นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

ที่ประชุมคณะกรรมการบริษัท เพียร์ ฟอร์ ยู จำกัด (มหาชน) ได้อนุมัตินโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นแนวทางในการกำหนดทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างมีประสิทธิภาพและปลอดภัย โดย บริษัท เพียร์ ฟอร์ ยู จำกัด (มหาชน) และบริษัทย่อย ได้กำหนด “ขอบเขตของการดำเนินการตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001 : 2013 Information Security Management System)” ที่ได้รับอนุมัติจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ และผู้ที่ได้รับมอบหมาย จึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศไว้ดังนี้

1. บริษัทฯ กำหนดนโยบายด้านความปลอดภัย ภายใน และสื่อสารให้พนักงานรับทราบทั่วกัน โดย พนักงานใหม่ต้องได้รับการอบรมนโยบายความปลอดภัยด้านสารสนเทศ ในระหว่างการปฐมนิเทศ (Orientation) พนักงานเก่าต้องได้รับการอบรมนโยบายความปลอดภัยด้านสารสนเทศ ประจำปี (Refresh Awareness Training) และพนักงานเก่าสามารถเข้าถึงนโยบายได้ตลอดเวลาในระบบ Document Management ที่กำหนด
2. กรณีที่มีกิจกรรมที่มีความเสี่ยงต่อความปลอดภัยของข้อมูลสูงบริษัทฯ จะมีการแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ของพนักงานอย่างเหมาะสม เพื่อป้องกันมิให้พนักงานผู้หนึ่งผู้ใดได้รับสิทธิ์ในการเข้าถึงระบบเกินกว่าหน้าที่ความรับผิดชอบของตำแหน่งงาน
3. บริษัทฯ กำหนดให้มีการระบุ Asset อยู่ในขอบเขตของการขอการรับรอง และกำหนดผู้รับผิดชอบ (Asset Owner) โดย Asset ของบริษัทฯ แบ่งออกเป็น 5 กลุ่ม ได้แก่ Information Asset, Software Asset, Physical Asset, Personal Asset , Service Asset ซึ่งทุกส่วนงาน จะต้องปฏิบัติตามข้อกำหนดในการดูแล Asset ต่างๆ อย่างเข้มงวดให้เกิดความปลอดภัย
4. บริษัทจัดให้มีการแบ่งชั้นความลับของเอกสาร (Classification of Information) รวมถึงการ Labeling และวิธีการเคลื่อนย้ายในส่วนของข้อมูล เพื่อให้ส่วนงานต่างๆ ถือปฏิบัติตามมาตรฐานที่กำหนด
5. บริษัทฯ กำหนดให้พนักงานที่เข้ามาใช้งานระบบเครือข่ายคอมพิวเตอร์ของ DC/Call center จะต้องปฏิบัติตามขั้นตอนที่กำหนดให้อย่างเคร่งครัด
6. บริษัทฯ ไม่อนุญาติให้ทำการดาวน์โหลด ติดตั้ง หรือทำการใช้โปรแกรมตรวจสอบทางด้านความมั่นคงปลอดภัย ในเครือข่ายคอมพิวเตอร์ DC โดยไม่ได้รับอนุญาต อาทิเช่น โปรแกรมประเภท Password Cracking, Packet Sniffer, Network Mapping Tools, Port Scanners เป็นต้น
7. บริษัทฯ ไม่อนุญาติให้ให้พนักงานทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัทฯและของผู้ว่าจ้าง
8. บริษัทฯ ไม่อนุญาติให้พนักงานนำซอฟต์แวร์ของบริษัทฯและของผู้ว่าจ้าง ไปติดตั้งใช้งานส่วนตัวหรือทำสำเนา โดยเด็ดขาดรายชื่อซอฟต์แวร์ หรือแอพพลิเคชั่น ที่ถูก ติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ต้องได้รับการจัดทำเป็นเอกสาร และ ได้รับการอนุมัติโดยผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่า ซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ ในการทำงานของบริษัทฯและของผู้ว่าจ้าง เท่านั้น

9. บริษัทฯ กำหนดเงื่อนไข หากต้องการใช้งานซอฟต์แวร์ให้พนักงานประสานงานหน่วยงานต้นสังกัด ในการขอทำการติดตั้งและอนุมัติจากส่วนงาน IT หากเป็นซอฟต์แวร์ที่ไม่มีค่าลิขสิทธิ์ และต้องได้รับการอนุมติจากผู้บริหารระดับสูงของบริษัทฯ หากมีการขอติดตั้งซอฟต์แวร์ที่มีค่าใช้จ่าย ก่อนการนำมาใช้งานทุกครั้ง
10. บริษัทฯ กำหนดผู้ใช้งานอีเมล์ทั้งหมด ต้องมี e-mail account เป็นของตนเอง ยกเว้นกรณีแผนกหรือส่วนงานที่จำเป็นต้องมีการใช้ e-mail รวมกัน บริษัทฯและผู้ว่าจ้าง อาจจะจัดหา e-mail account ให้แก่บุคคลที่ไม่ใช่พนักงานได้ถ้ามีความจำเป็นต้องใช้งานและอนุมัติจากหน่วยงานที่เกี่ยวข้อง E-mail account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วง ละเมิด และการนำอีเมล์ไปใช้ในทางที่ผิด
11. บริษัทฯ ไม่อนุญาติให้ใช้ e-mail account ของบริษัทฯเพื่อกระทำการใดๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น
12. บริษัทฯ ไม่อนุญาติให้พนักงานใช้ e-mail address ของบริษัทฯ ในการประกาศ ข้อมูลใดๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับบริษัทฯ เอง
13. บริษัทฯ ไม่อนุญาติให้ผู้ใช้งานทำสำเนาข้อความหรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูลผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่า ตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนของบริษัทฯ
14. บริษัทฯ กำหนดให้พนักงานต้องไม่ส่งหรือส่งต่ออีเมล์ที่มีรูปภาพหรือเนื้อหาดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ การพนัน หรือ ลามกอนาจารโดยเด็ดขาด
15. บริษัทฯ กำหนดให้พนักงานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับ จากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรม แฝง (โทรจัน) เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ ของตนถูกโจมตีโดยไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์ โดยทันทีจนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ
16. บริษัทฯ กำหนดให้พนักงานต้องใช้งานอินเตอร์เน็ทด้วยความระมัดระวัง และการใช้งานนั้นต้อง ไม่เป็นสาเหตุให้บริษัทฯ และบุคคลผู้ที่เกี่ยวข้องกับบริษัทฯเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเตอร์เน็ทในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (Computer Crime Act)
17. บริษัทฯ ไม่อนุญาติให้พนักงานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใดๆ ตัวอย่างเช่น ไวรัส หนอนอินเตอร์เน็ท โปรแกรมแฝง (ม้าโทรจัน) อีเมล์บอมบ์ ฯลฯ เข้าสู่ ระบบคอมพิวเตอร์ของบริษัทฯ
18. บริษัทฯ กำหนดให้การใช้งานรหัสผ่านต่างๆ ที่บริษัทฯ มอบให้ ต้องถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย ห้ามมิให้มีการใช้งาน User account ร่วมกันหรือ ให้ผู้อื่นเข้าใช้งาน User account ของตนโดยเด็ดขาด ทั้งนี้ รวมถึงสมาชิกใน ครอบครัวเมื่อผู้ใช้งานนำงานกลับไปทำที่บ้านด้วย
19. บริษัทฯ กำหนดเงื่อนไขการเข้าใช้งานอินเตอร์เน็ท โดยขอสงวนสิทธิ์ในการตรวจสอบการใช้งาน อินเตอร์เน็ทของผู้ใช้งาน เพื่อตรวจสอบการใช้งานที่ไม่เหมาะสม
20. บริษัทฯ ไม่อนุญาติให้ผู้ใช้งานเข้าชม ใช้งาน ดาวน์โหลด รับ หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
21. บริษัทฯ กำหนดให้พนักงานควรติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่สำนักงาน

22. บริษัทฯ กำหนดให้พนักงานควรตรวจสอบความมั่นคงปลอดภัยของ พื้นที่ทำงานของตนเป็นประจำ ทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่างๆ ได้รับการปิดล๊อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย
23. บริษัทฯ ไม่อนุญาติให้บุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัทฯและของผู้ว่าจ้าง โดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติ อย่างเหมาะสมก่อนทุกครั้ง
24. ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใดๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อ Incident Staff ที่เกี่ยวข้องทันที

- นายคณาวุฒิ วรรทนธีรัช -

(นายคณาวุฒิ วรรทนธีรัช)

ประธานกรรมการบริหารและประธานเจ้าหน้าที่บริหาร