

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริษัท บีซีพีจี จำกัด (มหาชน) ต่อไปนี้เรียกว่า “บริษัทฯ” มีนโยบายให้เทคโนโลยีสารสนเทศเป็นปัจจัยสำคัญที่ช่วยส่งเสริมการดำเนินธุรกิจให้สามารถแข่งขันได้กับธุรกิจชั้นนำทั่วไป โดยเป็นระบบที่มีความทันสมัยและมีมาตรฐาน มีประสิทธิภาพ มีการบริหารความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สอดคล้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ อีกทั้งมุ่งส่งเสริมพัฒนา ความรู้ความสามารถของพนักงานในด้านเทคโนโลยีสารสนเทศให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ และมีการใช้งานเป็นไปตามกฎหมาย ตลอดจนสนับสนุนการเรียนรู้และพัฒนาตนเองของพนักงานอย่างต่อเนื่องโดยผ่านระบบเทคโนโลยีสารสนเทศ จึงได้มีการจัดทำมาตรฐานการใช้ระบบสารสนเทศและเครือข่ายเพื่อเป็นแนวปฏิบัติขึ้นมา

ส่วนที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

บริษัทฯ มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านการรักษาความปลอดภัยข้อมูลส่วนบุคคล และการดำเนินการด้านความมั่นคงปลอดภัยสำหรับการใช้งานระบบสารสนเทศ เพื่อให้สอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งจัดทำเป็นลายลักษณ์อักษร โดยที่ผู้บริหารเห็นชอบและอนุมัติ และเผยแพร่ให้ผู้ใช้งานทรัพย์สินของบริษัทฯ ได้รับทราบและปฏิบัติตาม รวมทั้งบริษัทฯ ต้องทบทวนนโยบายฯ ตามระยะเวลาที่กำหนด พร้อมทั้งปรับเปลี่ยนนโยบายตามความเหมาะสม และให้สอดคล้องกับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท บางจาก คอร์ปอเรชั่น จำกัด (มหาชน)

ส่วนที่ 2 นโยบายโครงสร้างความมั่นคงปลอดภัยสารสนเทศของบริษัท (Organization of Information Security)

บริษัทฯ มีจุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ ที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับหน่วยงานภายนอก โดยจัดให้มีคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีการประสานงานความรับผิดชอบ ประเมินความเสี่ยง และตรวจสอบการทำงานด้านความมั่นคงปลอดภัย รวมทั้งประสานงานกับผู้ให้บริการภายนอกและผู้ใช้งานสารสนเทศจากภายนอก โดยมีการระบุและจัดทำข้อกำหนดที่ชัดเจนในการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ

ส่วนที่ 3 นโยบายความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

บริษัทฯ มีวัตถุประสงค์เพื่อสร้างความมั่นคงปลอดภัยทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และสิ้นสุดการเปลี่ยนตำแหน่ง หรือเปลี่ยนการจ้างงานของเจ้าหน้าที่และบุคคลภายนอกบริษัทฯ รวมทั้งเพื่อสร้างความรู้และตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยและวิธีปฏิบัติที่

เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติงาน

ส่วนที่ 4 นโยบายการบริหารจัดการทรัพย์สิน (Asset Management)

บริษัทฯ มีจุดประสงค์เพื่อป้องกันทรัพย์สินของบริษัทฯ จากความเสียหายที่อาจเกิดขึ้นได้ และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสม โดยมีการจัดทำบัญชีทรัพย์สิน ระบุผู้ครอบครองทรัพย์สิน ผู้เป็นเจ้าของทรัพย์สิน และกำหนดหลักเกณฑ์การใช้งานทรัพย์สินที่เหมาะสม มีการจัดหมวดหมู่ทรัพย์สินตามระดับชั้นความลับ และจัดทำป้ายชื่อ เพื่อการบริหารจัดการทรัพย์สินตามที่ได้จัดหมวดหมู่ไว้

ส่วนที่ 5 นโยบายการควบคุมการเข้าถึง (Access Control)

บริษัทฯ มีจุดประสงค์เพื่อกำหนดการบริหารจัดการสิทธิการเข้าถึงระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการและแอปพลิเคชันของบริษัทฯ เพื่อป้องกันการเปิดเผยหรือการขโมยสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ

ส่วนที่ 6 นโยบายความมั่นคงปลอดภัยสารสนเทศทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

บริษัทฯ มีจุดประสงค์เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ป้องกันทรัพย์สินไม่ให้เกิดการสูญหาย ถูกขโมย เกิดความเสียหาย เกิดการก่อวินาศกรรมหรือแทรกแซง ป้องกันการถูกเปิดเผยโดยไม่ได้รับอนุญาต และป้องกันไม่ให้เกิดกิจกรรมการดำเนินงานต่าง ๆ ของบริษัทฯ เกิดการติดขัดหรือหยุดชะงัก

ส่วนที่ 7 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศด้านการดำเนินการ (Operations Security)

บริษัทฯ มีวัตถุประสงค์เพื่อบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศด้านการดำเนินงาน สร้างกระบวนการด้านการบริหารจัดการ ป้องกันระบบสารสนเทศถูกบุกรุกจากมัลแวร์และไวรัส

ส่วนที่ 8 นโยบายความมั่นคงปลอดภัยทางด้านการสื่อสาร (Communications Security)

บริษัทฯ มีวัตถุประสงค์เพื่อบริหารจัดการการสื่อสาร ระบบเครือข่าย การส่งผ่านข้อมูลไปยังบุคคลภายนอกอย่างมั่นคงปลอดภัย เพื่อป้องกันไม่ให้สารสนเทศของบริษัทฯ ถูกเปิดเผย แก่ไข รวมไปถึงการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่าย ทั้งในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่าง ๆ จากผู้ให้บริการภายนอก

ส่วนที่ 9 นโยบายการจัดการหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

บริษัทฯ มีจุดประสงค์เพื่อให้การจัดการและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ ป้องกันความผิดพลาด การสูญหายและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์ รักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยวิธีการเข้ารหัสข้อมูล สร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์ สารสนเทศ และไฟล์ต่าง ๆ ของระบบที่ให้บริการ ลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

ส่วนที่ 10 นโยบายความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

บริษัทฯ มีจุดประสงค์เพื่อบริหารจัดการความสัมพันธ์กับผู้ให้บริการภายนอก เช่น เจือนโซฟี่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอก การประเมินผลผู้ให้บริการภายนอก

ส่วนที่ 11 นโยบายการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

บริษัทฯ มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัทฯ ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัทฯ

ส่วนที่ 12 นโยบายประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

บริษัทฯ มีจุดประสงค์เพื่อป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมต่าง ๆ ทางธุรกิจ ป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือไม่พร้อมใช้บริการที่มีต่อระบบสารสนเทศ และสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

ส่วนที่ 13 นโยบายการปฏิบัติตามข้อกำหนด (Compliance)

บริษัทฯ มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุด และมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

ส่วนที่ 14 นโยบายการปฏิบัติด้านการรักษาความปลอดภัยของข้อมูลสำหรับการใช้บริการคลาวด์ (Information Security for Use of Cloud Services)

บริษัทฯ มีจุดประสงค์เพื่อความปลอดภัยในระบบคลาวด์ขององค์กร มุ่งเน้นในการรักษาความปลอดภัยของระบบสารสนเทศและข้อมูลในองค์กร พร้อมกับการสนับสนุนพนักงานในการปฏิบัติงานของพวกเขาอย่างมีประสิทธิภาพ โดยใช้เทคโนโลยีที่หลากหลายต่าง ๆ โดยกำหนดหลักการในการใช้บริการคลาวด์ให้ปลอดภัย ลดความเสี่ยง และเพิ่มความสามารถในการดำเนินธุรกิจ นโยบายนี้จะตั้งกฎระเบียบสำหรับการเลือกและการบริหารจัดการบริการคอมพิวเตอร์คลาวด์ เพื่อให้ข้อมูลได้รับการปกป้องอย่างเหมาะสมตามค่าความสำคัญของธุรกิจและการจัดหมวดหมู่ข้อมูลตามระดับความลับในองค์กรอนาคต

ส่วนที่ 15 นโยบายการเข้ารหัสข้อมูล (Cryptography)

บริษัทฯ มีจุดประสงค์เพื่อกำหนดแนวทางในการเข้ารหัสและการบริหารจัดการกุญแจสำหรับการเข้ารหัส เพื่อแน่ใจว่ามีการใช้การเข้ารหัสอย่างถูกต้องและมีประสิทธิภาพ และสอดคล้องตามความต้องการของธุรกิจ ความมั่นคงปลอดภัยของข้อมูล และกฎหมาย ข้อบังคับ กฎระเบียบ และข้อตกลงหรือสัญญาที่เกี่ยวข้องกับการเข้ารหัส

นางสาวสัตยา มหัตถนาพาณิช
รองกรรมการผู้จัดการใหญ่
สายงานบริหารความเป็นเลิศองค์กร