ประกาศที่ 01/2564
เรื่องนโยบายความปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์

1. เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยด้านสารสนเทศ
2. เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ รวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม
3. เพื่อให้พนักงานและผู้ที่ต้องใช้หรือเชื่อมต่อระบบคอมพิวเตอร์ของบริษัท ให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม
4. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่าง ๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

ขอบเขต

นโยบายฉบับนี้ครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท ทั้งที่อยู่ภายในหรือ ภายนอกสถานที่ปฏิบัติงานของบริษัท รวมทั้งคลาวด์ที่บริษัทจัดหา ซึ่งครอบคลุมถึง

1. พนักงานและหน่วยงานทั้งหมดของบริษัท
2. บุคคลภายนอกบริษัทที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท
3. ยึดถือนโยบายตาม “มาตรฐานความปลอดภัยสารสนเทศ” ของบริษัทอย่างเคร่งครัด

หน้าที่และความรับผิดชอบ

หน้าที่ของผู้บังคับบัญชา

1. ชี้แจงให้พนักงานทราบถึงนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่าง ๆ ของบริษัทที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. ดูแล แนะนำ และตักเตือน กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม
3. พิจารณาลงโทษทางวินัยแก่ผู้กระทำผิดอย่างเสมอภาค และเป็นธรรม

หน้าที่ของพนักงาน

พนักงานทุกคน ต้องปฏิบัติดังต่อไปนี้

1. ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่าง ๆ ของบริษัทที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศโดยเคร่งครัด
2. ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท
3. แจ้งให้บริษัททราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นการบุกรุกโจรกรรม ทำลาย แทรกแซงการทำงาน หรือจารกรรมที่อาจสร้างความเสียหายต่อบริษัท
4. หากพบสิ่งผิดปกติเกิดขึ้นกับระบบคอมพิวเตอร์ให้หยุดการทำงาน ถอดสายแลน หรือ ตัดระบบออกจากเครือข่ายคอมพิวเตอร์ของบริษัททันที และแจ้งเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเข้าตรวจสอบปัญหาที่เกิดขึ้น

พนักงานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์ ต้องปฏิบัติดังต่อไปนี้

1. ต้องออกจากระบบ (Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน
2. ต้องล็อคหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือไปทำกิจกรรมอย่างอื่นเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน
3. ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส(Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย
4. ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่บริษัทกำหนด เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ หรือข้อมูลของบริษัทเป็นความลับส่วนตัวพนักงาน ซึ่งจะต้องเก็บ รักษาไว้มิให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น ทั้งนี้พนักงานต้องเปลี่ยนรหัสผ่านและรหัสอื่นใด เมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนดหรือเมื่อพนักงานเห็นสมควรต้องทำการเปลี่ยน รหัสผ่าน โดยตั้งรหัสผ่าน และรหัสอื่นใด ด้วยความรอบคอบ ห้ามตั้งรหัสซ้ำกับรหัสเก่า ห้ามตั้งรหัส ที่ผู้อื่นสามารถคาดเดาได้ง่าย และห้ามตั้งรหัสซ้ำกันในทุกระบบที่พนักงานมีสิทธิใช้งาน ทั้งนี้มาตรฐานการตั้งรหัสผ่านอย่างปลอดภัย อ้างอิงตามเอกสาร IT Security Standard

พนักงานทุกคน ต้องห้ามทำสิ่งดังต่อไปนี้

1. นำเอกสาร ข้อมูลสารสนเทศ ของบริษัทที่สำคัญ ออกจากบริษัทโดยไม่ได้รับอนุญาตจากผู้มีอำนาจโดยเด็ดขาด
2. ดัดแปลงข้อมูล, เปลี่ยนแปลงข้อมูลสารสนเทศของบริษัท โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ
3. เชื่อมต่อคอมพิวเตอร์ สมาร์ทโฟน อุปกรณ์ใดๆ ที่ไม่ได้รับอนุญาตจากบริษัท หรือ หน่วยงานที่สังกัด
4. ห้ามใช้อุปกรณ์บันทึกข้อมูล เช่น แฟลชไดร์ฟ, CD, DVD โดยไม่ได้รับอนุญาตจากผู้อำนาจหรือหน่วยงานที่สังกัด
5. นำอุปกรณ์คอมพิวเตอร์ออกจากบริษัทโดยไม่ได้รับอนุญาต
6. ติดตั้งโปรแกรมคอมพิวเตอร์ที่ไม่ได้รับอนุญาตจากบริษัท หรือ หน่วยงานที่รับผิดชอบ

พนักงานที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอก

ต้องจัดให้มีการควบคุมดูแลบุคคลภายนอกให้ปฏิบัติตามนโยบายความปลอดภัยสารสนเทศของบริษัทอย่างเคร่งครัด

ระยะเวลาทบทวน

เพื่อให้นโยบายความปลอดภัยด้านสารสนเทศ รวมทั้งแนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง บริษัท จึงจัดให้มีการทบทวนนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนการปฏิบัติ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายนี้เป็นประจำทุกปี หรือเมื่อเกิดเหตุการณ์ด้านความปลอดภัย ที่มีผลกระทบกับองค์กร

จึงประกาศมาให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ 1 มกราคม 2564

.....

(ดร.ปัญญา บุญญาภิวัฒน์)