นโยบายการเข้าถึงระบบสารสนเทศ

System Access Control Policy

รุ่นเอกสาร	1.5	เลขที่เอกสาร	ISMS-PL-05
สายงาน	บริหารความมั่นคงปลอดภัยระบบสารสนเทศ		
กลุ่ม	ดิจิทัลทรานส์ฟอร์เมชั่น		
อนุมัติโดย			
นโยบายนี้ให้มีผลใช้บังคับ ตั้งแต่วันที่ 22 สิงหาคม 2566 เป็นต้นไป ตามมติที่ประชุมคณะทำงานกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ครั้งที่ 3 เมื่อวันที่ 22 สิงหาคม 2566 ลงนามโดย คุณเคียน ฮิน ลิม (President)			

ประวัติการแก้ไข

รุ่นเอกสาร	วันที่	รายละเอียด	ทบทวนโดย
1.0	30/06/2017	จัดทำเอกสาร	นายมานะ ขจรมาศบุษป์
1.1	15/07/2019	ปรับปรุงเอกสาร	นายมานะ ขจรมาศบุษป์ นางกรกมล สุภวัฒนากูล
1.2	30/04/2020	ปรับปรุงเอกสาร	นายเต็มภาคย์ ภัทรรัชต์ภาคย์
1.3	12/06/2021	ปรับปรุงเอกสาร -เพิ่ม บริษัทฯ -เพิ่ม บทลงโทษ -ปรับข้อความให้สอดคล้องกับ ISMS-PC-01	นายเต็มภาคย์ ภัทรรัชต์ภาคย์
1.4	25/07/2022	ปรับปรุงเอกสาร -การทบทวนนโยบาย	นายสุวัฒชัย สันตินรศักดิ์
1.5	16/05/2023	ปรับปรุงเอกสาร - ปรับปรุงตัวอย่างการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน	น.ส.เมกรินทร์ วุฒิฑา

นโยบายการเข้าถึงระบบสารสนเทศ

1. บทนำ

1.1. วัตถุประสงค์

- เพื่อกำหนดกฎเกณฑ์และควบคุมการเข้าถึงข้อมูล ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของบริษัทฯ
- เพื่อปกป้องข้อมูล ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของบริษัทฯ จากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต
- เพื่อกำหนดกระบวนการในการบริหารจัดการ อนุมัติ และ หรือ อนุญาต สร้าง เปลี่ยนแปลง ถอดถอน และยกเลิกบัญชีผู้ใช้ รวมถึงสิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศที่สำคัญของบริษัทฯ

1.2. ขอบเขต

นโยบายนี้ครอบคลุมการเข้าถึงระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ รวมถึงการใช้ข้อมูลของบริษัทฯ

1.3. คำจำกัดความ

- **Need-to-know** หมายถึง สิทธิ์ที่ได้รับอนุญาตให้เข้าใช้งานหรือเข้าถึงข้อมูลเท่าที่มีความจำเป็นในการปฏิบัติงาน และต้องได้รับอนุมัติก่อน จึงจะสามารถใช้งานได้
- **Defense in Depth** หมายถึง การรักษาความมั่นคงปลอดภัยแบบหลายชั้น
- **Least Privilege** หมายถึง การอนุญาตให้มีสิทธิ์หรือเข้าถึงข้อมูลที่น้อยที่สุดโดยที่ยังสามารถปฏิบัติหน้าที่ได้

2. นโยบาย

2.1. หลักเกณฑ์ทั่วไปเกี่ยวกับการควบคุมระบบเครือข่าย

- การเข้าถึงระบบเทคโนโลยีสารสนเทศทั้งหมดของบริษัทฯ ต้องได้รับการตรวจพิสูจน์ตัวตนของผู้ใช้งานก่อนเสมอ และพิจารณาอนุญาตให้ใช้งานระบบเท่าที่จำเป็นตามหลักการ “Need-to-know” เท่านั้น ยกเว้น user account และ email account สำหรับพนักงานเข้าใหม่ ที่บริษัทฯ กำหนดให้โดยอัตโนมัติ
- การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศต้องเริ่มต้นด้วยการปฏิเสธคำร้องขอเข้าถึงระบบทุกประเภท จากนั้นจึงค่อยพิจารณาอนุมัติการเข้าถึงเฉพาะระบบที่มีความจำเป็นต่อผู้ใช้งานเท่านั้น

- หลักการ “Defense in Depth” ต้องถูกนำมาใช้งานโดยอ้างอิงจากการบริหารจัดการความเสี่ยง ด้วยการคัดเลือกวิธีการหลากหลายรูปแบบ เช่น การใช้เทคโนโลยีต่างๆ การกำหนดขั้นตอนการปฏิบัติงาน การควบคุมการเข้าถึงทางกายภาพ หรือการมอบหมายหน้าที่แก่พนักงาน เพื่อนำมาใช้งานร่วมกัน ซึ่งจะช่วยเพิ่มระดับการปกป้องข้อมูล และระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น
- การเข้าถึงระบบเทคโนโลยีสารสนเทศโดยบุคคลภายนอก และการเชื่อมต่อระบบเครือข่ายของบริษัทฯ จากภายนอกต้องได้รับการควบคุมดูแลให้เป็นไปตาม *ISMS-PL-10 Third Party Security Policy* และ *ISMS-PL-04 Network Management Policy* อย่างเคร่งครัด

3. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

- การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ และบริการต่างๆ ของบริษัทฯ ต้องครอบคลุม ตั้งแต่เริ่มต้นการได้รับสิทธิจนกระทั่งสิ้นสุดการได้รับสิทธิของผู้ใช้งานในทุกขั้นตอน
- คำร้องขอเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยผู้ใช้งานต้องได้รับการทบทวนและพิจารณาอนุมัติตามขั้นตอนที่ระบุไว้ใน *ISMS-PC-01 User Access Request Procedure* อย่างเคร่งครัด
- ผู้ใช้งานที่ได้รับอนุญาตเท่านั้นจึงจะมีสิทธิเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ และต้องมีการจำกัดสิทธิการเข้าถึงระบบของผู้ใช้งานให้อยู่ในระดับที่เหมาะสมต่อความจำเป็นในการทำงานตามหลักการ “Least Privilege” เสมอ นอกจากนี้ ต้องมีการแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ของพนักงานอย่างเหมาะสม เพื่อป้องกันพนักงานผู้หนึ่งผู้ใดได้รับสิทธิในการเข้าถึงระบบเกินกว่าหน้าที่ความรับผิดชอบของตำแหน่งงาน ทั้งนี้ บริษัทฯ สามารถเปลี่ยนแปลง จำกัด หรือเพิกถอนสิทธิการเข้าถึงระบบของผู้ใช้งานตามความเหมาะสมได้ตลอดเวลา
- ผู้ใช้งานที่ได้รับอนุญาตแต่ละคนต้องมี User Account เป็นของตนเอง และต้องใช้งาน User Account นั้นตลอดระยะเวลาการทำงานกับบริษัทฯ ทั้งนี้ User Account ต้องถูกเพิกถอนเมื่อผู้ใช้งานนั้นพ้นจากสภาพการเป็นพนักงานแล้ว สำหรับการใช้งาน User Account ร่วมกัน ต้องเป็นไปตาม *ISMS-PC-07 Share User Account Procedure* เสมอ
- ผู้ใช้งานต้องรับผิดชอบดูแล User Account และรหัสผ่านของตนเองให้มีความมั่นคงปลอดภัยอยู่เสมอ

- ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log in เข้าสู่ระบบ สำหรับวิธีการตรวจพิสูจน์นั้นให้คัดเลือกโดยยึดตามผลการประเมินความเสี่ยงและงบประมาณเป็นสำคัญ ซึ่งโดยทั่วไปแล้ว วิธีการตรวจพิสูจน์ตัวตนของผู้ใช้งานนั้นสามารถแบ่งได้ออกเป็น 3 ประเภท ดังนี้
  1. การตรวจพิสูจน์จากสิ่งที่ผู้ใช้งานทราบ เช่น รหัสผ่าน เป็นต้น
  2. การตรวจพิสูจน์จากสิ่งที่ผู้ใช้งานครอบครองอยู่ เช่น บัตรที่มีแถบแม่เหล็ก หรือบัตรสมาร์ทการ์ด เป็นต้น
  3. การตรวจพิสูจน์จากบางส่วนของร่างกายของผู้ใช้งาน เช่น ลายนิ้วมือ หรือใบหน้า เป็นต้น
- การพิจารณาคัดเลือกวิธีการตรวจพิสูจน์ตัวตนของผู้ใช้งานสำหรับระบบหรือแอปพลิเคชันที่สำคัญ ควรนำเอาวิธีการตรวจพิสูจน์ตั้งแต่ 2 ประเภทขึ้นไปมาใช้งานร่วมกัน เพื่อเพิ่มระดับความมั่นคงปลอดภัยให้สูงขึ้น
- เครื่องคอมพิวเตอร์ทุกประเภทต้องได้รับการปกป้องความมั่นคงปลอดภัยด้วยรหัสผ่าน โดยระบบปฏิบัติการต้องทำการตรวจสอบความถูกต้องของรหัสผ่าน เมื่อผู้ใช้งาน Log in เข้าสู่ระบบ
- เครื่องคอมพิวเตอร์ server, desktop และ laptop จะต้องตั้งค่าอุปกรณ์ให้ทำการ Log out หรือ lock หน้าจอโดยอัตโนมัติ เมื่อเครื่องคอมพิวเตอร์ไม่ถูกใช้งานเป็นระยะเวลาหนึ่ง ยกเว้นมีเหตุจำเป็นทางเทคนิคที่เป็นข้อจำกัดทำให้ไม่สามารถตั้งค่าได้ โดยจะต้องได้รับอนุมัติจากผู้อำนวยการสายงานบริหารความมั่นคงปลอดภัยระบบสารสนเทศ หรือผู้ที่ได้รับมอบหมาย
- รหัสผ่านต้องมีความมั่นคงปลอดภัย และในขณะเดียวกันก็ต้องง่ายต่อการจดจำของผู้เป็นเจ้าของด้วย ทั้งนี้ รหัสผ่านต้องได้รับการรักษาความลับตามข้อกำหนดที่ระบุไว้ใน ข้อบังคับเพื่อความปลอดภัยระบบสารสนเทศ และ *ISMS-ST-02 Password Standard* อย่างเคร่งครัด

4. การควบคุมการเข้าถึงระบบและแอปพลิเคชัน

- เจ้าของข้อมูล/ระบบต้องเป็นผู้พิจารณาอนุมัติคำร้องขอ การเข้าถึงข้อมูล/ระบบของตนเอง และต้องมีการกำหนดสิทธิ์ผู้ที่มีสิทธิ์อนุมัติคำร้องขอเข้าใช้งานตามที่กำหนดไว้ใน *ISMS-PC-01 User Access Request Procedure* อย่างเคร่งครัด
- บัญชีผู้ใช้งานในระดับ System (เช่น administrator เป็นต้น) ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นเท่านั้นตามขั้นตอนที่ระบุไว้ใน *ISMS-PC-03 Access Matrix Procedure* ทั้งนี้ ผู้ใช้งานต้องใช้สิทธิในระดับ System สำหรับการทำงานที่เกี่ยวข้องกับการดูแลระบบเท่านั้น ส่วนการทำงานทั่วไปอื่นๆ ให้ใช้บัญชีผู้ใช้งานที่มีสิทธิในระดับปกติ

- สิทธิการเข้าถึงในระดับพิเศษ (Privilege) หมายถึง สิทธิที่นอกเหนือจากการปฏิบัติงานปกติ โดยต้องดำเนินการดังต่อไปนี้
  1. กำหนดระยะเวลาใช้งานของบัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงในระดับพิเศษนั้น
  2. เพิกถอนสิทธิและ/หรือบัญชีผู้ใช้งานดังกล่าวทันทีที่กิจกรรมนั้นเสร็จสิ้นสมบูรณ์
  3. ระยะเวลาการเชื่อมต่อเข้าสู่ระบบ/แอปพลิเคชันที่มีความสำคัญต้องถูกจำกัดเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต
  4. ผู้ใช้งานต้องไม่ใช้งานระบบ/แอปพลิเคชันที่สำคัญแบบ Multiple Sessions โดย เด็ดขาด เว้นแต่ในกรณีที่จำเป็นเท่านั้น และหากมีการใช้งานแบบ Multiple Sessions เกิดขึ้น ผู้ใช้งานต้องรับผิดชอบต่อผลในแง่ลบที่อาจจะเกิดขึ้น
- การให้สิทธิการเข้าถึงในระดับพิเศษ (Privilege) ผู้บริหารตั้งแต่ระดับผู้ช่วยผู้อำนวยการสายงานขึ้นไป ของสายงานบริหารความมั่นคงปลอดภัยระบบสารสนเทศดำเนินการพิจารณาอนุมัติ ผู้มีสิทธิในการอนุมัติการเบิกใช้งานสิทธิการเข้าถึงในระดับพิเศษ
- บัญชีผู้ใช้งานประเภท “Guest” ที่สามารถเข้าถึงระบบ แอปพลิเคชัน และระบบเครือข่ายของบริษัทฯ ได้นั้น ต้องถูกระงับการใช้งาน
- พนักงานทุกคนต้องไม่ติดตั้ง Code ใดๆ ที่สามารถหลบเลี่ยงกลไกการควบคุมการเข้าถึง หรือการตรวจพิสูจน์ตัวตนของผู้ใช้งาน ทั้งที่เป็นกลไกของระบบปฏิบัติการ ซอฟต์แวร์ควบคุมการเข้าถึง หรือแอปพลิเคชันต่างๆ
- ระบบที่มีความสำคัญต้องถูกใช้งานบนเครื่องคอมพิวเตอร์ที่ได้รับการจัดหามาเพื่อรองรับระบบดังกล่าวโดยเฉพาะ และต้องใช้งานทรัพยากรร่วมกับระบบอื่นที่มีความน่าเชื่อถือที่ได้รับการกำหนดและจัดทำเป็นเอกสารไว้โดย สายงานโครงสร้างพื้นฐาน
- การเข้าถึงฐานข้อมูลต้องดำเนินการผ่านแอปพลิเคชันเท่านั้น และจำกัดการเข้าถึงโดยตรงให้มีเฉพาะกรณีที่จำเป็น หรือมีข้อจำกัดในแอปพลิเคชัน เช่น เพื่อการดูแลรักษาระบบฐานข้อมูลโดยผู้ดูแลระบบ หรือบุคคลที่ได้รับอนุญาต เป็นต้น
- การเข้าถึง System Utilities ที่ปฏิบัติการด้วยสิทธิพิเศษในระดับสูง ซึ่งทำให้สามารถเลี่ยงผ่านกลไกการควบคุมระบบ/แอปพลิเคชันต่างๆ ได้นั้น ต้องถูกจำกัดให้เฉพาะผู้ใช้งาน หรือผู้ดูแลระบบที่มีความจำเป็นต้องใช้งานเป็นประจำเท่านั้น สำหรับการใช้งานและการเข้าถึง System Utilities เหล่านั้นโดยบุคคลอื่น ให้พิจารณาอนุมัติในลักษณะชั่วคราวในทุกกรณี
- System Utilities ดังกล่าวข้างต้นต้องถูกแยกออกจากแอปพลิเคชัน และซอฟต์แวร์อื่นๆ เพื่อจำกัดการเข้าถึงให้แก่ผู้ใช้งานที่ได้รับอนุญาตเท่านั้น
- บริการ (Services) ที่ไม่เกี่ยวข้องกับการปฏิบัติงานหรือการดำเนินธุรกิจต้องถูกระงับการใช้งาน

4.1. การควบคุมการเข้าถึงข้อมูล

สิทธิการเข้าถึงไฟล์ข้อมูลต้องได้รับการควบคุม และได้รับการพิจารณาอนุมัติเท่าที่จำเป็นเท่านั้น ทั้งนี้ เพื่อรักษาความถูกต้องครบถ้วนของข้อมูล และเพื่อเป็นการแบ่งแยกอำนาจหน้าที่ของผู้ใช้งาน

4.2. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอก หรือคู่ค้า

- คำร้องขอเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยผู้ให้บริการภายนอก หรือคู่ค้าต้องได้รับการทบทวน และพิจารณาอนุมัติตามข้อกำหนดที่ระบุไว้ใน ISMS-PC-01 User Access Request Procedure อย่างเคร่งครัด
- ผู้ให้บริการภายนอก หรือคู่ค้าต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องทุกฉบับ และ Third Party Code of Conduct for vendor (เลขปี) (ภายใต้นโยบาย Third-Party Security Policy) อย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ
- การกำหนดเส้นทางเชื่อมต่อ และวิธีการควบคุมการเข้าถึงต่างๆ ต้องถูกนำมาใช้เพื่อจำกัดให้ผู้ให้บริการภายนอก หรือคู่ค้าสามารถเข้าถึง Host/Server เฉพาะส่วนที่บริษัทฯ กำหนดไว้เท่านั้น
- บัญชีผู้ใช้งานที่สร้างขึ้นสำหรับบุคคลที่ไม่ใช่พนักงานของบริษัทฯ ต้องได้รับการจำกัดอายุการใช้งาน โดยทั่วไปแล้วให้กำหนดอายุการใช้งานไว้ที่ 30 วัน เว้นแต่มีการพิจารณาเป็นอย่างอื่น การเข้าถึงระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศภายในของบริษัทฯ ต้องดำเนินการโดยใช้อุปกรณ์ที่บริษัทฯ เป็นผู้จัดหา หรืออุปกรณ์ที่ได้รับอนุญาตซึ่งผ่านการลงทะเบียนเท่านั้น

4.3. การทบทวน และการเพิกถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศ

- การสร้าง การเพิกถอน และการเปลี่ยนแปลงบัญชีผู้ใช้งานทั้งหมดที่ได้รับการดำเนินการโดยผู้ดูแลระบบ และบุคคลอื่นใดที่มีสิทธิในระดับพิเศษ ต้องได้รับการบันทึก Log เก็บไว้เสมอ
- สิทธิการเข้าถึงระบบที่สำคัญทั้งหมดต้องได้รับการทบทวนอย่างสม่ำเสมอ โดยพิจารณาตามเกณฑ์ดังต่อไปนี้
  1. ทบทวนตาม *ISMS-WI-05 Access and Privilege Matrix Work Instruction*
  2. สิทธิการเข้าถึงระบบของผู้ใช้งานต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง
  3. บัญชีผู้ใช้งานที่ได้รับสิทธิในระดับพิเศษ และ สิทธิการเชื่อมต่อจากระยะไกล (Remote Access) อย่างน้อยปีละ 1 ครั้ง
  4. สิทธิการเข้าถึงระบบของผู้ใช้งานต้องได้รับการทบทวนทุกครั้งที่มีการเปลี่ยนแปลง หรือเมื่อผู้ใช้งานนั้นสิ้นสุดสภาพการเป็นพนักงานของบริษัทฯ

- สิทธิการเข้าถึงระบบทั้งหมดต้องถูกยกเลิกทันที เมื่อผู้ใช้งานไม่มีความจำเป็นต้องเข้าถึงระบบอีกต่อไป ทั้งนี้ ถือเป็นความรับผิดชอบของผู้ใช้งาน และผู้บังคับบัญชาที่ต้องแจ้งให้ผู้ดูแลระบบทราบว่า ผู้ใช้งานนั้นไม่มีความจำเป็นต้องใช้สิทธิการเข้าถึงระบบอีกต่อไป
- ต้นสังกัด ต้องแจ้งให้ผู้ดูแลระบบ รับทราบทันทีเมื่อบุคคลภายนอกภายใต้การดูแลของตนเอง เช่น พนักงานชั่วคราว ที่ปรึกษา ฯลฯ ไม่มีความจำเป็นต้องเข้าถึงระบบ และอุปกรณ์เทคโนโลยีสารสนเทศของบริษัทฯ อีกต่อไป

5. การทบทวนและปรับปรุงนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศทั้งหมด รวมถึงระเบียบและคำสั่งต่างๆ ที่เกี่ยวข้อง ต้องได้รับการทบทวนและประเมินผลเพื่อปรับปรุงเนื้อหา หรือยืนยันเนื้อหาเดิมโดยผู้บริหารอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าเนื้อหาของนโยบายยังคงไว้ซึ่งความครบถ้วนสมบูรณ์ มีประสิทธิภาพ และสามารถนำไปใช้งานได้อย่างเหมาะสม

6. บทลงโทษ

การละเมิด ฝ่าฝืน ละเลย หรือไม่ปฏิบัติตามนโยบาย ตลอดจนวิธีการปฏิบัติงาน และเอกสารสนับสนุนต่างๆ ที่เกี่ยวข้อง ไม่ว่าโดยเจตนาหรือไม่ก็ตาม ถือเป็นความผิดทางวินัย ซึ่งจะต้องพิจารณาลงโทษทางวินัยตามกฎระเบียบของบริษัทฯ และหากการละเมิดหรือฝ่าฝืนนโยบายนั้นเข้าข่ายการกระทำที่ผิดกฎหมาย ผู้ละเมิดต้องได้รับการดำเนินคดีตามที่กฎหมายระบุไว้

7. เอกสารอ้างอิง

1. ISMS-PL-04 Network Management Policy
2. ISMS-PC-01 User Access Request Procedure
3. ISMS-PC-07 Share User Account Procedure
4. ISMS-PC-03 Access Matrix Procedure
5. ISMS-PL-10 Third Party Security Policy
6. ISMS-ST-02 Password Standard
7. ISMS-WI-05 Access and Privilege Matrix Work Instruction
8. Third Party Code of Conduct

End of Document