บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)

นโยบายการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

IT Security Policy

สารบัญ

1. วัตถุประสงค์

เพื่อให้มีนโยบายและกระบวนการปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลและระบบเทคโนโลยีสารสนเทศตามมาตรฐานทั้งภายในประเทศและสากล ส่งเสริมให้พนักงานและผู้ที่เกี่ยวข้องตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย สร้างความมั่นใจและความน่าเชื่อถือในการให้บริการแก่ลูกค้า ผู้ถือหุ้น ผู้ลงทุน และผู้มีส่วนได้เสียของ และสนับสนุนการปฏิบัติให้สอดคล้องตามข้อกำหนดของธนาคารแห่งประเทศไทย พระราชบัญญัติและกฎหมายที่เกี่ยวข้อง

2. ขอบเขตนโยบาย

นโยบายความปลอดภัยข้อมูลและระบบเทคโนโลยีสารสนเทศ ฉบับนี้มีผลบังคับใช้ต่อพนักงานและผู้บริหารของทุกระดับ พนักงานชั่วคราว พนักงานจ้างทดลอง ที่ปรึกษา บริษัทคู่ค้า คู่สัญญา บริษัทคู่ขาย และบุคคลอื่นๆ ที่ใช้ทรัพยากรข้อมูลและระบบเทคโนโลยีสารสนเทศทั้งหมด ได้แก่ ข้อมูลและทรัพยากรทั่วไป ระบบและทรัพยากรคอมพิวเตอร์ ระบบและทรัพยากรเครือข่าย ระบบปฏิบัติการ ระบบงานและโปรแกรมที่เป็นเจ้าของ เป็นผู้พัฒนา เป็นผู้ดูแล หรือเช่า/ซื้อจากอื่น รวมทั้งกรรมสิทธิ์ ลิขสิทธิ์ที่มีสิทธิ์โดยชอบธรรมตามกฎหมาย

ทั้งนี้ กำหนดให้ทบทวนนโยบายความปลอดภัยข้อมูลและระบบเทคโนโลยีสารสนเทศ อย่างน้อยปีละครั้ง หรือเมื่อมีการปรับปรุงเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และเพื่อกฎระเบียบ กฎหมายที่เกี่ยวข้องเปลี่ยนแปลง

3. คำจำกัดความ

ข้อมูล(Data) หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากการสกัดข้อมูลให้มีความหมายโดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย เช่น รายงาน ตาราง แผนภูมิ เป็นต้น และสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผนและการตัดสินใจและอื่น ๆ

เทคโนโลยีสารสนเทศ (Information Technology) หมายถึง ความรู้ในผลิตภัณฑ์ หรือในกระบวนการดำเนินการใด ๆ ที่อาศัยเทคโนโลยี ซอฟต์แวร์ ฮาร์ดแวร์ การติดต่อสื่อสาร การรวบรวม การนำสารสนเทศมาใช้หรือเผยแพร่

ระบบสารสนเทศ (Information System) หมายถึง ระบบข่าวสารของที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสารมาช่วยในการสร้างสารสนเทศ นำมาใช้ในการวางแผน การบริหารการพัฒนาและควบคุม ซึ่งมีองค์ประกอบดังนี้ ระบบคอมพิวเตอร์ (Computer System) ระบบสื่อสาร (Communication System) และสารสนเทศ (Information) ซึ่งดำเนินการในระบบคอมพิวเตอร์

ระบบคอมพิวเตอร์ (Computer System) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ประกอบด้วย ส่วนเครื่อง (Hardware) ส่วนชุดคำสั่ง (Software) และบุคลากรทางคอมพิวเตอร์ (People ware) ที่ใช้ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ

เครือข่ายระบบสารสนเทศ (Information Technology Network) หมายถึง การติดต่อสื่อสารหรือการส่งข้อมูลกัน ระหว่างระบบสารสนเทศของ เช่น ระบบอินทราเน็ต (Intranet) ระบบอินเตอร์เน็ต(Internet) เป็นต้น

ระบบการสื่อสาร (Communication System) หมายถึง ระบบที่ประกอบด้วยผู้รับ ผู้ส่ง และสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล(ตัวอักษร ตัวเลข ภาพ เสียง เป็นต้น) ทั้งระบบวงจรทางสาย เช่น สายเคเบิล (Cable) โคแอกเซียล (Coaxial Cable) เส้นใยนำแสง (Fiber Optic) และระบบไร้สาย (Wireless) เช่น โทรศัพท์เคลื่อนที่ ไมโครเวฟ (Microwave) ดาวเทียม (Satellite) รวมทั้งอุปกรณ์อื่น ๆ เช่น ฮับ (Hub) การสลับ (Switching) อุปกรณ์จัดเส้นทาง (Router)

พื้นที่ใช้งานระบบสารสนเทศ (Information System Workspaces) หมายถึง พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ หรือเตรียมข้อมูล เก็บอุปกรณ์คอมพิวเตอร์ พื้นที่ที่เป็นห้องทำงานของบุคลากรทางคอมพิวเตอร์ รวมทั้ง เครื่องคอมพิวเตอร์ส่วนบุคคลที่ติดตั้งประจำโต๊ะทำงาน

การรักษาความปลอดภัยข้อมูล (Information Security) หมายถึง การรักษาความลับของข้อมูล เพื่อให้ข้อมูลมีความครบถ้วนถูกต้องและพร้อมสำหรับนำไปใช้ โดยมีรายละเอียดในการรักษาความปลอดภัยข้อมูล ดังนี้

- การรักษาความลับของข้อมูล คือ การปกป้องความปลอดภัยข้อมูลอย่างเหมาะสม เพื่อให้บุคคลที่จะเข้าถึงระบบและข้อมูลของเป็นบุคคลที่ได้รับอนุญาตถูกต้อง
- ความครบถ้วนถูกต้องของข้อมูล คือ การป้องกันรักษาข้อมูลให้มีความครบถ้วนถูกต้อง โดยทุกครั้งที่มีการปรับปรุงเปลี่ยนแปลงจะต้องได้รับอนุญาต
- ความพร้อมใช้ของข้อมูล คือ การดูแลระบบและข้อมูลเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพและต่อเนื่องตามเกณฑ์เวลาที่กำหนด

ภัย (Threat) หมายถึง อันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศโดยคน สิ่งต่าง ๆ หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนา อันเป็นเหตุทำให้ข้อมูลข่าวสารของระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่น ๆ ตามความต้องการของภัยนั้น

ความอ่อนแอ (Vulnerability) หมายถึง จุดอ่อน หรือข้อบกพร่องใด ๆ ของระบบสารสนเทศ ที่ภัย(Threat) ในรูปแบบที่เหมาะกันสามารถนำไปใช้ประโยชน์เพื่อก่อให้เกิดอันตรายต่อระบบสารสนเทศ นั้น ๆ ได้

4. เนื้อหานโยบาย

4.1. นโยบายความมั่นคงปลอดภัย (Security Policy)

นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information Security Policy)

4.1.1. จัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศของเป็นลายลักษณ์อักษร โดยต้องได้รับอนุมัติจากผู้บริหารระดับสูงของก่อนนำไปใช้ ดำเนินการเผยแพร่ให้ พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบ

4.1.2. กำหนดหน่วยงานทำหน้าที่รับผิดชอบจัดทำแนวนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ และทำการทบทวนนโยบายตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

4.2. โครงสร้างทางด้านความมั่นคงปลอดภัยภายใน (Internal Organization Security)

4.2.1. โครงสร้างทางด้านความมั่นคงปลอดภัยภายใน (Internal Organization)

- กำหนดมาตรการและแนวปฏิบัติที่ชัดเจนในการบริหารจัดการทางด้านความมั่นคงปลอดภัย และสอดคล้องกับโครงสร้างของ รวมทั้งให้จัดตั้งตัวแทนของหน่วยงานในการบริหารจัดการ การประสานงาน และการให้คำแนะนำปรึกษาภายในหน่วยงาน
- กำหนดและแบ่งแยกหน้าที่ความรับผิดชอบของพนักงานให้ชัดเจน รวมทั้งจัดให้มีการตรวจสอบตามระยะเวลาที่กำหนด เพื่อให้สอดคล้องและเป็นไปตามนโยบายความมั่นคงปลอดภัยของ
- กำหนดมาตรการในการอนุมัติการใช้งานระบบ และ/หรืออุปกรณ์ประมวลผลสารสนเทศใหม่ รวมทั้งควบคุมให้ปฏิบัติตาม
- จัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับเรื่องการไม่เปิดเผยความลับของ รวมทั้งต้องปรับปรุงเงื่อนไขหรือข้อกำหนดต่าง ๆ ที่เกี่ยวข้องอย่างสม่ำเสมอ
- จัดให้มีมาตรการควบคุมการแลกเปลี่ยนข้อมูลที่เกี่ยวกับระบบความปลอดภัย โดยมาตรการที่นำมาปฏิบัติต้องรัดกุมเพียงพอที่จะทำให้ข้อมูลสำคัญของไม่ถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาต
- จัดทำรายชื่อและข้อมูลเพื่อการติดต่อประสานงานด้านความมั่นคงปลอดภัยทั้งหน่วยงานภายใน หน่วยงานของรัฐ และองค์กรต่าง ๆ ที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยสารสนเทศ

- กำหนดให้มีผู้ตรวจสอบอิสระทำการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ ตามระยะเวลาที่กำหนด หรือทุกครั้งที่มีการเปลี่ยนแปลงสำคัญ

4.2.2. โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)

- กำหนดมาตรการในการเข้าถึงสารสนเทศของหน่วยงานภายนอก โดยให้ทำการ ประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการเข้าถึงสารสนเทศ
- กรณีที่ลูกค้า ผู้ใช้บริการ หรือหน่วยงานภายนอก มีความจำเป็นต้องเข้าถึงสารสนเทศ หรือทรัพย์สินสารสนเทศของบริษัท ต้องระบุและจัดทำข้อตกลง/สัญญาที่เกี่ยวกับความมั่นคงปลอดภัย พร้อมระบุเหตุผลความจำเป็นในการเข้าใช้งานอย่างชัดเจน ทั้งนี้ต้องควบคุมการใช้งานของหน่วยงานภายนอกอย่างเคร่งครัด

4.3. การบริหารจัดการทรัพย์สินของ (Asset Management)

4.3.1. หน้าที่ความรับผิดชอบต่อทรัพย์สินของ (Responsibility for Assets)

- จัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินสารสนเทศให้ถูกต้องอยู่เสมอ โดยระบุผู้รับผิดชอบหน่วยงานผู้เป็นเจ้าของสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับ การประมวลผลสารสนเทศ รวมทั้งตรวจสอบบัญชีทรัพย์สินสารสนเทศตามระยะเวลาที่กำหนด
- จัดทำกฎ ระเบียบ หรือวิธีปฏิบัติสำหรับการใช้งานทรัพย์สินสารสนเทศ เพื่อป้องกันความเสียหายจากการใช้งานที่ไม่ถูกต้อง

4.3.2. การจัดหมวดหมู่สารสนเทศ (Information Classification) จัดหมวดหมู่ตามลำดับความสำคัญของข้อมูลและทรัพย์สินสารสนเทศ รวมทั้งกำหนดมาตรการ ในการควบคุมป้องกันที่เหมาะสม และเป็นไปตามข้อกำหนดทางกฎหมาย

4.4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

4.4.1. การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to Employment)

- กำหนดเงื่อนไขการจ้างงาน หน้าที่ความรับผิดชอบ การตรวจสอบคุณสมบัติ และจัดให้มีการลงนามในสัญญา/ข้อตกลงการจ้างงานระหว่างบุคลากรที่ต้องการจ้าง ผู้ที่มาปฏิบัติงานจากหน่วยงานภายนอก และ ทั้งนี้ต้องควบคุมให้ปฏิบัติตามสัญญา การจ้างงาน นโยบาย และวิธีปฏิบัติด้านความปลอดภัยสารสนเทศของอย่างเคร่งครัด

4.4.2. การสร้างความมั่นคงปลอดภัยระหว่างการจ้างงาน (During Employment)

- จัดการฝึกอบรมและประชาสัมพันธ์นโยบายความมั่นคงปลอดภัยอย่างสม่ำเสมอ เพื่อให้พนักงานและหน่วยงานภายนอกได้รับทราบและปฏิบัติตามได้ถูกต้อง โดยหน่วยงานที่เกี่ยวข้องต้องจัดทำ/ปรับปรุงคู่มือและขั้นตอนการปฏิบัติงานให้เป็นปัจจุบันเสมอ
- กำหนดมาตรการลงโทษทางวินัย เพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายและ/หรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของ

4.4.3. การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or Change of Employment)

- กำหนดวิธีปฏิบัติสำหรับผู้ที่เลิกจ้าง หรือเปลี่ยนลักษณะการจ้างให้หน่วยงานที่รับผิดชอบควบคุมให้ปฏิบัติตามอย่างเคร่งครัด
- พนักงานที่เลิกจ้าง หรือเปลี่ยนลักษณะการจ้าง ไม่อนุญาตให้มีสิทธิ์ใน การเข้าถึง เปลี่ยนแปลง หรือกระทำการใดๆ กับข้อมูลระบบสารสนเทศของ โดยกำหนดให้หน่วยงานที่รับผิดชอบต้องดำเนินการถอดถอนสิทธิ์ การเข้าถึงข้อมูลและระบบสารสนเทศของทุกระบบโดยเร็ว และต้องส่งมอบทรัพย์สินของทั้งหมดที่อยู่ในความรับผิดชอบในขณะปฏิบัติงานคืน

4.5. ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

4.5.1. บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

- กำหนดพื้นที่ควบคุมเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ดังกล่าวอย่างเคร่งครัด เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อระบบสารสนเทศ อุปกรณ์ และการประมวลผลสารสนเทศของ
- จัดการควบคุมและตรวจสอบการปฏิบัติของหน่วยงานภายนอกที่เข้ามาปฏิบัติงานในบริเวณพื้นที่ควบคุม โดยพนักงานเจ้าของพื้นที่ ตลอดเวลาของการปฏิบัติงานนั้น
- จัดให้มีการป้องกันทางกายภาพ และแนวทางปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยให้กับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ ของ เพื่อให้ปลอดภัยจากความเสี่ยงอันเนื่องมาจากอุบัติภัยและเหตุการณ์ภายนอก เช่น อุบัติเหตุ อัคคีภัย อุทกภัย แผ่นดินไหว การก่อการร้าย เป็นต้น

4.5.2. การรักษาความปลอดภัยสำหรับศูนย์คอมพิวเตอร์ (Securing Data Center)

- ควรจัดทำระเบียบปฏิบัติและระบบการรักษาความปลอดภัยในการเข้าออกศูนย์คอมพิวเตอร์ และจัดเตรียมอุปกรณ์หรือระบบในการป้องกัน เตือนภัยในศูนย์คอมพิวเตอร์อย่างเพียงพอ ในการป้องกันภัยที่จะเกิดขึ้น รวมทั้งตรวจสอบการทำงานของระเบียบและระบบดังกล่าว อย่างสม่ำเสมอ

- การเข้าออกศูนย์คอมพิวเตอร์ ต้องมีการควบคุม ตรวจสอบ และอนุญาตเฉพาะพนักงานที่มีสิทธิ หรือบุคคลภายนอกที่ได้รับอนุญาตจากผู้ดูแลศูนย์คอมพิวเตอร์เท่านั้น
- การปฏิบัติงานในศูนย์คอมพิวเตอร์ ควรมีเอกสารในการปฏิบัติงานและมีการปฏิบัติตาม
- คู่มือหรือเอกสารในการปฏิบัติงาน ต้องมีการปรับปรุงให้ทันสมัย และสามารถใช้งานได้
- ติดตั้งระบบตรวจสอบและป้องกันความเสียหายตามความเหมาะสม เช่น ระบบกล้องวงจรปิดระบบป้องกันกระแสไฟขัดข้อง ระบบป้องกันเพลิงไหม้ ระบบตรวจสอบความชื้นและควัน เป็นต้น
- ควรมีระบบการป้องกันมิให้ระบบคอมพิวเตอร์เกิดความเสียหายจากความไม่คงที่ของกระแสไฟ
- ระบบสำรองไฟ (UPS) ต้องมีการติดตั้ง เพื่อให้ระบบให้บริการได้ในกรณีระบบไฟฟ้าขาดแคลนหรือขัดข้อง
- ระบบไฟสำรอง (Grid) มีตามที่จำเป็น เพื่อให้ระบบให้บริการได้อย่างเพียงพอ ในกรณีระบบไฟฟ้าขัดข้องหรือขาดแคลน
- ตรวจสอบและทดสอบการทำงานของระบบป้องกันความเสียหายต่างๆภายในศูนย์คอมพิวเตอร์ อย่างสม่ำเสมอ ตามระยะเวลาที่กำหนดไว้ในข้อกำหนดของการดูแลแต่ละอุปกรณ์หรือระบบ

4.5.3. ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

- การจัดวางอุปกรณ์สำนักงานต้องคำนึงถึงความเสี่ยงในการเข้าถึงโดยไม่ได้รับอนุญาต และภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ ที่อาจเกิดขึ้น โดยกำหนดมาตรการจัดวางอุปกรณ์สำนักงานให้เป็นไปอย่างปลอดภัย
- ระบบและอุปกรณ์สนับสนุนที่มีความสำคัญ ได้แก่ ระบบกระแสไฟฟ้าสำรอง ระบบสื่อสารสำรอง ระบบควบคุมอุณหภูมิ ระบบปรับอากาศ ระบบระบายอากาศ เป็นต้น ต้องกำหนดวิธีการป้องกันให้สามารถใช้งานได้อย่างต่อเนื่อง ไม่เกิดปัญหาต่อระบบสารสนเทศของ
- สายไฟฟ้า สายสื่อสาร และสายเคเบิ้ลอื่น ๆ ต้องได้รับการป้องกันและดูแลอย่างเหมาะสม และป้องกันการเข้าถึง การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือ การทำให้สายสัญญาณเหล่านั้นเสียหายโดยไม่ได้รับอนุญาต
- กำหนดวิธีการและผู้รับผิดชอบในการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพสมบูรณ์พร้อมใช้งาน

- การนำทรัพย์สินสารสนเทศทุกประเภทออกนอก ต้องได้รับอนุญาตก่อน และต้องมีการควบคุมอย่างเคร่งครัด กำหนดวิธีปฏิบัติโดยพิจารณาจาก ความเสี่ยงหรือโอกาสต่าง ๆ ที่จะก่อความเสียหายต่ออุปกรณ์เหล่านั้น

4.6. การบริหารจัดการด้านการสื่อสารและการปฏิบัติงานเครือข่ายสารสนเทศของ(Communication and Operation Management)

4.6.1. หน้าที่ความรับผิดชอบและขั้นตอน การปฏิบัติงาน (Operational Procedures and Responsibilities)

- จัดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุง แก้ไขระบบและ/หรืออุปกรณ์ประมวลผลสารสนเทศ ให้หน่วยงานที่เกี่ยวข้องได้รับทราบและปฏิบัติ
- แบ่งแยกหน้าที่ความรับผิดชอบ วิธีปฏิบัติในการดำเนินงาน วิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือละเมิดความมั่นคงปลอดภัยเกี่ยวกับระบบสารสนเทศและเครือข่าย เพื่อป้องกัน ลดโอกาสในการเปลี่ยนแปลง หรือแก้ไขโดยไม่ได้รับอนุญาต หรือการใช้ทรัพย์สินสารสนเทศของผิดวัตถุประสงค์
- แยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการจริงออกจากกัน รวมทั้งแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบสารสนเทศออกจากเครื่องคอมพิวเตอร์ที่ใช้ให้บริการจริง เพื่อลดความเสี่ยงในการเข้าถึง หรือเปลี่ยนแปลงแก้ไขระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต

4.6.2. การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third Party Service Delivery Management)

การใช้บริการจากหน่วยงานภายนอก ต้องกำหนดให้ผู้ให้บริการปฏิบัติตามข้อกำหนดและ/หรือข้อตกลงด้านมาตรการรักษาความมั่นคงปลอดภัย ลักษณะของ การให้บริการ และระดับของการให้บริการ รวมทั้งการควบคุมการใช้งาน การเข้าถึงระบบตามสิทธิ์ที่ได้รับ นอกจากนั้นต้องทำการปรับปรุงเงื่อนไขการให้บริการเมื่อมี การเปลี่ยนแปลงที่สำคัญขององค์กรของผู้ให้บริการ ซึ่งอาจเกิดผลกระทบต่อระบบหรือกระบวนการที่เกี่ยวข้องกับการให้บริการของหน่วยงานภายนอก

4.6.3. การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance)

- กำหนดให้หน่วยงานดำเนินการวางแผนกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติม เพื่อให้ได้ระบบที่มีประสิทธิภาพและสามารถรองรับการใช้งานที่จะเพิ่มขึ้นได้ในอนาคต

- กำหนดเกณฑ์ที่ใช้ในการทดสอบ การตรวจรับระบบสารสนเทศใหม่ ปรับปรุงเพิ่มเติม เปลี่ยนเป็นรุ่นใหม่ และอื่น ๆ ก่อนนำมาใช้งานจริงทุกครั้ง

4.6.4. การป้องกันโปรแกรมไม่ประสงค์ดี (Protection against Malicious)

- กำหนดมาตรการและวิธีปฏิบัติในการตรวจจับ การป้องกัน การกู้กลับคืน และปรับปรุงให้ทันสมัยอยู่เสมอ ร่วมทั้งสร้างความตระหนักในการระมัดระวัง หลีกเลี่ยงการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ที่อาจเกิดความเสี่ยงต่อ การติดต่อและระบาดของโปรแกรมดังกล่าวให้กับผู้ใช้งานอย่างสม่ำเสมอ

4.6.5. การสำรองข้อมูล (Back-up)

สำรองและทดสอบข้อมูลสำรองอย่างสม่ำเสมอ รวมถึงการสำรองข้อมูลภายนอกหน่วยงาน โดยให้เป็นไปตามมาตรฐานการสำรองข้อมูลของ

4.6.6. การบริหารจัดการความมั่นคงปลอดภัยเครือข่ายสารสนเทศ (Network Security Management)

- กำหนดมาตรการและหน้าที่ความรับผิดชอบในการดูแลระบบปฏิบัติการ ระบบงานที่ใช้งานผ่านเครือข่าย และสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่ายสารสนเทศของ เพื่อลดความเสี่ยงและป้องกันภัยคุกคามต่างๆ ทางระบบเครือข่าย
- กำหนดคุณสมบัติด้านความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดใน การบริหารจัดการการให้บริการเครือข่าย การให้บริการเครือข่ายภายใน และบริการที่ได้รับจากหน่วยงานภายนอก สำหรับทุกข้อตกลงการใช้บริการเครือข่ายที่ใช้บริการ

4.6.7. การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media Handling)

- กำหนดขั้นตอนปฏิบัติและสิทธิ์สำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้
- กำหนดขั้นตอนวิธีปฏิบัติในการทำลายข้อมูลที่อยู่ในอุปกรณ์หรือสื่อบันทึกข้อมูล เพื่อให้มั่นใจว่าข้อมูลสำคัญ และซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในอุปกรณ์หรือสื่อบันทึกนั้นๆ ถูกทำลายทั้งหมดก่อนที่จะเลิกใช้หรือทิ้งไป ทั้งนี้เพื่อป้องกันข้อมูลถูกเปิดเผย หากมีการนำอุปกรณ์หรือสื่อบันทึกข้อมูลมาใช้อีก
- กำหนดขั้นตอนปฏิบัติสำหรับการจัดการ การจัดเก็บสารสนเทศ และการป้องกันเอกสารระบบงาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต หรือการใช้งานผิดวัตถุประสงค์ ป้องกันการรั่วไหล หรือข้อมูลสำคัญถูกเปิดเผยโดยไม่ได้รับอนุญาต

4.6.8. การแลกเปลี่ยนสารสนเทศ (Exchange of Information)

- กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับการควบคุมและป้องกันปัญหาการใช้งานระบบสำนักงานอัตโนมัติ การแลกเปลี่ยนสารสนเทศระหว่าง โดยผ่านช่องทางการสื่อสารทุกชนิด โดยป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเสียหาย ในระหว่างการส่งข้อมูลออกไปนอก
- การแลกเปลี่ยนสารสนเทศ และซอฟต์แวร์ระหว่างกับหน่วยงานภายนอกต้องจัดทำเป็นลายลักษณ์อักษร
- กำหนดระเบียบปฏิบัติการใช้งานไปรษณีย์อิเล็กทรอนิกส์ เพื่อป้องกันสารสนเทศที่มีการส่งผ่านทางอิเล็กทรอนิกส์
- กำหนดนโยบาย ขั้นตอนปฏิบัติและวิธีการควบคุมการเชื่อมต่อระบบสารสนเทศของกับบุคคลหรือหน่วยงานภายนอก

4.6.9. การเฝ้าระวังด้านความมั่นคงปลอดภัย (Monitoring)

- บันทึกเหตุการณ์การใช้งานสารสนเทศ (Audit log) กิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ การบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ และ/หรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนด และดำเนินการวิเคราะห์เพื่อหาแนวทางแก้ไขที่เหมาะสม
- กำหนดขั้นตอนปฏิบัติเพื่อตรวจสอบข้อมูล (Monitoring System Use) กิจกรรมการเข้าใช้งานที่ได้บันทึกเก็บไว้อย่างสม่ำเสมอตามระยะเวลาที่กำหนด รวมทั้งกำหนดมาตรการป้องกันการเข้าถึงข้อมูลบันทึกกิจกรรมหรือเหตุกาณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการถูกเปลี่ยนแปลงแก้ไขหรือทำลายโดยไม่ได้รับอนุญาต
- การปฏิบัติงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้อง ต้องบันทึกกิจกรรมและตรวจสอบอย่างสม่ำเสมอ
- เครื่องคอมพิวเตอร์ทุกเครื่องของต้องตั้งเวลาให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อใช้เป็นหลักฐานในการตรวจสอบช่วงเวลา

4.7. การควบคุมการเข้าถึง (Access Control)

4.7.1. ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

- จัดทำนโยบายและวิธีปฏิบัติเพื่อควบคุมการเข้าถึงสารสนเทศของ โดยพิจารณาจากความจำเป็นทางธุรกิจ และความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศ

4.7.2. การบริหารจัดการการเข้าถึงระบบของพนักงาน (User Access Management)

- กำหนดขั้นตอนการปฏิบัติและหน่วยงานผู้รับผิดชอบในการการกำหนดสิทธิ์ต่าง ๆ ให้กับพนักงานใหม่ รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งานเมื่อลาออก หรือเปลี่ยนตำแหน่งงานภายใน
- กำหนดสิทธิ์ ควบคุมและจำกัดสิทธิ์การใช้งานระบบสารสนเทศแต่ละระบบตามหน้าที่และความจำเป็นในการใช้งาน รวมทั้งจัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้
- มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน เพื่อควบคุมการจัดสรรหัสผ่านให้แก่ผู้ใช้งานอย่างมั่นคงปลอดภัย

4.7.3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

- กำหนดวิธีปฏิบัติในการกำหนดและเลือกใช้รหัสผ่าน การป้องกันผู้ไม่มีสิทธิ์ในการเข้าถึงอุปกรณ์สารสนเทศที่ไม่มีพนักงานดูแล และการควบคุมให้ทรัพย์สินสารสนเทศที่สำคัญอยู่ในสถานที่ที่ปลอดภัย

4.7.4. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

- กำหนดวิธีปฏิบัติและควบคุมการเข้าถึงบริการบนเครือข่ายของบริษัท โดยระบุบริการที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้และไม่สามารถใช้งานได้ สำหรับผู้ใช้บริการที่อยู่ภายนอกต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้เข้าใช้งานเครือข่ายและระบบสารสนเทศของ
- กำหนดให้อุปกรณ์บนเครือข่ายมีกระบวนการระบุและพิสูจน์ตัวตนเพื่อแสดงว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว รวมทั้งการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ก่อนที่จะเข้าใช้งานเครือข่ายของ
- กำหนดมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและการปรับแต่งระบบ ให้ครอบคลุมทั้งการป้องกันทางกายภาพ และการป้องกันการเข้าถึงโดยผ่านทางเครือข่ายสารสนเทศ

- กำหนดประเภทการเข้าใช้งานเครือข่ายของ เช่น แบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เป็นต้น
- กำหนดข้อจำกัดในการเชื่อมต่อทางเครือข่ายระหว่างกับหน่วยงานภายนอก โดยพิจารณาถึงการควบคุมการเข้าถึงและข้อกำหนดของระบบงานตามความต้องการทางธุรกิจ
- กำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อ และการไหลเวียนของสารสนเทศบนเครือข่าย ให้เป็นไปตามนโยบายควบคุมการเข้าถึง โดยให้ครอบคลุมถึงเครือข่ายที่มีการใช้งานร่วมกัน และเครือข่ายจากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อป้องกันการใช้เส้นทางอื่น ๆ

4.7.5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

- กำหนดขั้นตอนปฏิบัติและการควบคุมที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ
- กำหนดให้มีการพิสูจน์ตัวตนก่อนเข้าใช้งาน โดยผู้ใช้งานต้องมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน
- การบริหารจัดการรหัสผ่านต้องมีขั้นตอนปฏิบัติและวิธีการควบคุมการกำหนดรหัสผ่านที่มีประสิทธิภาพ
- การใช้งานโปรแกรมประเภทยูทิลิตี้ต้องเป็นไปอย่างเหมาะสม โดยให้มีการจำกัดและควบคุมเพื่อป้องกันการละเมิดหรือหลีกเลี่ยงความมั่นคงปลอดภัยของ
- กำหนดให้มีระบบตัดการใช้งานเมื่อผู้ใช้ไม่ได้ใช้งานระบบตามระยะเวลาที่กำหนดไว้ หรือจำกัดระยะเวลาการใช้งาน และระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญ/ความเสี่ยงสูง ทั้งนี้ให้รวมถึงเครื่องลูกข่ายที่ไม่ได้ใช้งานเป็นระยะเวลาหนึ่งด้วย

4.7.6. การควบคุมการเข้าถึงระบบงานและสารสนเทศ (Application and Information Access Control)

- จำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของระบบงาน โดยแยกการเข้าถึงตามประเภทของผู้ใช้งาน
- ระบบสารสนเทศที่มีความสำคัญ/ความเสี่ยงสูง ต้องแยกไว้ในบริเวณหรือขอบเขตที่กำหนดไว้โดยเฉพาะ

4.8. การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance)

4.8.1. ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

- วิเคราะห์และระบุข้อกำหนดหรือความต้องการทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว
- ระบุข้อกำหนดให้เป็นระบบสารสนเทศที่มีลักษณะ Straight through processing ที่หลีกเลี่ยงการป้อนข้อมูลซ้ำ (Re-Keying) หรือ การแทรกแซงโดยการป้อนข้อมูลด้วยมือ (Manual Intervention)

4.8.2. การประมวลผลสารสนเทศของระบบงาน (Correct Processing in Applications) เพื่อป้องกันความผิดพลาด การสูญหาย การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานผิดวัตถุประสงค์ ในการประมวลผลต้องกำหนดกระบวนการสอบทานความถูกต้องของข้อมูลดังนี้

- การตรวจสอบข้อมูลนำเข้า (Input Data Validation)
- การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of Internal Processing)
- การตรวจสอบความถูกต้องของข้อความสำหรับแอพพลิเคชั่น (Message Integrity)
- การตรวจสอบความถูกต้องของข้อมูลนำออกจากระบบงาน (Output data Validation)
- ห้ามนำข้อมูลออกไปประมวลผลภายนอกและนำกลับเข้าสู่ระบบด้วยการป้อนข้อมูลด้วยมือ (Manual Intervention) กรณีมีความจำเป็นเนื่องจากข้อจำกัดของระบบ ต้องจัดให้มีระเบียบระบุกระบวนการควบคุมความถูกต้อง ความครบถ้วน ความเร็วตามความจำเป็นในการใช้งาน การเก็บรักษา การรักษาความลับ และความพร้อมในการใช้งาน

4.8.3. มาตรการการเข้ารหัสข้อมูล (Cryptographic Controls)

- กำหนดนโยบายและวิธีปฏิบัติในการใช้กระบวนการและโปรแกรมการเข้ารหัส โดยระบบสารสนเทศและข้อมูลที่สำคัญของต้องได้รับการเข้ารหัส และต้องควบคุมการเข้ารหัสเป็นไปตามวิธีปฏิบัติอย่างเคร่งครัด
- กำหนดมาตรฐานวิธีการเข้ารหัสให้สามารถบริหารจัดการกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล รวมทั้งกำหนดให้มีการปรับปรุงมาตรฐานความยาวและอักขระของกุญแจเข้ารหัสให้เหมาะสม กับการปฏิบัติงานและเทคโนโลยีของบริษัท

4.8.4. การสร้างความมั่นคงปลอดภัยให้กับแฟ้มข้อมูลของระบบงาน (Security of System Files)

- กำหนดขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ยังระบบที่ให้บริการ และผ่านการทดสอบก่อนการติดตั้ง เพื่อลดความเสี่ยงที่จะทำให้ระบบทำงานผิดปกติ หรือไม่สามารถใช้งานได้
- ห้ามนำข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการมาใช้ทดสอบระบบ กรณีจำเป็นต้องใช้ต้องกำหนดขั้นตอนการอนุมัติ มาตรการป้องกัน และควบคุมการใช้งานอย่างเคร่งครัด
- ควบคุมการใช้งาน Library และจำกัดการเข้าถึง Source Code สำหรับระบบที่ให้บริการหรือระบบที่ใช้งานจริง ทั้งนี้เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนา

4.8.5. การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและกระบวนการสนับสนุน (Security in Development and Support Processes)

- กำหนดวิธีปฏิบัติในการควบคุมการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ และทำการตรวจสอบทางเทคนิคหลังจากที่เปลี่ยนแปลง เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหายหรือไม่สามารถใช้งานได้ และการเปลี่ยนแปลงแก้ไขแต่ละครั้งต้องคำนึงถึงมาตรการป้องกันการรั่วไหล หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป
- กรณีจำเป็นต้องแก้ไข หรือเปลี่ยนแปลงซอฟต์แวร์ที่มาจากผู้ผลิต ต้องแก้ไขตามความจำเป็นเท่านั้น และต้องควบคุมการแก้ไขนั้นอย่างเข้มงวด
- กำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก โดยเฉพาะการทำสัญญาว่าจ้างพัฒนาระบบ ต้องครอบคลุมสาระสำคัญ ได้แก่ ข้อตกลงทางด้านลิขสิทธิ์ การใช้งานระบบ การตรวจสอบระบบ และการรับรองคุณภาพของระบบเป็นต้น

4.8.6. การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

- กำหนดมาตรการในการบริหารจัดการช่องโหว่และควบคุมให้มีการลดช่องโหว่ที่เกิดขึ้นอย่างเหมาะสมและทันการ เพื่อลดความเสี่ยงที่เกิดจากช่องโหว่ในระบบ งานต่างๆ

4.9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information Security Incident Management)

4.9.1. การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events and Weakness)

- กำหนดขั้นตอนและวิธีปฏิบัติในการรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของ โดยพนักงานหรือผู้ที่ว่าจ้างหรือพนักงานของหน่วยงานภายนอกต้องปฏิบัติตามขั้นตอนดังกล่าวอย่างเคร่งครัด เพื่อให้สามารถแก้ไขปัญหาได้โดยเร็ว

4.9.2. การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of Information Security Incidents and Improvements)

- กำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อให้สามารถรองรับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของอย่างเป็นระบบ
- กำหนดรายละเอียดในการบันทึกเหตุการณ์ เช่น ประเภทเหตุการณ์ ปริมาณที่เกิดขึ้น ค่าใช่จ่ายที่เกิดขึ้นจากความเสียหาย เป็นต้น เพื่อใช้เป็นหลักฐานและเป็นข้อมูลประกอบในการแก้ไขปัญหาในครั้งต่อไป
- เก็บรวบรวมหลักฐานเหตุการณ์ที่เกิดขึ้น เพื่อสามารถใช้ในการดำเนินการทางกฎหมายทั้งทางแพ่งและ/หรือทางอาญา

4.10. การบริหารความต่อเนื่องทางธุรกิจของ (Business Continuity Management)

4.10.1. พื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานของ (Information Security Aspects of Business Continuity Management)

- กำหนดรายละเอียดในส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ โดยมีการวางแผนและการวิเคราะห์ความเสี่ยงจากการหยุดชะงักในการดำเนินงานที่สอดคล้องและครอบคลุมตามนโยบายความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ให้กำหนดระยะเวลาในการทดสอบและปรับปรุงแผนให้เหมาะสมและเป็นปัจจุบันเสมอ

4.11. การปฏิบัติตามข้อกำหนด (Compliance)

4.11.1. การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)

- ต้องระบุข้อกำหนดทางด้านกฎหมาย วิธีปฏิบัติที่ปรากฏในสัญญา (ระหว่าง และบุคคลหรือหน่วยงานภายนอกอื่น) เป็นลายลักษณ์อักษร ปรับปรุงให้เป็นปัจจุบัน และสอดคล้องกับข้อกำหนด ดำเนินการควบคุมให้มีการปฏิบัติตามอย่างเคร่งครัด
- กำหนดวิธีการป้องกันข้อมูลส่วนตัว ข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ จากการสูญหาย การถูก

ทำลายให้เสียหาย การปลอมแปลง การใช้งานอุปกรณ์ประมวลผลสารสนเทศ เพื่อป้องกันการใช้งานผิดวัตถุประสงค์ หรือนำไปใช้โดยไม่ได้รับอนุญาต

- มาตรการการเข้ารหัสข้อมูลของต้องสอดคล้องหรือเป็นไปในแนวเดียวกันกับนโยบายความมั่นคงปลอดภัยของ และไม่ขัดต่อข้อกำหนดของกฎหมาย

4.11.2. การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with Security Policies, Standards and Technical Compliance)

- กำหนดมาตรการให้ผู้บังคับบัญชาใช้กำกับดูแลและควบคุมการปฏิบัติของพนักงานผู้ใต้บังคับบัญชา ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศของ
- กำหนดให้มีการตรวจสอบระบบสารสนเทศ และรายละเอียดทางเทคนิคของระบบที่ใช้งานหรือให้บริการอยู่แล้วอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามนโยบาย และมาตรฐานด้านความปลอดภัยสารสนเทศของ

4.11.3. การตรวจประเมินระบบสารสนเทศ (Information Systems Audit Consideration)

- การตรวจประเมินระบบสารสนเทศของ ต้องกำหนดแนวทางในการตรวจให้ครอบคลุมและครบถ้วน ทั้งนี้แนวทางที่กำหนดไม่ควรกระทบ หรือกระทบต่อระบบและกระบวนการทางธุรกิจน้อยที่สุด
- การนำเครื่องมือต่างๆ มาใช้ในการตรวจประเมินผลระบบสารสนเทศ ต้องเป็นไปตามวิธีปฏิบัติในการเข้าถึงและได้รับการควบคุมเพื่อป้องกันไม่ให้มีการใช้งานผิดวัตถุประสงค์หรือการเปิดเผยข้อมูลต่อบุคคลที่ไม่ได้รับอนุญาต

4.11.4. การปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

- ระบุข้อกำหนดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้จัดทำระเบียบปฏิบัติที่เกี่ยวข้องกับการดำเนินธุรกิจ โดยปรับปรุงให้สอดคล้องกับพระราชบัญญัติดังกล่าว
- ให้การสนับสนุนในการป้องกันระบบคอมพิวเตอร์ใน เพื่อมิให้พนักงานใช้เป็นช่องทางก่อความเสียหาย รวมถึงชี้แจงให้พนักงานรับทราบความรับผิดชอบตามพระราชบัญญัติ และพนักงานที่ละเมิดถือเป็นความรับผิดชอบของพนักงานโดยตรง
- ให้ความร่วมมือกับเจ้าหน้าที่ในการตรวจสอบข้อมูลจากระบบคอมพิวเตอร์และข้อมูลบุคคลที่กระทำความผิดตามพระราชบัญญัติ

4.12. มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล

หลักการและเหตุผล

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพความพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ทั้งนี้เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลโดยปราศจากอำนาจ หรือโดยมิชอบ โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล

วัตถุประสงค์ของการรักษาความมั่นคงปลอดภัย เพื่อคุ้มครองสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และอำนาจในการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งกฎหมายรับรองไว้ให้ ด้วยเหตุนี้การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลจึงเป็นหน้าที่ประการหนึ่งตามกฎหมาย ที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องปฏิบัติเพื่อป้องกันมิให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งจะทำให้เกิดการละเมิดข้อมูลส่วนบุคคล

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

บริษัทจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล โดยครอบคลุมการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามกฎหมาย ทั้งมาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) โดยดำเนินการ ดังนี้

1. มาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard)

1.1 แจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ให้แก่ คณะกรรมการ ผู้บริหาร พนักงาน หรือผู้ปฏิบัติงานทุกระดับ และลูกจ้างทุกประเภทของบริษัท ตลอดจนคู่ค้า พันธมิตรทางธุรกิจ และ/หรือผู้มีส่วนได้เสียของบริษัททราบ รวมถึงสร้างเสริมความตระหนักรู้ถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าว เพื่อให้ปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

1.2 ระบุความเสี่ยงที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ การป้องกันความเสี่ยงที่อาจเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคาม และเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยให้เป็นไปตามนโยบายการรักษาความปลอดภัยทางสารสนเทศ กำหนดหน้าที่ความรับผิดชอบในการ

ดำเนินการเมื่อเกิดเหตุละเมิด และการรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ดังนี้

1.2.1 กำหนดตัวพนักงานผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ตัวแทนของบริษัทให้ ชัดเจน เช่น การส่งอีเมล และแจ้งทางโทรศัพท์มือถือเมื่อเกิดเหตุละเมิดที่มีความรุนแรง และเร่งด่วน

1.2.2 กำหนดวิธีการปฏิบัติให้ตัวแทนของบริษัท ที่มีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง นับแต่ทราบเหตุ ต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

1.2.3 การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตามข้อ 1.2.2 อาจได้รับการยกเว้นไม่ต้องดำเนินการได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล โดยจะดำเนินการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่น

a. ตัวอย่างกรณีความเสี่ยงต่ำ: ข้อมูลส่วนบุคคลถูกเข้ารหัส (ไม่สามารถเปิดอ่านได้หากไม่ทราบรหัสผ่าน) ถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เข้ารหัสจนไม่สามารถใช้งานได้ และไม่ได้ถูกโจรกรรมข้อมูลออกไป โดยระบบสำรองรองรับการบริการได้อย่างต่อเนื่อง กรณีนี้ถือได้ว่ามีความเสี่ยงต่ำที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล บริษัทจะดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) และไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลทราบ

b. ตัวอย่างกรณีความเสี่ยงสูง: เว็บไซต์รับสมัครงานออนไลน์ถูกละเมิด โดยผู้โจมตีทำการฝังมัลแวร์เพื่อเข้าถึงข้อมูลใบสมัครงานออนไลน์(ตรวจพบ หลังมัลแวร์ถูกติดตั้ง) เนื้อหาข้อมูลเป็นข้อมูลทั่วไปเพื่อการสมัครงาน อย่างไรก็ตาม ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ บริษัทจะดำเนินการบันทึก (เป็นการภายใน) ว่าเคยมีเหตุโจรกรรม พร้อมทั้งแจ้งเหตุดังกล่าว (ภายใน 72 ชั่วโมง) ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย

ทั้งนี้เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคลบริษัทต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยทุกครั้ง

1.3 กำหนดการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (User Responsibilities) โดยกำหนดสิทธิในรูปแบบต่างๆ เช่น สิทธิในการเข้าดู สิทธิในการแก้ไข

เพิ่มเติม สิทธิในการเปิดเผยและเผยแพร่ สิทธิในการตรวจสอบคุณภาพข้อมูล ตลอดจนสิทธิในการลบทำลาย

1.4 การบริหารจัดการการเข้าถึงมูลข้อมูลของผู้ใช้งาน (User Access Management) เพื่อเป็นการควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

1.5 จัดให้มีวิธีการตรวจสอบย้อนหลังในการเข้าถึง การเปลี่ยนแปลง การ หรือการถ่ายโอนข้อมูลส่วนบุคคล เพื่อให้สอดคล้อง เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

1.6 ในกรณีที่มีการฝ่าฝืนไม่ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยนี้ อันเนื่องมาจากความบกพร่องของบริษัททำให้เกิดการละเมิด หรือการรั่วไหลของข้อมูลส่วนบุคคล บริษัทจะดำเนินการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงรายละเอียดของเหตุการณ์ และแผนการเยียวยาความเสียหาย (หากมี) จากการละเมิดหรือการรั่วไหลดังกล่าว อย่างไรก็ตาม บริษัทจะไม่รับผิดชอบในความเสียหายใดๆ ที่เกิดจากการใช้ การเปิดเผย รวมถึงการประมาทเลินเล่อของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่นที่ได้รับความยินยอมจากเจ้าของข้อมูล

1.7 เมื่อพ้นระยะเวลาการใช้งานข้อมูลส่วนบุคคล หรือไม่มีความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลอีกต่อไป บริษัทจะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลออกจากระบบการจัดเก็บ เว้นแต่ในกรณีที่จะต้องเก็บรักษาข้อมูลส่วนบุคคลไว้ตามที่กฎหมายกำหนด

1.8 บริษัทจัดให้มีการดำเนินการสอบทาน และประเมินประสิทธิภาพของระบบรักษาข้อมูลส่วนบุคคลโดยหน่วยงานตรวจสอบภายใน

2. มาตรการป้องกันด้านเทคนิค (Technical Safeguard)

2.1 จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยดำเนินการ ดังนี้

2.1.1 ดำเนินการติดตามอย่างสม่ำเสมอ ว่าข้อมูลส่วนบุคคลที่อยู่ในความดูแลของบริษัทนั้น (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษาหรือไม่ (ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) หรือ ตามที่ขอความยินยอมไว้) ทั้งนี้เพื่อดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

2.1.2 กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอถอนความยินยอม) และบริษัทใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่นนี้ บริษัทจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

2.1.3 การลบทำลายข้อมูล หรือ การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ในกรณีที่บริษัทมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น

(ก) เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือสถิติ

(ข) เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

(ค) เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

(ง) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

2.2 การควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการจัดการข้อมูล ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย ซึ่งรวมถึงแต่ไม่จำกัดเพียง

2.2.1 การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญที่มีการพิสูจน์และยืนยันตัวตน และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสมโดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น

2.2.2 การบริหารจัดการการเข้าถึงของผู้ใช้งานที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอน สิทธิผู้ใช้งาน การจัดการสิทธิการเข้าถึงของผู้ใช้งาน การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน และการถอดถอนสิทธิหรือปรับปรุงสิทธิการเข้าถึง

2.3 การจัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่างๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง ทั้งนี้เป็นไปตามหลักเกณฑ์และวิธีปฏิบัติทางสารสนเทศของบริษัท

3. มาตรการป้องกันทางกายภาพ (Physical Safeguard)

3.1 การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บ และประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง และมีการล็อคตู้เก็บเอกสารข้อมูลส่วนบุคคล เป็นต้น ทั้งนี้ความเข้มข้นของมาตรการให้เป็นไปตามระดับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือถูกทำลายโดยมิชอบ

3.2 การกำหนดผู้ที่ได้รับอนุญาตให้เข้าถึงอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล ตามหน้าที่ความรับผิดชอบ ทั้งนี้เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก การดำเนินการป้องกันและระมัดระวังไม่ให้ข้อมูลรั่วไหล หรือถูกละเมิดอย่างหนึ่งอย่างใด เช่น ไม่เปิดไฟล์ข้อมูลส่วนบุคคลในที่สาธารณะ ปิด/เก็บข้อมูลส่วนบุคคลให้มิดชิดเมื่อลุกออกจากโต๊ะ กรณีการใช้เครื่องพิมพ์เอกสารร่วมกันต้องลบไฟล์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลออกจากหน้าจอเครื่องพิมพ์ทุกครั้ง และออกจากระบบให้เรียบร้อย จัดทำบันทึกคำร้องขอเข้าถึงข้อมูลส่วนบุคคล และทำลายเอกสารข้อมูลส่วนบุคคลด้วยตนเองทุกครั้งโดยไม่ฝากบุคคลอื่นทำลายแทน เป็นต้น

4. ข้อตกลงระหว่างบริษัท และผู้ประมวลผลข้อมูลส่วนบุคคล

กรณีมีข้อตกลงระหว่างบริษัทและผู้ประมวลผลข้อมูลส่วนบุคคล บริษัทจะกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการตามนโยบายนี้ เพื่อป้องกันการสูญหาย การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ หรือกระทำโดยปราศจากอำนาจโดยชอบด้วยกฎหมาย รวมทั้งแจ้งให้บริษัททราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น ทั้งนี้ความเข้มข้นของมาตรการให้เป็นไปตามระดับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือถูกทำลายโดยมิชอบ โดยดำเนินการ ดังนี้

4.1 การประเมินก่อนส่งมอบข้อมูล

4.1.1 ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือ นิติบุคคลรายอื่นนั้น ใช้เพื่อร้องขอข้อมูลส่วนบุคคล

4.1.2 สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด (เช่น จำเป็นต้องทราบวัน-เดือน-ปีเกิด หรือบ้านเลขที่ หรือไม่ หรือเพียงปี พ.ศ. เกิด และ รหัสไปรษณีย์ ก็เพียงพอ) และจำเป็นต้องทราบข้อมูลที่ชี้จำเพาะบุคคล (เช่น ชื่อ-นามสกุล เลขประจำตัว 13 หลัก)

หรือไม่ หากแปลงข้อมูลที่ชี้จำเพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงต่อการนำไปใช้ประโยชน์หรือไม่

4.2 เมื่อส่งมอบข้อมูล

4.2.1 จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน

4.2.2 ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน

4.2.3 แจ้งให้บุคคล หรือ นิติบุคคลนั้น ทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

4.3 หลังส่งมอบข้อมูล

4.3.1 ติดตามการใช้งานเป็นครั้งคราว เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็นใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิม ควรแจ้งให้บุคคล หรือนิติบุคคลนั้น ลบทำลายข้อมูล

4.3.2 กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ

5 การส่ง การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

การส่ง การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ รวมถึงการนำข้อมูลส่วนบุคคลไปเก็บบนฐานข้อมูลในระบบอื่นใด ซึ่งผู้ให้บริการรับโอนข้อมูลหรือบริการเก็บรักษาข้อมูลอยู่ต่างประเทศ ประเทศปลายทางที่เก็บรักษาข้อมูลต้องมีมาตรฐานการตุ้มครองข้อมูลส่วนบุคคลที่เทียบเท่าหรือดีกว่ามาตรการตามนโยบายนี้

6 การฝ่าฝืนมาตรการการรักษาความมั่นคงปลอดภัยของบริษัท

ในกรณีที่มีการฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัยของบริษัท จนเป็นเหตุให้มีการละเมิดข้อมูลส่วนบุคคลรั่วไหลสู่สาธารณะ บริษัทจะดำเนินการแจ้งเจ้าของข้อมูลให้ทราบโดยเร็ว รวมทั้งแจ้งแผนการเยียวยาความเสียหายจากการละเมิด หรือการรั่วไหลของข้อมูลส่วนบุคคลสู่สาธารณะในกรณีที่เกิดจากความบกพร่องของบริษัท

<u>การทบทวนมาตรการ</u>

บริษัทจะจัดให้มีการทบทวนมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลฉบับนี้เมื่อมีความจำเป็น และ/หรือเมื่อเทคโนโลยีมีการเปลี่ยนแปลงไป

คำสงวนสิทธิ

บริษัทจะไม่รับผิดชอบกรณีที่มีความเสียหายใดๆ อันเกิดจากการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่สาม รวมถึงการละเลยหรือเพิกเฉย การออกจากระบบ (Log Out) ฐานข้อมูลหรือระบบสื่อสารสังคมออนไลน์ของบริษัท โดยการกระทำของเจ้าของข้อมูลหรือบุคคลอื่นซึ่งได้รับความยินยอมจากเจ้าของข้อมูล