บริษัท ดับบลิวพี เอ็นเนอร์ยี่ จำกัด (มหาชน)
WP ENERGY PUBLIC COMPANY LIMITED
1 Eastwater Building, 15/F Vipavadeerangsit Soi 5,
Vipavadeerangsit Rd, Jomphol, Jatujak, Bangkok 10900
Tel : 02 272 3322 E-mail : info@wp-energy.co.th
www.wp-energy.co.th

นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

บริษัท ดับบลิวพี เอ็นเนอร์ยี่ จำกัด (มหาชน)

บริษัท ดับบลิวพี เอ็นเนอร์ยี่ จำกัด (มหาชน) ("บริษัทฯ") ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ (Information Security) อันเป็นทรัพย์สินที่มีคุณค่าและเป็นรากฐานของความน่าเชื่อถือทางธุรกิจ บริษัทฯ จึงจัดทำนโยบายนี้ขึ้นเพื่อกำหนดแนวทางการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ โดยคำนึงถึงความเสี่ยงที่จะเกิดกับการรักษาความมั่นคงปลอดภัยของสารสนเทศของบริษัทฯ ในด้านต่าง ๆ ที่จะเกิดขึ้น ได้มีประสิทธิภาพมากขึ้นให้สอดคล้องกับ

- มาตรฐานสากล ISO/IEC 27001:2022
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
- รวมถึงกฎเกณฑ์และระเบียบของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

ทั้งนี้ เพื่อให้นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศนั้นสอดคล้องกับมาตรฐานสากลที่เป็นที่ยอมรับ และสามารถนำไปปฏิบัติได้จริง

วัตถุประสงค์

1.1 ป้องกันความเสี่ยงที่อาจเกิดขึ้นต่อสารสนเทศ ทรัพย์สินทางเทคโนโลยี และข้อมูลของบริษัทฯ จากภัยคุกคามทางไซเบอร์ ทั้งภายในและภายนอกบริษัทฯ

1.2 ใช้เป็นข้อกำหนดของการปฏิบัติงานของผู้รับผิดชอบ ผู้ใช้งาน และผู้ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของบริษัท ดับบลิวพี เอ็นเนอร์ยี่ จำกัด (มหาชน)

1.3 กำหนดมาตรฐานการดำเนินงานด้านความมั่นคงปลอดภัยของสารสนเทศให้เป็นไปในทิศทางเดียวกันทั่วทั้งบริษัทฯ

1.4 รักษาความปลอดภัยข้อมูลในทุกรูปแบบ รวมถึงข้อมูลบนกระดาษ ข้อมูลบนคลาวด์ และดิจิทัล

1.5 สร้างความเชื่อมั่นให้กับลูกค้า พนักงาน คู่ค้า และผู้มีส่วนได้เสียเกี่ยวกับการจัดการข้อมูลและระบบสารสนเทศที่ปลอดภัยของบริษัทฯ

1.6 ส่งเสริมให้พนักงานทุกระดับมีความรู้ ความเข้าใจและตระหนักถึงบทบาทหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูล

ขอบเขต

นโยบายนี้ใช้บังคับกับกรรมการ ผู้บริหาร พนักงานทุกระดับ ผู้รับจ้างช่วง ผู้ให้บริการภายนอก และบุคคลอื่นใดที่เกี่ยวข้องกับการเข้าถึง การจัดการ หรือการใช้สารสนเทศของบริษัทฯ

หมวดที่ 1 ข้อความทั่วไป

ส่วนที่ 1 นิยามและคำจำกัดความ

1. คำนิยาม และ คำจำกัดความ

"บริษัท"	หมายถึง บริษัท ดับบลิวพี เอ็นเนอร์ยี่ จำกัด (มหาชน)
"ระบบสารสนเทศ"	หมายถึง อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนด คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงาน ให้ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
"ระบบเครือข่าย"	หมายถึง กลุ่มของเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารชนิดต่าง ๆ ที่นำมาเชื่อมต่อกันเพื่อให้ผู้ใช้ในเครือข่าย สามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และใช้อุปกรณ์ต่าง ๆ ร่วมกันในเครือข่ายได้
"ฮาร์ดแวร์"	หมายถึง ส่วนประกอบทางกายภาพของคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ที่สามารถมองเห็นและสัมผัสได้
"ซอฟต์แวร์"	หมายถึง โปรแกรมคอมพิวเตอร์แบบชุดคำสั่งที่ใช้สั่งงานให้คอมพิวเตอร์ทำงานตามลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยคำสั่งของคอมพิวเตอร์ คำสั่งเหล่านี้เรียงกันเป็นซอฟต์แวร์
"ผู้ใช้งาน"	หมายถึง พนักงาน บุคคลภายนอก หรือผู้หนึ่งผู้ใด ที่ใช้งานระบบสารสนเทศของบริษัทฯ และต้องรับผิดชอบต่อความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้งานนั้น ๆ

"พนักงาน" หมายถึง บุคคลที่บริษัทฯ ว่าจ้างมารับผิดชอบปฏิบัติหน้าที่ประจำต่าง ๆ ภายในบริษัทฯ เช่น พนักงานประจำ พนักงานชั่วคราว

"หน่วยงานภายนอก" หมายถึง บริษัทอื่น ๆ ที่เกี่ยวข้อง เช่น บริษัทขายฮาร์ดแวร์หรือซอฟต์แวร์ บริษัทให้คำปรึกษาเกี่ยวกับระบบสารสนเทศ เป็นต้น

"ข้อมูลส่วนบุคคล (Personal Data)"

หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ทั้งที่อยู่ในรูปแบบเอกสาร กระดาษ หรืออิเล็กทรอนิกส์ เช่น ชื่อ-นามสกุล หมายเลขบัตรประชาชน ที่อยู่ เบอร์โทรศัพท์ ข้อมูลทางการเงิน ข้อมูลสุขภาพ หรือข้อมูลชีวมิติ รวมถึงข้อมูลอื่นใดที่สามารถระบุตัวบุคคลได้ ทั้งนี้ ให้เป็นไปตามที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้อง

"เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ"

หมายถึง เหตุการณ์ใด ๆ ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ข้อมูล หรือเครือข่ายของบริษัทฯ ซึ่งอาจส่งผลให้เกิดการละเมิดความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) หรือความพร้อมใช้งาน (Availability) ของข้อมูล เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล การโจมตีทางไซเบอร์ (Cyber Attack) การติดมัลแวร์ หรือการทำลายข้อมูลโดยไม่ได้ตั้งใจ

"ทรัพย์สินสารสนเทศ (Information Asset)"

หมายถึง ข้อมูล ระบบสารสนเทศ อุปกรณ์เทคโนโลยี เครือข่าย ซอฟต์แวร์ สื่อบันทึกข้อมูล เอกสาร หรือองค์ประกอบอื่นใดที่ใช้ในการจัดเก็บ ประมวลผล หรือส่งต่อข้อมูล ซึ่งมีคุณค่าต่อการดำเนินธุรกิจของบริษัทฯ และต้องได้รับการคุ้มครองให้ปลอดภัยจากการสูญหาย การเข้าถึงโดยไม่ได้รับอนุญาต หรือการทำลาย

"ความต่อเนื่องทางธุรกิจ (Business Continuity)"

หมายถึง ความสามารถของบริษัทฯ ในการดำเนินงานหลักหรือให้บริการได้อย่างต่อเนื่องเมื่อเกิดเหตุการณ์ไม่คาดคิด เช่น ภัยพิบัติ การโจมตีทางไซเบอร์ หรือการหยุดชะงักของระบบเทคโนโลยี โดยอาศัยการเตรียมการและแผนฟื้นฟูระบบ (Business Continuity Plan: BCP และ Disaster Recovery Plan: DRP) เพื่อให้ผลกระทบทางธุรกิจอยู่ในระดับที่ยอมรับได้

บริษัท ดับบลิวพี เอ็นเนอร์ยี่ จำกัด (มหาชน)
WP ENERGY PUBLIC COMPANY LIMITED
1 Eastwater Building, 15/F Vipavadeerangsit Soi 5,
Vipavadeerangsit Rd, Jomphol, Jatujak, Bangkok 10900
Tel : 02 272 3322 E-mail : info@wp-energy.co.th
www.wp-energy.co.th

ส่วนที่ 2 การใช้บังคับ

2. การใช้บังคับ

2.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศฉบับนี้ ใช้บังคับกับกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง ผู้รับจ้างช่วง ผู้ให้บริการภายนอก และบุคคลอื่นใดที่มีหน้าที่หรือเกี่ยวข้องกับการเข้าถึง การจัดการ หรือการใช้สารสนเทศและระบบเทคโนโลยีสารสนเทศของบริษัทฯ

2.2 บรรดานโยบาย ข้อกำหนด มติคณะกรรมการ ระเบียบ หรือคำสั่งอื่นใดของบริษัทฯ ที่มีข้อความขัดหรือแย้งกับนโยบายฉบับนี้ ให้ใช้นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศฉบับนี้เป็นหลัก

2.3 ให้ผู้บริหารหน่วยงานสารสนเทศ (IT Department Head) หรือผู้ที่ได้รับมอบหมาย เป็นผู้รักษาการตามนโยบายนี้ และมีหน้าที่เผยแพร่ สื่อสาร กำกับ ตลอดจนประสานงานกับหน่วยงานต่าง ๆ ภายในบริษัทฯ เพื่อให้มั่นใจว่าการปฏิบัติเป็นไปตามแนวทางและมาตรการที่กำหนด

2.4 ในกรณีที่ผู้มีอำนาจหรือผู้รับผิดชอบตามข้อกำหนดของนโยบายนี้ไม่สามารถปฏิบัติหน้าที่ได้ ให้หัวหน้างานของบุคคลดังกล่าวมีอำนาจอนุมัติให้บุคคลอื่นปฏิบัติหน้าที่แทนได้ตามความเหมาะสม ทั้งนี้ ต้องไม่กระทบต่อการบังคับใช้นโยบายและความมั่นคงปลอดภัยของสารสนเทศ

ส่วนที่ 3 บทกำหนดโทษ

3. บทกำหนดโทษ

การกระทำใด ๆ ที่ฝ่าฝืน หรือไม่เป็นไปตามนโยบายนี้ ให้ถือเป็นการกระทำที่ฝ่าฝืนต่อระเบียบวินัย และข้อบังคับเกี่ยวกับการทำงานของบริษัทฯ และมีความผิดหรือได้รับโทษตามที่บริษัทฯ ได้กำหนดไว้

หมวดที่ 2 การจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

ส่วนที่ 1 โครงสร้างทางด้านความมั่นคงปลอดภัยของบริษัทฯ

4. มาตรการของบริษัทฯ (Organizational Controls)

4.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศฉบับนี้ จัดทำเป็นลายลักษณ์อักษรโดยกำหนดจุดประสงค์ ขอบเขต และแนวทางดำเนินการอย่างชัดเจน ได้รับการอนุมัติจากคณะกรรมการ

บริษัท และประกาศใช้ให้ถือปฏิบัติทั่วทั้งบริษัทฯ ทั้งนี้ บริษัทฯ จะมีการติดตาม ตรวจสอบ และประเมินผลการปฏิบัติตามนโยบายอย่างต่อเนื่อง

4.2 บริษัทฯ จัดให้มีการแบ่งแยกหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน ตามบทบาทของผู้บริหาร พนักงาน และหน่วยงานที่เกี่ยวข้อง เพื่อให้มั่นใจว่าการดำเนินงานด้านความมั่นคงปลอดภัยเป็นไปอย่างมีประสิทธิภาพและสามารถตรวจสอบได้

4.3 บริษัทฯ บริหารจัดการและกำกับการติดต่อสื่อสาร แลกเปลี่ยน หรือส่งต่อข้อมูลกับหน่วยงานภายนอก คู่ค้า ผู้ให้บริการ หรือบุคคลที่สามที่มีความสำคัญต่อการดำเนินธุรกิจ โดยต้องอยู่ภายใต้ข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Agreement) และการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย เพื่อให้การส่งต่อข้อมูลเป็นไปอย่างถูกต้อง ปลอดภัย และเป็นประโยชน์ต่อบริษัทฯ

4.4 บริษัทฯ จัดทำบัญชีทรัพย์สินสารสนเทศ (Information Asset Register) และกำหนดหลักเกณฑ์วิธีการใช้งาน การตรวจสอบ การติดตาม และการคืนทรัพย์สินสารสนเทศ เพื่อให้มั่นใจว่าทรัพย์สินสารสนเทศของบริษัทฯ มีความครบถ้วน ถูกต้อง เป็นปัจจุบัน และได้รับการคุ้มครองตามระดับความสำคัญของข้อมูล

4.5 บริษัทฯ กำหนดนโยบายและมาตรการควบคุมการเข้าถึงข้อมูล (Access Control) ครอบคลุมถึงการกำหนดสิทธิผู้ใช้งาน การพิสูจน์ตัวตน (Authentication) การบันทึกการใช้งาน และการทบทวนสิทธิอย่างสม่ำเสมอ เพื่อป้องกันการเข้าถึง การใช้ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

4.6 บริษัทฯ มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงการคุ้มครองทรัพย์สินทางปัญญาและข้อมูลลับทางการค้า เพื่อป้องกันการละเมิดสิทธิหรือการนำข้อมูลไปใช้ในทางที่ไม่เหมาะสม

4.7 บริษัทฯ กำหนดหลักเกณฑ์และมาตรการในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลที่เกี่ยวข้องกับการว่าจ้างผู้ให้บริการภายนอก การจ้างช่วง (Subcontracting) และการใช้บริการระบบคลาวด์ (Cloud Service) โดยให้ผู้ให้บริการต้องปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ และอยู่ภายใต้สัญญาหรือข้อตกลงที่กำหนดเงื่อนไขด้านความปลอดภัยอย่างชัดเจน

4.8 บริษัทฯ ดำเนินการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศทุกโครงการ ให้มีมาตรการควบคุมความมั่นคงปลอดภัยของข้อมูลตั้งแต่ขั้นตอนการวางแผน ออกแบบ พัฒนา ทดสอบ จนถึงการนำไปใช้งานจริง เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นในกระบวนการดำเนินงาน

4.9 บริษัทฯ จัดทำและบังคับใช้แผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เพื่อเตรียมความพร้อมในการตอบสนองและฟื้นฟูระบบกรณีเกิดเหตุไม่คาดคิด โดยมีการสื่อสารและฝึกซ้อมอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าบริษัทฯ สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง

5. มาตรการด้านบุคลากร (People Controls)

5.1 การคัดเลือกและตรวจสอบประวัติบุคลากร

บริษัทฯ ดำเนินการตรวจสอบประวัติ คุณสมบัติ และความเหมาะสมของบุคลากรที่เกี่ยวข้องกับการเข้าถึงหรือจัดการข้อมูลสารสนเทศให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และหลักจริยธรรมของบริษัทฯ ทั้งนี้ การตรวจสอบดังกล่าวรวมถึงผู้รับจ้างช่วง หรือผู้ให้บริการภายนอกที่มีสิทธิเข้าถึงข้อมูลสำคัญของบริษัทฯ เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยและข้อมูลส่วนบุคคล

5.2 ข้อกำหนดในสัญญาจ้างงานและข้อตกลงการรักษาความลับ

บริษัทฯ กำหนดให้มีการระบุหน้าที่ ความรับผิดชอบ และข้อผูกพันด้านความมั่นคงปลอดภัยสารสนเทศไว้ในสัญญาจ้างงานหรือข้อตกลงการจ้าง รวมถึงเงื่อนไขการรักษาความลับ (Non-Disclosure Agreement: NDA) ทั้งในระหว่างการจ้างงานและภายหลังพ้นสภาพการจ้างงาน โดยผู้ใดฝ่าฝืนหรือละเลยถือว่ามีความผิดตามระเบียบวินัยของบริษัทฯ และอาจถูกดำเนินการทางกฎหมายตามความร้ายแรงของการกระทำ

5.3 การสร้างความตระหนักรู้และฝึกอบรม

บริษัทฯ จัดให้มีการสื่อสาร ให้ความรู้ และอบรมด้านความมั่นคงปลอดภัยสารสนเทศแก่พนักงานทุกระดับอย่างต่อเนื่อง เพื่อสร้างความตระหนักรู้ ความเข้าใจ และความรับผิดชอบในการปฏิบัติตามนโยบายและมาตรการด้านความมั่นคงปลอดภัย รวมถึงให้หน่วยงานภายนอกที่เกี่ยวข้อง เช่น คู่ค้าหรือผู้ให้บริการ ได้รับทราบข้อกำหนดและแนวปฏิบัติที่เกี่ยวข้อง

5.4 การบริหารความมั่นคงปลอดภัยในการปฏิบัติงานจากระยะไกล (Remote Work Security)

บริษัทฯ กำหนดมาตรการควบคุมและแนวทางปฏิบัติสำหรับการทำงานจากระยะไกล เพื่อป้องกันการเข้าถึง การประมวลผล หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต เช่น การใช้เครือข่ายที่มีการเข้ารหัส (VPN) การควบคุมการเข้าถึงระบบผ่านอุปกรณ์ที่ได้รับอนุญาตเท่านั้น และการเก็บรักษาข้อมูลในอุปกรณ์อย่างปลอดภัย ทั้งนี้ เพื่อให้การทำงานจากระยะไกลเป็นไปตามหลักการรักษา

ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล

5.5 การออกจากงานและการเพิกถอนสิทธิการเข้าถึง

เมื่อพนักงานหรือผู้ให้บริการพ้นสภาพการจ้างงาน บริษัทฯ จะดำเนินการเพิกถอนสิทธิการเข้าถึงระบบสารสนเทศและข้อมูลทั้งหมดโดยทันที รวมถึงจัดการคืนทรัพย์สินและข้อมูลของบริษัทฯ ตามขั้นตอนที่กำหนด เพื่อป้องกันการรั่วไหลของข้อมูลหรือการเข้าถึงโดยไม่ได้รับอนุญาต

6. มาตรการทางกายภาพ (Physical Controls)

6.1 การกำหนดพื้นที่ปลอดภัย (Secure Area)

บริษัทฯ กำหนดขอบเขตพื้นที่ที่มีการจัดเก็บ ประมวลผล หรือเข้าถึงข้อมูลสารสนเทศและทรัพย์สินที่เกี่ยวข้อง เพื่อให้สามารถควบคุมและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ทั้งนี้ ต้องมีระบบรักษาความปลอดภัยทางกายภาพ เช่น การใช้บัตรผ่าน (Access Card), กล้องวงจรปิด (CCTV), ระบบควบคุมประตูอัตโนมัติ หรือเจ้าหน้าที่รักษาความปลอดภัย เพื่อเฝ้าระวังและควบคุมการเข้าออกพื้นที่ที่ต้องการการคุ้มครองเป็นพิเศษ

6.2 การรักษาความมั่นคงปลอดภัยของสถานที่ทำงานและอุปกรณ์

บริษัทฯ จัดให้มีมาตรการรักษาความปลอดภัยของสำนักงาน ห้องปฏิบัติงาน ศูนย์ข้อมูล (Data Center) และอุปกรณ์สารสนเทศทุกประเภท เพื่อป้องกันการเข้าถึง การขโมย การสูญหาย หรือการทำลายข้อมูลโดยไม่ได้รับอนุญาต โดยจะต้องมีการตรวจสอบระบบรักษาความปลอดภัยทางกายภาพอย่างสม่ำเสมอ

6.3 การเฝ้าระวังเหตุการณ์และแผนความต่อเนื่องทางธุรกิจ (Business Continuity and Recovery Planning)

บริษัทฯ บริหารจัดการและเฝ้าระวังภัยคุกคามทางกายภาพหรือภัยพิบัติที่อาจกระทบต่อระบบสารสนเทศ เช่น ไฟไหม้ น้ำท่วม หรือเหตุขัดข้องทางเทคนิค โดยจัดทำ แผนความต่อเนื่องทางธุรกิจ (BCP) และ แผนฟื้นฟูระบบในภาวะฉุกเฉิน (Disaster Recovery Plan: DRP) เพื่อให้มั่นใจว่าสามารถกู้คืนระบบและดำเนินธุรกิจได้อย่างต่อเนื่อง

6.4 การใช้และการคุ้มครองทรัพย์สินสารสนเทศ (Asset Protection)

บริษัทฯ กำหนดแนวทางการใช้ทรัพย์สินสารสนเทศทั้งภายในและภายนอกบริษัทฯ ให้เป็นไปอย่างปลอดภัย เช่น การยืมอุปกรณ์ การเคลื่อนย้าย การนำออกนอกสถานที่ หรือการนำกลับมาใช้ซ้ำ โดยต้องผ่านการอนุมัติจากหน่วยงานที่เกี่ยวข้องและมีการบันทึกตรวจสอบทุกครั้ง

6.5 การป้องกันความเสียหายของระบบและอุปกรณ์สนับสนุน (Infrastructure Protection)

อุปกรณ์สารสนเทศทุกประเภทต้องได้รับการป้องกันจากการล้มเหลวของระบบไฟฟ้า ความร้อนสูงเกินไป หรือเหตุขัดข้องของระบบสนับสนุน เช่น ระบบไฟฟ้าสำรอง (UPS) ระบบควบคุมอุณหภูมิ (Cooling System) และระบบสายสัญญาณ ต้องได้รับการติดตั้งและบำรุงรักษาตามมาตรฐาน เพื่อป้องกันการรบกวน การแทรกแซงสัญญาณ หรือการเสียหายที่อาจกระทบต่อความต่อเนื่องของการดำเนินงาน

6.6 การบริหารจัดการสื่อบันทึกข้อมูล (Media Handling)

บริษัทฯ จัดให้มีมาตรการในการจัดเก็บ เคลื่อนย้าย และทำลายสื่อบันทึกข้อมูลให้เป็นไปตามระดับความลับของข้อมูล (Data Classification) รวมถึงจัดการซอฟต์แวร์และข้อมูลสำคัญของบริษัทฯ อย่างเหมาะสม เพื่อป้องกันการรั่วไหลหรือการนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต

6.7 การบำรุงรักษาอุปกรณ์สารสนเทศและการสื่อสารภายในบริษัทฯ

บริษัทฯ จัดให้มีแผนการบำรุงรักษาอุปกรณ์สารสนเทศอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าอุปกรณ์พร้อมใช้งานและมีประสิทธิภาพสูงสุด ทั้งนี้ จะต้องมีการแจ้งเวียนให้พนักงานทุกระดับทราบแนวทางการดูแล การบำรุงรักษา และข้อควรระวังในการใช้อุปกรณ์สารสนเทศตามที่บริษัทฯ กำหนด

ส่วนที่ 2 การบริหารจัดการเทคโนโลยีสารสนเทศ

7. มาตรการทางเทคโนโลยี (Technological Controls)

7.1 การบริหารจัดการข้อมูลและการเข้ารหัสข้อมูล (Data Management & Encryption)

บริษัทฯ กำหนดให้มีมาตรการในการบริหารจัดการข้อมูลสารสนเทศอย่างเป็นระบบ รวมถึงการเข้ารหัสข้อมูลสำคัญที่จัดเก็บไว้ในอุปกรณ์ของผู้ใช้งาน ระบบสารสนเทศ หรือสื่อบันทึกข้อมูลอื่น ๆ เพื่อป้องกันการเข้าถึง การแก้ไข หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้ ต้องเป็นไปตามมาตรฐานด้านความปลอดภัยของข้อมูลและข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

บริษัท ดับบลิวพี เอ็นเนอร์ยี่ จำกัด (มหาชน)
WP ENERGY PUBLIC COMPANY LIMITED
1 Eastwater Building, 15/F Vipavadeerangsit Soi 5,
Vipavadeerangsit Rd, Jomphol, Jatujak, Bangkok 10900
Tel : 02 272 3322 E-mail : info@wp-energy.co.th
www.wp-energy.co.th

7.2 การสำรองและทดสอบข้อมูล (Backup & Recovery Testing)

บริษัทฯ จัดให้มีระบบสำรองข้อมูล (Data Backup) สำหรับข้อมูล ซอฟต์แวร์ และระบบงานที่สำคัญอย่างเพียงพอ พร้อมทั้งมีการทดสอบการกู้คืนข้อมูล (Recovery Test) อย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสามารถกู้คืนระบบและข้อมูลได้เมื่อเกิดเหตุฉุกเฉิน

7.3 การกำหนดมาตรฐานระบบเครือข่ายและการตั้งค่าความปลอดภัย (System Configuration & Hardening)

บริษัทฯ กำหนดและจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเครือข่าย การตั้งค่าระบบ และการปรับปรุงประสิทธิภาพการทำงานของระบบสารสนเทศให้เป็นไปตามมาตรฐานที่กำหนด พร้อมทั้งมีการทบทวนและตรวจสอบการตั้งค่าอย่างสม่ำเสมอ

7.4 การติดตั้งและบริหารจัดการซอฟต์แวร์ (Software Management)

การติดตั้งหรือปรับปรุงซอฟต์แวร์บนระบบเครือข่าย ต้องดำเนินการตามกระบวนการบริหารจัดการซอฟต์แวร์ของบริษัทฯ และได้รับอนุมัติจากหน่วยงานเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสี่ยงจากซอฟต์แวร์ที่ไม่ปลอดภัยหรือไม่มีใบอนุญาตถูกต้อง

7.5 การเฝ้าระวังและตรวจจับเหตุการณ์ (Monitoring & Detection)

บริษัทฯ จัดให้มีระบบตรวจสอบและเฝ้าระวังการทำงานของระบบเครือข่าย เซิร์ฟเวอร์ แอปพลิเคชั่น และอุปกรณ์ต่าง ๆ เพื่อค้นหาพฤติกรรมผิดปกติหรือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมประเมินและตอบสนองอย่างทันท่วงที

7.6 การป้องกันมัลแวร์และภัยคุกคามทางไซเบอร์ (Malware & Cyber Threat Protection)

บริษัทฯ จัดให้มีมาตรการในการป้องกัน ตรวจจับ และกำจัดโปรแกรมไม่พึงประสงค์ (Malware) การเข้าถึงเว็บไซต์ที่ไม่ปลอดภัย รวมถึงการบริหารจัดการช่องโหว่ทางเทคนิคของระบบสารสนเทศ เพื่อป้องกันการโจมตีทางไซเบอร์ และสร้างความเชื่อมั่นให้กับลูกค้าและคู่ค้า

7.7 การติดตั้งซอฟต์แวร์ในอุปกรณ์ผู้ใช้งาน (User Device Control)

การติดตั้งหรือปรับเปลี่ยนซอฟต์แวร์ในอุปกรณ์คอมพิวเตอร์ โทรศัพท์มือถือ หรือแท็บเล็ตของผู้ใช้งาน ต้องได้รับอนุมัติจากหน่วยงานเทคโนโลยีสารสนเทศเท่านั้น เพื่อป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ปลอดภัยหรือมีความเสี่ยงต่อข้อมูลของบริษัทฯ

บริษัท ดับบลิวพี เอ็นเนอร์ยี่ จำกัด (มหาชน)
WP ENERGY PUBLIC COMPANY LIMITED
1 Eastwater Building, 15/F Vipavadeerangsit Soi 5,
Vipavadeerangsit Rd, Jomphol, Jatujak, Bangkok 10900
Tel : 02 272 3322 E-mail : info@wp-energy.co.th
www.wp-energy.co.th

7.8 การควบคุมสิทธิการเข้าถึงระดับพิเศษ (Privileged Access Control)

บริษัทฯ กำหนดให้การใช้งานสิทธิระดับผู้ดูแลระบบหรือสิทธิพิเศษอื่น ๆ ต้องได้รับการอนุมัติและควบคุมอย่างเคร่งครัด รวมถึงมีการบันทึก ตรวจสอบ และทบทวนการใช้งานสิทธิเหล่านั้นอย่างต่อเนื่อง

7.9 การจัดการบันทึกข้อมูลการใช้งานระบบ (Log Management)

บริษัทฯ บันทึกและจัดเก็บข้อมูลกิจกรรมของผู้ใช้งาน ระบบ และอุปกรณ์ต่าง ๆ อย่างเหมาะสม เพื่อใช้ในการตรวจสอบย้อนหลังเมื่อเกิดเหตุการณ์ผิดปกติ โดยต้องมีการจัดเก็บและทบทวนข้อมูลดังกล่าวอย่างสม่ำเสมอ

7.10 การสำรองอุปกรณ์และระบบสนับสนุน (Hardware & Infrastructure Backup)

บริษัทฯ วางแผนและจัดเตรียมอุปกรณ์ประมวลผลข้อมูลและระบบสนับสนุนให้พร้อมใช้งานอยู่เสมอ เพื่อให้มั่นใจว่าการดำเนินธุรกิจไม่หยุดชะงักจากเหตุขัดข้องทางเทคนิค

7.11 มาตรฐานการพัฒนาซอฟต์แวร์ (Secure Software Development)

บริษัทฯ กำหนดแนวทางและมาตรฐานการพัฒนาซอฟต์แวร์ให้สอดคล้องกับหลัก Secure by Design และ Secure Coding Practice รวมถึงบริหารจัดการการเข้าถึงซอร์สโค้ด เครื่องมือ และไลบรารีต่าง ๆ อย่างปลอดภัย

7.12 การแยกสภาพแวดล้อมระบบ (Environment Segregation)

บริษัทฯ แยกสภาพแวดล้อมของระบบออกเป็นส่วนพัฒนา (Development) ทดสอบ (Testing) และใช้งานจริง (Production) อย่างชัดเจน เพื่อป้องกันการรั่วไหลของข้อมูลจากระบบจริงในระหว่างการพัฒนาและทดสอบ

7.13 การกำกับดูแลการพัฒนาโดยหน่วยงานภายนอก (Third-Party Development Control)

บริษัทฯ กำหนดให้มีการตรวจสอบ ควบคุม และติดตามกิจกรรมการพัฒนาระบบที่ว่าจ้างหน่วยงานภายนอกดำเนินการ เพื่อให้มั่นใจว่าการพัฒนาเป็นไปตามมาตรฐานความมั่นคงปลอดภัยของบริษัทฯ

7.14 การทดสอบระบบ (System Testing & Audit)

บริษัทฯ วางแผนการทดสอบระบบโดยผู้ตรวจประเมินภายในหรือภายนอก เพื่อประเมินประสิทธิภาพของระบบและระบุช่องโหว่ที่อาจก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูล

บริษัท ดับบลิวพี เอ็นเนอร์ยี่ จำกัด (มหาชน)
WP ENERGY PUBLIC COMPANY LIMITED
1 Eastwater Building, 15/F Vipavadeerangsit Soi 5,
Vipavadeerangsit Rd, Jomphol, Jatujak, Bangkok 10900
Tel : 02 272 3322 E-mail : info@wp-energy.co.th
www.wp-energy.co.th

7.15 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

บริษัทฯ กำหนดกระบวนการควบคุมและอนุมัติการเปลี่ยนแปลงใด ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ อุปกรณ์ หรือโครงสร้างพื้นฐาน เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และให้มั่นใจว่าการเปลี่ยนแปลงนั้นได้รับการทดสอบและบันทึกไว้อย่างถูกต้องครบถ้วน

หมวดที่ 3 การทบทวนนโยบาย

8. การทบทวนนโยบาย

กำหนดให้บริษัทฯ ทบทวนนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ให้เป็นปัจจุบันอย่างน้อย 2 ปีครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ ทั้งนี้ แผนกเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้อง ต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงต่อไป

นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศนี้ ผ่านการอนุมัติโดยคณะกรรมการบริษัท ครั้งที่ 13/2568 เมื่อวันที่ 23 ธันวาคม 2568 มีผลบังคับใช้ตั้งแต่วันที่ 23 ธันวาคม 2568

(ลงชื่อ).....

(นายจุลจิตต์ บุณยเกตุ)

ประธานกรรมการบริษัท