นโยบายด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

บทนำ

บริษัท ไทยเบฟเวอเรจ จำกัด (มหาชน) และบริษัทย่อย (ซึ่งต่อไปนี้จะเรียกรวมกันว่า "**ไทยเบฟ**") ตระหนักถึงความสำคัญและคุณค่าของระบบสารสนเทศและทรัพยากรการประมวลผล ทั้งที่เป็นการประมวลผลโดยบุคคลและโดยระบบอัตโนมัติ เพื่อเป็นการให้ความสำคัญในเรื่องนี้ ไทยเบฟมุ่งมั่นที่จะสร้างความเชื่อมั่นในเรื่องของการรักษาความลับ ความถูกต้อง และความพร้อมของสารสนเทศและระบบสารสนเทศของไทยเบฟ โดยไทยเบฟพร้อมที่จะดำเนินการในสิ่งที่จำเป็นเพื่อให้มั่นใจว่าไทยเบฟมีการควบคุมที่เหมาะสมเพื่อให้การป้องกันเป็นไปในระดับที่เพียงพอ

ขอบเขตของนโยบาย

นโยบายด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ("**นโยบาย**") ซึ่งหมายรวมถึงการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ นำมาใช้กับกรรมการ ผู้บริหาร และพนักงานทุกคนของไทยเบฟ รวมถึงพนักงานสัญญาจ้างหรือพนักงานชั่วคราว ผู้รับเหมางาน และบุคคลอื่นใดที่ถูกว่าจ้างโดยไทยเบฟ

1. คำจำกัดความ

1.1 **ประธานเจ้าหน้าที่บริหารด้านสารสนเทศ** หมายถึง ผู้บริหารระดับสูงที่รับผิดชอบในการบริหารจัดการ การดูแลให้พร้อมใช้งาน และการใช้งาน สารสนเทศและเทคโนโลยีเกี่ยวกับคอมพิวเตอร์

1.2 **ผู้บริหารสูงสุดด้านความมั่นคงปลอดภัยสารสนเทศ** หมายถึง ผู้บริหารระดับสูงที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ภายในองค์กร

1.3 **ไอที** หมายถึง เทคโนโลยีสารสนเทศ

1.4 **ผู้จัดการไอที** หมายถึง ผู้จัดการไอทีที่รับผิดชอบงานด้านไอทีแต่ละฟังก์ชั่นหรือไอทีของแต่ละหน่วยงาน

1.5 **ผู้ดูแลระบบไอที** หมายถึง พนักงานไอทีและผู้ดูแลระบบที่ได้รับอนุญาตให้จัดการและดูแลระบบต่าง ๆ ขององค์กร

1.6 **ผู้ใช้งาน** หมายถึง กรรมการ ผู้บริหาร พนักงาน และพนักงานสัญญาจ้าง/พนักงานชั่วคราวของหน่วยงานภายในไทยเบฟ และบุคคลหรือนิติบุคคลอื่นใด ที่ใช้ทรัพยากรคอมพิวเตอร์และโครงสร้างพื้นฐานทางด้านไอทีของไทยเบฟ

2. นโยบาย

2.1 ไทยเบฟจะจัดทำหลักเกณฑ์ กฎระเบียบ มาตรฐานการปฏิบัติงาน กระบวนการปฏิบัติงาน และแนวทางในการปกป้องทรัพย์สินด้านไอที รวมถึงทรัพยากรต่าง ๆ ของไทยเบฟ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต

การถูกเปิดเผยไม่ว่าโดยเจตนาหรือไม่เจตนา และการถูกทำลาย เพื่อให้กิจกรรมทางธุรกิจขององค์กรดำเนินไปได้โดยไม่หยุดชะงัก

2.2 ไทยเบฟจะกำหนดแนวทางปฏิบัติที่ชัดเจน และจะแสดงให้เห็นถึงการให้การสนับสนุนและความมุ่งมั่นในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยการจัดทำและบังคับใช้ระเบียบว่าด้วยการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศกับทุกหน่วยงานทั่วทั้งองค์กร

2.3 ผู้บริหารของไทยเบฟจะจัดให้มีมาตรการควบคุม รวมถึง กฎระเบียบ มาตรฐานการปฏิบัติงาน กระบวนการปฏิบัติงาน โครงสร้างองค์กร และการทำงานของโปรแกรมคอมพิวเตอร์ที่เหมาะสมเพื่อให้เกิดความมั่นคงปลอดภัยของสารสนเทศ

3. บทบาทและความรับผิดชอบในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

3.1 **ผู้ดูแลระบบไอที** มีหน้าที่รับผิดชอบในการศึกษาทำความเข้าใจและบังคับใช้กฎระเบียบ มาตรฐานการทำงาน และกระบวนการปฏิบัติงานทางด้านไอที

3.2 **ผู้จัดการไอที** มีหน้าที่รับผิดชอบในการควบคุมดูแลให้ผู้ดูแลระบบไอทีตระหนักถึงความรับผิดชอบในงานรักษาความมั่นคงปลอดภัยด้านไอทีประจำวัน รวมถึง กฎระเบียบ มาตรฐานการทำงาน และกระบวนการปฏิบัติงานด้านไอทีในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

3.3 **ผู้บริหารสูงสุดด้านความมั่นคงปลอดภัยสารสนเทศ** มีหน้าที่รับผิดชอบในการปรับปรุงกฎระเบียบ มาตรฐานการทำงาน และกระบวนการปฏิบัติงานด้านไอทีให้สอดคล้องกับพัฒนาการและแนวปฏิบัติที่ดีล่าสุด

3.4 **ประธานเจ้าหน้าที่บริหารด้านสารสนเทศ** มีหน้าที่รับผิดชอบในการพิจารณาตรวจสอบและอนุมัติกฎระเบียบ มาตรฐานการทำงาน และกระบวนการปฏิบัติงานด้านไอที เพื่อให้มั่นใจว่ามีความเหมาะสมเพียงพอ และมีประสิทธิภาพอย่างต่อเนื่อง รวมถึงการกำกับดูแลและการบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศและการควบคุมการรักษาความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร

4. วิธีการในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

4.1 **ผู้ดูแลระบบไอที** จะต้องปฏิบัติตามกฎระเบียบที่ระบุไว้ในระเบียบว่าด้วยการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รวมถึง มาตรฐานการปฏิบัติงานและกระบวนการการปฏิบัติงาน เพื่อเป็นการป้องกันทรัพย์สินและทรัพยากรด้านไอทีของไทยเบฟจากการถูกโจรกรรม การสูญหายและการถูกนำไปใช้ในทางที่มิชอบ

4.2 **ผู้ใช้งาน** จะต้องปฏิบัติตามนโยบาย มาตรฐานการปฏิบัติงาน และกระบวนการปฏิบัติงานสำหรับผู้ใช้งานที่ระบุไว้ในระเบียบว่าด้วยการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เพื่อเป็นการป้องกันทรัพย์สินและทรัพยากรด้านไอทีของไทยเบฟจากการถูกโจรกรรม การสูญหาย และการถูกนำไปใช้ในทางที่มิชอบ

5. กระบวนการในการแจ้งการละเมิด

ผู้ที่มีข้อสงสัยหรือข้อกังวลเกี่ยวกับการละเมิดการรักษาความมั่นคงปลอดภัยของไอทีและหรือความเสียหายที่อาจจะเกิดขึ้น ควรแจ้งการละเมิดไปยังผู้บริหาร และ/หรือประธานเจ้าหน้าที่บริหารด้านสารสนเทศโดยตรง