



บริษัท ห่องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

บริษัท ห่องเย็นโซติวัฒน์ หาดใหญ่ จำกัด (มหาชน) และบริษัทสาขา กำหนดนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้การบริหารข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ มีการควบคุมภายในที่ดี มีความมั่นคงปลอดภัย ถูกต้องเชื่อถือได้ สามารถดำเนินการได้อย่างต่อเนื่อง สามารถปกป้องรักษาสารสนเทศที่เป็นความลับของบริษัทฯ และสามารถป้องกันความเสียหายที่อาจเกิดกับทรัพย์สินด้านสารสนเทศของบริษัทฯ จากภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ ได้ ทั้งนี้ กรรมการผู้บริหาร พนักงานทุกคน และบุคคลใดๆ ที่ได้รับอนุญาตให้เข้าถึงข้อมูลสารสนเทศของบริษัทฯ จะต้องถือปฏิบัติตามนโยบายและแนวปฏิบัติกำหนดภายใต้แนบนโยบายนี้อย่างเคร่งครัด

นิยาม บริษัท และบริษัทสาขา ให้หมายรวมถึง บริษัท ห่องเย็นโซติวัฒน์ หาดใหญ่ จำกัด (มหาชน) สำนักงานใหญ่ และ บริษัท ห่องเย็นโซติวัฒน์ หาดใหญ่ จำกัด (มหาชน) สาขามหาชัย

หลักปฏิบัติสำคัญ

1. การบริหารจัดการทรัพย์สินของบริษัท

- 1.1 ทรัพย์สินด้านสารสนเทศ ได้แก่ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนาอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด ต้องมีการจัดทำบัญชีทรัพย์สิน แผนก Infrastructure เป็นผู้จัดทำบัญชีฮาร์ดแวร์ ส่วนงานเทคโนโลยีสารสนเทศจัดทำบัญชีซอฟต์แวร์ แอปพลิเคชัน และข้อมูล โดยผู้เป็นเจ้าของข้อมูลนั้นต้องร่วมจัดทำทะเบียนรายการทรัพย์สินด้านสารสนเทศรวมถึงต้องจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลของอุปกรณ์ทรัพย์สินด้านสารสนเทศ
- 1.2 บริษัทต้องกำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันทรัพย์สินด้านสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม เอกสารหรือสิ่งตีพิมพ์ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับ ซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีความลับเดียวกันกับต้นฉบับข้อมูลนั้น
- 1.3 การใช้งานทรัพย์สินที่เหมาะสม ต้องมีการจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรเพื่อป้องกันความเสียหายต่อทรัพย์สินด้านสารสนเทศ



บริษัท ห้องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

2. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร ลูกค้า คู่ค้า และผู้มาติดต่อ

- 2.1 มีการกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรและทางสื่ออิเล็กทรอนิกส์ สำหรับบุคลากร ลูกค้า คู่ค้า และผู้มาติดต่อ
 - 2.1.1 กรณีที่ว่าจ้างบุคคลภายนอกหรือผู้ประมวลผล มาปฏิบัติงาน ต้องมีการจัดทำ DPA (Data Processing Agreement) ระหว่างกัน
- 2.2 ต้องมีการตรวจสอบคุณสมบัติของผู้สมัครเข้าทำงานทุกกรณีโดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา หรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และต้องสร้างความตระหนักเรื่องความมั่นคงปลอดภัยเบื้องต้นให้พนักงานเข้าใหม่พร้อมทั้งจัดให้พนักงานมีการลงนามไม่เปิดเผยความลับของบริษัท และต้องมีการให้ความยินยอมโดยมีการคัดลอกสำเนาเป็นไฟล์อิเล็กทรอนิกส์
- 2.3 ต้องกำหนดให้ผู้ใช้งานที่ได้รับการว่าจ้างต้องปฏิบัติตามมาตรการความมั่นคงปลอดภัยให้สอดคล้องกับนโยบายของบริษัทที่กำหนดไว้
- 2.4 จัดอบรมให้ความรู้ แก่ผู้ใช้งานทุกคนเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและสารสนเทศ ต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากร ถ้ามีการเปลี่ยนแปลงทางด้านความมั่นคงปลอดภัยต้องแจ้งให้พนักงานทราบ
- 2.5 ต้องมีการกำหนดบทลงโทษทางวินัยสำหรับผู้ฝ่าฝืนนโยบาย กฎและแนวปฏิบัติของบริษัท หากเป็นการละเมิดข้อกำหนดบทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำ และเป็นไปตามระเบียบบริษัท
- 2.6 หากมีการแต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงตำแหน่งใด ๆ ฝ่ายพัฒนาทรัพยากรมนุษย์ ต้องแจ้งให้ผู้รับทราบว่าจ้างทราบ และฝ่ายเทคโนโลยีสารสนเทศทราบ และพนักงานซึ่งพ้นตำแหน่งจากการจ้างงานไม่ว่ากรณีใด ต้องคืนทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศ เช่น กุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออกศูนย์คอมพิวเตอร์ อุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน ซึ่งส่วนงานเทคโนโลยีสารสนเทศต้องถอดถอนสิทธิการเข้าใช้งานดังกล่าวด้วย



บริษัท ห้องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

3. ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

- 3.1 ต้องมีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงานห้องทำงานและทรัพย์สินอื่น ๆ และต้องจัดให้มีการป้องกันภัยคุกคามต่าง ๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อความไม่สงบ เป็นต้น รวมถึงการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัยต้องมีการจัดการป้องกันที่เพียงพอ
- 3.2 ในการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก ต้องมีบริเวณเฉพาะที่จัดไว้ต่างหากเพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศของบริษัทโดยไม่ได้รับอนุญาต
- 3.3 พนักงานต้องป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต
- 3.4 ทรัพย์สินด้านสารสนเทศจะต้องอยู่ในพื้นที่ที่เหมาะสมมีความปลอดภัย มีการจำแนกพื้นที่ในการใช้งานระบบสารสนเทศอย่างเหมาะสม มีการแยกศูนย์คอมพิวเตอร์ออกจากสถานที่ทำงานทั่วไปและกันเป็นห้องต่างหาก มีการควบคุมการเข้า-ออกพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยให้เข้า-ออกได้เฉพาะผู้ที่มีหน้าที่รับผิดชอบและผู้ที่ได้รับอนุญาตอย่างเป็นทางการเป็นลายลักษณ์อักษร โดยแสดงบัตรประชาชนหรือบัตรที่ราชการออกให้
- 3.5 มีระบบไฟฟ้าสำรองเพื่อให้สามารถทำงานได้ตลอดเวลา และต้องมีการตรวจสอบระบบไฟฟ้าสำรองอย่างน้อยปีละ 2 ครั้ง เพื่อเป็นการลดความเสียหายที่อาจจะเกิดขึ้น
- 3.6 การเดินสายเคเบิลต่าง ๆ ต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการเดินสายนั้นต้องติดป้ายกำกับให้รู้ต้นทางปลายทางของสาย
- 3.7 ต้องบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่าย อย่างสม่ำเสมอหรือตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต
- 3.8 ต้องมีมาตรการป้องกันอุปกรณ์ต่าง ๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น
- 3.9 พนักงานต้องมีการตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญที่อยู่ในอุปกรณ์ดังกล่าวได้ถูกลบทิ้งหรือถูกบันทึกทับก่อนที่จะนำอุปกรณ์ดังกล่าวทิ้งไป โดยต้องเป็นไปตามที่ส่วนงานเทคโนโลยีสารสนเทศกำหนด
- 3.10 ต้องมีขั้นตอนปฏิบัติสำหรับการจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้
- 3.11 ต้องมีการกำหนดมาตรการการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต



บริษัท ห้องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

- 3.12 ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- 3.13 ต้องมีมาตรการการกำจัดการสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร เช่น การเผาตัด หั่น หรือทำลายสื่อบันทึกข้อมูลที่มีข้อมูลสำคัญในนั้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยกำหนดให้มีบุคลากรผู้ทำหน้าที่ในการสอดส่องและดูแลการกำจัดหรือการทำลายสื่อบันทึกข้อมูล (ทั้งทำลายเองหรือจ้างบริษัทรับทำลายเป็นผู้ทำลายสื่อบันทึกข้อมูลเหล่านั้น) การทำลายเอกสาร และสื่อที่ใช้ในการบันทึกข้อมูล จะต้องได้รับการอนุมัติจากเจ้าของข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม

4. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของบริษัท

- 4.1 ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน เช่น ขั้นตอนการกู้คืนระบบ ขั้นตอนการบำรุงรักษาและดูแลระบบ เป็นต้น และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานเมื่อมีการเปลี่ยนแปลงขั้นตอนหรือผู้รับผิดชอบ และต้องทบทวนอย่างน้อยปีละ 1 ครั้ง และต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบคอมพิวเตอร์ ระบบเครือข่าย คอมพิวเตอร์แม่ข่ายฮาร์ดแวร์ และซอฟต์แวร์
- 4.2 ต้องมีการแบ่งหน้าที่ความรับผิดชอบของผู้ดูแลระบบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต
- 4.3 ต้องมีการแยกระบบสำหรับการพัฒนา และทดสอบแยกออกจากระบบงานจริง เพื่อป้องกันการเข้าถึงข้อมูลหรือเปลี่ยนแปลงต่อระบบงานที่ให้บริการจริงจากผู้ที่ไม่ได้รับอนุญาต และต้องติดตามสภาพการใช้งาน การวิเคราะห์ขีดความสามารถของทรัพยากรสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
- 4.4 การยอมรับระบบใหม่ต้องจัดให้มีเกณฑ์ในการยอมรับ และจัดให้มีการทดสอบระบบใหม่ก่อนที่จะตรวจรับระบบนั้นอย่างเป็นลายลักษณ์อักษร

5. การบริการจัดการการให้บริการของหน่วยงานภายนอก

- 5.1 ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการโดยหน่วยงานภายนอก เช่น มีการยอมรับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท และขอบเขตรายละเอียด ระดับการ



บริษัท ห้องเย็นโชติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

ให้บริการ ต้องได้รับการตรวจสอบจากฝ่ายกฎหมาย รวมถึงสัญญาในการไม่เปิดเผยข้อมูลของบริษัท เป็นต้น

- 5.2 หน่วยงานภายนอกหรือบุคคลภายนอกอื่น ๆ ที่ได้รับอนุญาตในการเข้าถึงระบบสารสนเทศของบริษัทต้องยอมรับและปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท
- 5.3 บริษัทจะประเมินความเสี่ยงในการเข้าถึงระบบสารสนเทศ หรือที่มีผลกระทบต่อบริษัท ของหน่วยงานภายนอกหรือบุคคลภายนอกอื่น ๆ ถ้าจำเป็นต้องมีการเปิดเผยข้อมูลนั้นออกไปหน่วยงานภายนอกหรือบุคคลภายนอกนั้นต้องเซ็นสัญญาว่าจะไม่เปิดเผยความลับของบริษัท
- 5.4 ต้องตรวจสอบการให้บริการหรือสัญญาที่ทำกับหน่วยงานภายนอกและบุคคลภายนอกที่เข้ามาให้บริการกับบริษัท โดยมีการทบทวนอย่างสม่ำเสมอตามความจำเป็น รวมถึงต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เช่น เมื่อมีการปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การเปลี่ยนเทคโนโลยีใหม่ เป็นต้น

6. การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่าย

- 6.1 ต้องกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และกำหนดสิทธิ์ผู้ที่ใช้งานผ่านเครือข่ายโดยอนุญาตเฉพาะผู้ที่มีสิทธิ์เท่านั้น
- 6.2 ต้องจำกัดการเชื่อมต่อจากภายนอกเข้าสู่ระบบเครือข่ายภายใน เช่น การเข้าถึงเครือข่ายจากระยะไกลผ่านทางอินเทอร์เน็ต รวมถึงไม่ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่ายโดยไม่ได้รับอนุญาต

7. การแลกเปลี่ยนสารสนเทศ

- 7.1 ต้องกำหนดนโยบาย แนวปฏิบัติ และมาตรการเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศภายในบริษัท ภายในกลุ่มบริษัท และหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิดอย่างเป็นลายลักษณ์อักษร เช่น การส่งข้อความทางอิเล็กทรอนิกส์ เป็นต้น
- 7.2 ต้องมีมาตรการตรวจทานก่อนส่งข้อมูลสารสนเทศออกสู่สาธารณะ โดยมีการประเมินความเสี่ยงและกำหนดมาตรการลดความเสี่ยงก่อนนำข้อมูลไปเผยแพร่



บริษัท ห้างเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

8 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์

- 8.1 ต้องกำหนดมาตรการป้องกันสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะรวมถึงการป้องกันสารสนเทศที่รับ - ส่ง ที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ - ส่ง หรือสารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่าย
- 8.2 สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะต้องได้รับการป้องกันให้มีความถูกต้องและความสมบูรณ์ก่อนที่จะนำไปเผยแพร่

9. การตรวจสอบการเข้าใช้งานระบบ

- 9.1 ต้องกำหนดให้มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ และกิจกรรมการใช้งานของผู้ใช้งานอย่างสม่ำเสมอและต้องมีมาตรการป้องกันข้อมูลที่บันทึกที่เกี่ยวข้องกับการใช้งานสารสนเทศไม่ให้มีการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต รวมถึงต้องบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบนั้น ๆ ด้วย
- 9.2 ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดที่เกี่ยวข้อง วิเคราะห์ข้อผิดพลาดเหล่านั้นและดำเนินการแก้ไขตามสมควร และต้องตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องของบริษัทถูกบุกรุก
- 9.3 การเข้าถึงและการใช้งานระบบสารสนเทศของพนักงานจะต้องถูกสอบทานและทบทวนตามรอบระยะเวลาที่กำหนดไว้จากส่วนงานตรวจสอบภายใน โดยส่วนงานตรวจสอบภายในมีสิทธิ์ที่จะสอดส่องดูแลการกระทำใดๆที่ผู้ตรวจสอบสงสัยว่า มีการฝ่าฝืนนโยบายดังกล่าว

10.การควบคุมการเข้าถึง

- 10.1 ต้องกำหนดให้มีขั้นตอนสำหรับการลงทะเบียนต่าง ๆ เพื่อให้มีสิทธิ์และควบคุมสิทธิ์ในการเข้าถึงสารสนเทศและระบบสารสนเทศของบริษัทตามความจำเป็น รวมถึงขั้นตอนการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกหรือเปลี่ยนแปลงตำแหน่ง เป็นต้น รวมถึงต้องมีกระบวนการจัดการรหัสผ่านสำหรับผู้ใช้งาน เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานตามความเหมาะสมหรือที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย
- 10.2 ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแลรักษาบัญชีผู้ใช้งานและรหัสผ่านของตนให้มีความมั่นคงปลอดภัยเพียงพอ



บริษัท ห้องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

- 10.3 พนักงานต้องมีวิธีป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล เช่น แจกหัวหน้าหน่วยงาน หรือเจ้าหน้าที่รักษาความปลอดภัยทุกครั้งที่พบเห็น รวมถึงมีนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย หรือพบเห็นได้ง่าย
- 10.4 ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมว่าบริการใดอนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้
- 10.5 การเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัท จะกระทำได้เมื่อได้รับอนุมัติโดยหัวหน้าหน่วยงานและหัวหน้าส่วนงานเทคโนโลยีสารสนเทศ สามารถใช้ได้เฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น และต้องถูกจำกัดการเข้าถึง ให้เฉพาะผู้ที่ได้รับอนุญาต หรือผู้ที่มีความจำเป็นต้องใช้ข้อมูลนั้น และต้องได้รับความยินยอมจากเจ้าของข้อมูล
- 10.6 การเข้าถึงระบบสารสนเทศใด ๆ ต้องได้รับการพิสูจน์ตัวตนทุกครั้งเมื่อเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัท สิทธิ์ในการเข้าถึงต้องถูกทบทวนสิทธิ์อย่างน้อยปีละ 1 ครั้ง
- 10.7 การเปลี่ยนแปลงระบบสารสนเทศ/ระบบเน็ตเวิร์ค หรือแอปพลิเคชันใด ๆ จะต้องได้รับการตรวจสอบและอนุญาตจากเจ้าของข้อมูล รวมถึงได้รับอนุมัติจากหัวหน้าส่วนงานเทคโนโลยีสารสนเทศ
- 10.8 ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้ สำหรับตรวจสอบและปรับแต่งระบบ โดยมาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย
- 10.9 ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด
- 10.10 ต้องจำกัดและควบคุมการใช้โปรแกรมยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เช่น จำกัดการใช้งานโปรแกรมดังกล่าวให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เป็นต้น และต้องกำหนดวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์เพื่อเครื่องคอมพิวเตอร์นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง รวมถึงต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูงด้วย



บริษัท ห้องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

- 10.11 ต้องมีการแยกระบบที่มีความสำคัญสูงไว้ในบริเวณแยกต่างหากสำหรับระบบงานนี้โดยเฉพาะ และต้องมีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับผู้ใช้งานที่จำเป็นต้องปฏิบัติงานของบริษัทจากภายนอกสำนักงาน
- 10.12 การเข้าถึงแอปพลิเคชันใด ๆ ต้องถูกควบคุมและจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตหรือได้รับมอบหมายให้มีสิทธิ์ เช่น ผู้ดูแลระบบ เป็นต้น รวมถึงการใช้ซอฟต์แวร์ ที่มีลิขสิทธิ์ ต้องอนุญาตเฉพาะผู้ที่มีสิทธิ์ตามจำนวนที่ซื้อเท่านั้น
- 10.13 การควบคุมการเข้าถึงเครือข่าย ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่ายให้ผู้ที่เข้าใช้งานต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยของบริษัทจัดสรรไว้ และออกแบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ
- 10.14 การควบคุมการเข้าถึงระบบปฏิบัติการ ต้องกำหนดสิทธิ์ให้ผู้ที่เข้าใช้งาน และต้องพิสูจน์ตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าใช้งาน ต้องระงับการใช้งานเมื่อผู้ใช้ไม่ใช้งานอย่างต่อเนื่องตามระยะเวลาที่กำหนด เพื่อจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศ (Session Time-out) การควบคุมการเข้าถึงคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารแบบพกพา (Mobile Computing and Communications) บริษัทมีนโยบายให้ผู้ใช้งานใช้อุปกรณ์สื่อสารแบบพกพาเฉพาะที่เป็นของบริษัทในการเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัทหากมีความจำเป็นต้องใช้อุปกรณ์สื่อสารแบบพกพาส่วนตัวในการเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัท ต้องขออนุญาตเป็นการเฉพาะ และอุปกรณ์สื่อสารแบบพกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัทต้องเป็นอุปกรณ์สื่อสารแบบพกพาที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัยหรือที่ละเมิดลิขสิทธิ์ ตามนโยบายที่ส่วนงานเทคโนโลยีสารสนเทศกำหนด
- 10.15 ต้องมีการแบ่งแยกระบบเครือข่ายตามกลุ่มที่ให้บริการ เช่น โชนภายในบริษัท โชนภายนอกบริษัท เป็นต้น เพื่อให้สามารถป้องกันการบุกรุกได้อย่างเป็นระบบ

11. นโยบายการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

- 11.1 บริษัทมีนโยบายให้ผู้ใช้งานใช้อุปกรณ์พกพาเฉพาะที่เป็นของบริษัทในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทเท่านั้น หากมีความจำเป็นต้องใช้อุปกรณ์พกพาส่วนตัวในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท บริษัทอนุญาตให้ใช้ได้ไม่เกิน 2 เครื่องหากจำเป็นต้องใช้



บริษัท ห้องเย็นโซติวิวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

มากกว่าที่กำหนดต้องได้ รับการอนุมัติจาก หัวหน้าหน่วยงานหรือเลขานุการบริษัทกรณีเป็น กรรมการ

11.2 อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทจะต้องเป็น อุปกรณ์พกพาที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัย เช่น “Jail breaking” หรือ “Rooting” ไม่ติดตั้ง Software ที่ละเมิดลิขสิทธิ์ รวมทั้งต้องกำหนดการห้ามผ่านและเข้ารหัสข้อมูลหรืออุปกรณ์ พกพาตามนโยบายที่ส่วนงานเทคโนโลยีสารสนเทศกำหนด ทั้งนี้ผู้ใช้งานต้องได้รับการอนุมัติการใช้งานจากผู้บังคับบัญชาหรือเลขานุการบริษัทกรณีผู้ใช้งานเป็นกรรมการและส่วนงานเทคโนโลยี สารสนเทศก่อนการใช้งาน

11.3 บริษัทขอสงวนสิทธิ์ในการตรวจสอบ ระบุ เพิกถอนการใช้งานบนอุปกรณ์พกพาทั้งที่เป็นของบริษัท และของส่วนตัวบุคคล ที่ใช้ในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท หากเห็นว่าการ ใช้งานมีความเสี่ยงต่อโครงสร้างพื้นฐานหรือข้อมูลและสารสนเทศของบริษัท

12.การจัดการ การพัฒนาและการบำรุงรักษาระบบสารสนเทศ

12.1 ผู้พัฒนาและผู้เป็นเจ้าของระบบต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบที่ จัดหาหรือพัฒนาขึ้นมาใช้งาน โดยการประเมินความเสี่ยงและระบุข้อกำหนดด้านความมั่นคง ปลอดภัยเพื่อลดความเสี่ยงนั้น

12.2 เพื่อป้องกันความผิดพลาดของสารสนเทศ การสูญหายของสารสนเทศหรือการใช้ งานสารสนเทศผิด วัตถุประสงค์ ต้องมีการตรวจสอบข้อมูลนำเข้าซึ่งผู้พัฒนาระบบต้องกำหนดกลไกว่าข้อมูลนำเข้านั้น มี ความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป ต้องมีการตรวจสอบข้อมูลที่อยู่ระหว่างการ ประมวลผลซึ่งผู้พัฒนาระบบต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการ ประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ การตรวจสอบความถูกต้องของข้อความเพื่อให้สามารถ ตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง และการตรวจสอบข้อมูลนำออกซึ่งผู้พัฒนาระบบและ เข้าของระบบต้องกำหนดกลไกเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้อง เป็นไปอย่างถูกต้องและเหมาะสม

13.การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

13.1 ต้องกำหนดมาตรการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี ซอฟต์แวร์ชุดช่องโหว่ ลงใน เครื่องที่ใช้งาน โดยก่อนติดตั้งต้องผ่านการตรวจสอบว่าไม่ก่อให้เกิดปัญหาให้กับเครื่องที่ให้บริการอยู่



บริษัท ห้องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

- 13.2 ผู้พัฒนาระบบต้องหลีกเลี่ยงการใช้ ข้อมูลจริงในการทดสอบระบบ หากจำเป็นต้องได้รับอนุญาตจาก เจ้าของข้อมูลก่อน และผู้พัฒนาระบบต้องควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริง และควรเก็บ Source Code ไว้ในที่ที่ปลอดภัย
- 13.3 ต้องกำหนดขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ ใช้งานจริงและต้องตรวจสอบเมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง เพื่อให้มั่นใจว่าแอป พลิเคชันที่ทำงานอยู่นั้น ทำงานผิดปกติหรือเกิดปัญหาขึ้นหรือไม่รวมทั้งไม่แก้ไขเปลี่ยนแปลงต่อ ซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นให้แก้ไขตามความจำเป็นเท่านั้น
- 13.4 ต้องป้องกันการรั่วไหลของสารสนเทศ หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไปและ ต้องกำหนดมาตรการควบคุมและตรวจสอบการว่าจ้างให้พัฒนาระบบต้องมีความชัดเจน รวมถึงการ รับรองคุณภาพของระบบ และกำหนดขอบเขตในการว่าจ้างด้วย
- 13.5 เพื่อลดความเสี่ยงจากการโจมตี โดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่ต้องมีการติดตาม ข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ อย่างสม่ำเสมอ

14. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท

- 14.1 ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท เช่น จุดอ่อนใด ๆ ให้แก่ผู้บังคับบัญชา หรือส่วนงานเทคโนโลยีสารสนเทศทันทีที่พบหรือสงสัยว่ามีสิ่งผิดปกติเกิดขึ้น และต้องกำหนดหน้าที่และความรับผิดชอบเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคง ปลอดภัยของหน่วยงานโดยต้องมีการบันทึกเหตุการณ์ พิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่ เกิดขึ้นและค่าใช้จ่ายที่เกิดขึ้นจากความเสียหาย
- 14.2 ต้องเก็บรวบรวมหลักฐานตามกฎหมายหรือหลักเกณฑ์เพื่อใช้สำหรับอ้างอิงในกระบวนการศาลหรือที่ เกี่ยวข้อง

15. การบริหารความต่อเนื่องในการดำเนินงานของบริษัท

- 15.1 ต้องจัดลำดับความสำคัญของกระบวนการสร้างความต่อเนื่องทางธุรกิจ ระบุเหตุการณ์ที่ทำให้ กระบวนการทางธุรกิจหยุดชะงัก ความเป็นไปได้และผลกระทบที่จะเกิดขึ้น และ แผนบริหารความ ต่อเนื่องทางธุรกิจจะจัดทำขึ้นสำหรับระบบงานที่มีความสำคัญ
- 15.2 แผนบริหารความต่อเนื่องทางธุรกิจทั้งหมดจะได้รับการทดสอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเมื่อเกิดเหตุฉุกเฉิน แผนที่นำมาทดสอบสามารถใช้งานได้จริง



บริษัท ห้องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

- 15.3 ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจเพื่อให้แผนทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- 15.4 จัดทำระบบสำรองข้อมูลของระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของบริษัทสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของผู้ดูแลระบบในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมในกรณีฉุกเฉินหรือในกรณีที่ไม่สามารถดำเนินการได้อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง และแผนบริหารความต่อเนื่องทางธุรกิจดังกล่าวต้องถูกทบทวนและปรับปรุงหากมีความจำเป็น

16. การป้องกันโปรแกรมไม่ประสงค์

- 16.1 บริษัทและส่วนงานเทคโนโลยีสารสนเทศจะต้องใช้ซอฟต์แวร์ ที่มีกระบวนการในการจัดการและป้องกันโปรแกรมไม่ประสงค์ และพนักงานทุกคนต้องให้ความร่วมมือปฏิบัติตามนโยบายดังกล่าว รวมทั้งไม่ติดตั้งซอฟต์แวร์เอง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ทำงานแทน

17. การปฏิบัติตามข้อกำหนด

- 17.1 ผู้ใช้งานทุกคนมีหน้าที่ต้องทำความเข้าใจและปฏิบัติตามนโยบาย กฎระเบียบข้อบังคับกฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด ทั้งนี้ รวมถึงแต่ไม่จำกัดเฉพาะ
- นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
 - พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ 2550
 - พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์
 - พ.ร.บ.ลิขสิทธิ์
 - พ.ร.บ.เครื่องหมายการค้า
 - พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- 17.2 ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบสารสนเทศของบริษัท ถือเป็นทรัพย์สินของบริษัท ยกเว้นข้อมูลที่เป็นทรัพย์สินของลูกค้าหรือบุคคลภายนอก ซอฟต์แวร์หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตรหรือลิขสิทธิ์ของบุคคลภายนอก



บริษัท ห้องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

- 17.3 ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและแนวปฏิบัติข้อกำหนดที่ปรากฏในสัญญาและข้อกำหนดทางธุรกิจ รวมถึงต้องมีมาตรการป้องกันข้อมูลส่วนตัวตามที่ระบุไว้ในกฎหมาย แนวปฏิบัติ และสัญญาที่เกี่ยวข้อง
- 17.4 ต้องกำหนดให้มีการป้องกันสารสนเทศ ระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่ายและคอมพิวเตอร์แม่ข่าย ไม่ให้ใช้งานไปในทางที่ผิดหรือโดยไม่มีสิทธิ์ และต้องกำหนดให้ใช้มาตรการเข้ารหัสข้อมูลโดยให้ยึดถือตามหรือสอดคล้องกับข้อตกลงทางกฎหมาย
- 17.5 การทบทวน ตรวจสอบการใช้งานระบบทุกระบบเป็นสิทธิ์ที่บริษัทสามารถกระทำได้หากบริษัทเห็นว่าจำเป็น โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า
- 17.6 ต้องมีการตรวจสอบระบบว่ามีความมั่นคงปลอดภัยเพียงพอหรือไม่ โดยใช้ซอฟต์แวร์ค้นหาช่องโหว่และทดสอบการโจมตีระบบเพื่อตรวจสอบข้อบกพร่องของระบบด้วย
- 17.7 ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ และต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบไม่ให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด โดยกำหนดให้มีการแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบระบบสารสนเทศ

18. การคุ้มครองข้อมูลส่วนบุคคล (PDPA)

18.1 การใช้งาน E-mail

- 18.1.1 พนักงานต้องใช้รหัสผ่านที่ปลอดภัยและเป็นความลับเพื่อเข้าถึง E-mail และการใช้งาน E-mail ของพนักงานเพื่อเป็นไปโดยวัตถุประสงค์ในการใช้งานของบริษัทเท่านั้น
- 18.1.2 พนักงานไม่สามารถเปิด E-mail ของผู้อื่นได้โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล
- 18.1.3 ห้ามสำรอง E-mail หรือไฟล์แนบ ที่มีข้อมูลส่วนบุคคลไว้ในเครื่องส่วนบุคคลส่วนตัว
- 18.1.4 ห้ามส่งต่อข้อมูลส่วนบุคคลของลูกค้า ผู้ค้า หรือผู้ติดต่อออกสู่ภายนอก หากมีความจำเป็นในการส่งต่อข้อมูล ต้องมีการจัดบันทึกตามข้อกำหนด ROPA และหากเป็นข้อมูลอ่อนไหว ต้องได้รับความยินยอมจากเจ้าของข้อมูลทุกครั้ง
- 18.1.5 ต้องมีการทบทวนการลบข้อมูล E-mail ตามระยะเวลาการเก็บข้อมูลของแต่ละแผนกอย่างสม่ำเสมอ



บริษัท ห้องเย็นโชติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

18.1.6 กรณีที่พนักงานผู้มีสิทธิ์ในการใช้ E-mail ลาออก จะต้องมีการตรวจสอบ E-mail พนักงานที่เกี่ยวข้อง และดำเนินการทำการลบข้อมูลยุติการใช้ Email ดังกล่าวในทันที และลบข้อมูลออกภายใน 15 วัน

18.2 การใช้งาน Application Line

ในการใช้งาน Application Line เพื่อติดต่อสื่อสารงานภายในบริษัทนั้น ต้องปฏิบัติตามข้อกำหนดดังนี้

18.2.1 ในการจัดตั้งกลุ่ม Line ต้องแจ้งให้ทางฝ่ายสารสนเทศรับทราบ ผ่านทางแบบฟอร์มในระบบ Ticket โดยระบุชื่อกลุ่ม จุดประสงค์ และผู้ดูแลประจำกลุ่มเพื่อควบคุมการใช้งานภายในกลุ่มนั้น ๆ หากมีการละเมิดจากการใช้งานกลุ่ม Line ที่ไม่ได้ขึ้นทะเบียนไว้ ทางบริษัทจะพิจารณาลงโทษทางวินัยขั้นร้ายแรงตามความเสียหายที่เกิดขึ้น

18.2.2 ห้ามส่งต่อข้อมูลส่วนบุคคลของลูกค้า ผู้ค้า หรือผู้ติดต่อออกสู่ภายนอก หากมีความจำเป็นในการส่งต่อข้อมูล ต้องมาการจดบันทึกตามข้อกำหนด ROPA และหากเป็นข้อมูลอ่อนไหว ต้องได้รับความยินยอมจากเจ้าของข้อมูลทุกครั้ง

18.2.3 ในกรณีมีพนักงานพ้นสภาพ ให้ทางผู้ดูแลกลุ่มลบบรายชื่อพนักงานผู้นั้นออกจากกลุ่มโดยทันที ภายใน 3 วัน

18.3 การใช้งาน Website และ Social Media

18.3.1 ห้ามพนักงาน Post ห้ามนำไปใช้หรือแอบอ้างข้อมูลของบริษัท ข้อมูลของลูกค้า ผู้ค้า หรือผู้ติดต่อไม่ว่าจะเป็นช่องทาง Website, Social Media หรือช่องทางอื่น ๆ ยกเว้น Website ของหน่วยงานรัฐ ที่จำเป็นต้องนำส่งข้อมูลดังกล่าวเท่านั้น

18.3.2 ให้พนักงานใช้สื่อ Social Media ด้วยความระมัดระวัง ไม่ Post หรือนำเข้าข้อมูลที่สามารถระบุถึงบริษัท หรือบุคคลอื่นในทางเสียหายโดยเด็ดขาด

18.4 การจัดเก็บและใช้ข้อมูลส่วนบุคคลของพนักงานในการทำงาน ในรูปแบบไฟล์ข้อมูลในเครื่องคอมพิวเตอร์ส่วนบุคคล และอุปกรณ์จัดเก็บข้อมูลส่วนบุคคลในการทำงานอื่น ๆ ที่เกี่ยวข้อง โดยทางฝ่ายเทคโนโลยีสารสนเทศทำการ Backup ข้อมูลสำรองไว้ (ภายในองค์กร)



บริษัท ห้องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

18.5 การนำส่งเครื่องคอมพิวเตอร์และอุปกรณ์จัดเก็บข้อมูลหรือให้บุคคลภายนอกทำการซ่อมแซม บำรุงรักษา จะต้องมีการทำข้อตกลงในการ Data Protection Agreement ระหว่างกันในการ รักษาข้อมูลส่วนบุคคล

18.6 มาตรการการรักษาความปลอดภัยของบุคลากร ลูกค้า คู่ค้า และผู้มาติดต่อที่เข้ามาในองค์กรจะมีการ จัดเก็บและปฏิบัติตาม นโยบายความเป็นส่วนตัวในการใช้งานกล้องวงจรปิด (CCTV)

18.7 การส่งโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ รวมถึงการนำข้อมูลส่วนบุคคลไปเก็บไว้ในบน ฐานข้อมูลในระบบอื่นใด ซึ่งผู้ให้บริการรับโอนข้อมูลหรือปลายทางที่มีการส่งข้อมูลในการเก็บรักษา ข้อมูลอยู่ต่างประเทศ ประเทศปลายทางที่เก็บรักษาข้อมูลต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคล ที่เทียบเท่าหรือดีกว่ามาตรการตามนโยบายนี้

18.8 ในกรณีเกิดการละเมิดการใช้ข้อมูลส่วนบุคคล ผู้ได้รับผลกระทบสามารถร้องเรียนเหตุที่เกิดขึ้น โดยตรงผ่านช่องทางการส่งเอกสารทางจดหมาย ถึง

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)


บริษัท ห้องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ 3 ถนนสายเอเชีย 43 ตำบลนาหม่อม อำเภอนาหม่อม จังหวัดสงขลา 90310

หรือ ผ่านทาง E-mail: dpo@kst-hatyai.com

หรือ ทาง Website: <https://www.kst-hatyai.com/pdpa>

ทั้งนี้ บริษัทฯ จะทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและการบริหารความต่อเนื่อง ของระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มีความสอดคล้องกับพัฒนาการด้านเทคโนโลยีสารสนเทศและ การดำเนินธุรกิจที่อาจมีการเปลี่ยนแปลง

ลงชื่อ.....

(ดร.สุรพล อารีย์กุล)

ประธานกรรมการบริษัท



บริษัท ห่องเย็นโซติวัฒน์หาดใหญ่ จำกัด (มหาชน)

4/2 หมู่ที่ 3 ถ.สายเอเชีย 43 ต.นาหม่อม อ.นาหม่อม จ.สงขลา 90310

TEL : 0-7422-2333 FAX : 0-7422-2300-1 www.kst-hatyai.com

เลขประจำตัวผู้เสียภาษี : 0107537002231

หมายเหตุ

1. ผ่านการพิจารณาอนุมัติทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ตามมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2567 เมื่อวันที่ 22 กุมภาพันธ์ 2567 และมีผลบังคับใช้ตั้งแต่วันที่ 23 กุมภาพันธ์ 2567 เป็นต้นไป