Chayo Group Pcl.

ระบบบริหารจัดการด้านความปลอดภัยข้อมูลสารสนเทศ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท ชโย กรุ๊ป จำกัด (มหาชน) (“**บริษัท**”) มีนโยบายที่จะให้พนักงาน และผู้ปฏิบัติงานที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศ อันประกอบด้วยวงจรเครือข่ายการสื่อสารข้อมูล ระบบซอฟท์แวร์ที่ใช้ในการปฏิบัติการและการประมวลผลข้อมูล เครื่องคอมพิวเตอร์ พร้อมอุปกรณ์ต่อพ่วง แฟ้มข้อมูล และข้อมูลของบริษัท อย่างมีประสิทธิภาพ ไม่ขัดต่อกฎหมาย หรือพระราชบัญญัติที่เกี่ยวข้อง โดยมีมาตรฐานความปลอดภัยที่เพียงพอ เพื่อประโยชน์และประสิทธิผลทางธุรกิจของบริษัท จึงกำหนดให้ถือปฏิบัติ ดังนี้

การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

1.1 การตรวจสอบและประเมินความเสี่ยง

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่บริษัทยอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจว่าการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศถูกจัดการอย่างเหมาะสม

1.2 การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์ของบริษัท โดยให้ครอบคลุมถึงการบริหารทรัพยากรบุคคลและระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

1.3 การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

1.3.1 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

(1) หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศของบริษัท ให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง และจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลของบริษัท

(2) การใช้งานคอมพิวเตอร์และเทคโนโลยีสารสนเทศของบริษัท จะต้องเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และที่ได้แก้ไขเพิ่มเติม) รวมถึงกฎหมายอื่นใดที่เกี่ยวข้อง

(3) บริษัทจะจำกัดการเข้าถึงข้อมูลภายในโดยให้เฉพาะผู้บริหารที่เข้าถึงข้อมูลดังกล่าวได้ หรือผู้ที่มีหน้าที่โดยตรงในการบริหารงานต่าง ๆ ที่เกี่ยวข้องเท่านั้น ทั้งนี้ ให้รวมถึงการเปิดเผยข้อมูลที่จำเป็นต่อพนักงานของบริษัท โดยบริษัทจะแจ้งให้พนักงานทราบว่าข้อมูลดังกล่าวนั้นเป็นความลับ และไม่สามารถเปิดเผยให้แก่บุคคลภายนอกได้

(4) บริษัทจะจัดระบบรักษาความปลอดภัยเพื่อป้องกันการเข้าถึงข้อมูล และเอกสารที่เป็นความลับอย่างเคร่งครัด

(5) พนักงานที่ได้รับอนุญาตให้เข้าถึงข้อมูลที่เป็นความลับ จะต้องใช้ระบบเทคโนโลยีสารสนเทศให้ถูกต้องตามสิทธิที่ได้รับอนุญาต และจะต้องไม่ยินยอมให้ผู้อื่นใช้ หรือเข้าถึงรหัสผ่านสำหรับเข้าใช้งานระบบเทคโนโลยีสารสนเทศนั้น

(6) ห้ามบุคคลใดใช้งานระบบเทคโนโลยีสารสนเทศเพื่อเข้าถึง หรือส่งข้อมูลส่วนตัว หรือข้อมูลที่มีเนื้อหาขัดต่อศีลธรรมอันดีเกี่ยวกับการพนัน การละเมิดสิทธิผู้อื่น หรือกระทบต่อความมั่นคงของประเทศชาติ

(7) หากมีการสื่อสารผ่านสังคมออนไลน์ จะต้องดำเนินการอย่างเหมาะสม ถูกต้องตามความเป็นจริง โดยคำนึงถึงความเป็นธรรมต่อผู้มีส่วนเกี่ยวข้องทุกฝ่าย ไม่ก่อให้เกิดความเสียหายต่อบริษัท และจะไม่สื่อสารข้อมูลส่วนตัวในฐานะพนักงานของบริษัท ทั้งนี้ การดำเนินการใด ๆ ในฐานะตัวแทนของบริษัทผ่านสื่อสังคมออนไลน์ จะดำเนินการได้ต่อเมื่อได้รับอนุมัติจากบุคคลหรือฝ่ายที่รับผิดชอบในเรื่องที่เกี่ยวข้องนั้น ๆ รวมถึงได้ดำเนินการตามอำนาจและขั้นตอนการอนุมัติของบริษัทแล้วเท่านั้น

1.3.2 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

(1) หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการป้องกันควบคุมการใช้งาน และการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของบริษัท ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

(2) ห้ามบุคคลใดทำการเปลี่ยนแปลง ทำซ้ำ ลบทิ้ง หรือทำลายข้อมูลของบริษัท รวมทั้งห้ามมิให้เปิดเผยข้อมูลที่มีอยู่ในระบบสารสนเทศของบริษัท โดยไม่ได้รับอนุญาต

1.3.3 การจัดการข้อมูลสารสนเทศและการรักษาความลับ

(1) การจำแนกประเภททรัพย์สินสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดแนวทางการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับบริษัท รวมถึงต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้

(2) การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดทำระบบสารสนเทศสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญ รวมทั้งจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสารสนเทศสำรอง และการจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างสม่ำเสมอ

(3) การควบคุมการเข้ารหัสข้อมูล

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

1.3.4 การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

(1) การควบคุมการใช้งานของผู้ใช้งาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการควบคุมการใช้งานทรัพย์สินสารสนเทศและระบบสารสนเทศ ดังนี้

(1.1) กำหนดมาตรการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดให้ผู้ใช้งานเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศโดยการใส่รหัสผ่าน และให้ออกจากระบบสารสนเทศระบบงานคอมพิวเตอร์ที่ใช้งาน และเครื่องคอมพิวเตอร์ โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน รวมถึงให้มีการล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์ตามเวลาที่กำหนดอย่างเหมาะสม

(1.2) กำหนดการใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอกบริษัท

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดให้มีมาตรการที่เหมาะสมควบคุมความมั่นคงปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของบริษัท รวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกบริษัท

(1.3) กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท อย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทรับทราบและปฏิบัติตาม

(2) การควบคุมดูแลผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing)

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดทำข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย โดยข้อกำหนดและกรอบการปฏิบัติงานต้องครอบคลุมกรณีที่ผู้รับดำเนินการมีการให้ผู้บริการภายนอกรายอื่น (Sub-Contract) รับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศ

1.3.5 การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

(1) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย และควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่าง ๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก รวมถึงจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

(2) การควบคุมการรับส่งข้อมูลสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการควบคุมข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัท รวมทั้งบริษัทย่อย และระหว่างบริษัทกับหน่วยงานภายนอกโดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(2.1) แผนกเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีข้อกำหนดสำหรับการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล รวมถึงควบคุมให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัท รวมทั้งบริษัทย่อย และระหว่างบริษัทกับหน่วยงานภายนอกอย่างเป็นลายลักษณ์อักษร

(2.2) แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-Mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

(2.3) หัวหน้าแผนกเทคโนโลยีสารสนเทศต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัทมีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของบริษัทอย่างเป็นลายลักษณ์อักษร

1.3.6 การป้องกันภัยคุกคามต่อระบบสารสนเทศ

(1) การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

(2) การบริหารจัดการช่องโหว่ทางเทคนิค

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องควบคุมให้ระบบสารสนเทศของบริษัท ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(2.1) จัดให้มีการทดสอบการเจาะระบบ (Penetration Test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอก (Untrusted Network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (Risk and Business Impact Analysis) ดังนี้

- กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อย ทุก 3 ปี และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ

- กรณีที่เป็นระบบงานที่มีความสำคัญอื่น ๆ ต้องทดสอบอย่างน้อยทุก 5 ปี

(2.2) จัดให้มีการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานที่เกี่ยวข้องเพื่อให้รับทราบและหาแนวทางการแก้ไขและป้องกัน

(2.3) จัดให้มีการทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (Cyber Security Drill)

1.3.7 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศที่เหมาะสม เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

1.4 การกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

แผนกเทคโนโลยีสารสนเทศ ต้องจัดให้มีมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานที่สอดคล้องกับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศที่ได้ประกาศใช้งาน และดำเนินการประกาศให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศได้ และต้องกำหนดผู้รับผิดชอบตามมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศดังกล่าวให้ชัดเจน โดยมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท แบ่งออกเป็น 14 ข้อ ได้แก่

1.4.1 มาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Standard)
1.4.2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)
1.4.3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)
1.4.4 การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)
1.4.5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)
1.4.6 การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)
1.4.7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
1.4.8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)
1.4.9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)
1.4.10 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)
1.4.11 การใช้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)
1.4.12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)
1.4.13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)
1.4.14 การปฏิบัติตามข้อกำหนด (Compliance)

1.5 นโยบายการจัดการบัญชีผู้ใช้งานระบบสารสนเทศ

การลงทะเบียนและเพิกถอนสิทธิผู้ใช้ (User Registration/De-registration Procedure) วัตถุประสงค์เพื่อการกระบวนการในการจัดการผู้ใช้ภายในระบบได้รับการอนุมัติอย่างเป็นทางการ มีการพิจารณาสิทธิ์การเข้าถึงของผู้ใช้ให้เหมาะสมและมีการส่งมอบรหัสผ่านที่ปลอดภัยให้กับผู้ใช้ โดยเมื่อมีพนักงานเข้าใหม่ ลาออก ย้ายหน่วยงาน หรือเลื่อนตำแหน่งงาน ฝ่ายบุคคลจะดำเนินการกรอกแบบฟอร์มการลงทะเบียนและเพิกถอนสิทธิผู้ใช้(CHAYO-FM-01) ดังกล่าวโดย ระบุชื่อ-นามสกุล, ชื่อเล่น, วัน เดือน ปี เกิด, มือถือส่วนตัว, มือถือออฟฟิศ, เบอร์ติดต่อภายใน, หน่วยงาน, รหัสพนักงาน, และPassword เบื้องต้น, รายละเอียดการร้องขอ, พื้นที่, ประเภทคำร้อง, วันที่เริ่มใช้ เพื่อส่งให้หน่วยงาน IT Support ดำเนินการต่อ

การกำหนดสิทธิ์ในการใช้โปรแกรม CCS (Access Right Matrix For Recovery Program) เพื่อกำหนดการเข้าถึงการทำงานในโปรแกรม CCS ของพนักงานตามเอกสารการกำหนดสิทธิ์ในการใช้โปรแกรม CCS (CHAYO -FM-04) ซึ่งในแต่ละระดับชั้นของพนักงานในแต่ละตำแหน่ง จะสามารถเรียกดู แก้ไขและทำงานได้เฉพาะงานของตนเองที่ได้รับ Assign เท่านั้น หัวหน้างานตามสายงาน สามารถเรียกดู แก้ไข งานของตนเองและเรียกดูเพื่อ Review งานของลูกทีมได้ สำหรับทีม IT Support จะเป็นผู้ดูแลงานในส่วนการ การเพิ่ม ลบ แก้ไขข้อมูล ของ User สำหรับการใช้โปรแกรม และแจ้งข่าวสาร คำสั่งต่างๆ ในโปรแกรม CCS นี้ให้กับพนักงานทราบ

1.6 นโยบายการสอบทานสิทธิ์ผู้ใช้งาน

การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)
จัดทำกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบและปรับปรุงบัญชีผู้ใช้งาน จำเป็นต้องจัดทำอย่างน้อยปีละ 1 ครั้ง หรือ ตามวาระที่ ผู้บริหาร เป็นฝ่ายเห็นชอบให้จัดทำในกรณี พิเศษ หรือเมื่อมีการลาออก เปลี่ยนแปลงตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง ในวาระการตรวจสอบสิทธิ์ทุกครั้งฝ่าย IT จะเป็นคน เรียกสิทธิ์มาให้กับ ผู้จัดการฝ่ายนั้นในการตรวจสอบ หลังจากการตรวจสอบหรือ Review สิทธิ์เสร็จ ผู้ทวนสิทธิ์ จะทำลงนามเป็นผู้ตรวจสอบสิทธิ์ หลังจากนั้น ผู้บริหารจะเป็นฝ่ายลงนามอนุมัติเอกสาร ทบทวนสิทธิ์ ประจำปีนั้นๆ

1.7 นโยบายการใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงในระบบเทคโนโลยีสารสนเทศ

การใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Account Management) การจัดการสิทธิ์สามารถดำเนินการได้หลากหลายวิธี ซึ่งทุกวิธีมีเป้าหมายที่เหมือนกันคือการพยายามจำกัดสิทธิ์ในการใช้งานให้น้อยที่สุด โดยจะระบุในรูปแบบของข้อจำกัดสิทธิ์ในการเข้าถึงและการได้รับอนุญาตจากผู้บริหาร หรือผู้ที่ถือครองสิทธิ์ นั้น
บัญชีผู้มีสิทธิ์สูง หรือเรียกว่า Superuser จะถูกใช้งานโดยผู้ที่ได้รับมอบหมาย เพื่อใช้บริหารและจัดการในการสั่งปฏิบัติการชุดคำสั่ง หรือแก้ไขค่าต่างๆในระบบ บัญชีผู้มีสิทธิ์สูง Superuser โดยทั่วไปจะถูกเรียกว่า “Root” ในระบบปฏิบัติการ Unix และ Linux และเรียกว่า “Administrator” ในระบบปฏิบัติการ Windows รวมทั้ง SA บน Database ด้วย บัญชีผู้มีสิทธิ์สูง นั้นสามารถเข้าถึงไฟล์ แฟ้ม และทรัพยากร ต่างๆบนเครื่องรวมทั้งสามารถอ่าน เขียน ดำเนินการ และสามารถแสดงการเปลี่ยนแปลงที่เกิดขึ้นในระบบเครือข่าย เช่น การสร้างไฟล์ ติดตั้ง

ซอฟต์แวร์ แก้ไขไฟล์ การตั้งค่า การลบผู้ใช้งานและข้อมูล บัญชีผู้มีสิทธิ์สูงยังสามารถกำหนดสิทธิ์ และเพิกถอนสิทธิ์สำหรับผู้ใช้งานอื่นๆหากบัญชีผู้มีสิทธิ์สูงถูกนำไปใช้งานในทางที่ผิดอาจส่งผลให้เกิดความเสียหายเนื่องจากความผิดพลาด (เช่น ทำการลบไฟล์ที่สำคัญโดยบังเอิญ หรือพิมพ์คำสั่งผิดพลาดซึ่งส่งผลกระทบต่อระบบ) หรือมีเจตนาที่ไม่ดีต่อระบบ บัญชีผู้ใช้ที่ได้รับสิทธิ์สูงนี้สามารถก่อให้เกิดความเสียหายทั้งระบบ ฉะนั้นสิทธิ์สูงทั้งหมดจึงถูกเก็บใส่ซองไว้ที่ผู้มีอำอาจ เช่น ผู้จัดการฝ่าย IT หรือ เซฟ ของผู้บริหาร กรณีเบิกใช้งาน จะต้องมีการเขียนคำขอโดยระบุชื่อผู้ขอ เวลาใช้งาน ระยะเวลาใช้ อนุมัติโดยใคร ทุกครั้ง และหลังมีการ ใช้เสร็จ ทาง ผู้จัดการฝ่าย IT หรือ ผู้บริหารที่มีการดูแล ในส่วนนี้ จะต้องทำการ เปลี่ยนรหัสก่อนเก็บเข้า ตู้เซฟ ก่อนทุกครั้ง

1.8 การแก้ไขเปลี่ยนแปลงโปรแกรม

1.8.1 <u>การร้องขอ</u>

- การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ จะต้องกรอกเอกแบบฟอร์ม CHAYO-FM-25 และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ ก่อนทุกครั้ง
- หัวหน้าฝ่าย IT ทำ การประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (operation) ระบบรักษาความปลอดภัย (security) และการทำงาน (functionality) ของระบบงานที่เกี่ยวข้อง

1.8.2 <u>การปฏิบัติงานพัฒนาระบบงาน</u>

- ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) ออกจากส่วนที่ใช้งานจริง (production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วน ตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้
- ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือ แก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ
- ควรตระหนักถึงระบบรักษาความปลอดภัย (security) และเสถียรภาพการทำงาน (availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

1.8.3 <u>การทดสอบ</u>

- ผู้ที่ร้องขอและฝ่าย IT รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วม ในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือ แก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

1.8.4 <u>การโอนย้ายเพื่อใช้ระบบงานจริง</u>

- ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

1.8.5 การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน ที่ได้รับการพัฒนา

- ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา เช่น เอกสาร CHAYO-FM-25
- ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน

- ต้องจัดเก็บโปรแกรม version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

1.9 การแบ่งแยกหน้าที่และสภาพแวดล้อม

1.9.1 เครื่อง (DEV) การกำหนดต้องให้มีการแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) ออกจากส่วนที่ใช้งานจริง (production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วน ตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

1.9.2 เครื่อง (Test Server) การกำหนดให้ เครื่อง Test ตามที่ฝ่าย IT กำหนดให้ เช่น เครื่องของ Client หรือ Client Server ตามที่ฝ่าย IT กำหนดให้

1.9.3 เครื่อง (Server Production) การกำหนดให้ เครื่อง Server Production ใช้สำหรับใช้งานจริงเท่านั้น โดยจะไม่มีการทดสอบระบบใดๆบนเครื่อง Server Production เด็ดขาด

1.10 การทดสอบความพร้อม การสำรองข้อมูล

1.10.1 ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งของโปรแกรมโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

1.10.2 ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

1.11 การรับแจ้งและแก้ไขปัญหาทางด้านเทคโนโลยีสารสนเทศ

1.11.1 ผู้ใช้ทำการเขียนแบบฟอร์ม CHAYO-FM-09 เพื่อทำการขอใช้บริการ ฝ่าย IT โดยให้ทางผู้จัดการฝ่ายทำการเซ็นอนุมัติ เพื่อให้ฝ่าย IT เข้าทำการเข้าแก้ไขและซ่อมแซมเครื่อง software หรือเรื่อง อื่นๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ตามที่ User ร้องขอหลังจากนั้นให้ทำการ แจ้งฝ่าย IT สำหรับการเข้ามาทำการแก้ไข้ในทันที โดยฝ่าย IT จะเก็บ แบบฟอร์ม CHAYO-FM-09 เพื่อทำการเก็บ Report สำหรับการทำงานต่อไป

1.12 การกู้คืนระบบสารสนเทศ

แผนการกู้คืนข้อมูล (Recovery Plan)

1.12.1 รายงานให้ผู้บริหารได้ทราบถึง สาเหตุ / ปัญหาที่ต้องทำการกู้คืนระบบงาน / ข้อมูล หากความเสียหายที่เกิดขึ้นกับระบบงานต่างๆหรือระบบเครือข่ายอินเตอร์เน็ตส่งผลกระทบต่อการให้บริการใช้งานของผู้ใช้ระบบ

1.12.2 ใช้ข้อมูลล่าสุด / ทันสมัยที่สุด ที่ได้สำรองไว้เพื่อกู้คืนระบบ

- กรณีเกิดความเสียหายกับระบบงานจะต้องติดตั้งระบบจาก Soure Code ที่มีการใช้งานล่าสุด
- กรณีเกิดความเสียหายกับฐานข้อมูล จะต้องนำฐานข้อมูลที่สำรองไว้ล่าสุดนำมากู้คืนเพื่อให้ข้อมูลสูญหายน้อยที่สุด
- กรณีเกิดความเสียหายกับระบบปฏิบัติการ โดยที่คอมพิวเตอร์แม่ข่ายยังคงทำงานปกติ ให้ติดตั้งระบบปฏิบัติการใหม่และระบบงานจาก Source Code ที่ใช้งานล่าสุดรวมทั้งฐานข้อมูลที่เก็บสำรองไว้ล่าสุด
- กรรีเกิดความเสียหายกับเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไขให้สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับ OS และระบบงาน จะต้องทำการติดตั้ง OS และระบบงานใหม่จาก Source Code ที่มีการใช้งานอยู่ล่าสุดและกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

1.12.3 ดำเนินการกู้คืนระบบงานและข้อมูลที่เกิดปัญหา

1.12.4 ตรวจสอบความถูกต้องของระบบงานและข้อมูล หลังกจากกู้คืนระบบงานเสร็จสิ้น

1.12.5 หากพบปัญหาและข้อผิดพลาดระหว่างดำเนินการกู้ข้อมูล จนทำให้การกู้ข้อมูลไม่สามารถทำได้สำเร็จ ให้รีบจัดทีมงานประชุมทีมงานผู้ดูแลระบบและผู้ที่เกี่ยวข้องเพื่อหาแนวทางในการสำรองข้อมูลใหม่อีกครั้ง

1.12.6 แจ้งผลการกู้คืนระบบงาน/ข้อมูลให้ผู้ใช้งานรับทราบ

1.12.7 กำหนดให้มีการทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง

1.13 การพัฒนาระบบสารสนเทศ

การพัฒนาระบบเทคโนโลยีสารสนเทศ (System development)

การพัฒนาระบบสารสนเทศขึ้นมาให้ผู้ใช้ได้ใช้งานนั้นมีสิ่งสำคัญที่ผู้พัฒนาระบบจะต้องคำนึงถึงก็คือระบบที่สร้างขึ้นมานั้นจะต้องตรงตามความต้องการของผู้ใช้งานและจะต้องสร้างให้เสร็จตามระยะเวลาที่กำหนดภายในวงเงินหรืองบประมาณที่วางไว้แต่สิ่งที่สำคัญที่ผู้พัฒนาระบบจะต้องคำนึงถึงอีกอย่างก็คือ ปัจจัยที่เป็นในการพัฒนาระบบให้ได้ประสิทธิภาพมากที่สุดซึ่งมีรายละเอียดดังนี้

1.13.1 ความร่วมมือผู้ใช้ระบบ (ใช้ระบบควรมีส่วนเกี่ยวข้องในการพัฒนาระบบมากที่สุดเนื่องจากการพัฒนาระบบขึ้นมานั้นเป็นการพัฒนาให้ผู้ใช้ระบบได้นำระบบที่ตรงกับความต้องการไปใช้งานและส่วนใหญ่แล้วผู้ใช้ระบบจะทราบถึงข้อมูลต่างๆและปัญหาที่เกิดขึ้นในระบบเก่าอยู่เก่า ดังนั้นผู้ใช้ระบบจึงมีส่วนร่วมในการพัฒนาระบบตั้งแต่ต้นจนจบแล้ว ก็ ทำให้เราได้ระบบที่สมบูรณ์ตรงตามความต้องการและความพึงพอใจของผู้ใช้ระบบ

1.13.2 การวางแผนการดำเนินการ ระบบที่ดีนั้นควรจะมีการวางแผนในการดำเนินการเป็นขั้นตอน และมีแนวทางในการพัฒนาอย่างถูกต้อง และสมบูรณ์

1.13.3 การพัฒนาอย่างรอบคอบในการออกแบบระบบ ตลอดจนในเรื่องของการนำฮาร์ดแวร์ และซอฟแวร์ต่างๆ มาใช้งาน ทีมพัฒนาระบบจะต้องมีความรอบคอบในการทำงานค่อนข้างมาก

1.13.4 การทดสอบ ทีมงานพัฒนาระบบจะต้องมีการทดสอบโปรแกรมหรือระบบงานที่สร้างขึ้นมาอย่างรอบคอบ

1.13.5 การจัดทำเอกสารคู่มือ ระบบงานที่พัฒนาขึ้นมาจะต้องมีเอกสารคู่มือการใช้งานอย่างละเอียดทุกขั้นตอน เพื่อเอาไว้อ้างอิงหรือเอาไว้ใช้ในการพัฒนาระบบในครั้งต่อไป

1.13.6 การเตรียมความพร้อม มีการวางแผนสร้างความเข้าใจและฝึกอบรมผู้ใช้ระบบเพื่อสร้างความมั่นใจว่าผู้ใช้ระบบสามารถปฏิบัติงานกับระบบงานที่ได้รับการพัฒนาอย่างมีประสิทธิภาพ

1.13.7 การติดตั้งระบบ มีการเตรียมความพร้อมและการวางแผนในการฝึกอบรมผู้ใช้เป็นอย่างดี

1.13.8 การตรวจสอบและประเมินผล หลังจากที่ได้ติดตั้งระบบเรียบร้อยแล้ว ควรมีการทดสอบและประเมินผลระบบว่าตรงตามความต้องการของผู้ใช้หรือไม่

1.13.9 การบำรุงรักษา ระบบงานที่ดีนั้นนอกจากจะนำมาใช้งานได้อย่างมีประสิทธิภาพแล้วปัจจัย ที่สำคัญอีกอย่างหนึ่งที่ควรนึกถึงก็คือ ควรจะมีการออกแบบให้มีการบำรุงรักษาในภายหลัง

1.14 การควบคุมผู้ให้บริการภายนอก ของระบบสารสนเทศ

เพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศของ "บริษัท" อย่างไม่เหมาะสม ทั้งนี้ นโยบายดังกล่าวต้องมีเนื้อหาขั้นต่ำครอบคลุมประเด็นดังต่อไปนี้

1.14.1 กำหนดข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและกระบวนการควบคุมอย่างเป็นลายลักษณ์อักษร และมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและผู้ให้บริการภายนอก

1.14.2 กำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอก

1.14.3 ระบุประเภทข้อมูลสารสนเทศที่อนุญาตให้ผู้บริการภายนอกเข้าถึง เพื่อให้การกาหนดมาตรการควบคุมและติดตามการเข้าถึงข้อมูลเป็นไปอย่างเหมาะสม ภายใต้หลักความจำเป็นในการรู้ข้อมูล

1.14.4 จัดให้มีขั้นตอนและกระบวนการติดตามควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม

1.14.5 มีการควบคุมความครบถ้วนถูกต้องของข้อมูลและการประมวลผลข้อมูลที่ได้รับจากผู้ให้บริการภายนอก

1.14.6 ติดตามการทางานของผู้ให้บริการภายนอก

1.14.7 ผู้ให้บริการภายนอกต้องกาหนดแผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy) ให้สอดคล้องกับแผนของผู้ประกอบธุรกิจ รวมทั้งกาหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกในการกู้คืนระบบงานให้เป็นไปตามข้อตกลงที่ได้กาหนดไว้ เพื่อให้ข้อมูลและการประมวลผลข้อมูลอยู่ในสภาพที่พร้อมใช้งานเสมอ

1.14.8 มีการจัดอบรมให้กับบุคคลที่เกี่ยวข้องกับการจัดหาผู้ให้บริการภายนอกเพื่อให้ทราบถึงนโยบาย ขั้นตอน และกระบวนการ

1.14.9 มีการรักษาความมั่นคงปลอดภัยในกรณีที่มีการเคลื่อนย้ายหรือถ่ายโอนข้อมูลสารสนเทศ

1.15 นโยบายรหัสผ่าน (Password)

รหัสผ่าน เป็นส่วนหนึ่งที่มีความสำคัญในการรักษาความปลอดภัยของบัญชีผู้ใช้งานหรือในระบบที่ต้องการความปลอดภัยซึ่งรหัสผ่านถือเป็นสิ่งที่ใช้สำหรับยืนยันความถูกต้องของบุคคลนั้น การใช้งานรหัสผ่านจึงช่วยป้องกันความปลอดภัยในการเข้าถึงข้อมูลโดยมิชอบนั้นได้ หากผู้ใช้งานไม่ให้ความสำคัญในการตั้งค่ารหัสผ่านก็จะทำให้ผู้ไม่หวังดีสามารถคาดเดารหัสผ่านและเข้าถึงข้อมูลของท่านได้ง่าย

ลักษณะความปลอดภัย

1. ใช้อักขระโดยมีความยาวไม่น้อยกว่า 8 ตัวอักษร
2. ไม่ใช้คำใดๆ ก็ตามที่เข้าข่ายสิ่งที่ไม่ควรนำมาใช้เป็นรหัสผ่าน
3. ไม่ใช้รหัสผ่านซ้ำกับ รหัสผ่านเดิมที่เคยใช้ไปแล้วจำนวน 3 รอบของการเปลี่ยนรหัสผ่าน
4. ควรประกอบด้วยอักขระอื่นๆ หลายๆ ตัว ผสมกันอยู่ในรหัสผ่าน ได้แก่ ตัวอักษรพิมพ์เล็ก (a-z),ตัวอักษรพิมพ์ใหญ่(A-Z),ตัวเลข(0-9)และตัวอักขระพิเศษ เช่น (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
5. ใช้คำที่ไม่มีในพจนานุกรม

สิ่งที่ไม่ควรนำมาใช้เป็นรหัสผ่าน

1. ข้อมูลที่ใช้ในการระบุตัวตนทั่วไป อย่างเช่น ชื่อ นามสกุล เลขบัตรประจำตัวต่างๆ หรือวัน เดือนปีเกิด
2. ข้อมูลการติดต่อ อย่างเช่น เบอร์โทรศัพท์
3. ชื่อบุคคลรอบข้างหรือ สัตว์เลี้ยง
4. ใช้คำที่มีความหมายและหาได้ในพจนานุกรม
5. คำทั่วๆไปที่มีการสะกดจากหลังไปหน้า อย่างเช่น admin -> nimda, root -> toor
6. ใช้รูปแบบตัวอักษรหรือตัวเลขที่เป็นที่นิยม อย่างเช่น qwerty, 12345, 123321
7. ใช้รูปแบบการตั้งรหัสผ่านที่คล้ายคลึงกันในแต่ละบัญชี อย่างเช่น secret1, 1secret, secret?

นอกเหนือจากหลักการตั้งรหัสผ่านที่ดีพอแล้วพฤติกรรมของผู้ใช้ยังเป็นปัจจัยในการเสริมความเข้มแข็งของรหัสผ่าน ดังนั้น การสร้างลักษณะนิสัยในการใช้งานรหัสผ่านที่ดี มีดังนี้

1. เมื่อใช้งานผ่านคอมพิวเตอร์ ไม่ควรเลือกฟังก์ชั่นจำรหัสผ่านอัตโนมัติ ต้องกรอกรหัสผ่านเองทุกครั้ง
2. เปลี่ยนรหัสผ่านทุกๆ 90 วัน หรือ ทุกๆ 3 เดือน
3. ในแต่ละบัญชีควรมีการตั้งรหัสผ่านที่แตกต่างกัน ไม่ควรใช้รหัสผ่านเดิมซ้ำ 3 ครั้ง
4. ตรวจสอบการเข้าถึงบัญชีเป็นประจำ
5. ออกจากระบบทุกครั้งหลังใช้งาน
6. ไม่เขียนรหัสผ่านไว้บนกระดาษและ แปะไว้ตามที่ต่างๆ เพื่อเตือนความจำ รวมถึงไม่เก็บรหัสผ่านไว้ในรูปแบบของไฟล์ในคอมพิวเตอร์
7. เมื่อจำเป็นต้องทำธุรกรรมออนไลน์ผ่านคอมพิวเตอร์สาธารณะให้เปลี่ยนรหัสผ่านให้เปลี่ยนรหัสผ่าน
8. เมื่อมีการ ใส่ Password ผิดเป็นจำนวน 3 ครั้ง ระบบจะทำการ Lock และทาง User จะต้องแจ้งกลับไปหา Admin เพื่อทำการ Unlock Password ให้ทุกครั้ง

2. **การรายงาน**

กำหนดให้มีการรายงานการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดใด ๆ ต่อคณะกรรมการบริษัท อย่างน้อยปีละ 1 ครั้ง หรือในกรณีที่มีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดอย่างมีนัยสำคัญ เช่น ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่บริษัท หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดที่บริษัทกำหนดไว้ ทั้งนี้ ผู้บริหารระดับสูงสุดของหน่วยงาน (ประธานเจ้าหน้าที่บริหาร : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

3. **การปฏิบัติการ**

3.1 เมื่อมีพนักงานเข้าใหม่ ลาออก ย้ายหน่วยงาน หรือเลื่อนตำแหน่งงาน ฝ่ายบุคคลจะดำเนินการกรอกแบบฟอร์มการลงทะเบียนและเพิกถอนสิทธิผู้ใช้ (CHAYO-FM-01) และให้ทางฝ่ายเทคโนโลยีสารสนเทศ (“IT”) ดำเนินการต่อไป

3.2 การกำหนดผู้มีสิทธิ์ในการเข้าถึงข้อมูล Internet ในแต่ละตำแหน่ง ทาง IT จะทำการตรวจสอบสิทธิ์ในแต่ละตำแหน่งงานตามเอกสารกำหนดผู้มีสิทธิ์ในการเข้าถึง Internet ในแต่ละตำแหน่ง (CHAYO-FM-03) และแบบฟอร์ม CHAYO-FM-08 ฝ่าย IT จะทำการเปิดระบบให้ใช้งานต่อไป

3.3 มีกำหนดการสแกนไวรัสอัตโนมัติทุกวันจันทร์เวลา 12.00น. ที่เครื่อง Server และเครื่อง Client ทุกเครื่อง

3.4 มีการสั่งให้คอมแต่ละเครื่องมี Pop Up การแจ้งเปลี่ยน Password ทุก 90 วัน หรือ ทุกๆ 3เดือน, และยังมีการ Log-Off หน้าจอที่ไม่มีการใช้งานทุก 15 นาที

3.5 มีการจัดทำแบบฟอร์มเพื่อบันทึกการเข้าใช้งานห้อง Server หลักจากบุคคลภายในและบุคคลภายนอก

3.6 จะมีการทำการสำรองข้อมูลและทดสอบเพื่อให้มั่นใจว่ามีความพร้อม โดยระบบจะทำการสำรองข้อมูลที่เครื่อง Server ลงใน External Hard Disk ทุกวันศุกร์ ส่งมอบให้ CEO เก็บรักษาไว้ในที่ปลอดภัย

3.7 การใส่รหัสผ่าน จะทำการตั้งรหัสผ่านครั้งแรกให้กับทุก User เมื่อ User มีการ Log In เข้าใช้งานในครั้งแรก ระบบจะสั่งให้ทำการเปลี่ยนรหัสผ่านในทันที โดยต้องทำการตั้งรหัสผ่านจำนวน 8 อักขระขึ้นไป และจะต้องเป็นภาษาอังกฤษ ตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ ตัวอย่างเช่น Chayo@#2023 เป็นต้นข้อยกเว้นสำหรับการเปลี่ยนรหัสผ่าน เช่น รหัส SA ที่ทำการผูกบนโปรแกรมฝ่าย IT จะขออนุญาตยกเว้นโดยทำการ เก็บเข้า ซอง เพื่อให้กับผู้จัดการฝ่าย IT เป็นผู้เก็บรักษา โดยผู้จัดการฝ่าย IT จะเก็บรักษารหัสการเข้าถึงดังนี้

1.รหัส SA DB 2. รหัส Admin ของระบบ ต่างๆ 3.รหัส Administrator ของระบบปฏิบัติการ OS

3.8 เพื่อความปลอดภัยของข้อมูลเมื่อเกิดเหตุไฟกระชาก หรือไฟดับชั่วคราว ทางบริษัทฯมีเครื่องสำรองไฟ ยี่ห้อ APC รุ่น APC Smart ขนาด 1KVA ตามจำนวนเครื่อง Server และมีการทำสัญญาซ่อมบำรุงรักษา โดยบริษัทฯตัวแทนจากภายนอกจะเข้าทำการตรวจเช็คความพร้อมของเครื่อง UPS ทุก เดือน

3.9 ให้ดูแลรักษาคอมพิวเตอร์และอุปกรณ์ของตนเอง ให้สะอาด อยู่ในสภาพดี ปิดเครื่องทุกครั้งเมื่อเลิกใช้งาน และแจ้งหน่วยงาน IT Support ทันที เมื่อพบว่ามี Virus จากสื่อภายนอก

3.10 ระหว่างปฏิบัติงานหากมีความจำเป็นต้องลุกจากที่นั่งบริเวณทำงาน พนักงานต้องทำการ Log Off โดยมี Password คอยควบคุมการ Log On หากต้องการใช้งานอีกครั้ง เพื่อป้องกันการเข้าถึงข้อมูลจากบุคคลอื่น

3.11 ห้ามพนักงานนำคอมพิวเตอร์หรืออุปกรณ์อื่นใดที่มิใช่ของบริษัทฯ มาเชื่อมต่อเข้ากับเครือข่ายบริษัทฯ

3.12 ห้ามคัดลอกข้อมูลบริษัทฯ ข้อมูลลูกค้า ข้อมูลธนาคารหรือข้อมูลอื่นใดออกจากบริษัทฯโดยเด็ดขาด

3.13 ห้ามพนักงานใช้เครื่องคอมพิวเตอร์ของพนักงานท่านอื่นที่ไม่อยู่ในพื้นที่ทำงานหรือไม่ได้มาปฏิบัติงาน หากมีความจำเป็นต้องใช้ ต้องได้รับอนุญาตจากผู้บังคับบัญชาของตนเองหรือสูงกว่าก่อนจึงจะดำเนินการใช้ได้

3.14 จัดให้มีการทดสอบแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้งเพื่อให้เกิดความพร้อมเมื่อเกิดเหตุฉุกเฉิน

3.15 ให้ความรู้พนักงานเกี่ยวกับภัยคุกคามทางด้าน IT พร้อมแนวทางการป้องกันที่เกิดขึ้นในปัจจุบัน

3.16 รูปภาพการเชื่อมต่อระบบ (Network Diagram) จะต้องมีการปรับปรุงให้ทันสมัยทุก 6 เดือน

3.17 การใช้งานเครื่องแม่ข่ายจะต้องใช้ตามช่องทางและสิทธิ์ในการเข้าถึงบริการที่ได้รับอนุญาตเท่านั้น

4. บทบังคับใช้

นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศนี้ให้ใช้บังคับกับ พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำของบริษัท รวมถึงบุคคลภายนอก และหน่วยงานภายนอกที่ให้บริการแก่บริษัท

นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัทครั้งที่ 3/2567 เมื่อวันที่ 8 มีนาคม 2567 ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ 8 มีนาคม 2567 เป็นต้นไป

ประกาศ ณ วันที่ 8 มีนาคม 2567

(นายวุฒิศักดิ์ ลาภเจริญทรัพย์)
ประธานกรรมการบริษัท