นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลและไซเบอร์

บริษัท แพลน บี มีเดีย จำกัด (มหาชน) รวมถึงบริษัทย่อย บริษัทร่วม และบริษัทอื่นที่บริษัทมีอำนาจควบคุม (ต่อไปนี้เรียกว่า "บริษัท") ให้ความสำคัญต่อการพัฒนาเทคโนโลยีดิจิทัลและการใช้ข้อมูลในการดำเนินธุรกิจของบริษัท ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของข้อมูล รวมถึงการป้องกันภัยคุกคามทางไซเบอร์ นโยบายนี้จัดทำขึ้นเพื่อสร้างแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลและไซเบอร์ของบริษัท

ขอบเขตนโยบาย

นโยบายนี้ใช้กับการดำเนินธุรกิจของบริษัท

แนวปฏิบัติ

1. จัดให้มีมาตรการต่างๆ เพื่อให้มั่นใจว่าการรักษาความปลอดภัยของข้อมูลมีความเพียงพอและเหมาะสมสอดคล้องกับการดำเนินธุรกิจและระดับความสำคัญของข้อมูล รวมถึงปัจจัยภายในและภายนอกที่ส่งผลกระทบต่อความปลอดภัยของข้อมูลของบริษัท ให้ความสำคัญกับการรักษาความลับ ความพร้อมใช้งาน ความครบถ้วนและถูกต้องของข้อมูล เพื่อให้เป็นไปตามกฎหมาย กฎเกณฑ์ และข้อบังคับของบุคคลภายนอกที่เกี่ยวข้อง
2. กำหนดแนวปฏิบัติให้กรรมการ ผู้บริหาร และพนักงานทุกคนปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลและไซเบอร์ รักษาความลับของบริษัท ตามที่กำหนดไว้ในจรรยาบรรณทางธุรกิจของบริษัทอย่างเคร่งครัด ดังนี้

   2.1. ในระหว่างการจ้างงาน กรรมการ ผู้บริหาร และพนักงานทุกคน ต้องตระหนักถึงข้อมูลของบริษัทที่เรียกว่า "ความลับทางการค้า" ซึ่งหมายถึง ข้อมูลการค้าที่ยังไม่รู้จักกันโดยทั่วไปหรือยังเข้าถึงไม่ได้ในหมู่บุคคลซึ่งโดยปกติแล้วบุคคลที่เข้าถึงได้จะต้องเกี่ยวข้องกับข้อมูลดังกล่าว ข้อมูลที่เป็นประโยชน์ทางการค้าเนื่องจากเป็นความลับ และเป็นข้อมูลที่ผู้ควบคุมความลับทางการค้าใช้มาตรการที่เหมาะสมในการรักษาความลับ เพื่อให้ข้อมูลดังกล่าวสามารถระบุไว้ในสัญญาหรือข้อตกลงอื่นใดของบริษัท ตามที่ระบุไว้ในพระราชบัญญัติความลับทางการค้า พ.ศ. 2545 กรรมการ ผู้บริหาร และพนักงานทุกคน ตกลงที่จะรักษา "ความลับทางการค้า" ของบริษัทที่ได้ทราบหรือได้รับเพราะการทำงานในบริษัท และจะไม่ส่งต่อหรือคัดลอกไปยังบุคคลอื่นโดยไม่ได้รับอนุญาต รวมถึงการเปิดเผย และ/หรือ กระทำหรือไม่กระทำใดๆ ที่ทำให้เสียหายต่อชื่อเสียงหรือธุรกิจของบริษัท

   2.2. รักษาความลับของลูกค้า คู่ค้าทางธุรกิจ หรือบุคคลที่เกี่ยวข้องอื่นของบริษัท

   2.3. ไม่เปิดเผยความลับ เอกสาร หรือความลับทางการค้าใดๆ เป็นเวลา 1 ปี หลังจากพ้นจากตำแหน่งหน้าที่

2.4. กรรมการ ผู้บริหาร และพนักงานทุกคนจะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลและไซเบอร์ของบริษัทอย่างเคร่งครัด โดยไม่ละเมิดความเป็นส่วนตัวของผู้อื่น ไม่ใช้ข้อมูลที่เป็นความลับที่ไม่ได้รับอนุญาต รวมถึงการเข้าถึงข้อมูลและไฟล์ของผู้ใช้งานรายอื่นโดยไม่ได้รับอนุญาต ตามกฎและข้อบังคับของบริษัทเกี่ยวกับการใช้อุปกรณ์ และ/หรือเครื่องมือในระบบคอมพิวเตอร์

2.5. ห้ามใช้ทรัพย์สินหรือใช้งานอินเทอร์เน็ตของบริษัท เพื่อวัตถุประสงค์ทางการค้าหรือเพื่อผลประโยชน์ส่วนตัว ยกเว้นเพื่อประโยชน์โดยตรงของบริษัท รวมทั้งหลีกเลี่ยงการใช้เว็บไซต์หรือจดหมายอิเล็กทรอนิกส์ที่เสี่ยงต่อการถูกคุกคามทางไซเบอร์

2.6. ห้ามติดตั้งซอฟต์แวร์หรือทำการบันทึกข้อมูลใดๆ ลงในอุปกรณ์ และ/หรือเครื่องมือในระบบคอมพิวเตอร์ของบริษัทโดยไม่ได้รับอนุญาต

2.7. ห้ามนำซอฟต์แวร์ของบริษัทไปให้กับบุคคลอื่น ซึ่งรวมถึงซัพพลายเออร์ ผู้รับเหมา ลูกค้าของบริษัท และเพื่อวัตถุประสงค์ส่วนตัว นอกจากนี้การใช้งานอินเทอร์เน็ตหรือเชื่อมต่อกับอินเทอร์เน็ตโดยพนักงานเพื่อการโอนข้อมูล การแพร่กระจายสื่อลามก การส่งและรับข้อมูลทางอีเมล (e-mail) ที่ฝ่าฝืนกฎหมายหรือละเมิดกฎหมายลิขสิทธิ์ โดยมีเจตนาหรือวัตถุประสงค์ที่ฝ่าฝืนนโยบายหรือข้อบังคับเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท หรือพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือกฎหมายอื่นที่เกี่ยวข้อง

2.8. ห้ามละเมิดลิขสิทธิ์ของบริษัท และ/หรือ บริษัทอื่นๆ ที่อนุญาตให้บริษัทใช้ซอฟต์แวร์คอมพิวเตอร์ โดยไม่คำนึงถึงสัญญา และ/หรือวิธีการใดๆ ไม่ว่าจะมีการกระทำซ้ำ หรือแก้ไข หรือเผยแพร่สู่สาธารณะ หรือให้เช่า หรือคัดลอก ไม่ว่าจะเพื่อผลกำไรหรือไม่ก็ตาม

3. จัดให้มีการฝึกอบรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลและความปลอดภัยทางไซเบอร์ตลอดจนการสื่อสารที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ความปลอดภัยของข้อมูล และภัยคุกคามทางไซเบอร์ให้กับพนักงานทุกคนอย่างสม่ำเสมอ

4. กำหนดบทบาท ความรับผิดชอบ และหน้าที่ในการดำเนินการให้เหมาะสมกับการดำเนินงานเกี่ยวกับระบบสารสนเทศและความปลอดภัยของข้อมูล รวมถึงการตั้งค่าการอนุญาตและการควบคุมการเข้าถึงข้อมูลสำคัญ นอกจากนี้อุปกรณ์หรือพื้นที่ที่ใช้ในการจัดเก็บข้อมูลสำคัญ ควรได้รับการควบคุมอย่างเหมาะสมผ่านระบบจัดเก็บข้อมูลทางกายภาพและสารสนเทศ เพื่อป้องกันการเข้าถึงข้อมูลที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต

5. กำหนดนโยบายรหัสผ่านให้สอดคล้องกับการดำเนินธุรกิจและสถานการณ์ปัจจุบัน ตลอดจนสื่อสารให้พนักงานทุกคนทราบว่าจะต้องเก็บรหัสผ่านและรหัสอื่นใดที่บริษัทกำหนดไว้เพื่อเข้าถึงระบบคอมพิวเตอร์หรือ

ข้อมูลบริษัท หรือข้อมูลส่วนบุคคลอย่างเป็นความลับ รหัสผ่านจะต้องถูกเก็บไว้โดยไม่ให้ผู้อื่นทราบและห้ามแบ่งปันกับบุคคลอื่น ต้องปฏิบัติตามนโยบายรหัสผ่านอย่างเคร่งครัด

6. พนักงานต้องใช้ทรัพย์สินของบริษัทอย่างระมัดระวังและรับผิดชอบ อุปกรณ์ที่ได้รับจากบริษัทควรอยู่ในสภาพดีอย่างสม่ำเสมอ โดยสามารถติดต่อแผนกซ่อมแซมเมื่อเกิดความเสียหาย ทรัพย์สินของบริษัทจะต้องไม่สูญหายหรือถูกทำลาย แม้ว่าอุปกรณ์นั้นจะไม่ได้เป็นความรับผิดชอบของพนักงานโดยตรง ห้ามนำทรัพย์สินใดๆ ไปใช้เพื่อวัตถุประสงค์อื่น เว้นแต่เพื่อผลประโยชน์ของบริษัท อุปกรณ์ใดๆ ที่มีข้อมูลสำคัญหรือสามารถเข้าถึงระบบข้อมูลของบริษัทได้ จะต้องป้องกันมิให้ผู้ที่ไม่ได้รับอนุญาตนำไปใช้ เช่น การตั้งรหัสผ่านหรือโปรแกรมรักษาหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งาน หากอุปกรณ์สูญหายหรือถูกขโมย ให้แจ้งฝ่ายระบบสารสนเทศเพื่อการจัดการโดยเร็วที่สุด เพื่อความปลอดภัยของข้อมูล
7. การใช้อุปกรณ์ส่วนบุคคลเชื่อมต่อกับระบบข้อมูลของบริษัทจะต้องเป็นไปตามกฎและข้อบังคับที่กำหนดโดยผู้รับผิดชอบระบบข้อมูล
8. การส่ง การใช้ การประมวลผล การจัดเก็บ การทำลายข้อมูล และอุปกรณ์ที่มีข้อมูลสำคัญต้องมีกระบวนการที่เหมาะสมเพื่อให้มั่นใจว่ามีการรักษาความปลอดภัยของข้อมูลเพียงพอ เพื่อป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตหรือเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต
9. การพัฒนาระบบสารสนเทศต้องมีกระบวนการที่ถูกต้องและเชื่อถือได้ ครอบคลุมถึงกระบวนการออกแบบ พัฒนา ทดสอบ และการนำมาใช้งาน มีระบบที่แยกอย่างชัดเจนระหว่างระบบที่ใช้ในการพัฒนาและระบบที่ใช้งานจริง รวมถึงให้ความสำคัญกับการออกแบบระบบที่มีความปลอดภัยเพียงพอและมีการตรวจสอบความปลอดภัยก่อนใช้งานจริง
10. การแก้ไขระบบข้อมูลหรืออุปกรณ์ใดๆ ที่เกี่ยวข้อง จะต้องมีขั้นตอนและกระบวนการที่เหมาะสม มีการประเมินผลกระทบและมีการสื่อสารกับผู้ที่เกี่ยวข้อง รวมถึงการทดสอบที่เพียงพอและอัปเดตเอกสารที่เกี่ยวข้องเป็นปัจจุบัน
11. มีมาตรการรักษาความปลอดภัยเครือข่ายที่เพียงพอและเหมาะสม ติดตั้งโปรแกรมเพื่อป้องกันการคุกคามจากภายนอกที่เป็นอันตรายต่อเซิร์ฟเวอร์หลักและเซิร์ฟเวอร์ของลูกค้า และโปรแกรมควรได้รับการอัปเดตในเวลาที่เหมาะสม
12. มีการจัดเก็บระบบสารสนเทศที่สำคัญ (Log) และกำหนดระยะเวลาการเก็บรักษาที่เหมาะสม Log จะถูกนำมาใช้ในการตรวจสอบและติดตามประวัติการใช้งานที่สอดคล้องตามกฎหมาย ระเบียบ และกฎระเบียบของหน่วยงานภายนอกที่เกี่ยวข้อง

13. มีกระบวนการป้องกันการหยุดชะงักของระบบสารสนเทศและการถูกโจมตีทางไซเบอร์อย่างทันท่วงที รวมถึงการพิจารณาดำเนินการเพื่อป้องกันการเกิดซ้ำของสถานการณ์ และรายงานไปยังคณะกรรมการบริหาร
14. ข้อมูลที่สำคัญต้องถูกจัดเก็บอย่างปลอดภัย รวมถึงการกำหนดแผนความต่อเนื่องทางธุรกิจและขั้นตอนการตอบสนองต่อเหตุการณ์ฉุกเฉิน โดยมีการทดสอบแผนการกู้คืนจากความเสียหายอย่างสม่ำเสมอ
15. มีการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับการจัดเก็บไว้ที่ส่วนกลาง เพื่อรักษาให้อุปกรณ์อยู่ในสภาพดีและพร้อมใช้งานอย่างต่อเนื่อง
16. การใช้บริการเทคโนโลยีสารสนเทศจากภายนอกจะต้องมีความปลอดภัยเพียงพอตามนโยบายของบริษัท มีกระบวนการคัดเลือก ติดตาม และประเมินผลการบริการอย่างเหมาะสม
17. มีการประเมินความเสี่ยงขององค์กรและผู้ที่เกี่ยวข้องเกี่ยวกับความมั่นคงปลอดภัยของข้อมูลและภัยคุกคามทางไซเบอร์โดยกำหนดแนวทางการบริหารความเสี่ยงอย่างเหมาะสม
18. มีการตอบสนองในกรณีเร่งด่วนที่ชัดเจน ซึ่งพนักงานและผู้มีส่วนได้เสียในองค์กรสามารถร้องเรียนหรือรายงานสิ่งที่น่าสงสัยเกี่ยวกับความปลอดภัยของข้อมูลและภัยคุกคามทางไซเบอร์ เพื่อให้บริษัทมีการปรับปรุงและมีการสื่อสารเพื่อจัดการกับปัญหา พนักงานทุกคนมีหน้าที่รายงานข้อมูลทันทีเมื่อมีเหตุการณ์ที่น่าสงสัยที่อาจนำไปสู่การละเมิดนโยบายหรือมาตรการ การโจรกรรมข้อมูล การแทรกแซง การบุกรุก หรือการทำลายระบบข้อมูลที่ส่งผลกระทบต่อความปลอดภัยของข้อมูลหรือทำให้เกิดความเสียหายต่อบริษัท
19. พนักงานต้องรับทราบและปฏิบัติตามแนวปฏิบัติในการใช้คอมพิวเตอร์และระบบเครือข่ายอย่างเหมาะสม รวมถึงขั้นตอนการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันมิให้ข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ตั้งใจ บริษัทส่งเสริมให้การรักษาความปลอดภัยของข้อมูลเป็นส่วนหนึ่งของการประเมินประสิทธิภาพการทำงานของพนักงานเพื่อการพัฒนาทรัพยากรบุคคลอย่างเหมาะสม
20. ในระหว่างการจ้างงาน พนักงานจะต้องไม่กระทำการใดๆ และ/หรือ ละเว้นการกระทำใดๆ ที่ก่อให้เกิดความเสียหายแก่บริษัท อันเป็นผลจากข้อมูลอันเป็นเท็จ และ/หรือ รายงาน หรือบันทึก หรือการสื่อสาร ไม่ว่าจะด้วยวิธีใดก็ตาม หากมีการจงใจละเมิดนโยบายหรือมาตรการที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลที่ก่อให้เกิดความเสียหายต่อบริษัท ผู้ที่ฝ่าฝืนจะถูกลงโทษตามกฎ และข้อบังคับของบริษัท และจะถูกดำเนินคดีตามกฎหมายหากการกระทำนั้นเป็นการละเมิดกฎหมาย