่ทำกับหน่วยงานภายนอกและบุคคลภายนอกที่เข้ามาให้บริการกับบริษัท โดยมีการทบทวนอย่างสม่ำเสมอตามความจำเป็น รวมถึงต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เช่น เมื่อมีการปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การเปลี่ยนเทคโนยีใหม่ เป็นต้น

4.6. การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่าย

1. ต้องกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และกำหนดสิทธิผู้ที่ใช้งานผ่านเครือข่ายโดยอนุญาตเฉพาะผู้ที่มีสิทธิเท่านั้น
2. ต้องจำกัดการเชื่อมต่อจากภายนอกเข้าสู่ระบบเครือข่ายภายใน เช่น การเข้าถึงเครือข่ายจากระยะไกลผ่านทางอินเตอร์เน็ต รวมถึงไม่ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย โดยไม่ได้รับอนุญาต

4.7. การแลกเปลี่ยนสารสนเทศ

1. ต้องกำหนดนโยบาย แนวปฏิบัติ และมาตรการเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศภายในบริษัท ภายในกลุ่มบริษัท และหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิดอย่างเป็นลายลักษณ์อักษร เช่น การส่งข้อความทางอิเล็กทรอนิกส์ เป็นต้น
2. ต้องมีมาตรการตรวจทานก่อนส่งข้อมูลสารสนเทศออกสู่สาธารณะ โดยมีการประเมินความเสี่ยงและกำหนดมาตรการลดความเสี่ยงก่อนนำข้อมูลไปเผยแพร่

4.8. การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์

1. ต้องกำหนดมาตรการป้องกันสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะรวมถึงการป้องกันสารสนเทศที่รับ–ส่ง ที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ–ส่ง หรือสารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่าย
2. สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะต้องได้รับการป้องกันให้มีความถูกต้องและความสมบูรณ์ก่อนที่จะนำไปเผยแพร่

4.9. การตรวจสอบการเข้าใช้งานระบบ

1. ต้องกำหนดให้มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศและกิจกรรมการใช้งานของผู้ใช้งานอย่างสม่ำเสมอ และต้องมีมาตรการป้องกันข้อมูลที่บันทึกที่เกี่ยวข้องกับการใช้งานสารสนเทศไม่ให้มีการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต รวมถึงต้องบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบนั้น ๆ ด้วย
2. ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดที่เกี่ยวข้อง วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร และต้องตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องของบริษัทฯ ถูกบุกรุก
3. การเข้าถึงและการใช้งานระบบสารสนเทศของพนักงานจะต้องถูกสอบทานและทบทวนตามรอบระยะเวลาที่กำหนดไว้จากส่วนงานตรวจสอบภายใน โดยส่วนงานตรวจสอบภายในมีสิทธิที่จะสอดส่องดูแลการกระทำใดๆที่ผู้ตรวจสอบสงสัยว่ามีการฝ่าฝืนนโยบายดังกล่าว

4.10. การควบคุมการเข้าถึง

1. ต้องกำหนดให้มีขั้นตอนสำหรับการลงทะเบียนต่าง ๆ เพื่อให้มีสิทธิและควบคุมสิทธิในการเข้าถึงสารสนเทศและระบบสารสนเทสของบริษัทฯ ตามความจำเป็น รวมถึงขั้นตอนการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกหรือเปลี่ยนแปลงตำแหน่ง เป็นต้น รวมถึงต้องมี

กระบวนการจัดการรหัสผ่านสำหรับผู้ใช้งาน เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานตามความเหมาะสมหรือที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย

2. ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษาบัญชีผู้ใช้งานและรหัสผ่านของตนให้มีความมั่นคงปลอดภัยเพียงพอ
3. พนักงานต้องมีวิธีป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล เช่น แจ้งหัวหน้าหน่วยงาน หรือเจ้าหน้าที่รักษาความปลอดภัยทุกครั้งที่พบเห็น รวมถึงมีนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย หรือพบเห็นได้ง่าย
4. ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมว่าบริการใดอนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้
5. การเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัทฯ จะกระทำได้เมื่อได้รับอนุมัติโดยหัวหน้าหน่วยงานและหัวหน้าส่วนงานเทคโนโลยีสารสนเทศ สามารถใช้ได้เฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น และต้องถูกจำกัดการเข้าถึงให้เฉพาะผู้ที่ได้รับอนุญาต หรือผู้ที่มีความจำเป็นต้องใช้ข้อมูลนั้น และต้องได้รับความยินยอมจากเจ้าของข้อมูล
6. การเข้าถึงระบบสารสนเทศใดๆ ต้องได้รับการพิสูจน์ตัวตนทุกครั้งเมื่อเข้าถึงระบบสารสนเทศ และสารสนเทศของบริษัทฯ สิทธิในการเข้าถึงต้องถูกทบทวนสิทธิอย่างน้อยปีละ 1 ครั้ง
7. การเปลี่ยนแปลงระบบสารสนเทศ/ระบบเน็ตเวิร์ค หรือแอพพลิเคชั่นใด ๆ จะต้องได้รับการตรวจสอบและอนุญาตจากเจ้าของข้อมูล รวมถึงได้รับอนุมัติจากหัวหน้าส่วนงานเทคโนโลยีสารสนเทศ
8. ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้ สำหรับตรวจสอบและปรับแต่งระบบ โดยมาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย
9. ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด
10. ต้องจำกัดและควบคุมการใช้โปรแกรมใดๆ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เช่น จำกัดการใช้งานโปรแกรมดังกล่าวให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เป็นต้น และต้องกำหนดวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ เพื่อเครื่องคอมพิวเตอร์นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง รวมถึงต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูงด้วย
11. ต้องมีการแยกระบบที่มีความสำคัญสูงไว้ ในบริเวณแยกต่างหากสำหรับระบบงานนี้โดยเฉพาะ และต้องมีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับผู้ใช้งานที่จำเป็นต้องปฏิบัติงานของบริษัทฯ จากภายนอกสำนักงาน
12. การเข้าถึงแอพพลิเคชั่นใด ๆ ต้องถูกควบคุมและจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตหรือได้รับมอบหมายให้มีสิทธิ เช่น ผู้ดูแลระบบ เป็นต้น รวมถึงการใช้ซอฟแวร์ที่มีลิขสิทธิ์ต้องอนุญาตเฉพาะผู้ที่มีสิทธิตามจำนวนที่ซื้อเท่านั้น
13. การควบคุมการเข้าถึงเครือข่าย ต้องกำหนดสิทธิในการเข้าถึงเครือข่ายให้ผู้ที่จะเข้าใช้งานต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเตอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยของบริษัทฯ จัดสรรไว้ และออกแบบเครือข่ายโดยแบ่งเขต

(Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

14. การควบคุมการเข้าถึงระบบปฏิบัติการ ต้องกำหนดสิทธิให้ผู้ที่จะเข้าใช้งาน และต้องพิสูจน์ตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าใช้งาน ต้องระงับการใช้งานเมื่อผู้ใช้ไม่ใช้งานอย่างต่อเนื่องตามระยะเวลาที่กำหนด เพื่อจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศ (Session Time-out) การควบคุมการเข้าถึงคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารแบบพกพา (Mobile Computing and Communications) บริษัทมีนโยบายให้ผู้ใช้งานใช้อุปกรณ์สื่อสารแบบพกพาเฉพาะที่เป็นของบริษัทฯ ในการเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัทฯ หากมีความจำเป็นต้องใช้อุปกรณ์สื่อสารแบบพกพาส่วนตัวในการเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัทฯ ต้องขออนุญาตเป็นการเฉพาะ และอุปกรณ์สื่อสารแบบพกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัทฯ ต้องเป็นอุปกรณ์สื่อสารแบบพกพาที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัยหรือที่ละเมิดลิขสิทธิ์ตามนโยบายที่ส่วนงานเทคโนโลยีสารสนเทศกำหนด
15. ต้องมีการแบ่งแยกระบบเครือข่ายตามกลุ่มที่ให้บริการ เช่น โซนภายในบริษัท โซนภายนอกบริษัทฯ เป็นต้น เพื่อให้สามารถป้องกันการบุกรุกได้อย่างเป็นระบบ

4.11. นโยบายการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

1. บริษัทฯ มีนโยบายให้ผู้ใช้งาน ใช้อุปกรณ์พกพาในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทฯ ได้
2. อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทฯ จะต้องเป็นอุปกรณ์พกพาที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัย เช่น “Jail breaking” หรือ “Rooting” ไม่ติดตั้ง Software ที่ละเมิดลิขสิทธิ์รวมทั้งต้องกำหนดค่ารหัสผ่านและเข้ารหัสข้อมูลหรืออุปกรณ์พกพาตามนโยบายที่ส่วนงานเทคโนโลยีสารสนเทศกำหนด ทั้งนี้ ผู้ใช้งานต้องได้รับการอนุมัติการใช้งานจากผู้บังคับบัญชาหรือเลขานุการบริษัทกรณีผู้ใช้งานเป็นกรรมการและส่วนงานเทคโนโลยีสารสนเทศก่อนการใช้งาน
3. บริษัทฯ ขอสงวนสิทธิในการตรวจสอบ ระงับเพิกถอนการใช้งาน และลบข้อมูลทั้งหมด (Wipe) บนอุปกรณ์พกพาที่ใช้ในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทฯ หากเห็นว่าการใช้งานมีความเสี่ยงต่อโครงสร้างพื้นฐานหรือข้อมูลและสารสนเทศของบริษัทฯ

4.12. การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ

1. ผู้พัฒนาและผู้เป็นเจ้าของระบบต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบที่จัดหาหรือพัฒนาขึ้นมาใช้งาน โดยการประเมินความเสี่ยงและระบุข้อกำหนดด้านความมั่นคงปลอดภัยเพื่อลดความเสี่ยงนั้น
2. เพื่อป้องกันความผิดพลาดของสารสนเทศ การสูญหายของสารสนเทศหรือการใช้งานสารสนเทศผิดวัตถุประสงค์ ต้องมีการตรวจสอบข้อมูลนำเข้าซึ่งผู้พัฒนาระบบต้องกำหนดกลไกว่าข้อมูลนำเข้านั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป ต้องมีการตรวจสอบข้อมูลที่อยู่ระหว่างการประมวลผลซึ่งผู้พัฒนาระบบต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ การตรวจสอบความถูกต้องของข้อความเพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความ

ต้นฉบับที่ถูกต้อง และการตรวจสอบข้อมูลนำออกซึ่งผู้พัฒนาระบบและเข้าของระบบต้องกำหนดกลไกเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม

4.13. มาตรการการเข้ารหัสข้อมูล

ต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้ในบริษัท และต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้ จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานของบริษัทฯ

4.14. การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

1. ต้องกำหนดมาตรการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งาน โดยก่อนติดตั้งต้องผ่านการตรวจสอบว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่
2. ผู้พัฒนาระบบต้องหลีกเลี่ยงการใช้ข้อมูลจริงในการทดสอบระบบ หากจำเป็นต้องได้รับอนุญาตจากเข้าของข้อมูลก่อน และผู้พัฒนาระบบต้องควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริง และควรเก็บ Source Code ไว้ในที่ ๆ ปลอดภัย
3. ต้องกำหนดขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริงและต้องตรวจสอบเมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงเพื่อให้มั่นใจว่าแอปพลิเคชั่นที่ทำงานอยู่นั้นทำงานปกติหรือไม่เกิดปัญหาขึ้น อีกทั้งไม่แก้ไขเปลี่ยนแปลงซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นให้แก้ไขตามความจำเป็นเท่านั้น
4. ต้องป้องกันการรั่วไหลของสารสนเทศ หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป และต้องกำหนดมาตรการควบคุมและตรวจสอบการว่าจ้างให้พัฒนาระบบต้องมีความชัดเจน รวมถึงการรับรองคุณภาพของระบบ และกำหนดขอบเขตในการว่าจ้างด้วย
5. เพื่อลดความเสี่ยงจากการโจมตี โดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่ต้องมีการติดตามข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ อย่างสม่ำเสมอ

4.15. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทฯ

1. ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทฯ เช่น จุดอ่อนใด ๆ ให้แก่ผู้บังคับบัญชา หรือส่วนงานเทคโนโลยีสารสนเทศทันทีที่พบหรือสงสัยว่ามีสิ่งผิดปกติเกิดขึ้นและต้องกำหนดหน้าที่และความรับผิดชอบเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงานโดยต้องมีการบันทึกเหตุการณ์ พิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้นและค่าใช้จ่ายที่เกิดขึ้นจากความเสียหาย
2. ต้องเก็บรวบรวมหลักฐานตามกฎหรือหลักเกณฑ์เพื่อใช้สำหรับอ้างอิงในกระบวนการศาลหรือที่เกี่ยวข้อง

4.16. การบริหารความต่อเนื่องในการดำเนินงานของบริษัทฯ

1. ต้องจัดลำดับความสำคัญของกระบวนการสร้างความต่อเนื่องทางธุรกิจ ระบุเหตุการณ์ที่ทำให้กระบวนการทางธุรกิจหยุดชะงัก ความเป็นไปได้และผลกระทบที่จะเกิดขึ้น และแผนบริหารความต่อเนื่องทางธุรกิจจะจัดทำขึ้นสำหรับระบบงานที่มีความสำคัญ
2. แผนบริหารความต่อเนื่องทางธุรกิจทั้งหมดจะได้รับการทดสอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเมื่อเกิดเหตุฉุกเฉิน แผนที่นำมาทดสอบสามารถใช้งานได้จริง
3. ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจเพื่อให้แผนทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
4. จัดทำระบบสำรองข้อมูลของระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของบริษัทฯ สามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของผู้ดูแลระบบในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมในกรณีฉุกเฉินหรือในกรณีที่ไม่สามารถดำเนินการได้อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง และแผนบริหารความต่อเนื่องทางธุรกิจดังกล่าวต้องถูกทบทวนและปรับปรุงหากมีความจำเป็น

4.17. การป้องกันโปรแกรมไม่ประสงค์ดี

บริษัทฯ และส่วนงานเทคโนโลยีสารสนเทศจะต้องใช้ซอฟแวร์ที่มีกระบวนการในการจัดการและป้องกันโปรแกรมไม่ประสงค์ดี และพนักงานทุกคนต้องให้ความร่วมมือปฏิบัติตามนโยบายดังกล่าว รวมทั้งไม่ติดตั้งซอฟแวร์เอง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ทำงานแทน

4.18. การปฏิบัติตามข้อกำหนด

1. ผู้ใช้งานทุกคนมีหน้าที่ต้องทำความเข้าใจ และปฏิบัติตามนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด ทั้งนี้ รวมถึงแต่ไม่จำกัดเฉพาะ
    - นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
    - พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
    - พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
    - พ.ร.บ. ลิขสิทธิ์
    - พ.ร.บ. เครื่องหมายการค้า
    - พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบสารสนเทศของบริษัทฯ ถือเป็นทรัพย์สินของบริษัทฯ ยกเว้นข้อมูลที่เป็นทรัพย์สินของลูกค้าหรือบุคคลภายนอก ซอฟต์แวร์หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตรหรือลิขสิทธิ์ของบุคคลภายนอก
3. ต้องกำหนดให้มีการป้องกันข้อมูล ที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและแนวปฏิบัติข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ รวมถึงต้องมีมาตรการป้องกันข้อมูลส่วนตัวตามที่ระบุไว้ในกฎหมาย แนวปฏิบัติและสัญญาที่เกี่ยวข้อง
4. ต้องกำหนดให้มีการป้องกัน สารสนเทศ ระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่ายและคอมพิวเตอร์แม่ข่าย ไม่ให้ใช้งานไปในทางที่ผิดหรือโดยไม่มีสิทธิและต้อง

กำหนดให้ใช้มาตรการเข้ารหัสข้อมูลโดยให้ยึดถือตามหรือสอดคล้องกับข้อตกลงทางกฎหมาย

5. การทบทวน ตรวจสอบการใช้งานระบบทุกระบบเป็นสิทธิที่บริษัทสามารถกระทำได้หากบริษัทเห็นว่าจำเป็น โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า
6. ต้องมีการตรวจสอบระบบว่ามีความมั่นคงปลอดภัยเพียงพอหรือไม่โดยใช้ซอฟต์แวร์ค้นหาช่องโหว่ และทดสอบการโจมตีระบบเพื่อตรวจข้อบกพร่องของระบบด้วย
7. ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ และต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ ไม่ให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด โดยกำหนดให้มีการแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบระบบสารสนเทศ

5. การแจกจ่ายเอกสารนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

5.1 แผนการเผยแพร่นโยบาย

เอกสารนโยบายฉบับนี้จะจัดทำให้ผู้ใช้งานทุกคนได้อ่านและทำความเข้าใจ และประกาศบนเวปไซต์ของบริษัทฯ

5.2 แผนการฝึกอบรม

1. วิเคราะห์ว่าพนักงานส่วนไหนได้รับผลกระทบจากนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
2. พนักงานที่ได้รับผลกระทบดังกล่าวต้องได้รับการฝึกอบรมเรื่องนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
3. ทำแผนการฝึกอบรมเรื่องนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามความจำเป็น

6. วิธีการปฏิบัติให้เป็นไปตามนโยบาย

ส่วนงานเทคโนโลยีสารสนเทศ ได้จัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความมั่นคงปลอดภัยแก่สารสนเทศ

7. บทลงโทษ

ผู้ใช้งานคนใดที่ฝ่าฝืนนโยบายฉบับนี้ บริษัทฯ พิจารณาลงโทษทางวินัยตามระเบียบบริหารงานบุคคล รวมทั้งอาจมีความรับผิดทั้งทางอาญาและทางแพ่ง

8. การทบทวนนโยบาย

หัวหน้าส่วนงานเทคโนโลยีสารสนเทศ ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำอย่างน้อยปีละ 1 ครั้ง และต้องเสนอให้ต่อที่ประชุมคณะกรรมการบริษัทพิจารณาอนุมัติ หากมีการเปลี่ยนแปลง

นโยบายด้านความปลอดภัยสารสนเทศฉบับนี้ได้มีการปรับแก้ไขให้เป็นปัจจุบัน และได้รับอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 2/2566 เมื่อวันที่ 7 เมษายน 2566 โดยให้มีผลบังคับใช้ตั้งแต่วันที่ 7 เมษายน 2566 เป็นต้นไป

บริษัท พีเอ็มซี เลเบิล แมททีเรียลส์ จำกัด (มหาชน)

(นายอัฒฑวุฒิ หิรัญบูรณะ)
ประธานกรรมการบริษัท