The Electricity Generating PCL

End User Security Guideline

Document Effective Date: July 2021

1. Introduction

1.1. Objectives

The End User Security Guideline has been developed with the following objectives:

1. To provide guidance and procedures for information security/ cybersecurity management in accordance with relevant laws and related security requirements.
2. To ensure all EGCO's employees and others who are authorized to access EGCO's information system comply with such guideline, appropriately and safely.
3. To protect EGCO's information from loss, destruction, unauthorized modification, smuggling or unauthorized access disclosure of sensitive information as well as ensures the integrity, availability and confidentiality of EGCO's information.

1.2. Scope

This document is applied and made available to all EGCO's employees and all users who are given the privilege to gain access to EGCO's system and use information processing facilities.

บริษัท ผลิตไฟฟ้า จำกัด (มหาชน)

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศสำหรับผู้ใช้งาน

รหัสเอกสาร :	[Document ID]
หมายเลขปรับปรุงเอกสาร :	draft
วันที่เอกสารมีผลบังคับใช้ :	<วันบังคับใช้เอกสาร>
เจ้าของเอกสาร :	<เจ้าของเอกสาร>
ผู้อนุมัติเอกสาร :	<ผู้อนุมัติเอกสาร>

ประวัติการปรับปรุงเอกสาร

เวอร์ชั่น	คำอธิบายและเหตุผลในการแก้ไข	ผู้แก้ไข	วันที่
1.0	เอกสารเผยแพร่ฉบับแรก		

หมายเลขข้อปฏิบัติสอดคล้องตามมาตรฐาน ISO/IEC 27001:2013

ขั้นตอนปฏิบัติในเอกสารฉบับนี้ได้รับการจัดทำขึ้นเพื่อให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2013 Annex A

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ	ลายเซ็น	ตำแหน่ง	วันที่
จัดทำโดย	<ผู้จัดทำเอกสาร>			
ตรวจทาน	<ผู้ตรวจทานเอกสาร>			
อนุมัติโดย	<ผู้อนุมัติเอกสาร>			

เอกสารอ้างอิง

ISO/IEC 27001:2013	Information technology-Security techniques-Information security management systems-Requirements
ISO/IEC 27002:2013	Information technology-Security techniques-Code of practice for information security controls

1. บทนำ

1.1 วัตถุประสงค์

วัตถุประสงค์ของแนวปฏิบัติการรักษาความมั่นคงความปลอดภัยของระบบเทคโนโลยีสารสนเทศสำหรับผู้ใช้งานฉบับนี้

1. เพื่อเป็นแนวทางในการใช้งานข้อมูล การปฏิบัติงาน ระบบเทคโนโลยีสารสนเทศขององค์กรให้เป็นไปอย่างเหมาะสม สอดคล้องกับกฎหมาย ตลอดจนข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง
2. เพื่อให้บุคลากรในองค์กร ตลอดจนบุคคลอื่นใดที่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศรับทราบเข้าใจและปฏิบัติตามนโยบาย ได้อย่างถูกต้อง เหมาะสม และปลอดภัย
3. เพื่อปกป้องสารสนเทศให้ปลอดภัยจากความสูญเสียในรูปแบบต่างๆ เช่น การสูญหาย การถูกทำลาย การแก้ไขโดยไม่ได้รับอนุญาต การลักลอบนำข้อมูลไปใช้หรือเปิดเผย ตลอดจนสร้างความมั่นใจว่าระบบสารสนเทศมีความมั่นคงปลอดภัย น่าเชื่อถือ และสามารถให้บริการได้อย่างต่อเนื่อง

1.2 ขอบเขต

แนวปฏิบัตินี้บังคับใช้กับเจ้าหน้าที่หรือพนักงานทุกคน หรือหน่วยงานภายนอกที่เข้าถึงระบบสารสนเทศของ บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) (บผฟ.)หรือ เอ็กโก กรุ๊ป

1.3 นิยามหรือคำจำกัดความ

(1) “**บริษัท/องค์กร**” หมายถึง บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) หรือ เอ็กโก กรุ๊ป

(2) “**ผู้บังคับบัญชา**” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของ บผฟ.

(3) **“ฝ่ายบริหาร บผฟ.”** หมายถึง คณะกรรมการกำกับดูแลการพัฒนาเทคโนโลยีสารสนเทศ

(4) **“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง”** หมายถึง ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ สารสนเทศ ที่ได้รับมอบหมายให้กำกับดูแลงานด้านระบบเทคโนโยลีสารสนเทศขององค์กร

(5) **“พนักงาน”** หมายถึง พนักงานและลูกจ้างของ บผฟ. รวมถึงบุคคลอื่นที่ บผฟ. มอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลงหรือใบสั่งจ้าง

(6) **“เจ้าของสินทรัพย์”** หมายถึง บุคคลหรือหน่วยงานที่รับผิดชอบ ตัดสินใจ กำหนดมาตรการในการจัดการสินทรัพย์นั้น โดยเจ้าของสินทรัพย์เป็นผู้ได้รับผลกระทบโดยตรงหากสินทรัพย์เกิดการสูญหาย เสียหาย

(7) **“ผู้ดูแลระบบแม่ข่าย”** หมายถึง พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบสารสนเทศ ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา และอุปกรณ์ต่อพ่วงต่างๆ ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ และการปฏิบัติงานในระบบงานสารสนเทศของ บผฟ.

(8) **“ผู้ดูแลระบบเครือข่าย”** หมายถึง พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่าย ซึ่งสามารถเข้าถึงระบบโดยใช้โปรแกรมเครือข่ายในการจัดการฐานข้อมูลและอุปกรณ์ภายในระบบ

(9) **“ผู้พัฒนาระบบ”** หมายถึง พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาและปรับปรุงระบบงานสารสนเทศของ บผฟ.

(10) **“เจ้าของระบบ (System Owner)”** หมายถึง หน่วยงานภายในซึ่งเป็นเจ้าของระบบคอมพิวเตอร์ และมีความรับผิดชอบในระบบคอมพิวเตอร์นั้นๆ

(11) **“ผู้อารักขา (Custodian)”** หมายถึง ผู้ที่ได้รับมอบหมายจากเจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศในการสนับสนุนงานการดูแล จัดการ และควบคุมการเข้าใช้ข้อมูลสารสนเทศให้เป็นไปตามข้อกำหนดหรือระดับสิทธิที่เจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศกำหนด

(12) **“ผู้ใช้งาน (User)”** หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของ บผฟ. ดังนี้

(10.1) พนักงาน

(10.2) ผู้รับบริการ

(10.3) บุคคลที่ บผฟ. อนุญาตให้สามารถเข้าใช้ระบบสารสนเทศและระบบเครือข่ายขององค์กรเพื่อประโยชน์ในการดำเนินงาน ได้แก่ พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบ หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้างหรือนิสิตนักศึกษาฝึกงาน

(13) **“การรักษาความมั่นคงปลอดภัย”** หรือ **“ความมั่นคงปลอดภัย (Security)”** หมายถึง กระบวนการ และการกระทำใดๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจากความพยายามใดๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอก ในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินธุรกิจของบริษัท ได้รับความเสียหาย

(14) **“ทรัพยากร”** หมายถึง องค์ประกอบทั้งทางตรรกะและทางกายภาพเพื่อใช้ในการดำเนินการระบบเทคโนโลยีสารสนเทศ ได้แก่ ระบบสารสนเทศ ระบบเครือข่าย บุคคลากร งบประมาณ และเวลาที่ใช้ในการดำเนินงาน

(15) **“สินทรัพย์”** หมายถึง สิ่งใดก็ตามที่มีมูลค่าต่อ บผฟ.

(16) **“ข้อมูลสารสนเทศ”**ซึ่งต่อไปนี้เรียกว่า **“ข้อมูล”** หมายถึง ข้อมูล ข่าวสาร บันทึกประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่างๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

(17) **“ข้อมูลสำคัญ”** หรือ **“ข้อมูลที่เป็นความลับ (Sensitive Information)”** หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัทมีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัท ไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง

(18) **“ข้อมูลส่วนบุคคล”** หมายถึง ข้อมูลที่เกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ทั้งนี้ให้หมายความรวมถึงทั้งข้อมูลส่วนบุคคลทั่วไปและข้อมูลส่วนบุคคลที่ละเอียดอ่อน เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน ความเชื่อ ศาสนาหรือข้อมูลที่มีชื่อของผู้นั้นหรือมีหมายเลขประจำตัว รหัสการระบุตัวตนผ่านการออนไลน์ ข้อมูลระบุตำแหน่ง หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้หรือระบุตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย ข้อมูลชีวภาพ ข้อมูลพันธุกรรม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(19) **“การประมวลผล”** หมายถึง การดำเนินการหรือชุดของการดำเนินงานใด ๆ ที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลหรือชุดของข้อมูลส่วนบุคคลไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่อัตโนมัติ เช่น การรวบรวม การบันทึก การจัดการ การจัดเก็บ การปรับหรือการเปลี่ยนแปลง การนำไปใช้ การพิจารณา การเปิดเผยโดยการส่งผ่านช่องทางต่างๆ การเผยแพร่หรือนำใช้งาน การจำกัด การลบหรือการทำลาย

(20) **“ผู้ควบคุม”** หมายถึง บุคคลธรรมดาหรือนิติบุคคล, หน่วยงานสาธารณะหรือหน่วยงานอื่น ๆ ซึ่งซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพียงคนเดียวหรือร่วมกับผู้อื่น ในกำหนดวัตถุประสงค์และวิธีการของการประมวลผลข้อมูลส่วนบุคคล

(21) **“ระบบเทคโนโลยีสารสนเทศ (Information Technology System)”** หมายถึง ระบบงานของบผฟ. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบสารสนเทศ เครื่องคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างข้อมูลสารสนเทศ

(22) **“ระบบที่มีความสำคัญ (Important System)”** หมายถึง ระบบคอมพิวเตอร์ที่บริษัทใช้ประโยชน์ เพื่อให้บริการทางธุรกิจทั้งระบบที่ก่อให้เกิดรายได้โดยตรง และระบบที่สนับสนุนให้เกิดรายได้ รวมถึงระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยในการดำเนินธุรกิจของบริษัท ให้เป็นปกติ และระบบที่ได้รับการกำหนดโดยหน่วยงานด้านความปลอดภัยข้อมูลและระบบสารสนเทศของบริษัท ทั้งนี้หากระบบที่มีความสำคัญดังกล่าวหยุดการทำงานหรือมีความสามารถในการทำงานที่ลดถอยลงจะทำให้การดำเนินธุรกิจของบริษัทต้องหยุดชะงัก หรือด้อยประสิทธิภาพ

(23) **“เครื่องคอมพิวเตอร์”** หมายถึง เครื่องคอมพิวเตอร์ ได้แก่ เครื่องคอมพิวเตอร์ตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา ในบางกรณีอาจรวมถึงเครื่องคอมพิวเตอร์แม่ข่ายหรือเครื่องคอมพิวเตอร์เซิร์ฟเวอร์

(24) **“เครื่องคอมพิวเตอร์แบบพกพา (Mobile Computer)”** หมายถึง เครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นใดที่สามารถประมวลผลและพกพาหรือเคลื่อนย้ายได้ ได้แก่ เครื่องคอมพิวเตอร์โน้ตบุ๊ก (Notebook) สมาร์ทดีไวซ์ (Smart Device) แท็บเล็ต (Tablet)

(25) **Bring your own device(BYOD)** หมายถึง อุปกรณ์คอมพิวเตอร์ที่มีการประมวลผลส่วนตัวของพนักงานนำมาใช้ปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศขององค์กร

(26) **“Remote Access”** หมายถึง การเชื่อมต่อเพื่อเข้าถึงคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท (ผ่านช่องทางการสื่อสารภายในบริษัท) หรือ จากภายนอกบริษัท (ผ่าน Internet)

(27) **“ซอฟต์แวร์ไม่ประสงค์ดี”** หมายถึง ซอฟต์แวร์ที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ทำให้ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ได้แก่ ไวรัสคอมพิวเตอร์ โปรแกรมแอบจับข้อมูลประเภทสปายแวร์(Spyware)

(28) **“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ”** หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบสารสนเทศ ทั้งทางตรรกะและทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้น สำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(29) **“เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)”** หมายถึง การระบุเหตุการณ์ในระบบเทคโนโยโลยีสารสนเทศของ บผฟ. ที่มีความเป็นไปได้ว่าเกิดการละเมิดนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการล้มเหลว หรือสถานการณ์ที่เกิดขึ้นและมีความสุ่มเสี่ยงด้านความมั่นคงปลอดภัย

(30) **“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด หรือ เหตุละเมิดด้านความมั่นคงปลอดภัย (Security Incident)”** ซึ่งต่อไปนี้เรียกว่า “เหตุ

ละเมิด”หมายถึง เหตุการณ์หนึ่งหรือหลายๆเหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่คาดคิดว่าจะเกิดขึ้น (Unwanted/ Unexpected) โดยเหตุการณ์ดังกล่าวมีความเป็นไปได้อย่างมากที่เกิดจากการบุกรุกหรือโจมตีการดำเนินการ และคุกคามต่อความมั่นคงปลอดภัยสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์

(31) **“สิทธิของผู้ใช้งาน”** หมายถึง สิทธิต่างๆ ในการใช้งานระบบสารสนเทศ ได้แก่ สิทธิพิเศษในการจัดการระบบ สิทธิทั่วไป สิทธิจำเพาะ เป็นต้น

(32) **“รหัสผ่าน (Password)”** หมายถึง ตัวอักษร และ/หรืออักขระ และ/หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(33) **“จดหมายอิเล็กทรอนิกส์ หรืออีเมล์ (e-Mail)”** หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail Box) ที่กำหนดไว้สำหรับผู้ใช้ในระบบเครือข่าย ผู้รับสามารถเปิดอ่านข่าวสาร หรือพิมพ์ลงกระดาษ หรือจะลบทิ้งไปก็ได้

(34) **“บันทึกการเข้าใช้งาน (logs)”** หมายถึง ข้อมูลเหตุการณ์ต่างๆ ที่เกิดขึ้นจากการใช้งานของระบบสารสนเทศ

(35) **“เอกสารและบันทึก” หมายถึง** ข้อมูลที่ได้จัดทำเพื่อใช้ในการอ้างอิง สามารถนำมาใช้เป็นหลักฐาน หรือสนับสนุนการทำงาน เอกสารและบันทึกสามารถจัดเก็บอยู่ในรูปแบบใดก็ได้ เช่น กระดาษ ไฟล์คอมพิวเตอร์ อีเมล์ เป็นต้น

สารบัญ

แนวปฏิบัติการใช้งานทรัพย์สินสารสนเทศอย่างมั่นคงปลอดภัย

1. การจำแนกและการจัดการข้อมูล

1.1 ประเภทข้อมูล

1.1.1 ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบายและแผนงบประมาณ

1.1.2 ข้อมูลสารสนเทศด้านการบริการ ได้แก่ ข้อมูลข่าวสารประชาสัมพันธ์ กฎหมาย หลักเกณฑ์ ระเบียบ ประกาศ ข้อมูลส่วนบุคคลที่มีความจำเป็นต้องใช้ในการดำเนินธุรกิจตามขอบเขตวัตถุประสงค์สำหรับการให้บริการ

1.2 ระดับชั้นความลับและการจัดการการเข้าถึง

1.2.1 กำหนดให้มีการจัดระดับชั้นข้อมูลภายในแผนกสารสนเทศออกเป็น 4 ระดับ ดังนี้

1) ลับมาก (Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ขององค์กรอย่างร้ายแรง เช่น แผนกลยุทธ์ในการดำเนินธุรกิจ แผนการตลาด ฯลฯ
2) ลับ (Confidential) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ขององค์กร เช่น แผนผังเครือข่าย รหัสผ่าน งบประมาณ คู่มือการปฏิบัติงานของแต่ละแผนก ข้อมูลส่วนบุคคลที่มีความจำเป็นต้องใช้ในการดำเนินธุรกิจตามขอบเขตวัตถุประสงค์สำหรับการให้บริการฯลฯ
3) ใช้งานภายในเท่านั้น (Internal) หมายถึง หากเปิดเผยทั้งหมดโดยไม่ได้รับอนุญาตโดยทั่วไปไม่ทำความเสียหายร้ายแรง เช่น รายการทรัพย์สิน ใบแจ้งซ่อม คู่มือการใช้งานระบบ นโยบาย ประกาศ คำสั่ง ฯลฯ
4) เปิดเผยได้ (Public) หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้ในวงกว้าง เช่น ข่าวสาร ประชาสัมพันธ์ขององค์กร ข้อมูลองค์กร รายงานประจำปี ฯลฯ

1.2.2 การกำหนดวิธีการเข้าถึง

1) ผู้ใช้งานสามารถเข้าถึงบริการระบบสารสนเทศได้โดยการเข้าถึงระบบต้องผ่านระบบการยืนยันตัวตน

1.2.3 การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

1) การเข้าถึงจากภายในหน่วยงาน ต้องเข้าถึงผ่านระบบเครือข่ายของบริษัทเท่านั้น
2) การเข้าถึงจากภายนอกหน่วยงาน ต้องเข้าถึงผ่านทางระบบ VPN เท่านั้น
3) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ทั้งนี้รวมถึงข้อมูลส่วนบุคคลที่มีการเก็บข้อมูลในฐานข้อมูลซึ่งมีเซิร์ฟเวอร์ตั้งอยู่ในต่างประเทศ เช่น คลาวด์ (cloud) ต้องได้การป้องกันตามมาตรการด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

เช่น ข้อมูลที่รับ/ส่งหรือโอนไปยังปลายทางต้องได้รับการเข้ารหัส (Encryption) เช่น การเข้ารหัสด้วยโปรโตคอล SSL บนเว็บไซต์ เป็นต้น

1.2.4 ระดับชั้นความลับกำหนดโดยผู้ที่เป็นเจ้าของข้อมูล โดยระดับชั้นความลับอาจมีการเปลี่ยนแปลงได้เมื่อ

1) เมื่อมีความจำเป็นต้องส่งข้อมูลไปยังหน่วยงานภายนอก เช่น ผู้ขาย (Vendor) หรือลูกค้า โดยอาจลบข้อมูลที่เป็นส่วนที่สำคัญ/เป็นความลับเพื่อให้มีความเหมาะสมและสอดคล้องกับระดับชั้นความลับของข้อมูลก่อนส่งออก
2) เมื่อข้อมูลไม่มีความทันสมัยทำให้ข้อมูลลดความสำคัญ/ความจำเป็นที่ต้องรักษาความลับเปลี่ยนไป

1.2.5 ในการจัดการข้อมูลหลายระดับชั้นความลับ ให้ปฏิบัติตามระดับชั้นความลับที่สูงที่สุด

2. แนวทางปฏิบัติการจัดการข้อมูลของผู้ใช้งาน

- ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดการข้อมูล (Information classification, Labeling and Handling Guideline) โดยแนวปฏิบัติครอบคลุมมาตรการสำหรับการดำเนินการของข้อมูลดังต่อไปนี้:
    - การจำแนกประเภทข้อมูล
    - การติดป้ายเพื่อบ่งชี้ระดับความสำคัญของข้อมูล
    - การจัดเก็บทั้งทางกายภาพและทางอิเล็กทรอนิกส์
    - การทำสำเนา
    - การส่งหรือถ่ายโอนข้อมูล ทั้งทางไปรษณีย์ แฟกซ์ อีเมล์ และอื่นๆ ที่กำหนดให้สามารถดำเนินการได้
    - การทำลายข้อมูลและสื่อบันทึกข้อมูล

2.1 การใช้งานและการปกป้องข้อมูล

- ผู้ใช้งานทุกคนต้องใช้งานข้อมูลขององค์กรตามระเบียบ คำสั่ง ประกาศและข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ และให้บริหารจัดการข้อมูลตามแนวทางการปฏิบัติปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดการข้อมูล (Information classification, Labeling and Handling Guideline) อย่างเคร่งครัด
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษในการใช้งานข้อมูลประเภท “Confidential” และ “Secrete” (ต่อไปในเอกสารนี้เรียกว่า “ข้อมูลลับ”) ตามที่ระบุไว้ในแนวทางการปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดการข้อมูล (Information classification, Labeling and Handling Guideline) เพื่อป้องกันไม่ให้ข้อมูล รั่วไหล ถูกเข้าถึงหรือเปิดเผยโดยไม่ได้รับอนุญาต

- ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่างๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร เครื่องโทรสาร ฯลฯ ทันที
- ผู้ใช้งานต้องไม่เปิดเผยข้อมูลขององค์กรกับผู้อื่นหรือบุคคลภายนอก เว้นแต่ได้มีการลงนามข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure agreement: NDA) และต้องเปิดเผยตามความจำเป็นในการปฏิบัติงานเท่านั้น
- หากต้องส่งข้อมูลไปยังองค์กรอื่น เจ้าหน้าที่ที่รับผิดชอบในการส่งข้อมูลจะต้องแจ้งความสำคัญของเอกสารและข้อกำหนดในการจัดการข้อมูลกับผู้รับทราบก่อนที่จะดำเนินการส่งมอบต่อไป
- ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน รวมถึงอุปกรณ์คอมพิวเตอร์ที่สามารถบันทึกข้อมูลได้
- ไม่อนุญาตให้รับหรือส่งไฟล์ที่เป็นการละเมิดกฎหมาย หรือนโยบายของบริษัท และข้อมูลส่วนบุคคลที่ไม่ได้รับอนุญาตหรือยินยอมจากเจ้าของบุคคลอย่างเป็นทางการ
- ผู้ใช้งานสามารถเข้าถึงข้อมูลหรือใช้งานข้อมูลตามสิทธิ์ที่ได้รับมอบหมายเท่านั้น
- สื่อบันทึกข้อมูลแบบพกพา รวมถึงสื่อบันทึกข้อมูลทั้งหมดที่ใช้ในองค์กร ผู้ใช้งานควรคำนึงถึงมาตรการควบคุม การจัดการสื่อดังกล่าวจะต้องเป็นไปตามข้อกำหนดในแนวทางการปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดการข้อมูล (Information classification, Labeling and Handling Guideline)
- เมื่อสื่อถูกนำออกไปนอกสำนักงาน ผู้ใช้งานจะต้องมีความตระหนักด้านความปลอดภัยในการใช้งานว่าข้อมูลที่สำคัญอาจสูญหายหรือถูกบุกรุกได้
- เมื่อไม่มีการใช้งานสื่อบันทึกข้อมูลแล้ว ควรกำจัดสื่อตามมาตรฐานการทำลายสื่อที่เหมาะสม
- หากพบเห็นหรือทราบว่ามีการใช้งานข้อมูลลับหรือลับมากของบริษัทในทางที่ไม่ถูกต้องจะต้องแจ้งให้ผู้บังคับบัญชาทราบทันที
- การจัดเก็บ การทำลายข้อมูลข้อมูลสารสนเทศและข้อมูลส่วนบุคคลให้เป็นไปตามแนวทางการปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดการข้อมูล (Information classification, Labeling and Handling Guideline)
-

3. การใช้งานเครื่องคอมพิวเตอร์ คอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์แบบพกพา

- ห้ามใช้ทรัพยากรสารสนเทศของบริษัท ผลิตไฟฟ้า จำกัด (มหาชน) (บผฟ.) หรือ เอ็กโก กรุ๊ป เพื่อหรือสนับสนุนวัตถุประสงค์ที่ผิดกฎหมายตามที่กฎหมายได้บัญญัติไว้โดยเด็ดขาด
- ห้ามใช้ทรัพย์สินสารสนเทศขององค์กรทำกิจกรรมทางการเมืองในภายในองค์กรโดยเด็ดขาด
- การใช้งานทรัพย์สินจะทำได้เฉพาะพนักงานหรือผู้ที่ได้รับอนุญาตเท่านั้น

- การใช้งานจะต้องไม่เป็นการขัดขวางประสิทธิภาพในการปฏิบัติงานภายในองค์กร เช่น ไม่อนุญาตให้ส่งอีเมล์ลูกโซ่ ฯลฯ
- ข้อมูล ข้อความ และเอกสารใดๆ ที่จัดเก็บไว้ในระบบสารสนเทศขององค์กรให้ถือเป็นทรัพย์สินขององค์กร
- พนักงานระดับผู้จัดการส่วนหรือเทียบเท่าขึ้นไปของ บผฟ. มีหน้าที่จะต้องดูแลให้เครื่องคอมพิวเตอร์ที่ใช้งานในความรับผิดชอบทุกระดับได้รับการติดตั้งโปรแกรมใช้งานโดยถูกต้องตามนโยบายของบริษัท
- พนักงานที่อนุญาตให้บุคคลอื่น ใช้งานเครื่องคอมพิวเตอร์ของบริษัท ให้ถือว่าเป็นความรับผิดชอบของพนักงานที่เป็นผู้อนุญาต
- พนักงานมีหน้าที่จะต้องดูแลให้เครื่องคอมพิวเตอร์ที่ใช้งานได้รับการติดตั้งโปรแกรมงานโดยถูกต้องตามนโยบายของบริษัท
- พนักงานต้องพึงระวังรักษาเครื่องคอมพิวเตอร์ ซึ่งเป็นทรัพย์สินของบริษัท หากเกิดสูญหายหรือเสียหายเนื่องจากสาเหตุที่ไม่ได้เกิดจากการใช้งานตามปกติ พนักงานจะต้องเป็นผู้รับผิดชอบค่าเสียหายที่เกิดขึ้น
- ผู้ใช้งานจะต้องใช้ทรัพย์สินของบริษัทที่มอบหมายให้ดูแลในการใช้งานเพื่อการประมวลผล จัดเก็บข้อมูล และ/หรือการเข้าถึงระบบบริการขององค์กร เพื่อวัตถุประสงค์ในการทำงานเท่านั้น ผู้ใช้งานจะต้องรับผิดชอบในการดูแลและปกป้องอุปกรณ์ที่ได้รับ
- หากอุปกรณ์ในการทำงาน ไม่ได้เป็นทรัพย์สินของบริษัท จะต้องได้รับการอนุมัติให้ใช้งานได้ภายใต้ข้อกำหนดด้านความปลอดภัยสารสนเทศ และการตรวจสอบด้านความปลอดภัยในการตั้งค่าอุปกรณ์ รวมถึงการติดตั้งและตั้งค่าอุปกรณ์ให้เป็นไปตามข้อกำหนดด้านความปลอดภัยสารสนเทศ ซึ่งผู้ใช้งานต้องตรวจสอบให้แน่ใจว่าซอฟต์แวร์ทั้งหมดรวมถึงโปรแกรมป้องกันไวรัสได้รับการอัปเดตด้วยแพตช์ล่าสุดหรือมีลิขสิทธิ์การใช้งานถูกต้อง
- เมื่อเดินทางควรถืออุปกรณ์พกพาเป็นกระเป๋าถือเว้นแต่กฎหมายห้ามไว้ ในสถานการณ์เช่นนี้จะต้องตรวจสอบให้แน่ใจว่ากระเป๋าเช็คอินที่มีอุปกรณ์พกพานั้นได้รับการรักษาความปลอดภัยและมีการสำรองข้อมูลทางธุรกิจภายในอุปกรณ์พกพาและนำไปพร้อมกับพนักงานในระหว่างการเดินทาง
- ต้องดูแลให้สภาพแวดล้อมมีความปลอดภัยเช่น ไม่มีใครสามารถเห็นหน้าจอหรือกล้องวงจรปิดที่ชี้ไปที่หน้าจอก่อนที่จะใช้อุปกรณ์มือถือ
- ควรปฏิบัติตามคำแนะนำของผู้ผลิตในการปกป้องอุปกรณ์ตลอดเวลาเช่นการป้องกันการสัมผัสกับสนามแม่เหล็กไฟฟ้าแรง ๆ การป้องกันแสงแดดโดยตรง ฯลฯ
- อุปกรณ์เคลื่อนที่ควรได้รับการปกป้องที่เหมาะสม เมื่อมีการใช้งานในพื้นที่สาธารณะ
- หากอุปกรณ์เสียหาย สูญหาย หรือเกิดการลักขโมย จะต้องแจ้งผู้บังคับบัญชาและผู้ดูแลระบบให้ทราบทันทีเพื่อให้มีการติดตามและมีวิธีการจัดการกับเหตุการณ์ได้อย่างมีประสิทธิภาพ

- การจัดการข้อมูลที่อยู่ภายในอุปกรณ์จะต้องเป็นไปตามวิธีการจัดการข้อมูลตามระดับชั้นความลับสูงสุดของข้อมูลนั้น
- ผู้ใช้งานต้องทำการสำรองข้อมูลบนพื้นที่ที่จัดไว้ให้ และจัดเก็บอย่างสม่ำเสมอ

4. การทำงานจากระยะไกล

- อนุญาตให้ใช้อุปกรณ์เป็นทรัพย์สินของ บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) หรือ เอ็กโก กรุ๊ป และ/หรืออุปกรณ์ที่ได้รับอนุญาตเท่านั้น
- การทำงานจากระยะไกล ต้องผ่านช่องทางที่มีความปลอดภัยตามที่กำหนดไว้เท่านั้น

5. การนำอุปกรณ์ส่วนตัวใช้ในการปฏิบัติงาน (BYOD Policy)

(1) อุปกรณ์ส่วนตัวที่ได้รับอนุญาตให้นำมาใช้ในการปฏิบัติงานภายในองค์กรได้ (BYOD) ทั้งหมด ผู้ใช้งานจะต้องได้ทำการการตรวจสอบดังนี้:
   - อุปกรณ์เคลื่อนที่ไม่ได้มีการแก้ไขระบบปฏิบัติการมาก่อน
   - มีการอับแพตช์ระบบปฏิบัติการและแอปพลิเคชันให้เป็นปัจจุบัน
   - มีการเปิดใช้งานการพิสูนจ์ตัวตนเมื่อมีการเข้าถึงอุปกรณ์
   - มีการบังคับใช้หน้าจอล็อกอัตโนมัติ
   - หากเป็นไปได้ให้ดำเนินการป้องกันที่เหมาะสมสำหรับโค้ดที่เป็นอันตราย (โดยใช้แอปพลิเคชันป้องกันไวรัสที่ได้รับอนุมัติ)

(2) ควรติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตหรือซอฟต์แวร์ที่เกี่ยวข้องกับวัตถุประสงค์การทำงานบนอุปกรณ์ที่ได้รับอนุญาตให้นำมาใช้ในการปฏิบัติงานภายในองค์กร (BYOD) เท่านั้น

(3) อุปกรณ์ที่ได้รับอนุญาตให้นำมาใช้ในการปฏิบัติงานภายในองค์กร (BYOD) ทั้งหมดที่นำเข้ามาในห้องเซิร์ฟเวอร์จะต้องได้รับการอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

6. การป้องกันซอฟต์แวร์ไม่ประสงค์ดี

- ผู้ใช้งานจะต้องตรวจสอบให้แน่ใจว่าไฟล์อับเดทโปรแกรมแอนตี้ไวรัสเป็นข้อมูลล่าสุดก่อนที่จะดาวน์โหลดไฟล์ภายนอกหรือเชื่อมต่อบริการอินเทอร์เน็ต
- ผู้ใช้งานจะต้องไม่พยายามเปิดไฟล์ที่ไม่ได้ร้องขอหรือน่าสงสัย ผ่านอีเมลอิเล็กทรอนิกส์ การส่งข้อความแชท หรือระบบเครือข่ายสังคมอื่น ๆ พวกเขาควรพยายามขอคำชี้แจงเกี่ยวกับวัตถุประสงค์ของไฟล์กับผู้ส่งก่อนที่จะทำการเปิด
- ผู้ใช้งานจะต้องสแกนสื่อบันทึกข้อมูลภายนอก ซึ่งเคยเชื่อมต่อกับระบบสารสนเทศอื่นที่ไม่ใช่ขององค์กรเพื่อตรวจสอบไวรัส

- ผู้ใช้งานจะต้องไม่ท่องเว็บไซต์ที่ไม่คุ้นเคยหรือน่าสงสัย และไม่ควรปิดการทำงานของฟังก์ชั่นการป้องกันป๊อปอัปหรือฟิชชิ่งของโปรแกรมอินเทอร์เน็ตเบราว์เซอร์เมื่อเข้าใช้งานเว็บไซต์ที่ไม่คุ้นเคย
- หากอุปกรณ์คอมพิวเตอร์ที่ผู้ใช้งานดูแลติดไวรัสและไม่สามารถจัดการได้ด้วยตนเองให้ดำเนินการดังนี้

1) ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์และระบบเครือข่าย
2) ติดต่อผู้ดูแลระบบให้เร็วที่สุด
3) ไม่พยายามลบหรือแก้ไขไฟล์ระบบ (System Files) ด้วยตนเอง
4) ให้ความร่วมมือผู้ดูแลระบบในการแก้ไขปัญหาจนกว่าผู้ดูแลระบบจะตรวจสอบว่าไวรัสทั้งหมดถูกลบออกแล้ว
5) หากการดูแลระบบไม่สามารถลบไวรัสทั้งหมดในระบบที่ติดไวรัส ซอฟต์แวร์และไฟล์ทั้งหมดในคอมพิวเตอร์จะต้องถูกลบรวมถึงข้อมูลการบูตเครื่องหากจำเป็น และซอฟต์แวร์จะได้รับการติดตั้งใหม่และสแกนหาไวรัสอีกครั้ง

7. โทรศัพท์ ข้อความเสียง และเครื่องโทรศาร (Telephone Voice Mail and Fax)

- หลีกเลี่ยงการพูดคุยหรือส่งต่อข้อมูลที่สำคัญทางโทรศัพท์ยกเว้นในกรณีที่เร่งด่วนที่สุด ข้อมูลที่ถูกจำกัดและข้อมูลที่เป็นความลับจะต้องไม่ถูกพูดคุยทางโทรศัพท์ โดยแนวทางการพิจารณาว่าเป็นข้อมูลที่สำคัญมีดังต่อไปนี้:
  - ตามประเภทข้อมูลตามแนวทางการปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดการข้อมูล (Information classification, Labeling and Handling Guideline)
  - รหัสผ่าน แต่ไม่รวมรหัสผ่านครั้งเดียว (OTP)
  - ข้อมูลที่บริษัทยังไม่มีการเปิดเผยออกไป
- ควรรายงานการใช้ระบบโทรศัพท์และเครื่องโทรสารในทางที่ผิด หรือใช้ในทางที่ผิดต่อหัวหน้างานหรือผู้บังคับบัญชาทันทีตามขั้นตอนการจัดการเหตุการณ์ด้านความปลอดภัย
- ไม่ควรมีการสื่อสารข้อมูลที่มีระดับชั้นความลับในพื้นที่ที่ไม่มีการควบคุม หรือมีบุคคลที่ไม่มีส่วนเกี่ยวข้องอยู่ในสถานที่นั้นด้วย
- ควรมีการกำหนดรหัสผ่านเพื่อใช้เปิดข้อความเสียง ยกเว้นมีข้อจำกัดทางเทคนิค
- ไม่ควรระบุรายละเอียดของเจ้าของกล่องข้อความตอบรับมากเกินไป เพื่อป้องกันการนำข้อมูลไปใช้ในการหลอกลวงทางสังคม (Social Engineering)
- ควรมีการระบุชื่อผู้รับ จำนวนหน้า ของเอกสารที่จัดส่งในหน้าแรก
- ควรมีการตรวจสอบหมายเลขที่ต้องการจัดส่งก่อนทุกครั้ง

- หากพบว่ามีข้อผิดพลาด เช่น ส่งโทรสารไม่ผ่าน ให้ตรวจสอบหมายเลขโทรสารกับผู้รับก่อนจัดส่งใหม่
- ควรหลีกเลี่ยงการจัดส่งข้อมูลส่วนบุคคลทางโทรสาร ยกเว้นมีเหตุจำเป็น เช่น ใบสมัครของลูกค้าเป็นต้น
- หากมีความจำเป็นต้องส่งข้อมูลที่มีชั้นความลับตั้งแต่ระดับลับ (Confidential) ขึ้นไป กำหนดให้มีการสื่อสารไปยังผู้รับให้ทราบก่อนจัดส่ง ทั้งนี้ควรแจ้งให้ผู้รับรอรับเอกสารหน้าเครื่องโทรสาร และปฏิบัติแนวทางการปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดการข้อมูล (Information classification, Labeling and Handling Guideline)

8. เครื่องถ่ายเอกสาร

- ข้อมูลทั้งหมดที่ทำซ้ำจะต้องเป็นไปตามแนวทางการปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดการข้อมูล (Information classification, Labeling and Handling Guideline)
- ห้ามจัดเก็บเอกสารสำคัญไว้ที่ตัวเครื่องถ่ายเอกสาร
- การใช้เครื่องถ่ายเอกสารในทางที่ผิดหรือในทางที่ผิดจะต้องรายงานต่อหัวหน้างานหรือผู้บังคับบัญชาตามขั้นตอนการจัดการเหตุการณ์ด้านความปลอดภัย

9. การใช้งานระบบเครือข่าย

- บุคคลภายนอกสามารถเข้าถึงบริการในเครือข่ายบริการสาธารณะได้และไม่มีสิทธิ์เข้าถึงทรัพยากรภายในขององค์กร
- ไม่อนุญาตให้บุคคลภายนอกเชื่อมต่อกับเครือข่ายสำนักงานโดยไม่ได้รับอนุญาตอย่างเป็นทางการจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ในกรณีที่การเชื่อมต่อได้รับการอนุมัติ ควรตรวจสอบกิจกรรมบนเครือข่ายของบุคคลภายนอก
- ต้องใช้เฉพาะอุปกรณ์ต่อพ่วงไร้สายที่ได้รับการอนุญาตให้ติดตั้งภายในสำนักงาน รวมถึงห้องเซิร์ฟเวอร์และห้องอุปกรณ์

10. การใช้งานสังคม/เครือข่ายออนไลน์

- เฉพาะเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้นที่สามารถเป็นตัวแทนบริษัท ผลิตไฟฟ้า จำกัด (มหาชน) หรือ เอ็กโก กรุ๊ป เพื่อการสื่อสารบนเครือข่ายออนไลน์
- ผู้ใช้งานจะต้องปฏิบัติตามกฎหมายลิขสิทธิ์และอ้างอิงหรืออ้างอิงแหล่งที่มาอย่างเหมาะสม เมื่อโพสต์เนื้อหาในโซเชียลมีเดีย

- ผู้ใช้งานจะต้องไม่เผยแพร่ โพสต์หรือปล่อยข้อมูลใด ๆ ที่ถือว่าเป็นความลับหรือไม่เปิดเผยต่อสาธารณะ
- ห้ามใช้โลโก้และเครื่องหมายการค้าของ บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) หรือ เอ็กโก กรุ๊ป โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษร
- การนำเข้าข้อความใด ๆ ที่เกี่ยวข้องกับบริษัท ผลิตไฟฟ้า จำกัด (มหาชน) หรือ เอ็กโก กรุ๊ป จะต้องได้รับอนุญาตอย่างเป็นทางการก่อน
- ห้ามเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตอย่างเป็นทางการ

11. การใช้อินเตอร์เน็ตและข้อความอิเล็กทรอนิกส์ (ระบบ Internet, Intranet และ E-mail)

- ผู้ใช้งานจะต้องใช้อินเทอร์เน็ต อีเมลอิเล็กทรอนิกส์ และการส่งข้อความแชท เพื่อวัตถุประสงค์ในการปฏิบัติงานสอดคล้องกับการดำเนินธุรกิจขององค์กร หรือได้รับการอนุมัติเท่านั้น โดยค่าเริ่มต้นระบบที่ได้รับการอนุมัติในปัจจุบันสำหรับการใช้งานทางธุรกิจคือระบบสารสนเทศขององค์กร
- ห้ามใช้งานระบบ internet, Intranet และ E-mail ในลักษณะดังนี้
    - การยุยงที่ก่อให้เกิดความแตกแยกหรือขัดแย้งเรื่อง เพศ เชื้อชาติ ศาสนา การเมืองหรือสถานบันพระมหากษัตริย์
    - ก่อกวนสร้างความไม่พอใจให้กับผู้อื่นหรือเป็นอันตรายต่อขวัญกำลังใจโดยเด็ดขาด
    - ใช้ในทางที่ผิดกฎหมายหรือจริยธรรม
    - การพนันทุกชนิด
    - การส่งต่อจดหมายอิเล็กทรอนิกส์ที่เกี่ยวกับการล่วงละเมิดหรือข่มขู่ หรือมีเนื้อหาข้อความที่ขัดต่อกฎหมายและศีลธรรม และใช้จดหมายอิเล็กทรอนิกส์เป็นเครื่องมือในการกระจายข่าวสาร เว้นแต่เป็นการประกาศที่เหมาะสม
    - การใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ละเมิดสิทธิส่วนบุคคล ยุยง ทำให้เกิดความแตกแยกหรือข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร
    - การส่งข้อความ รูปภาพ หรือวัสดุใดๆ ที่สิ่งผิดกฎหมาย สร้างความอับอาย คุกคาม ก้าวร้าว สร้างความเกลียดชังหรือสนับสนุนให้มีการดำเนินการซึ่งถือเป็นความผิดทางอาญา สร้างความวุ่นวายให้กับพลเรือนหรือเป็นการละเมิดกฎหมายใดๆ
    - การส่งข้อความที่น่ารังเกียจหรือก้าวร้าว รวมทั้งสื่อลามกอนาจารทุกชนิด
    - การส่งต่อจดหมายอิเล็กทรอนิกส์ลูกโซ่ หรือสแปมจดหมายอิเล็กทรอนิกส์ ฯลฯ
    - ไม่นำเข้าข้อมูลหรือแสดงความเห็นส่วนตัวเสมือนเป็นความเห็นขององค์กร
- ผู้ใช้งานไม่ควรใช้อีเมลในการดำเนินงานทางธุรกิจที่มีเงื่อนไขของเวลาเข้ามาเกี่ยวข้อง

- ผู้ใช้งานควรใช้งานระบบ internet, Intranet และ E-mail ด้วยความรอบคอบและมีวิจารณญาณ โดยให้ระลึกเสมอว่าพนักงานคือตัวแทนของบริษัทในการทำธุรกิจ
- ผู้ใช้งานที่เยี่ยมชมเว็บไซต์ลามกอนาจาร อาจจะถูกลงโทษทางวินัยและอาจถูกเลิกจ้าง
- เมื่อใช้บริการส่งข้อความแชท และการส่งข้อความภายนอกองค์กร ผู้ใช้จะต้องระวังการส่งข้อมูลองค์กรตามแนวทางการปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดการข้อมูล (Information classification, Labeling and Handling Guideline) เท่านั้น
- ข้อมูลที่ส่งทางอีเมลควรได้รับการปกป้องด้วยกลไกการรักษาความปลอดภัยตามที่กำหนดตามแนวทางการปฏิบัติการจัดระดับชั้นความลับ การติดป้ายและการจัดการข้อมูล (Information classification, Labeling and Handling Guideline)
- อีเมลทั้งหมดควรมีการบันทึกถึงข้อตกลงการรักษาความลับ และระบุข้อความการปฏิเสธความรับผิดชอบหากมีการนำอีเมลไปใช้งานโดยไม่ได้รับอนุญาต
- ไม่อนุญาตให้ทำการปลอมแปลงต้นทางของการสื่อสารอิเล็กทรอนิกส์ การเปลี่ยนแปลงข้อมูลของระบบที่ใช้ในการระบุที่มาของข้อความ หรือปิดบังต้นทางของการสื่อสาร
- ห้ามิให้เข้าถึงระบบเพื่อพยายามในการเฝ้าติดตาม อ่าน คัดลอก ลบ หรือเจาะเข้าไปในการสื่อสารทางอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับความยินยอมจากบุคคลนั้น (ยกเว้นบุคคลากรระบบเครือข่ายที่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร)
- ไม่ควรใช้ระบบ E-mail เพื่อเก็บข้อมูลสะสมไว้เป็นเวลานาน
- ห้ามใช้ฟังก์ชั่น Automatic Forward เพื่อการส่ง E-mail ต่อไปให้คอมพิวเตอร์ที่ไม่ใช่ของบริษัท
- ห้ามส่งข้อมูลส่วนบุคคลไปยังหน่วยงานอื่น ทั้งภายในและภายนอกหากไม่ได้รับอนุญาตอย่างเป็นทางการ

12. การบริหารจัดการรหัสผ่าน

- รหัสผ่านจะถูกเปลี่ยนอย่างน้อยทุกๆ 90 วันหรือเมื่อใดก็ตามที่มีข้อบ่งชี้ว่าอาจมีการรั่วไหลของข้อมูล
- รหัสผ่านที่ใช้ร่วมกัน(share password) จะใช้สำหรับการทดสอบระบบเท่านั้นและได้รับการดูแลรักษาโดยแผนกพัฒนาระบบสารสนเทศ
- รหัสผ่านจะต้องไม่ถูกเก็บไว้ในระบบประมวลผลข้อมูลหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ใด ๆ โดยไม่มีการเข้ารหัสข้อมูลไว้
- รหัสผ่านจะไม่ถูกบันทึกไว้ เว้นแต่จะสามารถจัดเก็บได้อย่างปลอดภัย
- ผู้ใช้งานจะต้องรับผิดชอบต่อบัญชีผู้ใช้งานและรหัสผ่านของตน และจะไม่เปิดเผยต่อผู้ใดโดยไม่คำนึงถึงสถานการณ์
- ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านเริ่มต้นหรือรีเซ็ตทันทีเมื่อเข้าสู่ระบบสำเร็จครั้งแรกหากระบบไม่ได้รับแจ้งให้ดำเนินการดังกล่าว

- การเปลี่ยนรหัสผ่านต้องไม่ซ้ำกับ 5 รหัสผ่านเดิมที่เคยตั้งไว้
- หากใส่รหัสผ่านผิดจำนวน 5 ครั้งภายใน 15 นาที ระบบจะปิดสถานะการใช้งานของบัญชีผู้ใช้งานทันที (หากระบบรับรองการตั้งค่าดังกล่าว)
- ระบบจะเปิดสถานะการใช้งานของบัญชีหลังจาก 15 นาทีไปแล้ว หากต้องการใช้งานก่อนเวลาดังกล่าว ให้ติดต่อเจ้าหน้าที่ดูและรบบเพื่อเปิดสถานะการใช้งานบัญชีผู้ใช้
- เนื่องจากการโจมตีแบบฟิชชิ่งได้แพร่หลายอย่างมากในปัจจุบัน ผู้ใช้งานพึงทราบ บริษัทจะไม่ขอข้อมูลส่วนบุคคลหรือรหัสผ่านใด ๆ จากคุณผ่านสื่ออิเล็กทรอนิกส์หรือเสียง (เช่น facebook, whatsapp, line, อีเมลและโทรศัพท์) ในกรณีที่ได้รับคำขอดังกล่าวคุณควรลบข้อความทันทีหรือวางสายโดยไม่ต่อความยาวกับผู้ส่ง / ผู้โทร หากคุณมีข้อสงสัยโปรดตรวจสอบความถูกต้องของคำขอกับฝ่ายเทคโนโลยีสารสนเทศ

13. การสร้างรหัสผ่าน

1) รหัสผ่านผู้ใช้งานต้องเปลี่ยนทุก 90 วัน
2) รหัสผ่านต้องมีความยาวอย่างน้อยแปด (8) ตัวอักษรและประกอบด้วยคุณสมบัติอย่างน้อยสาม (3) ลักษณะดังต่อไปนี้:
    - อักขระตัวเลขอย่างน้อยหนึ่งตัว (0 - 9)
    - อักขระตัวพิมพ์เล็กอย่างน้อยหนึ่งตัว (a - z)
    - อักขระตัวพิมพ์ใหญ่อย่างน้อยหนึ่งตัว (A - Z)
    - อักขระพิเศษอย่างน้อยหนึ่งตัว (~! @ # $% ^ & * - +?) สำหรับระบบที่รองรับอักขระพิเศษ
3) ผู้ใช้งานจะต้องพิจารณาสิ่งต่อไปนี้ เมื่อสร้างรหัสผ่านเพื่อเพิ่มความซ้ำซ้อนของรหัส:
    - ห้ามใช้คำในภาษาสแลงภาษาถิ่นศัพท์แสง ฯลฯ
    - ห้ามใช้ข้อมูลส่วนบุคคลเช่นชื่อ (ญาติสัตว์เลี้ยง ฯลฯ) หรือวันที่เช่นวันเกิดวันหยุดและวันครบรอบ (เช่น“ 09Aug2009”)
    - ห้ามใช้คำาวลีหรือตัวย่อที่เกี่ยวข้องกับ EGCO (เช่น“ EGCOCgroup”)
    - ห้ามใช้ข้อกำหนดคำสั่งเว็บไซต์ชื่อคอมพิวเตอร์หรือแอปพลิเคชันซอฟต์แวร์ (เช่น“ winipcfg”,“ yahoodotcom”)
    - ห้ามใช้คำหรือรูปแบบตัวเลข (เช่น“ 12345678”,“ abcdefgh”)
    - อย่าเพิ่มรหัสผ่านก่อนหน้านี้ด้วยการเติม / ต่อท้ายอักขระเพิ่มเติม (เช่น“ oldpassword1”,“ 1oldpassword”)
4) การสร้างรหัสผ่านที่สามารถได้ง่ายโดยใช้ Mnemonics ตัวอย่างเช่น "ตรุษจีน" กลายเป็น "Ch1n353N3wY3 @ r" (ไม่ควรใช้ตัวอย่างที่แสดงนี้เป็นรหัสผ่าน เนื่องจากเป็นตัวอย่างที่ใช้กันทั่วไปในหนังสือการเรียนการสอน)

14. การดูแลโต๊ะทำงานให้ปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

- ผู้ใช้งานจะต้องเปิดใช้งานการล็อกหน้าจอเมื่อออกจากเครื่องคอมพิวเตอร์ โดยไม่มีใครดูแล
- ข้อมูลที่จัดเก็บในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ จะต้องได้รับการปกป้องตามการจำแนกประเภทข้อมูลตามที่กำหนดไว้ ในมาตรฐานการจำแนกประเภทข้อมูล การติดป้ายและการจัดเก็บข้อมูล
- เครื่องคอมพิวเตอร์และเทอร์มินัลทั้งหมด จะต้องมีโปรแกรมรักษาหน้าจอที่ป้องกันด้วยรหัสผ่านหรือการควบคุมอื่น ๆ ที่เปิดใช้งานหลังจากไม่มีการใช้งานเป็นระยะเวลาหนึ่ง (สูงสุด 15 นาที)
- ผู้ใช้งานต้องไม่วางเอกสาร/ข้อมูลลับ รวมถึงข้อมูลส่วนบุคคลไว้บนหน้าจอหรือ บนโต๊ะโดยไม่มีใครดูแล

15. การรายงานเหตุการณ์ จุดอ่อนและการใช้ในทางที่ผิดในด้านความมั่นคงปลอดภัย

15.1 การตอบสนองต่อเหตุการณ์/จุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศและการรักษาความปลอดภัยทางไซเบอร์

15.1.1 ผู้ใช้งานจะต้องรายงานเหตุการณ์และ/หรือจุดอ่อนด้านความมั่นคงปลอดภัยไปยังทีมผู้ที่เกี่ยวข้องการในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทันที ตามแนวปฏิบัติในการการรายงานเหตุละเมิดด้านความมั่นคงปลอดภัย

15.1.2 ห้ามมิให้ผู้ใช้งานตอบคำถามที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยและความผิดพลาดของระบบกับสื่อใดๆ เองโดยเด็ดขาด การสื่อสารข้อมูลกับหน่วยงานภายนอกทั้งหมดจะเป็นหน้าที่ของคณะทำงานที่ได้รับมอบหมายในการสื่อสารเท่านั้น

15.2 การรายงานการทำงานผิดปกติของฮาร์ดแวร์และซอฟต์แวร์

1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการรายงานซอฟต์แวร์หรือฮาร์ดแวร์ที่พบว่าทำงานไม่เหมาะสม/ไม่เป็นปกติ เพื่อแก้ไขตามแนวปฏิบัติในการรายงานเหตุละเมิดด้านความมั่นคงปลอดภัย

2) ในกรณีเกิดเหตุการณ์ต้องสงสัยว่าเป็นซอฟต์แวร์ที่เป็นอันตรายที่ผู้ที่มีหน้าที่รับผิดชอบต้องปฏิบัติตามรายการด้านล่างนี้เป็นอย่างน้อย :

    - สังเกตและบันทึกอาการ รวมถึงข้อความที่ปรากฏบนหน้าจอ
    - หยุดการใช้อุปกรณ์ประมวลผลและแยกอุปกรณ์ประมวลผลออกจากระบบอื่น ถ้าเป็นไปได้
    - รายงานความผิดปกติตามช่องทางการรายงานที่กำหนดไว้

3) ห้ามผู้ใช้งานลบซอฟต์แวร์ที่ต้องสงสัย นอกจากจะได้รับอนุญาต

4) เฉพาะบุคคลที่มีอำนาจเท่านั้นที่จะสามารถกู้คืนระบบได้

16. ความปลอดภัยของทรัพย์สินทางปัญญาของบุคคลหรือหน่วยงานอื่น

16.1 การจัดการใบอนุญาต

- ต้องใช้ซอฟต์แวร์ที่ได้รับอนุญาตหรือได้รับการรับรองอย่างถูกต้องเพื่อการใช้งานภายในองค์กรเท่านั้น โดยผู้รับผิดชอบทรัพย์สินประเภทซอฟต์แวร์นี้ต้องตรวจสอบให้แน่ใจว่าซอฟต์แวร์ถูกใช้ภายในขอบเขตตามข้อกำหนดและเงื่อนไขที่ระบุไว้ในข้อตกลง
- ซอฟต์แวร์ที่ติดตั้งเพื่อทดลองใช้งานจะต้องถูกลบออกจากระบบ เมื่อหมดระยะเวลาทดลองใช้งาน
- การดูแลระบบซอฟต์แวร์จะต้องเก็บรักษาบันทึกการติดตั้งให้เป็นปัจจุบัน เพื่อให้แน่ใจว่าจำนวนสิทธิ์การใช้งานสูงสุดที่ซื้อไม่เกิน ใบอนุญาตต้นฉบับและสำเนาหลักให้เก็บไว้เป็นหลักฐานในการเป็นเจ้าของ
- พนักงานจะต้องไม่ทำสำเนาซอฟต์แวร์ลิขสิทธิ์โดยไม่ได้รับอนุญาต
- พบว่าพนักงานติดตั้งซอฟต์แวร์ที่ไม่มีลิขสิทธิ์จะต้องรับผิดชอบอย่างเต็มที่ต่อการละเมิดลิขสิทธิ์

16.2 ลิขสิทธิ์และสิทธิบัตร

- ห้ามใช้การออกแบบเครื่องหมายการค้าหรือสิทธิบัตรที่มีลิขสิทธิ์ ซึ่งไม่ได้พัฒนาขึ้นภายในองค์กร เว้นแต่จะได้รับความยินยอมจากเจ้าของลิขสิทธิ์หรือเจ้าของสิทธิบัตร
- ผู้ใช้งานต้องปฏิบัติตามกฎหมายลิขสิทธิ์ เพื่อป้องกันการละเมิดทรัพย์สินทางปัญญา
- ผู้ใช้งานจะใช้รายการซอฟต์แวร์ตามข้ออนุญาตของเจ้าของลิขสิทธิ์ซอฟต์แวร์ และไม่มีสิทธิในการทำซ้ำเพื่อการอื่นใด นอกจากการเก็บสำรอง
- ผู้ใช้งานติดตั้งซอฟต์แวร์เฉพาะที่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศเท่านั้น
- ห้ามละเลยการดูแลอุปกรณ์ ห้ามวางอุปกรณ์ไว้ห่างตัว หรือฝากบุคคลอื่นในการดูแลรักษาอุปกรณ์
- หากพบเห็นหรือทราบว่ามีการใช้งานซอฟต์แวร์หรือเอกสารที่เกี่ยวข้องของบริษัทในทางที่ไม่ถูกต้องจะต้องแจ้งให้ผู้บังคับบัญชาทราบ
- ผู้ใช้งานที่มีส่วนในการผลิตซ้ำซอฟต์แวร์ อาจได้รับโทษต้องชดใช้ค่าเสียหายในทางแพ่ง และโทษทางอาญาทั้งจำและปรับ บริษัท มิได้ส่งเสริมหรือสนับสนุการทำซ้ำซอฟต์แวร์ที่ผิดกฎหมาย พนักงานที่ทำ ซื้อ หรือใช้ซอฟต์แวร์คอมพิวเตอร์ที่ไม่ได้รับอนุญาตอาจได้รับโทษทางวินัยตามความเหมาะสมของสถานการณ์
- หากผู้ใช้งานมีข้อสงสัยใดๆ ที่เกี่ยวข้องกับเรื่องการทำซ้ำหรือใช้งานซอฟต์แวร์อย่างใดอย่างหนึ่ง ให้หารือกับผู้จัดการในส่วนงานที่รับผิดชอบก่อนที่จะดำเนินการต่อไป

17. การคุ้มครองข้อมูลส่วนบุคคล

17.1 การบริหารจัดการข้อมูลส่วนบุคคล

17.1.1 การจัดทำทะเบียนรายการข้อมูลส่วนบุคคล

องค์กรต้องดำเนินการจัดทำรายการข้อมูลส่วนบุคคลที่เก็บรวบรวม ใช้ หรือเปิดเผยและหน่วยงานที่เกี่ยวข้อง ไม่ว่าจะอยู่ในรูปแบบอิเล็กทรอนิกส์หรือรูปแบบกระดาษ โดยต้องมีการทบทวนอย่างสม่ำเสมอทุก 1 ปี หรือเมื่อมีการเปลี่ยนแปลงบริการ ข้อมูลส่วนบุคคล หรือ หน่วยงานที่เกี่ยวข้อง

17.1.2 การระบุฐานการประมวลผลข้อมูลส่วนบุคคล

หลักการที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

1) ข้อมูลส่วนบุคคลจะต้อง:

(ก) ประมวลผลอย่างถูกต้องตามกฎหมาย เป็นธรรม และโปร่งใสเกี่ยวกับเรื่องข้อมูล

(ข) เก็บรวบรวมเพื่อวัตถุประสงค์ที่ระบุไว้ให้ชัดเจนและถูกต้องตามกฎหมาย และไม่ดำเนินการเพิ่มเติมในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์เหล่านั้น ข้อมูลส่วนบุคคลอาจถูกจัดเก็บเป็นระยะเวลานานตราบเท่าที่ข้อมูลส่วนบุคคลจะถูกประมวลผล เพื่อประโยชน์สำคัญต่อชีวิต หรือเพื่อวัตถุประสงค์ด้านการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์หรือวัตถุประสงค์ทางสถิติ เพื่อวัตถุประสงค์ตามภารกิจของรัฐเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย โดยสอดคล้องตามพระราชบัญญัติว่าด้วยคณะกรรมการว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2560 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติความปลอดภัยทางไซเบอร์ พ.ศ. 2562 ซึ่งมีผลบังคับใช้ในปัจจุบันและจะมีการแก้ไขหรือเพิ่มเติมในอนาคต

(ค) เหมาะสม เกี่ยวเนื่องและจำกัด เฉพาะสิ่งที่จำเป็นเกี่ยวกับวัตถุประสงค์ในการประมวลผล

(ง) มีความถูกต้องและหากจำเป็นปรับให้เป็นปัจจุบัน โดยจะต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่ผิดไปจากวัตถุประสงค์จะถูกลบหรือแก้ไขโดยทันที

(ก) เก็บไว้ในแบบฟอร์มที่อนุญาต โดยให้ระบุเจ้าของข้อมูลได้และไม่เกินความจำเป็นสำหรับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลอาจถูกจัดเก็บเป็นระยะเวลานานตราบเท่าที่ข้อมูลส่วนบุคคลจะถูกประมวลผล เพื่อประโยชน์สำคัญต่อชีวิต หรือเพื่อวัตถุประสงค์ด้านการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์หรือวัตถุประสงค์ทางสถิติ เพื่อวัตถุประสงค์ตามภารกิจของรัฐเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย โดยสอดคล้องตามพระราชบัญญัติว่าด้วยคณะกรรมการความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ พ.ศ. 2560 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติความปลอดภัยทางไซเบอร์ พ.ศ. 2562 ภายใต้การดำเนินมาตรการทางเทคนิคและองค์กรที่เหมาะสมตามข้อบังคับนี้ เพื่อปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูล

(ฉ)ประมวลผลในลักษณะที่รับประกันถึงความปลอดภัยของข้อมูลส่วนบุคคลรวมถึงการป้องกันการประมวลผลที่ไม่ได้รับอนุญาตหรือผิดกฎหมายและจากการสูญเสียการทำลายหรือความเสียหายโดยไม่ตั้งใจโดยใช้มาตรการทางเทคนิคหรือองค์กรที่เหมาะสม

2) ผู้ควบคุมข้อมูลจะต้องรับผิดชอบและสามารถแสดงให้เห็นถึงการปฏิบัติตามหลักการการประมวลผลข้อมูล

องค์กรต้องตรวจสอบให้แน่ใจว่ากาประมวลผลข้อมูลส่วนบุคคลจะเป็นไปตามหลักการเหล่านี้ทั้งหมด และมีการดำเนินงานของระบบบริหารการจัดการความมั่นคงปลอดภัยของข้อมูล (ISMS) ที่สอดคล้องกับมาตรฐานสากล ISO/IEC27001 เป็นมาตรการปกป้องข้อมูลส่วนบุคคลเป็นสำคัญ

จากหลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลดังกล่าว องค์กรต้องระบุฐานในการประมวลผลข้อมูลส่วนบุคคล ตามเหตุผลและความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล เพื่อให้การบริหารจัดการข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและถูกต้อง ดังฐานต่อไปนี้

- ฐานสัญญา (Contract)
- ฐานความยินยอม (Consent)
- ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)
- ฐานหน้าที่ตามกฎหมาย (Legal Obligation)
- ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)
- ฐานจดหมายเหตุ/วิจัย/สถิติ (Research)
- ฐานภารกิจสาธารณธ/อำนาจรัฐ (Public Task)

ฐานการประมวลผลข้อมูล	รายละเอียด
ฐานสัญญา (Contract Basis)	การประมวลผลข้อมูลที่จำเป็นต่อการให้บริการตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล โดยข้อมูลส่วนบุคคลที่ถูกจัดอยู่ในฐานสัญญา ไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเพิ่มเติม โดยข้อมูลอ่อนไหว (Sensitive data) ไม่สามารถถูกระบุอยู่ในฐานสัญญาได้
ฐานความยินยอม (Consent Basis)	การประมวลผลที่ทำได้เฉพาะในกรณีเจ้าของข้อมูลได้สมัครใจเลือก ที่จะยินยอมให้ประมวลผลได้ โดยเจ้าของข้อมูลสามารถเลือกที่จะปฏิเสธได้ และไม่เป็นเงื่อนไขในการรับบริการ
ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest Basis)	การประมวลผลข้อมูลมีความจำเป็นต่อการปกป้องประโยชน์สำคัญของเจ้าของข้อมูลหรือบุคคลอื่น เช่น ป้องกันอันตรายร้ายแรงอันอาจเกิดต่อสุขภาพและชีวิตด้วยการประมวลผลข้อมูลสุขภาพหรือข้อมูลอ่อนไหว (Sensitive data) นอกจากนั้นฐานการประมวลผลนี้สามารถประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลอยู่ในสภาวะที่ไม่สามารถให้ความยินยอมได้ และไม่มีวิธีอื่นที่สามารถปกป้องชีวิตบุคคลอื่นโดยไม่ต้องประมวลผลข้อมูลนี้แล้ว

ฐานหน้าที่ตามกฎหมาย (Legal Obligation Basis)	การประมวลผลข้อมูลจำเป็นต่อการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลตามที่กฎหมายกำหนด ที่ไม่สามารถเลือกที่จะไม่ปฏิบัติได้ โดยต้องระบุบทบัญญัติตามข้อกฎหมาย หรือคำสั่งของหน่วยงานของรัฐที่มีอำนาจอย่างชัดเจน
ฐานประโยชน์อันชอบธรรม (Legitimate Interest Basis)	การประมวลผลที่จำเป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลและบุคคลอื่น โดยไม่เกินขอบเขตที่เจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผล
ฐานจดหมายเหตุ/วิจัย/สถิติ (Research)	การประมวลผลที่จำเป็นต่อการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุเพื่อประโยชน์สาธารณะ และการศึกษาวิจัยและสถิติ โดยต้องอ้างอิงฐานใดฐานหนึ่งใน 6 ฐานด้านบนประกอบเสมอ
ฐานภารกิจสาธารณธ/อำนาจรัฐ (Public Task)	การประมวลผลข้อมูลที่จำเป็นต่อการดำเนินงานตามภารกิจของรัฐเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย

17.1.3 ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

หน่วยงานที่เก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล ต้องไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บไว้ให้บุคคลอื่น เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลเป็นลายลักษณ์อักษร หรือ เป็นไปตามกฎหมาย โดยให้ปฏิบัติตามมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสริภาพของเจ้าของข้อมูลส่วนบุคคล

17.2 การรักษาความมั่นคงปลอดภัยข้องข้อมูลส่วนบุคคล

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นเรื่องที่สำคัญ และถือเป็นหนึ่งในหลักการของการคุ้มครองข้อมูลส่วนบุคคล โดยหลักการของการรักษาความมั่นคงปลอดภัย คือการรักษาไว้ซึ่ง

1 การรักษาความลับ (Confidentiality)

2 ความถูกต้องครบถ้วน (Integrity) และ

3 ความพร้อมใช้ (Availability)

โดยหน่วยงานที่เก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล ต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเพื่อมิให้ข้อมูลส่วนบุคคลสูญหาย ถูกทำลาย รวมถึงเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย โดยไม่ได้รับอนุญาตดังต่อไปนี้

1. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และมีมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศของข้อมูลส่วนบุคคลอย่างเหมาะสมและเคร่งครัด
2. มีการจัดลำดับชั้นความลับ จัดการ และทำลายข้อมูลส่วนบุคคลตามกระบวนการจัดลำดับชั้นความลับของข้อมูล

3. ต้องมีการจัดเก็บข้อมูลส่วนบุคคลและการทำลายข้อมูล สื่อบันทึกข้อมูลส่วนบุคคลหรืออุปกรณ์ที่มีการบันทึกข้อมูลส่วนบุคคล อย่างปลอดภัยตามกระบวนการเลิกใช้หรือทำลายอย่างปลอดภัย
4. ต้องมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของระบบงานที่ประมวลผลหรือ เก็บข้อมูลส่วนบุคคลอย่างสม่ำเสมอทุกปีหรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
5. ต้องมีการสื่อสารนโยบายด้านความมั่นคงปลอดภัยสารสนเทศให้แก่บุคลากรบริษัท ผู้รับจ้างหรือผู้ให้บริการภายนอกที่เข้าถึงข้อมูลส่วนบุคคลทราบ รวมถึงสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด
6. ต้องกำหนดสิทธิ์ในการเข้าถึงระบบสำหรับการประมวลผลข้อมูลส่วนบุคคลสอดคล้องกับหลักการให้สิทธิเท่าที่จำเป็น (Need to know principle)
7. ต้องมีการกำหนดสิทธิ์การเข้าถึงหรือการใช้งานข้อมูลส่วนบุคคลอย่างชัดเจนตามบทบาทหน้าที่และความรับผิดชอบที่ได้รับ โดยได้รับการอนุญาตในการเข้าถึงอย่างเป็นทางการ
8. จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนปลง ลบหรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
9. ผู้ใช้งานไม่มีสิทธิ์ในการยกเลิก หรือเปลี่ยนแปลงการตั้งค่าในการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์
10. ต้องระบุข้อกำหนดในการรักษาความลับและการปฏิบัติตามระเบียบข้อบังคับ นโยบายและกฎหมายที่เกี่ยวข้องในสัญญากับผู้รับจ้าง หรือผู้ให้บริการภายนอก หากมีการว่าจ้างและมีการที่เข้าถึงข้อมูลส่วนบุคคล เป็นผู้ประมวลผลข้อมูลส่วนบุคคล

17.3 การบันทึกข้อมูลการเข้าใช้งานเว็บไซต์ของผู้ใช้งาน

บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) มีระเบียบในการจัดเก็บบันทึกการเข้าเว็บไซต์ โดยอัตโนมัติที่สามารถเชื่อมโยงกับข้อมูลที่สามารถระบุตัวบุคคลได้ เช่น หมายเลขไอพีต้นทาง (Source IP Address) หมายเลขไอพีปลายทาง (Destination IP Address) วัน เวลา เส้นทาง ชนิดของบริการ และข้อมูลอื่นๆ ที่จำเป็นเพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

17.4 การใช้งาน Cookies

เว็บไซต์ของ บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) มีการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลของผู้เข้าเยี่ยมชมผ่าน คุกกี้ (Cookies) โดยมีการขอความยินยอมจากผู้ใช้งาน

17.5 สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการจัดการข้อมูลส่วนบุคคลของตนที่ได้ให้ไว้กับ บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) ดังต่อไปนี้

1) สิทธิในการเพิกถอนความยินยอม (Right to withdraw consent)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมกับบริษัท ผลิตไฟฟ้า จำกัด (มหาชน) ได้

2) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of access)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนเองและขอให้บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) ทำสำเนาข้อมูลส่วนบุคคลดังกล่าวให้แก่เจ้าของข้อมูลส่วนบุคคลได้ รวมถึงขอให้เปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าว

3) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (Right to rectification)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการร้องขอให้แก้ไขข้อมูลส่วนบุคคลของตนที่ไม่ถูกต้อง หรือเพิ่มเติมข้อมูลที่ไม่สมบูรณ์

4) สิทธิในการลบข้อมูลส่วนบุคคล (Right to erasure)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการขอลบข้อมูลของตนได้

5) สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (Right to restriction of processing)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการระงับการใช้ข้อมูลส่วนบุคคลของตนได้

6) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right to data portability)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการโอนย้ายข้อมูลส่วนบุคคลของตนที่ให้ไว้กับบริษัท ผลิตไฟฟ้า จำกัด (มหาชน) ไปยังผู้ควบคุมข้อมูลรายอื่น หรือ ตัวท่านเองได้

7) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to object)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนได้ เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อมายังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อดำเนินการยื่นคำร้องขอดำเนินการตามสิทธิข้างต้นได้ ตามรายละเอียดช่องทางการติดต่อในหัวข้อช่องทางการติดต่อ โดยไม่มีค่าใช้จ่ายในการดำเนินตามสิทธิข้างต้น โดยบริษัทจะพิจารณาคำร้องและแจ้งผลการพิจารณาตามคำร้องของท่านภายใน 30 วันทำการนับแต่วันที่เราได้รับคำร้องขอดังกล่าว สิทธิ์แต่ละสิทธิ์เหล่านี้จะต้องได้รับการดำเนินการโดยขั้นตอนที่เหมาะสม โดยองค์กรได้รับอนุญาตให้ดำเนินการเท่าที่จำเป็นและดำเนินการภายในระยะเวลาที่เหมาะสม ดังตารางต่อไปนี้

คำขอเรื่องข้อมูลส่วนบุคคล	ระยะเวลาการดำเนินการ
สิทธิในการเพิกถอนความยินยอม	โดยไม่ชักช้า
สิทธิในการเข้าถึงข้อมูลส่วนบุคคล	หนึ่งเดือน
สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	หนึ่งเดือน
สิทธิในการลบข้อมูลส่วนบุคคล	โดยไม่ชักช้า
สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล	โดยไม่ชักช้า
สิทธิในการโอนย้ายข้อมูลข้อมูลส่วนบุคคล	หนึ่งเดือน
สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล	เมื่อได้รับคำคัดค้าน
สิทธิที่เกี่ยวข้องกับการตัดสินใจและการทำโปรไฟล์อัตโนมัติ	ไม่ได้ระบุ

ตารางที่ 1 - ระยะเวลาสำหรับการร้องขอเรื่องข้อมูล

17.6 ความยินยอม

หากมีความจำเป็นด้วยเหตุผลที่ระบุในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะต้องได้รับความยินยอมจากเจ้าของข้อมูลเพื่อรวบรวมและประมวลผลข้อมูล ในกรณีที่เด็กอายุต่ำกว่า 18 ปี ต้องได้รับความยินยอมจากผู้ปกครอง ข้อมูลที่เกี่ยวข้องและการนำข้อมูลส่วนบุคคลของพวกเขาไปใช้จะต้องได้รับความยินยอมโดยเจ้าของข้อมูลในเวลาที่ได้รับความยินยอมและบ่งบอกสิทธิของพวกเขาที่สามารถกระทำได้ เช่นสิทธิในการเพิกถอนความยินยอม เจ้าของข้อมูลเหล่านี้จะต้องรับทราบและสามารถเข้าถึงได้โดยง่ายและไม่มีค่าใช้จ่าย

ข้อมูลส่วนบุคคลอื่นๆที่ไม่เกี่ยวเนื่องโดยตรง จะต้องระบุระยะเวลาที่เหมาะสมหลังจากที่ได้รับข้อมูลที่แน่นอนภายในหนึ่งเดือน

17.7 ความเป็นส่วนตัว

บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) ได้นำหลักการของความเป็นส่วนตัวมาใช้โดยการออกแบบและจะทำให้แน่ใจว่าคำจำกัดความและการวางแผนของระบบใหม่ทั้งหมด หรือมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่จำเป็นต้องรวบรวมหรือประมวลผล ข้อมูลส่วนบุคคลจะต้องได้รับการพิจารณา โดยคำนึงถึงความเป็นส่วนตัว รวมถึงการดำเนินการประเมินผลที่อาจกระทบด้านความเป็นส่วนตัวได้

การประเมินผลกระทบด้านความเป็นส่วนตัวจะรวมถึง:

- การพิจารณาวิธีการประมวลผลข้อมูลส่วนบุคคลและเพื่อวัตถุประสงค์ต่างๆ
- การประเมินว่าการประมวลผลข้อมูลส่วนบุคคลที่เสนอนั้นจำเป็นและเป็นไปตามวัตถุประสงค์หรือไม่
- การประเมินความเสี่ยงต่อบุคคลในการประมวลผลข้อมูลส่วนบุคคล

- การควบคุมต่างๆเพื่อจัดการกับความเสี่ยงต่างๆและแสดงให้เห็นถึงการปฏิบัติตามกฎหมาย

การใช้เทคนิคต่างๆ เช่น การลดข้อมูลและนามแฝงจะได้รับการพิจารณาตามความเหมาะสม

17.8 การเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่สาม

1) ห้ามผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

   (1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า โดยต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือ

   (2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด (มาตรา 25 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล)

2) บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) จะไม่เปิดเผยหรือแลกเปลี่ยนข้อมูลส่วนบุคคลกับบุคคลที่สามโดยไม่ได้รับความยินยอมจากบุคคลที่สามารถระบุตัวได้ยกเว้นในกรณีต่อไปนี้:

   (1) เมื่อกฎหมาย กระบวนการทางกฎหมาย การดำเนินคดี หรือกระบวนการบังคับใช้กฎหมายอื่นๆ กำหนดให้มีการเปิดเผยข้อมูลส่วนบุคคลของคุณ ซึ่งรวมถึงการเปิดเผยต่อหน่วยงานของรัฐหรือรัฐบาล หน่วยงาน หรือองค์กรเพื่อวัตถุประสงค์ในการบังคับใช้กฎหมายหรือเพื่อตอบสนองต่อคำขอที่ถูกต้องตามกฎหมาย หรือ

   (2) เมื่อพิจารณาแล้วว่าการเปิดเผยข้อมูลส่วนบุคคลเป็นไปตามความจำเป็นเพื่อป้องกันอันตรายหรือความเสียหายใดๆ หรือเพื่อตรวจสอบกิจกรรมใดๆ ที่อาจผิดกฎหมาย

บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) อาจแบ่งปันข้อมูลส่วนบุคคลกับบริษัทภายในกลุ่มเอ็กโก นอกจากนี้ บริษัท อาจแบ่งปันข้อมูลส่วนบุคคลกับผู้ให้บริการของบริษัท ที่ให้บริการในนามของบริษัท ผลิตไฟฟ้า จำกัด (มหาชน) โดยผู้ให้บริการเหล่านี้จะไม่เปิดเผยข้อมูลส่วนบุคคลของคุณเว้นแต่จะระบุไว้เป็นอย่างอื่นในนโยบายความเป็นส่วนตัวนี้หรือการเปิดเผยดังกล่าวเป็นสิ่งจำเป็นต่อการปฏิบัติตามกฎหมาย บริษัทขอสงวนสิทธิ์ในการถ่ายโอนข้อมูลส่วนบุคคลในกรณีที่มีการปรับโครงสร้างองค์กรหรือในกรณีที่มีการซื้อสินทรัพย์ที่สำคัญจาก บริษัท ผลิตไฟฟ้า จำกัด (มหาชน)

17.9 การจัดการกับการปฏิบัติตามข้อกำหนด

การดำเนินการดังต่อไปนี้ จะสร้างความมั่นใจว่าบริษัท ผลิตไฟฟ้า จำกัด (มหาชน) จะปฏิบัติตามหลักความรับผิดชอบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1) พื้นฐานทางกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลมีความชัดเจนและไม่คลุมเครือ
2) เจ้าหน้าที่คุ้มครองข้อมูลได้รับการแต่งตั้งด้วยความรับผิดชอบเฉพาะสำหรับการปกป้องข้อมูลในองค์กร

3) พนักงานทุกคนที่เกี่ยวข้องในการจัดการข้อมูลส่วนบุคคลเข้าใจความรับผิดชอบของพวกเขาในการทำตามแนวทางปฏิบัติด้านการปกป้องข้อมูลที่ดี
4) การฝึกอบรมในการปกป้องข้อมูลให้กับพนักงานทุกคน
5) กฎเกี่ยวกับความยินยอมที่ต้องปฏิบัติตาม
6) ช่องทางที่เจ้าของข้อมูลสามารถสอบถาม ใช้สิทธิ์ที่เกี่ยวกับข้อมูลส่วนบุคคล และการสอบถามดังกล่าวจะได้รับการจัดการอย่างมีประสิทธิภาพ
7) มีการตรวจสอบขั้นตอนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นประจำ
8) ความเป็นส่วนตัวจะถูกนำมาใช้สำหรับระบบและกระบวนการใหม่ทั้งหมดหรือที่มีเปลี่ยนแปลง
9) มีการบันทึกเอกสารการประมวลผลต่อไปนี้:
    - ชื่อองค์กรและรายละเอียดที่เกี่ยวข้อง
    - วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล
    - หมวดหมู่ของบุคคลและข้อมูลส่วนบุคคลที่ประมวลผล
    - ประเภทของผู้รับข้อมูลส่วนบุคคล
    - ข้อตกลงและวิธีการในการถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศที่ไม่ใช่สหภาพยุโรป รวมถึงรายละเอียดของการควบคุมที่เกี่ยวข้อง
    - กำหนดการเก็บรักษาข้อมูลส่วนบุคคล
    - การควบคุมทางเทคนิคและองค์กรที่เกี่ยวข้อง

การดำเนินการเหล่านี้จะได้รับการตรวจสอบเป็นประจำซึ่งเป็นส่วนหนึ่งของกระบวนการตรวจสอบการจัดการของระบบการจัดการความปลอดภัยของข้อมูล