

กฎบัตรคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1. วัตถุประสงค์

บริษัท แอดเทค ฮับ จำกัด (มหาชน) และบริษัทย่อย (“กลุ่มบริษัท”) ได้จัดให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่ออำนวยความสะดวก เพิ่มประสิทธิภาพ และให้ประสิทธิผลต่อการทำงานทั้งระบบ ทั้งนี้ เพื่อให้การให้บริการและการให้บริการสามารถดำเนินการใช้งานร่วมกันได้อย่างเหมาะสมสอดคล้องกับนโยบายทางธุรกิจ มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายอื่นที่เกี่ยวข้อง และป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ทั้งจากผู้ใช้งานและภัยคุกคามต่าง ๆ ซึ่งอาจส่งผลกระทบต่อระบบธุรกิจของกลุ่มบริษัทให้ได้รับความเสียหายได้ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทคงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ รวมถึงผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ

2. องค์ประกอบและคุณสมบัติของคณะกรรมการ

1. คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจะต้องได้รับการแต่งตั้งโดยคณะกรรมการบริษัท
2. คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอาจประกอบด้วยกรรมการบริษัทที่เป็นผู้บริหาร (Executive Director) ผู้บริหาร ผู้จัดการฝ่าย หรือบุคคลอื่นใดที่มีความเหมาะสมตามที่บริษัทกำหนด
3. คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศมีวาระการดำรงตำแหน่งคราวละ 3 ปี และให้เป็นไปตามวาระการดำรงตำแหน่งกรรมการบริษัท (กรณีคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศดำรงตำแหน่งเป็นกรรมการบริษัทด้วย) ทั้งนี้ คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งจากคณะกรรมการบริษัทอีกได้
4. กรณีที่ตำแหน่งสมาชิกคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศว่างลงเพราะเหตุอื่น นอกจากถึงคราวออกตามวาระตามข้อ 3. ได้แก่ การพ้นสภาพการเป็นกรรมการหรือพนักงานบริษัท การลาออก หรือการถูกถอดถอนโดยคณะกรรมการบริษัท ให้คณะกรรมการบริษัทแต่งตั้งบุคคลที่มีคุณสมบัติครบถ้วนเป็นสมาชิกคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศมีจำนวนตามที่คณะกรรมการบริษัทได้เห็นควร โดยบุคคลที่ได้รับแต่งตั้งเป็นสมาชิกคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแทนสมาชิกซึ่งพ้นจากตำแหน่งไป จะอยู่ในตำแหน่งได้เพียงเท่าวาระที่ยังเหลืออยู่ของสมาชิกคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศซึ่งตนเองเข้ามาแทน

5. คณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจะเลือกคณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศคนหนึ่งเป็นประธานคณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

3. ขอบเขต อำนาจ หน้าที่ของคณะทำงาน

3.1 ตัวแทนฝ่ายบริหารระบบการจัดการความปลอดภัยข้อมูล (ISMR)

- นำเสนอขอบเขตและขอบข่ายการนำระบบการจัดการความปลอดภัยข้อมูล
- ทบทวนและกำหนดหน้าที่ความรับผิดชอบให้กับคณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
- จัดให้มีการทบทวนบริบทและความเสี่ยงของบริษัทด้านความปลอดภัยข้อมูล
- จัดให้มีการทบทวนการระบุปัญหาและประเมินความเสี่ยง และหาโอกาสในการปรับปรุงด้านความปลอดภัยข้อมูล
- จัดทำและนำเสนอการทบทวนนโยบายระบบการจัดการความปลอดภัยข้อมูลที่นำมาประยุกต์ใช้
- จัดทำและนำเสนอวัตถุประสงค์ เป้าหมาย และแผนการดำเนินงานระบบการจัดการความปลอดภัยข้อมูล
- จัดให้มีการตรวจติดตามภายในระบบการจัดการความปลอดภัยข้อมูล
- จัดให้มีการประชุมทบทวนระบบการจัดการความปลอดภัยข้อมูล
- จัดให้มีการเฝ้าติดตามและตรวจวัดในระบบการจัดการความปลอดภัยข้อมูล
- ติดตามประสิทธิผลการควบคุมการปฏิบัติในเรื่องต่าง ๆ ด้านความปลอดภัยข้อมูล

3.2 เจ้าหน้าที่ควบคุมเอกสาร (Document Controller)

- ควบคุมเอกสารในระบบความปลอดภัยข้อมูลสารสนเทศให้เป็นไปตามขั้นตอนปฏิบัติ เรื่อง การควบคุมเอกสาร
- ควบคุมบันทึกในระบบความปลอดภัยข้อมูลสารสนเทศให้เป็นไปตามขั้นตอนปฏิบัติ เรื่อง การควบคุมบันทึก
- ติดตามและปรับรายชื่อเอกสารต่าง ๆ ให้เป็นปัจจุบัน

3.3 เจ้าหน้าที่ประเมินความเสี่ยงด้านความปลอดภัยข้อมูล

- ระบุงานต่าง ๆ ของฝ่ายเพื่อนำมาระบุบริบทของหน่วยงานและประเมินความเสี่ยงเพื่อนำมาตรการด้านต่าง ๆ มาควบคุม
- จัดทำเอกสารข้อมูลการระบุบริบทของหน่วยงานและประเมินความเสี่ยง รวมถึงทำการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีกิจกรรมต่าง ๆ เปลี่ยนแปลง
- กำหนดแผนการดำเนินงานเพื่อแก้ไขความเสี่ยงหรือโอกาสในการปรับปรุงที่มีนัยสำคัญ
- สื่อสารผลการประเมินความเสี่ยง รวมถึงมาตรการควบคุมต่าง ๆ ให้กับพนักงานในฝ่ายได้รับทราบและเกิดความตระหนักด้านความปลอดภัยข้อมูล

3.4 เจ้าหน้าที่ด้านกฎหมาย

- ระนุกฎหมายหรือข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจ ระบบการจัดการความปลอดภัยข้อมูลที่เกี่ยวข้องกับกิจกรรม ผลิตภัณฑ์ และบริการต่าง ๆ ขององค์กร
- ติดตามการเปลี่ยนแปลงกฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจ ระบบการจัดการความปลอดภัยข้อมูลที่เกี่ยวข้องกับกิจกรรม ผลิตภัณฑ์ และบริการต่าง ๆ ขององค์กร
- ประเมินความสอดคล้องของกฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจ ระบบการจัดการความปลอดภัยข้อมูลที่เกี่ยวข้องกับกิจกรรม ผลิตภัณฑ์ และบริการต่าง ๆ ขององค์กร
- สื่อสารกฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจ ระบบการจัดการความปลอดภัยข้อมูลที่เกี่ยวข้องกับกิจกรรม ผลิตภัณฑ์ และบริการต่าง ๆ ขององค์กรให้กับผู้มีส่วนเกี่ยวข้องรับทราบและนำไปปฏิบัติ

3.5 เจ้าหน้าที่ด้านสื่อสารและประชาสัมพันธ์

- กำหนดหัวข้อที่จะประชาสัมพันธ์ในระบบการจัดการความปลอดภัยข้อมูล เพื่อให้พนักงานมีความตระหนักในระบบการจัดการความปลอดภัยข้อมูลที่บริษัทนำมาประยุกต์ใช้
- ดำเนินการประชาสัมพันธ์หัวข้อระบบการจัดการความปลอดภัยข้อมูลผ่านช่องทางต่าง ๆ ให้ตรงกับกลุ่มเป้าหมายและเกิดประสิทธิผล
- ประเมินประสิทธิผลของการสื่อสารและประชาสัมพันธ์เป็นระยะ ๆ
- รับและติดตามข้อร้องเรียนระบบการจัดการความปลอดภัยข้อมูล

3.6 เจ้าหน้าที่ตรวจประเมินภายในระบบการจัดการความปลอดภัยข้อมูล

- กำหนดโปรแกรมการตรวจติดตามภายในตามระยะเวลาที่ได้รับมอบหมายจากตัวแทนฝ่ายบริหารระบบการจัดการความปลอดภัยข้อมูลให้ครอบคลุมทุกหน่วยงานและพื้นที่
- เตรียมความพร้อมก่อนการตรวจติดตามภายในระบบการจัดการความปลอดภัยข้อมูล
- ดำเนินการตรวจติดตามภายในระบบการจัดการความปลอดภัยข้อมูลและรายงานผลการตรวจติดตามภายในให้ตัวแทนฝ่ายบริหารระบบการจัดการความปลอดภัยข้อมูลตามระยะเวลาที่กำหนด
- ติดตามการแก้ไขปัญหาที่เกิดขึ้นจากการตรวจติดตามภายในระบบการจัดการความปลอดภัยข้อมูลและรายงานผลให้ตัวแทนฝ่ายบริหารระบบการจัดการความปลอดภัยข้อมูลตามระยะเวลาที่กำหนด

3.7 เจ้าหน้าที่ด้านคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer, DPO)

- ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกค้าหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (รวมทั้งที่มีการแก้ไขเพิ่มเติม) ("PDPA")

- ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตาม PDPA
- ประสานงานและให้ความร่วมมือกับคณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตาม PDPA
- รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตาม PDPA

4. ความรับผิดชอบ

คณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศมีความรับผิดชอบต่อคณะกรรมการบริษัทโดยตรงตามหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย

และกำหนดให้ประธานเจ้าหน้าที่บริหาร (CEO) สนับสนุนการดำเนินงานของคณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ดังนี้

- ทบทวนและอนุมัติขอบเขตและขอบข่ายการนำระบบความปลอดภัยข้อมูลสารสนเทศมาประยุกต์ใช้อย่างน้อยปีละ 1 ครั้ง
- ทบทวนและอนุมัตินโยบาย วัตถุประสงค์ เป้าหมายของระบบความปลอดภัยข้อมูลสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
- เข้าร่วมการทบทวนการนำระบบความปลอดภัยข้อมูลสารสนเทศมาประยุกต์ใช้ตามระยะเวลาที่กำหนด
- ให้การสนับสนุนทรัพยากรต่าง ๆ ในการนำระบบความปลอดภัยข้อมูลสารสนเทศมาประยุกต์ใช้ และเกิดการพัฒนาอย่างต่อเนื่อง
- สนับสนุนและส่งเสริมให้ผู้บริหารในแต่ละหน่วยงานมีส่วนร่วมในการนำระบบความปลอดภัยข้อมูลสารสนเทศมาประยุกต์ใช้ในงานที่รับผิดชอบ

5. การประชุม

1. จัดให้มีการประชุมอย่างน้อยปีละ 1 ครั้ง โดยอาจเชิญฝ่ายจัดการ ผู้บริหาร หรือพนักงานของบริษัทที่เกี่ยวข้อง หรือผู้ที่เห็นสมควรมาร่วมประชุมให้ความเห็นหรือส่งเอกสารข้อมูลตามที่เห็นว่าเกี่ยวข้องหรือจำเป็น
2. ในการประชุมคณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศทุกครั้ง องค์กรประชุมต้องประกอบด้วยสมาชิกคณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นจำนวนไม่น้อยกว่ากึ่งหนึ่งของจำนวนสมาชิกทั้งหมดที่มีอยู่ในตำแหน่งขณะนั้น จึงจะถือว่าครบองค์ประชุม
3. สมาชิกคณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่มีส่วนได้เสียในเรื่องที่พิจารณาเรื่องใด มิให้ออกเสียงลงคะแนนในเรื่องนั้น ๆ
4. ในการออกเสียงลงมติ ให้สมาชิกคณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศมีสิทธิออกเสียงคนละ 1 เสียง และในการวินิจฉัยชี้ขาดให้ถือคะแนนเสียงข้างมากของจำนวนสมาชิกคณะทำงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เข้าร่วมประชุม ในกรณีที่การลงมติ

มีคะแนนเสียงเท่ากัน ให้ประธานคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศมีสิทธิออกเสียงอีกหนึ่งเสียงเพื่อเป็นการชี้ขาด

6. การรายงาน

รายงานผลการปฏิบัติงานของคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้คณะกรรมการบริษัทรับทราบ และจัดทำรายงานของคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเพื่อเปิดเผยไว้ในรายงานประจำปีของบริษัท และลงนามโดยประธานคณะกรรมการด้านรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

7. การทบทวนและปรับปรุงกฎบัตร

คณะกรรมการด้านรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจะทบทวนกฎบัตรนี้ทุกปี และจะเสนอแนะการแก้ไขเปลี่ยนแปลงตามความเห็นสมควร เพื่อให้คณะกรรมการบริษัทพิจารณาอนุมัติ

กฎบัตรคณะกรรมการด้านรักษาความมั่นคงปลอดภัยของระบบสารสนเทศนี้ ให้มีผลใช้บังคับตั้งแต่วันที่ 10 พฤษภาคม 2567 เป็นต้นไป



นายจิรพันธ์ สิ้นสุนาวา

ประธานกรรมการ

บริษัท แอดเทค ฮับ จำกัด (มหาชน)