นโยบายด้านความมั่นคงและความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ฉบับปรับปรุงครั้งที่ 1

บริษัท แอลทีเอ็มเอช จำกัด (มหาชน)

LTMH Public Company Limited

โดยมีผลบังคับใช้ตั้งแต่วันที่ 18 กุมภาพันธ์ 2568 เป็นต้นไป

บันทึกประวัติการทบทวน/แก้ไขเอกสาร

วันที่	ฉบับที่	เลขหน้า	รายละเอียดการทบทวน/แก้ไข	ผู้ขอทบทวน/แก้ไข
19 เมษายน 2566	ต้นฉบับ	-	-	-
6 กุมภาพันธ์ 2567	ต้นฉบับ	ทั้งฉบับ	ทบทวนประจำปี 2566	ฝ่ายเลขานุการบริษัท
7 พฤศจิกายน 2567	ต้นฉบับ	ทั้งฉบับ	ทบทวนประจำปี 2567	ฝ่ายเลขานุการบริษัท
18 กุมภาพันธ์ 2568	ปรับปรุงครั้งที่ 1	1 - 8	- ปรับปรุงและเพิ่มเติมข้อความในหมวดที่ 1 การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ หัวข้อ 1.3 การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ	ฝ่ายเทคโนโลยีสารสนเทศ
		9 - 14	- เพิ่มหมวดที่ 2 การออกแบบและพัฒนาแอปพลิเคชันและเว็บไซต์	ฝ่ายเทคโนโลยีสารสนเทศ
11 พฤศจิกายน 2568	ปรับปรุงครั้งที่ 1	ทั้งฉบับ	ทบทวนประจำปี 2568	ฝ่ายเลขานุการบริษัท

นโยบายด้านความมั่นคงและความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

บริษัท แอลทีเอ็มเอช จำกัด (มหาชน) (“**บริษัทฯ**”) มีนโยบายที่จะให้พนักงาน และผู้ปฏิบัติงานที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศ อันประกอบด้วยวงจรเครือข่ายการสื่อสารข้อมูล ระบบซอฟท์แวร์ที่ใช้ในการปฏิบัติการและการประมวลผลข้อมูล เครื่องคอมพิวเตอร์ พร้อมอุปกรณ์ต่อพ่วง แฟ้มข้อมูล และข้อมูลของบริษัทฯ อย่างมีประสิทธิภาพ ไม่ขัดต่อกฎหมาย หรือพระราชบัญญัติที่เกี่ยวข้อง โดยมีมาตรฐานความปลอดภัยที่เพียงพอ เพื่อประโยชน์และประสิทธิผลทางธุรกิจของบริษัทฯ จึงกำหนดให้ถือปฏิบัติ ดังนี้

หมวดที่ 1 การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

1.1 การตรวจสอบและประเมินความเสี่ยง

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่บริษัทฯ ยอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจว่าการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศถูกจัดการอย่างเหมาะสม

1.2 การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์ของบริษัทฯ โดยให้ครอบคลุมถึงการบริหารทรัพยากรบุคคลและระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

1.3 การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

1.3.1 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

1. หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศของบริษัทฯ ให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง และจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลของบริษัทฯ
2. กำหนดให้มีการลงทะเบียนบัญชีผู้ใช้งาน เพื่อให้มีสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศของบริษัทฯ ตามความจำเป็น และหากเป็นระบบสำคัญ จะต้องกำหนดให้มีการยืนยันตัวตนโดยใช้หลายปัจจัย (MFA)
3. การกำหนดรหัสผ่าน (Password) สำหรับเข้าถึงบัญชีผู้ใช้งาน จะต้องสอดคล้องกับแนวปฏิบัติดังต่อไปนี้
    1. รหัสผ่านจะต้องมีตัวอักษร ตัวเลข และตัวอักขระพิเศษ รวมกันไม่ต่ำกว่า 8 ตัวอักษร
    2. มีการเปลี่ยนรหัสผ่านทุก 3 เดือน
    3. ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่สามารถใช้รหัสซ้ำของเดิมครั้งล่าสุดได้
4. การใช้งานคอมพิวเตอร์และเทคโนโลยีสารสนเทศของบริษัทฯ จะต้องเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และที่ได้แก้ไขเพิ่มเติม) รวมถึงกฎหมายอื่นใดที่เกี่ยวข้อง

5. บริษัทฯ จะจำกัดการเข้าถึงข้อมูลภายในโดยให้เฉพาะผู้บริหารที่เข้าถึงข้อมูลดังกล่าวได้ หรือผู้ที่มีหน้าที่โดยตรงในการบริหารงานต่าง ๆ ที่เกี่ยวข้องเท่านั้น ทั้งนี้ ให้รวมถึงการเปิดเผยข้อมูลที่จำเป็นต่อพนักงานของบริษัทฯ โดยบริษัทฯ จะแจ้งให้พนักงานทราบว่าข้อมูลดังกล่าวนั้นเป็นความลับ และไม่สามารถเปิดเผยให้แก่บุคคลภายนอกได้
6. บริษัทฯ จะจัดระบบรักษาความปลอดภัยเพื่อป้องกันการเข้าถึงข้อมูล และเอกสารที่เป็นความลับอย่างเคร่งครัด
7. พนักงานที่ได้รับอนุญาตให้เข้าถึงข้อมูลที่เป็นความลับ จะต้องใช้ระบบเทคโนโลยีสารสนเทศให้ถูกต้องตามสิทธิที่ได้รับอนุญาต และจะต้องไม่ยินยอมให้ผู้อื่นใช้ หรือเข้าถึงรหัสผ่านสำหรับเข้าใช้งานระบบเทคโนโลยีสารสนเทศนั้น
8. ห้ามบุคคลใดใช้งานระบบเทคโนโลยีสารสนเทศเพื่อเข้าถึง หรือส่งข้อมูลส่วนตัว หรือข้อมูลที่มีเนื้อหาขัดต่อศีลธรรมอันดีเกี่ยวกับการพนัน การละเมิดสิทธิผู้อื่น หรือกระทบต่อความมั่นคงของประเทศชาติ
9. หากมีการสื่อสารผ่านสังคมออนไลน์ จะต้องดำเนินการอย่างเหมาะสม ถูกต้องตามความเป็นจริง โดยคำนึงถึงความเป็นธรรมต่อผู้มีส่วนเกี่ยวข้องทุกฝ่าย ไม่ก่อให้เกิดความเสียหายต่อบริษัทฯ และจะไม่สื่อสารข้อมูลส่วนตัวในฐานะพนักงานของบริษัทฯ ทั้งนี้ การดำเนินการใด ๆ ในฐานะตัวแทนของบริษัทฯ ผ่านสื่อสังคมออนไลน์ จะดำเนินการได้ต่อเมื่อได้รับอนุมัติจากบุคคลหรือฝ่ายที่รับผิดชอบในเรื่องที่เกี่ยวข้องนั้น ๆ รวมถึงได้ดำเนินการตามอำนาจและขั้นตอนการอนุมัติของบริษัทฯ แล้วเท่านั้น
10. ในกรณีพนักงานมีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ความรับผิดชอบ กำหนดให้มีการเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับตำแหน่งหรือหน้าที่ความรับผิดชอบนั้นๆ
11. ในกรณีที่พนักงานพ้นสภาพการเป็นพนักงาน หรือสิ้นสุดจุดประสงค์ใช้งานบัญชีผู้ใช้งาน กำหนดให้มีการดำเนินการเพิกถอนสิทธิการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศทันที
12. การใช้งานบัญชี Privileged accounts ต้องเป็นไปตามหลักเกณฑ์ดังต่อไปนี้
    1. ควบคุมดูแลการให้สิทธิโดยจำกัดตามตำแหน่งหน้าที่ และความจำเป็นในการใช้งาน
    2. การขอใช้งานบัญชี Privileged account ให้พนักงานแจ้งขออนุญาตโดยระบุบัญชีที่ต้องการและเหตุผลในการขอใช้งาน โดยกำหนดให้ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) เป็นผู้อนุมัติเท่านั้น
13. มีการทบทวนบัญชีผู้ใช้งานและสิทธิการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง และดำเนินการเพิกถอนบัญชีที่ไม่ได้ถูกใช้งานแล้วโดยทันทีเมื่อตรวจสอบพบ
14. ในกรณีที่มีความจำเป็นให้ไม่สามารถปฏิบัติตามกระบวนการข้างต้นได้ ให้มีการประเมินความเสี่ยง ควบคุมความเสี่ยง และขออนุมัติยกเว้นจากประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) และประธานเจ้าหน้าที่บริหาร (CEO) อย่างเป็นลายลักษณ์อักษร

1.3.2 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดมาตรการป้องกัน ควบคุมการใช้งานและการบำรุงรักษาด้านกายภาพของพื้นที่การปฏิบัติงานและทรัพย์สินสารสนเทศ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ดังนี้

1. การยืนยันตัวตนผู้เข้า-ออกพื้นที่การปฏิบัติงาน ผ่าน Access card door พร้อมทั้งบันทึกเหตุการณ์เข้า-ออก
2. การควบคุมและติดตามการปฏิบัติงานของหน่วยงานหรือบุคคลภายนอกที่เข้ามาในพื้นที่การปฏิบัติงาน โดยต้องได้รับการอนุมัติจากผู้มีอำนาจ และมีการควบคุมโดยพนักงานเจ้าของพื้นที่ตลอดระยะเวลาปฏิบัติงาน
3. มีระบบรักษาความมั่นคงปลอดภัยให้กับพื้นที่การปฏิบัติงาน ประกอบด้วย ระบบกล้องวงจรปิด ระบบแจ้งเตือนและระงับอัคคีภัย และระบบสำรองไฟฟ้า โดยอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ พร้อมทั้งมีการบำรุงรักษาอย่างสม่ำเสมอ
4. การควบคุมมิให้นำทรัพย์สินสารสนเทศหรืออุปกรณ์สารสนเทศออกนอกพื้นที่โดยมิได้รับอนุญาต ยกเว้นอุปกรณ์คอมพิวเตอร์สำหรับพนักงานใช้ในการปฏิบัติงาน
5. ในกรณีมีการเปลี่ยนแปลงสิทธิการเข้าถึงพื้นที่การปฏิบัติงาน ให้ดำเนินการปรับปรุงหรือเพิกถอนสิทธิทันที
6. ห้ามบุคคลใดทำการเปลี่ยนแปลง ทำซ้ำ ลบทิ้ง หรือทำลายข้อมูลของบริษัทฯ รวมทั้งห้ามมิให้เปิดเผยข้อมูลที่มีอยู่ในระบบสารสนเทศของบริษัทฯ โดยไม่ได้รับอนุญาต

1.3.3 การจัดการข้อมูลสารสนเทศและการรักษาความลับ

1. การจำแนกประเภททรัพย์สินสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดแนวทางการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับบริษัทฯ รวมถึงต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้

การจัดลำดับชั้นความลับของข้อมูลสารสนเทศ มี 3 ระดับ ดังนี้

ระดับชั้นความลับ	ลักษณะของข้อมูล	ตัวอย่างข้อมูล	เจ้าของข้อมูล
ลับ (Secret)	ข้อมูลที่ส่งผลกระทบต่อการดำเนินยุทธศาสตร์ทางธุรกิจของบริษัทฯ หากเปิดเผยเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อธุรกิจ ชื่อเสียง ความเชื่อมั่น และทรัพย์สินของบริษัทฯ คู่ค้า และ/หรือของลูกค้าของบริษัทฯ จำเป็นต้องจำกัดการเข้าถึงเฉพาะบุคคลภายในองค์กรที่มีหน้าที่รับผิดชอบโดยตรงหรือได้รับมอบหมายจากเจ้าของข้อมูล	- แผนการตลาด/การพัฒนาผลิตภัณฑ์ - แผนกลยุทธ์ทางธุรกิจ - ข้อมูลลูกค้า - งบการเงิน ผลประกอบการของบริษัทฯ - ข้อมูลเงินเดือนของพนักงาน	บุคคลที่ได้รับมอบหมายจาก CEO

	เท่านั้น และต้องมีการตรวจสอบสิทธิการเข้าถึงเป็นระยะ		
ใช้ภายใน (Internal)	ข้อมูลที่มีจุดประสงค์ใช้งานภายในบริษัทฯ เท่านั้น	- ประกาศภายในบริษัทฯ - นโยบายการปฏิบัติงาน - บทความที่อยู่ระหว่างการพัฒนาเนื้อหา	หัวหน้าแผนกที่เกี่ยวข้อง
ข้อมูลทั่วไป (Public)	ข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้	- ข้อมูลประชาสัมพันธ์ - บทความที่เปิดเผยต่อสาธารณะแล้ว	หัวหน้าแผนกที่เกี่ยวข้อง

2. การสำรองข้อมูลและระบบสารสนเทศ

   หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดทำระบบสารสนเทศสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญ และให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศและระบบสำรองอย่างน้อยปีละ 1 ครั้ง

3. การเตรียมพร้อมกรณีเกิดเหตุฉุกเฉิน

   หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีกระบวนการบริหารจัดการเหตุฉุกเฉินในกรณีที่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ตามแนวทางดังต่อไปนี้

   1. กำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
   2. จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน โดยมีรายละเอียดอย่างน้อย ดังนี้
      1. หน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องทั้งหมด
      2. เงื่อนไข/ขั้นตอนการประกาศใช้แผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน
      3. ขั้นตอนกระบวนการดำเนินงานเพื่อรับมือเหตุการณ์
      4. เงื่อนไข/ขั้นตอนการประกาศยกเลิกแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน
   3. ในการรับมือกับเหตุฉุกเฉิน บริษัทฯ หน่วยงาน และบุคลากรที่เกี่ยวข้องจะต้องยึดปฏิบัติตามแนวทางที่ระบุไว้ในแผนกู้คืนระบบเทคโนโลยีสารสนเทศ
   4. ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งาน อย่างน้อยปีละ 1 ครั้ง

5. ทดสอบการปฏิบัติตามแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ พร้อมทั้งบันทึกผลการทดสอบ

4. การควบคุมการเข้ารหัสข้อมูล

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

1.3.4 การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

1. การควบคุมการใช้งานของผู้ใช้งาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีการควบคุมการใช้งานทรัพย์สินสารสนเทศและระบบสารสนเทศ ดังนี้

1.1 กำหนดการใช้งานอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint)

1. กำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งานในการเข้าถึงระบบสารสนเทศผ่านบัญชีผู้ใช้งาน และหากเป็นระบบสำคัญ จะต้องกำหนดให้มีการยืนยันตัวตนหลายปัจจัย (MFA) เพิ่มเติม
2. กรณีที่ระบบงานไม่รองรับการยืนยันตัวหลายปัจจัย (MFA) หรือมีความจำเป็นที่ไม่สามารถใช้งานการยืนยันตัวตนหลายปัจจัย (MFA) ได้ จะต้องดำเนินการตามมาตรการความปลอดภัยเพิ่มเติม ดังนี้
    1. กำหนดรหัสผ่าน (Password) ในการเข้าถึงบัญชีผู้ใช้งานตามแนวทางการจัดการรหัสผ่าน
    2. ติดตั้งเครื่องมือในการป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี เช่น Anti-virus, Anti-malware และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ
3. กำหนดให้ออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน และเครื่องคอมพิวเตอร์ โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน รวมถึงให้มีการล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์ตามเวลาที่กำหนดอย่างเหมาะสม

1.2 กำหนดการใช้งานอุปกรณ์เคลื่อนที่ (Mobile Device)

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดให้มีมาตรการที่เหมาะสมควบคุมความมั่นคงปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของบริษัทฯ รวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกบริษัทฯ

1.3 กำหนดการปฏิบัติงานจากเครือข่ายภายนอกหรือระยะไกล (Remote access)

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเข้าสู่ระบบงานจากภายนอก ดังต่อไปนี้

1. ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานอย่างเพียงพอ เพื่อขอสิทธิการเข้าถึงระบบจากระยะไกล
2. การเข้าสู่ระบบจากระยะไกล ต้องมีการพิสูจน์ยืนยันตัวตนของผู้ใช้งาน โดยใช้รหัสผ่าน หรือวิธีการเข้ารหัส
3. ต้องได้รับการอนุมัติจากประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) และมีการควบคุมอย่างเข้มงวด ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด
4. ตัดการเชื่อมต่อทันทีที่การปฏิบัติงานเสร็จสิ้นหรือไม่ได้ใช้งานแล้ว
5. กำหนดให้ระบบสารสนเทศที่มีความสำคัญ มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

1.4 กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน และป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัทฯ อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทฯ รับทราบและปฏิบัติตาม

2. การควบคุมดูแลผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing)

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดทำข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย โดยข้อกำหนดและกรอบการปฏิบัติงานต้องครอบคลุมกรณีที่ผู้รับดำเนินการมีการให้ผู้บริการภายนอกรายอื่น (Sub-Contract) รับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศ

1.3.5 การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

1. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย และควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่าง ๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก รวมถึงจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศและระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

2. การควบคุมการรับส่งข้อมูลสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีการควบคุมข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัทฯ รวมทั้งบริษัทย่อย และระหว่างบริษัทฯ กับหน่วยงานภายนอก โดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

1. แผนกเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีข้อกำหนดสำหรับการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล รวมถึงควบคุมให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัทฯ รวมทั้งบริษัทย่อย และระหว่างบริษัทฯ กับหน่วยงานภายนอกอย่างเป็นลายลักษณ์อักษร

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

3. หัวหน้าแผนกเทคโนโลยีสารสนเทศต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัทฯ มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของบริษัทอย่างเป็นลายลักษณ์อักษร

1.3.6 การป้องกันภัยคุกคามต่อระบบสารสนเทศ

1. การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม ดังนี้

1. แต่ละหน่วยงานมีการจัดหาซอฟต์แวร์ที่เหมาะสมและเพียงพอต่อการใช้งาน
2. ระบบคอมพิวเตอร์และซอฟต์แวร์ที่ใช้งานในบริษัทฯ ทั้งหมด จะต้องติดตั้งซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์และมีสิทธิ์ใช้งานอย่างถูกต้องตามเงื่อนไขของซอฟต์แวร์ต่างๆ
3. การติดตั้งซอฟต์แวร์เพิ่มเติม จะต้องได้รับการอนุมัติจากบุคคลที่ได้รับมอบหมายจากประธานเจ้าหน้าที่บริหาร (CEO) เท่านั้น โดยคำนึงถึงประสิทธิผลของการทำงานเป็นสำคัญ
4. มีการตรวจสอบการใช้งานซอฟต์แวร์ในอุปกรณ์ที่ใช้ปฏิบัติงานอย่างต่อเนื่อง
5. เมื่อพบสิ่งผิดปกติ ผู้ใช้งานจะต้องแจ้งเหตุแก่บุคลากรที่เกี่ยวข้องโดยทันที

2. การบริหารจัดการช่องโหว่ทางเทคนิค

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องควบคุมให้ระบบสารสนเทศของบริษัทฯ ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

1. จัดให้มีการทดสอบการเจาะระบบ (Penetration Test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอก (Untrusted Network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้าน

เทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (Risk and Business Impact Analysis) ดังนี้

- กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อย ทุก 3 ปี และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ
- กรณีที่เป็นระบบงานที่มีความสำคัญอื่น ๆ ต้องทดสอบอย่างน้อยทุก 5 ปี

ทั้งนี้ ต้องมีการรายงานผลการทดสอบการเจาะระบบไปยังหน่วยงานที่เกี่ยวข้อง และติดตามให้มีการแก้ไขช่องโหว่ภายในระยะเวลาที่กำหนดไว้

2. จัดให้มีการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานที่เกี่ยวข้องเพื่อให้รับทราบและหาแนวทางการแก้ไขและป้องกัน
3. จัดให้มีการทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (Cyber Security Drill)

1.3.7 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดให้มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศที่เหมาะสม เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

1.3.8 การปฏิบัติตามข้อกำหนด

ผู้ใช้งานระบบสารสนเทศมีหน้าที่ทำความเข้าใจ และปฏิบัติตามกฎหมาย นโยบาย ระเบียบ และข้อบังคับต่างๆ ที่เกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด ทั้งนี้รวมถึง

1. พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
2. พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.4 การกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

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

1. มาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Standard)
2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)
3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

4. การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)
5. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)
6. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)
7. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
8. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)
9. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)
10. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)
11. การใช้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)
12. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)
13. การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)
14. การปฏิบัติตามข้อกำหนด (Compliance)

หมวดที่ 2 การออกแบบและพัฒนาแอปพลิเคชันและเว็บไซต์

บริษัทฯ กำหนดแนวทางและขั้นตอนในการออกแบบและพัฒนาแอปพลิเคชันและเว็บไซต์ให้สอดคล้องกับมาตรฐานขององค์กร โดยมุ่งเน้นให้กระบวนการพัฒนาเป็นไปอย่างมีประสิทธิภาพและปลอดภัย โดยหน่วยงานที่ได้รับมอบหมายให้ออกแบบและพัฒนาระบบจะต้องยึดปฏิบัติ

2.1 การควบคุมการให้สิทธิในกระบวนการพัฒนาและแก้ไขระบบ

1. กำหนดสิทธิและขอบเขตความรับผิดชอบให้เหมาะสมกับตำแหน่งหน้าที่ เพื่อให้สอดคล้องกับการรักษาความมั่นคงปลอดภัยของระบบ และลดความเสี่ยงจากข้อผิดพลาด โดยยึดปฏิบัติตามตารางควบคุมการให้สิทธิ (Authorization matrix)

Role/Responsibility	System Development				
	Change Request	Ticket Management	Development	Testing	Production Approval
ประธานเจ้าหน้าที่บริหาร (CEO)	✓				
ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO)	✓		✓		✓
หัวหน้าแผนกเทคโนโลยีสารสนเทศ			✓		✓

ผู้บริหารจัดการผลิตภัณฑ์ (Product Manager)	✓	✓			
ผู้พัฒนา/แก้ไขระบบ (Software Developer)			✓		
ผู้ทดสอบระบบ (Quality Assurance)				✓	

2. กำหนดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) สำหรับบุคลากรที่เกี่ยวข้องกับขั้นตอนการพัฒนาระบบ การทดสอบระบบ และการอนุมัติการนำระบบขึ้นใช้งาน โดยบุคลากรที่รับผิดชอบหน้าที่ข้างต้น จะต้องเป็นบุคคลที่แตกต่างกัน เพื่อความโปร่งใสในการดำเนินงานเป็นสำคัญ

2.2 วงจรการพัฒนาระบบ

2.2.1 การกำหนดความต้องการของระบบ

1. ผู้ที่มีส่วนร่วมในการกำหนดรายละเอียดความต้องการของระบบ (Requirement) หรือการแก้ไขเปลี่ยนแปลงระบบ (Change) จะต้องได้รับมอบหมายจากประธานเจ้าหน้าที่บริหาร (CEO) ยกเว้นเป็นความต้องการหรือการเปลี่ยนแปลงทางเทคนิคที่ส่งผลต่อระบบสารสนเทศโดยตรง จะต้องได้รับมอบหมายจากประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO)
2. จัดประเภทของความต้องการหรือการเปลี่ยนแปลง (Change category) เพื่อให้บุคลากรที่ทำหน้าที่ในการพัฒนาระบบงานและผู้เกี่ยวข้องเข้าใจลักษณะของงาน และสามารถจัดลำดับความสำคัญได้อย่างเหมาะสม

   การจัดประเภทของความต้องการหรือการเปลี่ยนแปลง มี 3 ประเภท ดังนี้

   1. การสร้างใหม่หรือปรับเพิ่ม (Story)

      การพัฒนาระบบเพื่อให้เกิดความสามารถหรือกระบวนการทำงานใหม่ เพื่อตอบโจทย์ผู้ใช้งานมากขึ้น

   2. การแก้ไขปัญหาหรือข้อผิดพลาด (Bug)

      การแก้ไขข้อผิดพลาดที่เกิดขึ้นในระบบ ซึ่งส่งผลกระทบต่อการปฏิบัติงานหรือประสบการณ์ของผู้ใช้งาน ทั้งนี้ต้องมีการประเมินระดับความรุนแรง (Severity) และโอกาสเกิด (Likelihood) เพื่อจัดลำดับความสำคัญของงาน และกำหนดระยะเวลาแก้ไขอย่างเหมาะสม

ระดับความรุนแรง	ลักษณะของปัญหาหรือข้อผิดพลาด
Critical	• แอปพลิเคชันหรือเว็บไซต์ไม่สามารถใช้งานได้ • ส่งผลกระทบต่อความมั่นคงปลอดภัยของแอปพลิเคชันหรือเว็บไซต์ หรือตัวเลขทางการเงิน • ส่งผลกระทบต่อผู้ใช้งานทั้งหมด
Major	• ระบบโครงสร้างพื้นฐานในแอปพลิเคชันหรือเว็บไซต์ไม่สามารถใช้งานได้ • ส่งผลกระทบต่อผู้ใช้งานส่วนใหญ่

Minor	• ระบบโครงสร้างพื้นฐานในแอปพลิเคชันหรือเว็บไซต์ยังสามารถใช้งานได้ แต่ประสิทธิภาพในการปฏิบัติงานลดลง • ส่งผลกระทบต่อการผู้ใช้งานเพียงส่วนน้อย
Trivial	• ความผิดปกติของ UX/UI • ไม่มีผลกระทบในการใช้งาน

โอกาสเกิด	ความน่าจะเป็น
Certain	มากกว่า 90%
Occasional	มากกว่า 1%
Possible	มากกว่า 0.1%
Unlikely	น้อยกว่าหรือเท่ากับ 0.1%

Priority		Severity			
		Critical	Major	Minor	Trivial
Likelihood	Certain	P1	P1	P3	P4
	Occasional	P1	P2	P3	P4
	Possible	P2	P3	P3	P4
	Unlikely	P2	P3	P4	P4

P4 – ไม่มีกำหนดการ (ขึ้นกับความเหมาะสมของแผนงาน)
P3 - ดำเนินการแก้ไขภายใน 28 วัน
P2 - ดำเนินการแก้ไขภายใน 2 วัน
P1 - ดำเนินการแก้ไขภายใน 4 ชั่วโมง

3. การวิจัยหรือการทดสอบแนวทางแก้ไข (Spike)

   การวิจัยและทดสอบแนวทางก่อนการพัฒนาจริง การประเมินเครื่องมือใหม่ที่อาจจะเหมาะสมสำหรับการพัฒนา หรือการปรับปรุงเครื่องมือปัจจุบันที่ใช้ในการพัฒนา เพื่อให้มีความรู้ความเข้าใจ และมีความพร้อมเพียงพอที่จะดำเนินการพัฒนาระบบอย่างต่อเนื่อง

3. บุคลากรในตำแหน่ง Product Manager (PM) ดำเนินการจัดทำแผนงาน โดยกำหนดวันเวลาที่ต้องการดำเนินงาน และทรัพยากรที่จำเป็น วิเคราะห์ผลกระทบและความเสี่ยงในการดำเนินการเปลี่ยนแปลง เพื่อเตรียมมาตรการรองรับอย่างเหมาะสม พร้อมทั้งแจ้งให้ผู้มีอำนาจอนุมัติ

   - การเปลี่ยนแปลงระบบเพื่อตอบสนองความต้องการทางธุรกิจ จะต้องได้รับการอนุมัติจากประธานเจ้าหน้าที่บริหาร (CEO) ก่อนดำเนินการ
   - การเปลี่ยนแปลงระบบเพื่อตอบสนองความต้องการทางเทคนิค จะต้องได้รับการอนุมัติจากประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) ก่อนดำเนินการ

4. บุคลากรในตำแหน่ง Product Manager (PM) สร้างคำขอ (Ticket) ให้พัฒนาหรือแก้ไขผ่านระบบ Ticket (Ticketing system: Jira)

2.2.2 การพัฒนาระบบ

1. การพัฒนาระบบจะทำอยู่บนสภาพแวดล้อมสำหรับการพัฒนาและทดสอบเท่านั้น (Staging) ซึ่งแยกออกจากระบบที่ใช้งานจริง (Production)
2. ผู้พัฒนาหรือแก้ไขระบบ (Software Developer) จะต้องปฏิบัติงานตามที่ระบุใน Ticket เท่านั้น และต้องปฏิบัติตามรายละเอียดที่ระบุไว้อย่างเคร่งครัด หากมีการเปลี่ยนแปลงที่นอกเหนือไปจากนั้น ต้องแจ้งให้ Product Manager ที่รับผิดชอบรับทราบและอนุมัติการเปลี่ยนแปลงนั้นก่อนดำเนินการต่อ
3. การพัฒนาจะต้องมีการควบคุม Version ของชุดคำสั่งที่พัฒนา โดยจัดเก็บ Version ก่อนการเปลี่ยนแปลงไว้เพื่อสำหรับกรณีมีข้อผิดพลาดจนทำให้ระบบไม่สามารถใช้งานได้
4. ผู้ที่ร้องขอให้มีการพัฒนาหรือแก้ไขระบบ จะต้องมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้สามารถพัฒนาระบบได้ตรงตามความต้องการ

2.2.3 การทดสอบระบบ

1. การทดสอบระบบจะทำอยู่บนสภาพแวดล้อมสำหรับการพัฒนาและทดสอบเท่านั้น (Staging) ซึ่งแยกออกจากระบบที่ใช้งานจริง (Production)
2. กำหนดให้ผู้ที่มีหน้าที่รับผิดชอบการทดสอบระบบงานที่พัฒนาโดยบริษัทฯ เป็นบุคลากรในตำแหน่ง Quality Assurance (QA) เท่านั้น ทั้งนี้ ในกรณีที่เป็นระบบงานภายนอก เช่น ผลิตภัณฑ์ของคู่ค้า หรือลูกค้าของบริษัทฯ การทดสอบระบบงานจะดำเนินการในรูปแบบของ User Acceptance Testing (UAT) โดยต้องมีผู้ใช้งานปลายทางร่วมทดสอบและยืนยันความถูกต้องด้วย
3. ผู้พัฒนาหรือแก้ไขระบบต้องจัดทำแนวทางการทดสอบ (Test suggestion) โดยระบุใน Ticket ให้เหมาะสมกับการเปลี่ยนแปลงระบบโดยยังคงตอบสนองต่อผลลัพธ์ที่คาดหวังของงาน เพื่อกำหนดขอบเขตของการทดสอบให้ชัดเจน ลดความเสี่ยงจากการทดสอบที่ตกหล่นหรือเกินความจำเป็น รวมถึงเป็นแนวทางในการยกเว้นการทดสอบในส่วนที่ไม่มีการระบุไว้ ทั้งนี้ ผู้ทดสอบ (QA) ต้องดำเนินการทดสอบตามแนวทางที่ระบุไว้เท่านั้น
4. มีการกำหนดสถานการณ์ที่ใช้ในการทดสอบ (Test scenario) หรือกรณีที่ใช้ในการทดสอบ (Test case) เพื่อให้ครบถ้วนตรงตามความต้องการทางธุรกิจ โดยระบุใน Ticket ให้ครอบคลุมทุกเงื่อนไขและสถานการณ์
5. บันทึกผลการทดสอบ (Test result) สำหรับแต่ละเงื่อนไขและสถานการณ์ โดยระบุใน Ticket
6. หากมีการตรวจพบข้อบกพร่องของระบบ ให้พิจารณาแนวทางการปรับปรุงเพื่อให้สอดคล้องกับผลลัพธ์ที่คาดหวัง และติดตามให้ผู้พัฒนาดำเนินการแก้ไข
7. สำหรับการพัฒนาหรือแก้ไขระบบที่มีความสำคัญสูง หรือมีความเสี่ยงสูง กำหนดให้มีการรายงานการตรวจสอบต่อผู้บริหารของบริษัทฯ ถึงขอบเขต ขั้นตอน กระบวนการพัฒนา และการทดสอบ ก่อนที่จะนำขึ้นใช้งานจริง

2.2.4 การนำระบบขึ้นใช้งานจริง

1. ผู้พัฒนาหรือแก้ไขระบบ แจ้งขออนุมัติผลการทดสอบจากประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) หรือผู้ที่ได้รับมอบหมาย ซึ่งต้องไม่ใช่บุคคลที่พัฒนาหรือแก้ไขระบบนั้น

2. ผู้พัฒนาหรือแก้ไขระบบ รับผิดชอบในการนำระบบขึ้นใช้งานจริง หลังจากได้รับการอนุมัติแล้ว
3. ติดตามสถานะของระบบระหว่างนำขึ้นใช้งานจนแล้วเสร็จ เพื่อสามารถระบุและแก้ไขปัญหาที่อาจเกิดขึ้นได้อย่างทันท่วงที
4. มีการกำหนดแผนการเปลี่ยนแปลงระบบที่เหมาะสมกับความสำคัญและความเสี่ยง เช่น การเปลี่ยนแปลงไปยังระบบใหม่ทันที (Direct changeover) การเปลี่ยนแปลงระบบทีละเฟส (Phase changeover) เป็นต้น

2.2.5 การบำรุงรักษาระบบ

1. มีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอ เพื่อสามารถระบุความผิดปกติที่อาจเกิดขึ้นได้
2. มีการตรวจสอบประสิทธิภาพการทำงานของระบบอย่างสม่ำเสมอ เพื่อให้เป็นไปตามมาตรฐาน

2.2.6 การบันทึกการเปลี่ยนแปลง จัดทำเอกสารและคู่มือการใช้งาน

1. มีการบันทึกรายละเอียดเกี่ยวกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงตลอดทั้งวงจรการพัฒนา ตั้งแต่การสร้างคำขอ การพัฒนาหรือแก้ไข การทดสอบ จนถึงการนำขึ้นใช้งานจริง
2. มีการบันทึกเหตุผลกรณีมีการปรับเปลี่ยนหรือยกเลิกแผนการดำเนินงาน
3. จัดทำเอกสารประกอบระบบงานทั้งหมด พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ โดยจัดเก็บในรูปแบบอิเล็กทรอนิกส์

ทั้งนี้ ในกรณีที่มีความจำเป็นให้ไม่สามารถปฏิบัติตามกระบวนการข้างต้นได้ ให้มีการประเมินความเสี่ยง ควบคุมความเสี่ยง และขออนุมัติยกเว้นจากประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) อย่างเป็นลายลักษณ์อักษร

2.3 การควบคุมการใช้งาน Privilege account ภายในแอปพลิเคชันและเว็บไซต์

2.3.1 Privilege accounts สำหรับการพัฒนาหรือทดสอบระบบ

1. ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) รับผิดชอบในการกำหนดบัญชี Privilege account
2. พนักงานที่จะเข้าถึงและใช้งานบัญชี Privilege account จะต้องได้รับการอนุมัติจากประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) เท่านั้น พร้อมทั้งแจ้งให้ทราบว่าข้อมูลดังกล่าวนั้นเป็นความลับ และไม่สามารถเปิดเผยแก่บุคคลภายนอกได้
3. พนักงานที่ได้รับอนุญาตให้เข้าถึงและใช้งานบัญชี Privilege account จะต้องใช้เพื่อจุดประสงค์ในการพัฒนาหรือทดสอบระบบเท่านั้น

2.3.2 Privilege accounts สำหรับการบริหารจัดการข้อมูลของบริษัทฯ และหน่วยงานที่เกี่ยวข้อง

1. ประธานเจ้าหน้าที่บริหาร (CEO) รับผิดชอบในการกำหนดบัญชีผู้ใช้งานที่สามารถขึ้นทะเบียนเป็นบัญชี Privilege account ได้
2. พนักงานที่ต้องการขึ้นทะเบียนบัญชีผู้ใช้งานเป็นบัญชี Privilege account จะต้องแจ้งขออนุญาตโดยระบุบัญชีที่ต้องการและเหตุผลในการขอใช้งาน โดยกำหนดให้ประธานเจ้าหน้าที่บริหาร (CEO) เป็นผู้อนุมัติเท่านั้น โดยคำนึงถึงตำแหน่งหน้าที่ และความจำเป็นในการใช้งาน

3. ในกรณีพนักงานมีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ความรับผิดชอบที่ไม่มีความจำเป็นต้องใช้งาน Privilege account หรือพ้นสภาพการเป็นพนักงาน กำหนดให้มีการดำเนินการเพิกถอนบัญชีผู้ใช้งานของพนักงานออกจากการเป็น Privilege account ทันที
4. มีการทบทวนบัญชีผู้ใช้งาน Privilege account อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งหน้าที่ความรับผิดชอบหรือการพ้นสภาพการเป็นพนักงานของพนักงานในหน่วยงานที่เกี่ยวข้อง และดำเนินการเพิกถอนบัญชีของบุคคลที่ไม่ได้มีความเกี่ยวข้องแล้วโดยทันทีเมื่อตรวจสอบพบ

หมวดที่ 3 การรายงาน

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

นโยบายด้านความมั่นคงและความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ ฉบับนี้ ได้รับการอนุมัติโดยที่ประชุมคณะกรรมการบริษัทและให้มีผลบังคับใช้ตั้งแต่วันที่ 18 กุมภาพันธ์ 2568 จึงประกาศมาเพื่อทราบโดยทั่วกัน

.....

(นายธันวา เลาหศิริวงศ์)

ประธานกรรมการ