นโยบายเทคโนโลยีสารสนเทศ

(Information Technology Policy)

สารบัญ

บทนำ

บริษัท เจเอเอส แอสเซ็ท จำกัด บริษัทร่วมและบริษัทย่อย ตระหนักถึงความสำคัญของเทคโนโลยีสารสนเทศใน (มหาชน) กระบวนการดำเนินธุรกิจและการบริหารจัดการข้อมูลที่มีประสิทธิภาพ เพื่อสนับสนุนการดำเนินงานอย่างต่อเนื่อง ปลอดภัย และสอดคล้องกับหลักบรรษัทภิบาล บริษัทจึงกำหนดนโยบายเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อเป็นแนวทางสำหรับการดำเนินงานและบริหารจัดการระบบเทคโนโลยีสารสนเทศขององค์กรให้เป็นไปอย่างเหมาะสม โปร่งใส และมีปลอดภัย

หลักการและเหตุผล

บริษัทให้ความสำคัญกับการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือสำคัญในการดำเนินธุรกิจ การให้บริการ และการสื่อสารข้อมูลกับผู้มีส่วนได้เสียทุกภาคส่วน เพื่อให้เกิดประสิทธิภาพ ความถูกต้อง และความรวดเร็วในการทำงาน พร้อมทั้งป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ และการรั่วไหลของข้อมูลที่อาจส่งผลกระทบต่อบริษัทและผู้มีส่วนได้เสีย บริษัทจึงกำหนดนโยบายเทคโนโลยีสารสนเทศเพื่อใช้เป็นกรอบแนวทางในการดำเนินงานและกำกับดูแลให้เป็นไปตามมาตรฐานสากลและกฎหมายที่เกี่ยวข้อง

วัตถุประสงค์

1. เพื่อกำหนดแนวทางการบริหารจัดการระบบเทคโนโลยีสารสนเทศของบริษัทให้มีประสิทธิภาพ ปลอดภัย และสอดคล้องกับกฎหมายเกี่ยวข้อง
2. เพื่อสร้างความเข้าใจและตระหนักรู้แก่พนักงานในการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและมีความรับผิดชอบ
3. เพื่อป้องกันความเสี่ยงที่อาจเกิดจากการใช้เทคโนโลยีสารสนเทศ ทั้งในด้านการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล และภัยคุกคามทางไซเบอร์

ขอบเขตการบังคับใช้นโยบาย

นโยบายฉบับนี้มีผลบังคับใช้ครอบคลุมถึงกรรมการ ผู้บริหาร พนักงานทุกระดับ ของบริษัท เจเอเอส แอสเซ็ท จำกัด (มหาชน) ร่วมไปถึงคู่ค้าที่ดำเนินการทางธุรกิจร่วมกันกับบริษัท

คำนิยาม

เทคโนโลยีสารสนเทศ (Information Technology: IT)

หมายถึง ระบบ เครื่องมือ อุปกรณ์ หรือซอฟต์แวร์ที่ใช้ในการจัดเก็บ ประมวลผล ส่งต่อ หรือแลกเปลี่ยนข้อมูลภายในบริษัท

ข้อมูลส่วนบุคคล (Personal Data)

หมายถึง ข้อมูลใด ๆ ที่สามารถระบุตัวบุคคลได้ ไม่ว่าจะโดยทางตรงหรือทางอ้อม ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

มัลแวร์ (Malware)

หมายถึง โปรแกรมหรือซอฟต์แวร์ที่มีเจตนาทำลายหรือรบกวนการทำงานของระบบคอมพิวเตอร์ เช่น ไวรัส

ระบบสำรองข้อมูล (Backup System)

หมายถึง ระบบหรือกระบวนการจัดเก็บสำเนาของข้อมูลไว้ในพื้นที่ที่ปลอดภัย เพื่อใช้ในการกู้คืนข้อมูลในกรณีที่เกิดเหตุฉุกเฉิน

การกู้คืนข้อมูล (Data Recovery)

หมายถึง กระบวนการกู้คืนข้อมูลที่สูญหายหรือเสียหายให้สามารถใช้งานได้ตามปกติ

ภัยคุกคามทางไซเบอร์ (Cyber Threat)

หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่มีเจตนาหรืออาจส่งผลให้ระบบเทคโนโลยีสารสนเทศ ข้อมูล หรืออุปกรณ์ของบริษัท ได้รับความเสียหาย สูญหาย หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

ขอบเขตนโยบายเทคโนโลยีสารสนเทศ

1. การบริหารจัดการเทคโนโลยีสารสนเทศ

บริษัทจะจัดให้มีระบบบริหารจัดการเทคโนโลยีสารสนเทศที่มีมาตรฐานและประสิทธิภาพ เพื่อให้การดำเนินงานทางธุรกิจเป็นไปอย่างราบรื่น ปลอดภัย และลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยี

แนวทางปฏิบัติที่ดี

1. ฝ่ายเทคโนโลยีสารสนเทศควรจัดทำแผนบริหารความเสี่ยงและแผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ
2. ดำเนินการตรวจสอบและบำรุงรักษาระบบเทคโนโลยีสารสนเทศเป็นประจำ เพื่อป้องกันผลกระทบที่อาจสร้างความเสียหายต่อความต่อเนื่องในการดำเนินธุรกิจ
3. จัดให้มีการฝึกอบรมหรือให้ความรู้แก่พนักงานเกี่ยวกับการใช้เทคโนโลยีอย่างปลอดภัย โดยเฉพาะแผนกที่ต้องใช้เทคโนโลยีในการทำงานเป็นประจำ

2. การใช้งาน ดูแลรักษาอุปกรณ์และระบบสารสนเทศ

พนักงานทุกคนต้องใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศของบริษัทเพื่อประโยชน์ในการทำงานเท่านั้น และต้องดูแลรักษาอุปกรณ์ให้พร้อมใช้งานอยู่เสมอ ทั้งนี้ ห้ามกระทำการใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบ ข้อมูล หรืออุปกรณ์เทคโนโลยีของบริษัท

แนวทางปฏิบัติที่ดี

1. ใช้อุปกรณ์ของบริษัทด้วยความระมัดระวังและเพื่อวัตถุประสงค์ในการดำเนินงานของบริษัทเท่านั้น
2. หลีกเลี่ยงการติดตั้งโปรแกรมหรือแอปพลิเคชันที่ไม่ได้รับอนุญาต
3. ตรวจสอบอุปกรณ์และซอฟต์แวร์ให้อยู่ในสภาพพร้อมใช้งานเสมอ หากพบปัญหาควรรีบแจ้งฝ่ายเทคโนโลยีสารสนเทศเพื่อเข้าตรวจสอบทันที

3. ความมั่นคงปลอดภัยของข้อมูล

บริษัทจะดำเนินการจัดเก็บ ใช้และดูแลข้อมูลอย่างถูกต้อง ปลอดภัยและเป็นไปตามกฎหมายที่เกี่ยวข้อง โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

แนวทางปฏิบัติที่ดี

1. ส่วนงานซึ่งมีหน้าที่จัดเก็บหรือสามารถเข้าถึงข้อมูลที่มีความละเอียดอ่อน ต้องดำเนินการจัดเก็บและใช้ข้อมูลอย่างเป็นระบบ พร้อมทั้งกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสม
2. จำกัดการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต และอยู่ภายใต้การควบคุมของผู้บังคับบัญชาหรือผู้รับผิดชอบโดยตรง
3. ฝ่ายเทคโนโลยีสารสนเทศควรจัดให้มีการสื่อสารและให้ความรู้แก่พนักงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง ผ่านช่องทางที่พนักงานสามารถเข้าถึงได้ง่ายและศึกษาได้ตลอดเวลา

4. การควบคุมการเข้าถึงระบบสารสนเทศ

บริษัทจะกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศตามบทบาทหน้าที่ของแต่ละบุคคล เพื่อให้มั่นใจว่าการเข้าถึงข้อมูลเกิดขึ้นอย่างเหมาะสม ปลอดภัย และมีการตรวจสอบอย่างต่อเนื่อง

แนวทางปฏิบัติที่ดี

1. สำหรับฝ่ายงานที่จำเป็นต้องใช้ข้อมูลที่มีความละเอียดอ่อนในการดำเนินงาน ผู้บังคับบัญชาต้องกำหนดสิทธิ์การเข้าถึงข้อมูลตามตำแหน่งหน้าที่และความจำเป็นในการใช้งาน
2. พนักงานและผู้บริหารต้องตั้งค่ารหัสผ่านสำหรับการเข้าระบบและอุปกรณ์เทคโนโลยีของบริษัทให้มีความปลอดภัย และเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ
3. ฝ่ายทรัพยากรบุคคลต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศให้ดำเนินการยกเลิกสิทธิ์การเข้าถึงข้อมูลของพนักงานทันทีเมื่อพนักงานลาออกหรือมีการเปลี่ยนแปลงหน้าที่
4. ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีระบบบันทึกและตรวจสอบการเข้าถึงระบบสารสนเทศ เพื่อใช้ในการติดตามตรวจสอบ หรือดำเนินการทางเทคนิคเมื่อเกิดเหตุจำเป็น

5. การสำรองและกู้คืนข้อมูล

บริษัทจะดำเนินการสำรองข้อมูลที่สำคัญเป็นระยะ และจัดให้มีแผนการกู้คืนข้อมูลในกรณีเกิดเหตุฉุกเฉิน เพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง และลดความเสียหายที่อาจเกิดขึ้นจากการสูญหายของข้อมูล

แนวทางปฏิบัติที่ดี

1. ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอในระบบที่มีความปลอดภัย และจัดเก็บข้อมูลสำรองแยกจากระบบหลัก เพื่อป้องกันความเสียหายที่อาจเกิดจากเหตุขัดข้องของระบบหรือภัยคุกคามทางไซเบอร์
2. จัดทำและทดสอบแผนการกู้คืนข้อมูล (Data Recovery Plan) เป็นระยะ เพื่อให้มั่นใจว่าสามารถดำเนินการได้อย่างมีประสิทธิภาพเมื่อเกิดเหตุฉุกเฉิน
3. ตรวจสอบความสมบูรณ์ของข้อมูลสำรองอย่างต่อเนื่อง และปรับปรุงขั้นตอนให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอยู่เสมอ

6. การป้องกันภัยคุกคามทางไซเบอร์

ฝ่ายเทคโนโลยีสารสนเทศจะดำเนินการเฝ้าระวัง ป้องกัน และตอบสนองต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เพื่อรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและข้อมูลของบริษัท รวมถึงสร้างความตระหนักรู้แก่พนักงานในการระมัดระวังและป้องกันความเสี่ยงด้านความปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ

แนวทางปฏิบัติที่ดี

1. ฝ่ายเทคโนโลยีสารสนเทศต้องติดตั้งและอัปเดตโปรแกรมป้องกันไวรัส มัลแวร์ และระบบรักษาความปลอดภัยของเครือข่ายอย่างสม่ำเสมอ
2. พนักงานต้องหลีกเลี่ยงการเปิดไฟล์แนบหรือคลิกลิงก์จากแหล่งที่ไม่รู้จัก หรืออีเมลต้องสงสัยที่อาจมีมัลแวร์แฝง
3. ฝ่ายเทคโนโลยีสารสนเทศควรจัดให้มีระบบเฝ้าระวังและตรวจสอบเหตุผิดปกติของระบบ (Monitoring) เพื่อให้สามารถตอบสนองและแก้ไขปัญหาได้อย่างทันท่วงที
4. จัดให้มีการทดสอบและจำลองเหตุการณ์ภัยคุกคามทางไซเบอร์เป็นระยะ เพื่อประเมินความพร้อมและปรับปรุงมาตรการป้องกันให้มีประสิทธิภาพยิ่งขึ้น
5. ส่งเสริมให้พนักงานทุกคนมีความรู้ ความเข้าใจ และปฏิบัติตามหลักความปลอดภัยทางไซเบอร์ให้แก่ผู้บริหารและพนักงานอย่างสม่ำเสมอ

7. การใช้ระบบอินเทอร์เน็ตและอีเมลในองค์กร

พนักงานต้องใช้ระบบอินเทอร์เน็ต อีเมล และช่องทางการสื่อสารออนไลน์ของบริษัทเพื่อวัตถุประสงค์ในการทำงานเท่านั้น ห้ามใช้เพื่อกิจกรรมส่วนตัวหรือกิจกรรมอื่นใดที่อาจก่อให้เกิดความเสียหายต่อระบบ ความปลอดภัย หรือชื่อเสียงของบริษัท

แนวทางปฏิบัติที่ดี

1. พนักงานต้องใช้ระบบอินเทอร์เน็ตและอีเมลของบริษัทเพื่อการดำเนินงานที่เกี่ยวข้องกับธุรกิจของบริษัทเท่านั้น
2. ห้ามใช้ระบบอินเทอร์เน็ตหรืออีเมลของบริษัทในการเข้าถึงเว็บไซต์ เนื้อหา หรือสื่อที่ไม่เหมาะสม รวมถึงกิจกรรมที่อาจละเมิดกฎหมาย
3. ผู้บริหารและพนักงานควรตรวจสอบความถูกต้องของที่อยู่อีเมลผู้รับทุกครั้งก่อนส่งข้อมูล โดยเฉพาะเอกสารที่มีข้อมูลภายในหรือข้อมูลที่เป็นความลับของบริษัท
4. ผู้บริหารและพนักงานควรหลีกเลี่ยงการส่งต่อข้อมูล ข่าวสาร หรือเนื้อหาที่ไม่ได้รับการยืนยันจากแหล่งที่เชื่อถือได้
5. ผู้บริหารและพนักงานไม่ใช้บัญชีอีเมลของบริษัทในการสมัครสมาชิกเว็บไซต์ หรือบริการออนไลน์ส่วนบุคคลที่ไม่เกี่ยวข้องกับการทำงาน
6. หากพบการใช้งานระบบอินเทอร์เน็ตหรืออีเมลของบริษัทในลักษณะที่ผิดปกติ หรืออาจเสี่ยงต่อความปลอดภัยของข้อมูล ต้องรีบแจ้งฝ่ายเทคโนโลยีสารสนเทศเพื่อดำเนินการตรวจสอบทันที

8. การรายงานเหตุการณ์ด้านเทคโนโลยีสารสนเทศ

ในกรณีที่ผู้บริหารและพนักงานพบเหตุผิดปกติ ความเสียหาย หรือภัยคุกคามที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ให้รีบรายงานต่อผู้บังคับบัญชาหรือฝ่ายเทคโนโลยีสารสนเทศทันที เพื่อให้สามารถดำเนินการตรวจสอบ แก้ไข และป้องกันไม่ให้เกิดเหตุซ้ำในอนาคต

แนวทางปฏิบัติที่ดี

1. พนักงานทุกคน ทุกระดับควรรายงานเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่พบเห็น ซึ่งหมายรวมถึงการเข้าถึงข้อมูลโดยไม่ได้รับ อนุญาต การหยุดชะงักของระบบ การสูญหายของข้อมูล หรืออีเมลต้องสงสัย ไปยังฝ่ายเทคโนโลยีสารสนเทศโดยเร็วที่สุด
2. ในการรายงานเหตุการณ์ให้ระบุรายละเอียดที่เกี่ยวข้อง ได้แก่ วันเวลา ลักษณะของเหตุการณ์และข้อมูลประกอบอื่น ๆ ที่สำคัญ เพื่อช่วยในการตรวจสอบสาเหตุและจัดทำแนวทางแก้ไขอย่างเหมาะสม
3. ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการตรวจสอบ วิเคราะห์ และจัดทำรายงานผลการดำเนินการ รวมถึงแนวทางป้องกันเพื่อไม่ให้เกิดเหตุซ้ำ

4. พนักงานทุกคนต้องให้ความร่วมมือกับฝ่ายเทคโนโลยีสารสนเทศในการตรวจสอบเหตุการณ์ เพื่อให้สามารถดำเนินการแก้ไขได้อย่างรวดเร็วและมีประสิทธิภาพ
5. หากเหตุการณ์มีแนวโน้มส่งผลกระทบรุนแรง หรือเกี่ยวข้องกับข้อมูลส่วนบุคคล ฝ่ายเทคโนโลยีสารสนเทศต้องประสานงานกับผู้บริหารและหน่วยงานที่เกี่ยวข้อง เพื่อรายงานและดำเนินการตามขั้นตอนที่บริษัทกำหนด

การติดตามและการทบทวนนโยบาย

บริษัทได้กำหนดให้ฝ่ายที่เกี่ยวข้องดำเนินการติดตามการปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจว่านโยบายดังกล่าวยังคงมีความเหมาะสม ครอบคลุม และสอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี หรือโครงสร้างการดำเนินงานของบริษัท

ทั้งนี้ บริษัทจะทำการทบทวนนโยบายเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญด้านเทคโนโลยี โครงสร้างองค์กร หรือข้อกำหนดทางกฎหมาย เพื่อปรับปรุงให้สอดคล้องกับสถานการณ์และความจำเป็นขององค์กร

ประกาศให้มีผลบังคับใช้ตั้งแต่วันที่ 07 พฤศจิกายน 2568 เป็นต้นไป

.....

ผู้อนุมัตินโยบายสิทธิแรงงานสตรี

นายสุคนธ์ กาญจนหัตถกิจ

ประธานกรรมการบริษัท

ประวัติการแก้ไข

แก้ไขครั้งที่	ฝ่ายดำเนินการ	วันที่ทบทวน	วันที่บังคับใช้	รายละเอียดการแก้ไข
REV00	นักลงทุนสัมพันธ์	ณ การประชุม BOD ครั้งที่ 7/2568 วันที่ 07 พฤศจิกายน 2568	07 พฤศจิกายน 2568	จัดทำนโยบายครั้งแรก