บริษัท พลังงานบริสุทธิ์ จำกัด (มหาชน)
Energy Absolute Public Company Limited
89 อาคารเอไอเอ แคปปิตอล เซ็นเตอร์ ชั้น16 ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
โทรศัพท์ 02 248 2488-92 ,02 002 3667-9 แฟกซ์ 02 248 2493 ทะเบียนเลขที่ 0107551000061

ความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลสารสนเทศขององค์กร จัดเป็นสินทรัพย์ทางธุรกิจที่ต้องได้รับการดูแลรักษาอย่างมีประสิทธิภาพ การกำหนดกระบวนการเข้าถึง การใช้งาน และการป้องกันกำหนดมาตรฐานความปลอดภัยต่อข้อมูล และระบบสารสนเทศภายในขององค์กรจึงมีความสำคัญอย่างยิ่ง เพื่อทำให้องค์กรปราศจากความเสี่ยง และป้องกันความเสียหายที่จะมีผลต่อความปลอดภัยของข้อมูล รวมถึงระบบสารสนเทศขององค์กร

โดยกลุ่มธุรกิจพลังงานบริสุทธิ์เล็งเห็นถึงความสำคัญในการปกป้องข้อมูล และระบบสารสนเทศและส่งเสริมให้พนักงานทุกคนในองค์กรมีความรู้ความเข้าใจ และมีส่วนร่วมในการปกป้องข้อมูลและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

แนวทางการบริหารจัดการ

กลุ่มธุรกิจพลังงานบริสุทธิ์ได้มีการกำหนดแนวทางการจัดการและบริหารความเสี่ยงในเรื่องความปลอดภัยของเทคโนโลยีสารสนเทศ รวมถึงความปลอดภัยด้านข้อมูลทางไซเบอร์ โดยนำ NIST Cybersecurity Framework ซึ่งเป็นมาตราฐานสากลมาประยุกต์ใช้งานโดยแบ่งออกเป็น 5 ขั้นตอนสำคัญคือ

1.การประเมิน (Identify) และเข้าใจสภาพแวดล้อม ทรัพย์สิน เพื่อบริหารความเสี่ยงของระบบ

2.การป้องกัน (Protect) วางมาตรฐานควบคุมเพื่อปกป้องระบบ และข้อมูล

3.การตรวจจับ (Detect) และเฝ้าระวังภัยคุกคามที่อาจจะเกิดขึ้น

4.การตอบสนอง (Response) เมื่อพบภัยคุกคาม เพื่อลดผลกระทบหรือจำกัดความเสียหาย

5.การกู้คืน (Recover) ระบบขึ้นมาให้บริการตามปกติได้อย่างรวดเร็ว

นโยบาย และกลยุทธ์ความปลอดภัยด้านเทคโนโลยีสารสนเทศ

กลุ่มธุรกิจพลังงานบริสุทธิ์ได้มีการกำหนดนโยบายในการจัดการความปลอดภัยด้านสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง รวมถึงสร้างความตระหนักรู้กับพนักงานเพื่อให้มีความรู้ความเข้าใจสามารถปฏิบัติตามนโยบาย ขั้นตอนการปฏิบัติงาน รวมถึงกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศอย่างถูกต้องและเหมาะสม

● **นโยบายการทำงานจากภายนอกสำนักงาน (Work from Anywhere)** บริษัทจัดให้มีช่องทางเข้าถึงระบบงานเพื่อให้พนักงานสามารถปฏิบัติงานได้อย่างต่อเนื่องจากทุกที่อย่างมีประสิทธิภาพ มุ่งเน้นความปลอดภัย การควบคุมและเฝ้าระวังในการเข้าใช้งาน พร้อมยกระดับความปลอดภัยไซเบอร์ในการใช้งานระบบ Microsoft Office 365 ครอบคลุมทั้งด้านการเข้าใช้งาน โดยปรับให้มีการพิสูจน์ตัวตนแบบ Multi-Factor Authentication (MFA) ในการเข้าใช้งานระบบ การกำหนดสิทธิการเข้าถึงข้อมูล

● **จัดฝึกอบรมและให้ความรู้แก่พนักงานทุกคนในเรื่องความปลอดภัยสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์** เพื่อป้องกันความเสี่ยงแก่องค์กร และพนักงานโดยให้พนักงานปฏิบัติตามข้อกำหนด ทั้งนี้หากไม่ปฏิบัติตาม จะมีการลงโทษทางวินัยตามที่บริษัทฯ กำหนด

● **จัดฝึกอบรมและให้ความรู้แก่พนักงานทุกคนในเรื่องการปกป้องข้อมูลส่วนบุคคล**ทั้งของพนักงานและผู้มีส่วนได้ส่วนเสียทุกฝ่ายขององค์กร ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยให้พนักงานปฏิบัติตามข้อกำหนด ทั้งนี้หากไม่ปฏิบัติตาม จะมีการลงโทษทางวินัยตามที่บริษัทฯ กำหนด

● **ตรวจสอบความเสี่ยงที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ** และความมั่นคงปลอดภัยทางไซเบอร์ในทุกระบบ พร้อมเพิ่มการป้องกัน

● บริษัทจะดำเนินมาตรการที่เข้มงวดในการรักษาความปลอดภัย ตลอดจนจะป้องกันมิให้มีการนำข้อมูลของท่านไปใช้ในวัตถุประสงค์อื่นใดนอกเหนือจากที่กำหนดไว้ใน นโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ โดยมิได้รับอนุญาตจากท่านก่อน

ผลการดำเนินงานในปี 2565

ร้อยละของพนักงานที่ได้รับการอบรมเรื่อง ความมั่นคปลอดภัยทางไซเบอร์และการปกป้องข้อมูลส่วนบุคคล

ปี 2565	100%
ปี 2564	100%
ปี 2563	100%

- จำนวนครั้งของการละเมิดความมั่นคงปลอดภัยทางไซเบอร์ ในปี 2565 = 0
- จำนวนครั้งที่ได้รับเรื่องร้องเรียนการละเมิดข้อมูลส่วนบุคคล ในปี 2565 = 0
- จำนวนครั้งในการนำข้อมูลของลูกค้าไปใช้ในวัตถุประสงค์อื่นใดนอกเหนือจากที่ได้รับการยินยอม ในปี 2565 = 0
- ผ่านการทดสอบแผนบริหารความต่อเนื่องทางธุรกิจขององค์กร (Business Continuity Plan)
- เพิ่มประสิทธิภาพในการทำงาน การสื่อสาร และยกระดับความปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยการนำระบบ Cloud Collaboration Platform (MS Office 365) มาใช้งาน
- ดำเนินการปรับปรุงระบบ Data Center ของกลุ่มธุรกิจโดยให้เป็นไปตามมาตราฐาน ISO27001 และ ISO27017
- ดำเนินการปรับปรุงด้านความปลอดภัยด้วยแนวทาง Zero Trust เพื่อยกระดับมาตรฐานด้านความปลอดภัย จัดการความเสี่ยงและช่องโหว่ของระบบ

เป้าหมาย ปี 2566

- ปรับปรุงแผนทดสอบ การโจมตีทางไซเบอร์และภัยคุกคาม เพื่อวัดความ ตระหนักรู้ภายในองค์กรและเป็นการเตรียมพร้อมให้หน่วยงานที่ เกี่ยวข้องสามารถรับมือได้หากเกิดเหตุภัยคุกคาม