นโยบายความมั่นคงปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ บริษัท ไทยวาโก้ จำกัด (มหาชน)

บทนำ

ตามที่ บริษัท ไทยวาโก้ จำกัด (มหาชน) ได้จัดให้มีระบบเทคโนโลยีสารสนเทศและการสื่อสารขึ้นเพื่ออำนวยความสะดวกรวดเร็วในการบริหารงานของผู้บริหารและการปฏิบัติงานของพนักงาน ซึ่งจะช่วยให้การดำเนินธุรกิจของบริษัทฯ เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยเชื่อถือได้ และสามารถดำเนินงานได้อย่างต่อเนื่อง

บริษัทฯ ตระหนักถึงบทบาทของปัญญาประดิษฐ์ (Artificial Intelligence: AI) ซึ่งเป็นเทคโนโลยีที่เปี่ยมด้วยศักยภาพเชิงยุทธศาสตร์และเป็นพลังขับเคลื่อนสำคัญในการปฏิรูปอุตสาหกรรมและสังคมทั่วโลก โดยเฉพาะอย่างยิ่งเทคโนโลยี Generative AI ที่มีความสามารถในการสร้างสรรค์เนื้อหาหลากหลายรูปแบบ เช่น ข้อความ ภาพ วิดีโอ เสียง หรือซอร์สโค้ด ซึ่งสามารถช่วยลดระยะเวลาและเพิ่มประสิทธิภาพในการดำเนินงานได้

อย่างไรก็ตาม การนำเทคโนโลยี AI และ Generative AI (ต่อไปนี้เรียกว่า “ระบบ AI”) มาประยุกต์ใช้ มาพร้อมกับความท้าทายและความเสี่ยงที่ซับซ้อน ซึ่งภัยคุกคามเหล่านี้ไม่ได้จำกัดอยู่แค่ภัยคุกคามทางไซเบอร์แบบดั้งเดิม แต่ยังรวมถึงภัยคุกคามที่จำเพาะเจาะจงต่อระบบ AI

ดังนั้น การรักษาไว้ซึ่งความลับ ความถูกต้อง ความสมบูรณ์ครบถ้วน และความพร้อมใช้งานของข้อมูลธุรกิจและระบบสารสนเทศ รวมถึงระบบ AI จึงเป็นสิ่งสำคัญยิ่ง อีกทั้งเป็นการสร้างความเชื่อมั่นให้แก่ลูกค้าและคู่ค้า ตลอดจนสอดคล้องกับข้อกำหนดของกฎหมายที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น บริษัทฯ จึงกำหนดนโยบายความมั่นคงปลอดภัยของข้อมูลและระบบคอมพิวเตอร์และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติ

1. นโยบายนี้จัดทำขึ้นสำหรับพนักงานหรือบุคคลภายนอกที่บริษัทฯ อนุญาตให้เข้าใช้งานระบบเครือข่ายและคอมพิวเตอร์ ระบบข้อมูลของบริษัทฯ และระบบ AI รวมถึงการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ต (Internet) โดยผ่านระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ และให้ถือปฏิบัติอย่างเคร่งครัด
2. บริษัทฯ ดำเนินกิจการภายใต้กฎหมายไทย ดังนั้นการใช้งานระบบเครือข่ายและคอมพิวเตอร์รวมทั้งการเชื่อมต่อระบบอินเทอร์เน็ต (Internet) ของบริษัทฯ จึงให้เป็นไปตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ที่มีผลบังคับใช้ และกฎหมายอื่นที่เกี่ยวข้อง
3. ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ และอุปกรณ์เชื่อมต่อเป็นสินทรัพย์ของบริษัทฯ จัดหาไว้เพื่อการบริการที่เกี่ยวข้องกับกิจการของบริษัทฯ เท่านั้น
4. บริษัทฯ สงวนสิทธิในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอันสมควร หากพบว่ามีการละเมิดนโยบายความมั่นคงปลอดภัยของข้อมูลและระบบคอมพิวเตอร์

.../ 2

หมวดที่ 1

คำนิยามศัพท์

1. **“บริษัทฯ”** หมายความว่า บริษัท ไทยวาโก้ จำกัด (มหาชน)
2. **“ผู้บังคับบัญชา”** หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของบริษัทฯ
3. **“พนักงาน”** หมายความว่า บุคคลที่บริษัทฯ ได้ว่าจ้างและมอบหมายให้ปฏิบัติงานตามที่บริษัทฯ กำหนด
4. **“ผู้ดูแลระบบข้อมูล”** หมายความว่า พนักงานที่ได้รับมอบหมายจากบริษัทฯ ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบข้อมูลคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมระบบคอมพิวเตอร์ เพื่อจัดการฐานข้อมูล และได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนา แก้ไข ปรับปรุง และบำรุงรักษาระบบข้อมูลและโปรแกรมต่าง ๆ ที่เกี่ยวข้องกับระบบข้อมูลที่ใช้งานอยู่ในบริษัทฯ
5. **“ผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์”** หมายความว่า พนักงานที่ได้รับมอบหมายจากบริษัทฯ ให้มีหน้าที่รับผิดชอบในการดูแลรักษาและพัฒนาระบบเครือข่ายและคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อจัดการฐานข้อมูลของระบบเครือข่ายและคอมพิวเตอร์
6. **“ผู้พัฒนาซอฟต์แวร์และฮาร์ดแวร์”** หมายความว่า พนักงานที่ได้รับมอบหมายจากบริษัทฯ ให้มีหน้าที่รับผิดชอบในการออกแบบ สร้าง วางแผนการพัฒนาโปรแกรม ซอฟต์แวร์ (Software) หรือแอปพลิเคชัน (Application) หรือฮาร์ดแวร์ (Hardware) เน้นในเรื่องของการเขียนโปรแกรมโดยใช้ภาษาโปรแกรมใดภาษาหนึ่ง
7. **“เจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศ”** หมายความว่า พนักงานที่ได้รับมอบหมายจากบริษัทฯ ให้มีหน้าที่รับผิดชอบในการดูแลรักษาและพัฒนาระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยมีหน่วยงานตามโครงสร้างที่ผู้บังคับบัญชาระดับฝ่ายของศูนย์เทคโนโลยีสารสนเทศกำหนด
8. **“บุคคลภายนอก”** หมายความว่า บุคคลที่ไม่ได้สังกัดอยู่ในบริษัทฯ แต่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ โดยมีสิทธิและหน้าที่ตามที่กำหนด
9. **“ศูนย์เทคโนโลยีสารสนเทศ”** หมายความว่า หน่วยงานตามโครงสร้างของบริษัทฯ มีหน้าที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ และเป็นศูนย์กลางในการศึกษา วิเคราะห์ พัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ
10. **“ข้อมูล”** หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงข้อมูลหรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพ หรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
11. **“ระบบข้อมูล”** หมายความว่า ระบบงานโปรแกรมคอมพิวเตอร์ของบริษัทฯ ที่ทำงานเกี่ยวข้องกับการเก็บ (นำเข้า) จัดการ (ประมวลผล) และเผยแพร่ (แสดงผล) ข้อมูลและสารสนเทศ เพื่อสนับสนุนกลไกการทำงานของบริษัทฯ

.../ 3

12. **“ระบบคอมพิวเตอร์”** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
13. **“ระบบเครือข่ายและคอมพิวเตอร์”** หมายความว่า เครื่องคอมพิวเตอร์ที่เป็นสินทรัพย์ของบริษัทฯ รวมทั้งอุปกรณ์ต่อพ่วงต่าง ๆ ตลอดจนอุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่าง ๆ ภายในบริษัทฯ รวมทั้งการเชื่อมโยงคอมพิวเตอร์ในระยะไกลเข้าด้วยกัน
14. **“สินทรัพย์”** หมายความว่า ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ข้อมูล และระบบข้อมูลด้านเทคโนโลยีสารสนเทศและการสื่อสาร ภายใต้การกำกับดูแลของศูนย์เทคโนโลยีสารสนเทศ
15. **“บัญชีชื่อผู้ใช้งาน” (Account)** หมายความว่า รายชื่อผู้มีสิทธิใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารของบริษัทฯ
16. **“ชื่อผู้ใช้” (Username)** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารของบริษัทฯ ที่มีการกำหนดสิทธิการใช้งานไว้
17. **“รหัสผ่าน” (Password)** หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข นำมารวมกันเพื่อใช้เป็นเครื่องมือในการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ
18. **“ลงบันทึกเข้า” (Login)** หมายความว่า กระบวนการที่ผู้ใช้งาน เข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารของบริษัทฯ ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง
19. **“ลงบันทึกออก” (Logout)** หมายความว่า กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารของบริษัทฯ
20. **“การพิสูจน์ยืนยันตัวตน” (Authentication)** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งาน ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
21. **“ระบบอินเทอร์เน็ต” (Internet)** หมายความว่า ระบบเครือข่ายสื่อสารที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ของบริษัทฯ เข้ากับเครือข่ายระบบอินเทอร์เน็ต (Internet) ทั่วโลก
22. **“ดาวน์โหลด” (Download)** หมายความว่า การนำไฟล์หรือข้อมูลจากเครื่องคอมพิวเตอร์เครื่องอื่นมายังคอมพิวเตอร์ที่เราใช้งานผ่านทางเครือข่ายระบบอินเตอร์เน็ต (Internet)
23. **“อัปโหลด” (Upload)** หมายความว่า การโอนย้ายไฟล์หรือข้อมูลจากเครื่องคอมพิวเตอร์ของพนักงานไปไว้บนระบบอินเตอร์เน็ต (Internet) หรือว่าโอนไฟล์ไปไว้คอมพิวเตอร์เครื่องอื่น ๆ ที่มีการเชื่อมต่อกันอยู่

.../4

24. **“ข้อมูลจราจรทางคอมพิวเตอร์” (Log)** หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์
25. **“ฮาร์ดแวร์” (Hardware)** หมายความว่า ชุดขององค์ประกอบต่าง ๆ ที่ประกอบรวมกันเป็นระบบคอมพิวเตอร์ ฮาร์ดแวร์คอมพิวเตอร์เป็นส่วนประกอบกายภาพ เช่น จอภาพ เมาส์ คีย์บอร์ด แหล่งเก็บข้อมูลคอมพิวเตอร์ ฮาร์ดดิสก์ การ์ดจอ การ์ดเสียง หน่วยความจำ (RAM) แผงวงจรหลัก เป็นต้น ทั้งหมดเป็นวัตถุที่จับต้องได้
26. **“ซอฟต์แวร์” (Software)** หมายความว่า ชุดคำสั่งหรือโปรแกรมที่สั่งให้เครื่องคอมพิวเตอร์ทำงานตามลำดับขั้นตอนที่กำหนดไว้ เพื่อให้ได้ผลลัพธ์ตามที่ผู้ใช้คอมพิวเตอร์ต้องการ ซอฟต์แวร์จะทำหน้าที่จัดการ ควบคุมการประมวลผลของคอมพิวเตอร์ตั้งแต่เปิดเครื่องจนกระทั่งปิดเครื่อง
27. **“แอปพลิเคชัน” (Application)** หมายความว่า โปรแกรม หรือชุดสั่ง ที่ใช้ควบคุมการทำงานของคอมพิวเตอร์และอุปกรณ์ต่อพวงต่างๆ เพื่อให้ทำงานตามคำสั่ง และตอบสนองความต้องการของผู้ใช้
28. **“จดหมายอิเล็กทรอนิกส์” (e-mail)** หมายความว่า ระบบที่บุคลากรใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายสื่อสารที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว เสียงและอื่น ๆ ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP, POP3 และ IMAP เป็นต้น
29. **“โปรแกรมประสงค์ร้าย” (Malware)** หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ ทำให้เกิดขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เช่น ไวรัสคอมพิวเตอร์ (Computer Virus), สปายแวร์ (Spyware), หนอน (Worm), ฟิชชิง (Phishing), ม้าโทรจัน (Trojan horse), จดหมายลูกโซ่ (Mass Mailing) เป็นต้น
30. **“ปัญญาประดิษฐ์ (Artificial Intelligence : AI)”** หมายความว่า เทคโนโลยีที่ถูกพัฒนาขึ้น เพื่อให้ระบบประมวลผลของคอมพิวเตอร์ หุ่นยนต์ เครื่องจักร หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ มีคุณสมบัติ หรือพฤติกรรมใกล้เคียงมนุษย์ตามวัตถุประสงค์ที่มนุษย์กำหนด เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผล และการแก้ไขปัญหา เป็นต้น
31. **“Generative AI”** หมายความว่า เทคโนโลยี AI ประเภทหนึ่งที่มีความสามารถ ในการสร้างเนื้อหาใหม่ในหลากหลายรูปแบบตามข้อความหรือคำสั่ง (Prompt) ที่มนุษย์เป็นผู้กำหนด เช่น ข้อความ ภาพ วิดีโอ ซอร์สโค้ด หรือรูปแบบอื่น เป็นต้น

.../5

32. **“ข้อมูลส่วนบุคคล”** หมายความว่า ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

33. **“ข้อมูลส่วนบุคคลอ่อนไหว”** หมายความว่า ข้อมูลส่วนบุคคลตามที่ถูกบัญญัติไว้ในมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้แก่ ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูล ส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

หมวดที่ 2

ข้อปฏิบัติการใช้งานระบบ

1. ข้อปฏิบัติการใช้งานระบบเครือข่ายและคอมพิวเตอร์

1.1 บริษัทฯ ได้ดำเนินการให้สอดคล้องกับข้อกำหนดของกฎหมาย ดังนั้น การใช้งานระบบเครือข่ายและคอมพิวเตอร์ ระบบข้อมูล และระบบอินเทอร์เน็ต (Internet) ของบริษัทฯ ให้ปฏิบัติตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง

1.2 บริษัทฯ ไม่สนับสนุนหรือยินยอมให้พนักงานหรือบุคคลภายนอก กระทำผิดต่อกฎหมายว่าด้วยกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง

1.3 ระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ มีไว้เพื่อให้บริการที่เกี่ยวข้องกับการดำเนินงานของ บริษัทฯ เท่านั้น ไม่อนุญาตให้ใช้ในกิจการอื่นที่ไม่เกี่ยวข้องกับการดำเนินงานของบริษัทฯ

1.4 การเข้าใช้งานระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ จะต้องปฏิบัติตามขั้นตอนในการขออนุญาตเข้าใช้ โดยต้องมีการลงทะเบียนการเข้าใช้งาน ตามขั้นตอนของบริษัทฯ

1.5 ในการขออนุญาตเข้าใช้งาน ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาโดยตรงของพนักงาน และปฏิบัติตามขั้นตอนที่บริษัทฯ กำหนดไว้

1.6 การใช้งานระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ จะต้องใช้งานผ่านเครื่องคอมพิวเตอร์ของบริษัทฯ เท่านั้น

1.7 การใช้งานระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ จากเครื่องคอมพิวเตอร์ที่ไม่ใช่ของบริษัทฯ จะต้องได้รับอนุญาตจากผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์ก่อน และหากพบว่ามีการใช้งานโดยไม่ได้รับอนุญาต ผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์สามารถตัดการใช้งานออกจากระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ ได้ทันที

.../6

1.8 บริษัทฯ ขอสงวนสิทธิเพิกถอนการให้บริการระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

2. ข้อปฏิบัติการใช้งานระบบข้อมูล

2.1 การพัฒนาระบบข้อมูลหรือการแก้ไข ผู้ดูแลระบบข้อมูลต้องมีการทดสอบร่วมกันกับพนักงานก่อนการใช้งานจริง

2.2 การใช้งานระบบข้อมูลให้เป็นไปตามการกำหนดสิทธิที่ผู้ดูแลระบบข้อมูลได้ตกลงไว้กับพนักงานตามตารางกำหนดสิทธิที่จัดทำไว้ โดยผู้บังคับบัญชาตามสายงานบริหารและผู้บังคับบัญชาระดับฝ่ายของศูนย์เทคโนโลยีสารสนเทศให้ความเห็นชอบ

3. ข้อปฏิบัติการใช้ระบบ AI

3.1 **การใช้ระบบ AI ที่ยอมรับได้:**

ผู้ใช้งานต้องศึกษาข้อมูล ศักยภาพ ประโยชน์ ความเสี่ยง และข้อจำกัดของระบบ AI แต่ละประเภทและประยุกต์ใช้อย่างเหมาะสม เพื่อสนับสนุนการดำเนินงานของบริษัทฯ ในบริบทที่กำหนด ดังต่อไปนี้

1) การวิเคราะห์ข้อมูลและสร้างรายงาน
2) การเขียนชุดคำสั่งหรือโปรแกรม
3) การจัดทำร่างหนังสือหรือเอกสารต่าง ๆ เช่น บันทึกข้อความ นโยบาย เป็นต้น
4) การให้คำแนะนำหรือแนวทางเบื้องต้นในการแก้ปัญหาด้านต่าง ๆ
5) การสร้างเนื้อหาสำหรับการสื่อสารภายในองค์กร หรือสร้างสื่อประชาสัมพันธ์
6) ดำเนินงานอื่น ๆ ที่ได้รับมอบหมายจากผู้บังคับบัญชา

3.2 **ข้อห้ามในการใช้ระบบ AI:**

ห้ามใช้ระบบ AI ในลักษณะที่อาจก่อให้เกิดความเสียหายต่อบุคคล บริษัทฯ สังคม หรือประเทศชาติ โดยเฉพาะ

1) ห้ามใช้แทนการตัดสินใจของผู้ใช้งานในกรณีที่มีความเสี่ยงสูง เช่น การตัดสินใจทางกฎหมาย ทางการเงิน หรือการตัดสินใจที่อาจส่งผลกระทบต่อชีวิต ทรัพย์สิน และสิทธิของบุคคล
2) ห้ามใช้เพื่อสร้างข้อมูลอันเป็นเท็จ หรือเนื้อหาที่อาจก่อให้เกิดความเสียหายต่อบุคคล บริษัทฯ หรือสังคม
3) ห้ามใช้หรือเปิดเผยข้อมูลที่เป็นความลับของบริษัทฯ รวมถึงข้อมูลภายใน เอกสารสำคัญ หรือข้อมูลที่อาจส่งผลกระทบต่อการดำเนินงาน
4) ห้ามใช้ข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูล หรือใช้ข้อมูลที่อาจเป็นความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมายอื่นที่เกี่ยวข้อง

.../7

5) ห้ามใช้เพื่อสร้างเนื้อหาที่ละเมิดทรัพย์สินทางปัญญา (ลิขสิทธิ์ สิทธิบัตร เครื่องหมายการค้า) รวมถึงการทำซ้ำ คัดลอก หรือดัดแปลงโดยไม่ได้รับอนุญาต

6) ห้ามใช้เพื่อสร้างเครื่องมือหรือเนื้อหาที่เป็นอันตรายโดยตรง เช่น การสร้างสื่อสังเคราะห์ปลอม (Deepfake) เพื่อโจมตีผู้อื่น หรือการเขียนโค้ดเพื่อพัฒนามัลแวร์ (Malware) หรือไวรัสคอมพิวเตอร์ (Computer Virus)

3.3 **การรักษาความลับและความมั่นคงปลอดภัยของข้อมูลจากการใช้ระบบ AI:**

1) ห้ามนำข้อมูลภายในบริษัทฯ และข้อมูลที่มีชั้นความลับ เช่น รหัสผ่าน, เอกสารสัญญา, เอกสารที่มีข้อความลับ ไปใช้งานร่วมกับระบบ AI โดยเฉพาะบริการสาธารณะที่ไม่มีค่าใช้จ่าย ที่มีความเสี่ยงที่ข้อมูลอาจถูกบันทึกและนำไปใช้ในการฝึกสอนโมเดล AI

2) กรณีจำเป็นต้องใช้ระบบ AI ร่วมกับข้อมูลที่มีความลับหรือข้อมูลส่วนบุคคลอ่อนไหว ผู้ใช้งานจะต้องใช้ระบบ AI ที่บริษัทฯ ประกาศกำหนดเท่านั้น และต้องได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล และได้รับอนุมัติจากผู้อำนวยการฝ่ายตามสายการบังคับบัญชา

3) ห้ามนำข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ เช่น รหัสผ่าน, ข้อมูล API Key ไปใช้งานร่วมกับระบบ AI

4) ต้องตรวจสอบซอร์สโค้ดที่สร้างโดยระบบ AI ก่อนนำมาใช้งานจริง โดยพิจารณาถึงความถูกต้องและการตรวจสอบช่องโหว่อย่างถี่ถ้วนทุกครั้ง

5) หากพบเหตุการณ์ละเมิดความมั่นคงปลอดภัยจากระบบ AI ต้องแจ้งผู้บังคับบัญชาตามลำดับชั้นทราบโดยทันที และปฏิบัติตามขั้นตอนการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย

3.4 **หน้าที่และความรับผิดชอบในการใช้ระบบ AI:**

ผู้ใช้งานและบุคคลที่เกี่ยวข้องกับการประยุกต์ใช้ระบบ AI มีหน้าที่และความรับผิดชอบที่สำคัญ

1) ผู้ใช้งานต้องตรวจสอบและรับผิดชอบต่อการตัดสินใจขั้นสุดท้าย ต่อผลลัพธ์ที่เกิดขึ้นจากการใช้ข้อมูลที่สร้างโดยระบบ AI อย่างเคร่งครัดก่อนนำไปใช้งานหรือเผยแพร่ โดยเฉพาะอย่างยิ่งในประเด็นความถูกต้อง ผลกระทบทางกฎหมาย และการรักษาความลับ

2) ต้องรายงานให้ผู้บังคับบัญชารับทราบโดยทันที ในกรณีที่ระบบ AI เกิดความผิดพลาด หรือให้ผลลัพธ์ที่อาจส่งผลกระทบเชิงลบ

3) การนำเนื้อหาที่สร้างจากระบบ AI มาใช้งาน ควรระบุให้ชัดเจนตามความเหมาะสม เพื่อให้เกิดความโปร่งใส เช่น เนื้อหานี้สร้างหรือได้รับความช่วยเหลือจากเทคโนโลยี AI

.../8

หมวดที่ 3

ข้อปฏิบัติสำหรับพนักงาน

1. นโยบายความมั่นคงปลอดภัยของข้อมูลและระบบคอมพิวเตอร์นี้ ถือเป็นส่วนหนึ่งของข้อกำหนดในการปฏิบัติงาน พนักงานที่เข้าใช้ระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ ต้องยอมรับและรับทราบนโยบายหรือระเบียบข้อบังคับที่บริษัทฯ กำหนดขึ้น จะอ้างว่าไม่ทราบนโยบายหรือระเบียบข้อบังคับของบริษัทฯ มิได้ และพนักงานต้องปฏิบัติตามนโยบาย / ข้อกำหนด / ข้อบังคับ / คำแนะนำที่บริษัทฯ กำหนดไว้ รวมถึงที่จะกำหนดขึ้นในอนาคต และหากไม่ปฏิบัติตามจะถือเป็นความผิดตามระเบียบของบริษัทฯ
2. พนักงานทุกคนมีสิทธิใช้ระบบเครือข่ายและคอมพิวเตอร์ และระบบข้อมูล ภายใต้นโยบายและข้อกำหนดนี้ การฝ่าฝืน จนเป็นเหตุหรืออาจเป็นเหตุให้เกิดความเสียหายแก่บริษัทฯ หรือบุคคลหนึ่งบุคคลใด บริษัทฯ จะพิจารณาดำเนินการทางวินัยและกฎหมายแก่พนักงานที่ฝ่าฝืนตามความเหมาะสม
3. บริษัทฯ จัดให้มีการลงทะเบียนบัญชีชื่อผู้ใช้งาน (Account) ซึ่งประกอบด้วย ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้กับพนักงานที่มีหน้าที่เกี่ยวข้องกับการใช้งานระบบเครือข่ายและคอมพิวเตอร์ ระบบข้อมูล และระบบอินเทอร์เน็ต (Internet) เป็นรายบุคคลและมีกฎระเบียบในการใช้งานรหัสผ่าน (Password) เช่น จำนวนของตัวอักษรต้องไม่น้อยกว่า 8 ตัว และไม่ควรเป็นคำที่เดาได้ง่าย ระยะเวลาที่ต้องเปลี่ยนรหัสผ่านทุก ๆ 90 วัน หรือตามความเหมาะสมของระบบนั้น ๆ พนักงานที่เข้าใช้ระบบเครือข่ายและคอมพิวเตอร์ต้องทำการลงบันทึกเข้า (Login) เพื่อใช้ในการพิสูจน์ยืนยันตัวตน (Authentication) ของพนักงานเอง และเมื่อทำงานเสร็จต้องทำการลงบันทึกออก (Logout) จากระบบทุกครั้ง ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม และรักษาสิทธิในการใช้พื้นที่ และข้อมูลเอกสารของพนักงาน
4. รหัสผ่าน (Password) ของพนักงาน ถือเป็นสินทรัพย์ของบริษัทฯ ไม่อนุญาตให้มีการบอกรหัสผ่าน (Password) ที่ถือเป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และไม่อนุญาตให้ใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ร่วมกัน หากมีความจำเป็นต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร และพนักงานทุกคนมีหน้าที่ในการป้องกันรหัสผ่าน (Password) อย่างเคร่งครัด
5. พนักงานอาจจะได้รับมอบหมายให้เข้าใช้ระบบงานอื่น ๆ ที่บริษัทฯ กำหนดให้ใช้ จะต้องปฏิบัติตามกฎการใช้ระบบและเก็บรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ไว้ ห้ามมิให้เปิดเผยกับบุคคลอื่นยกเว้นได้รับอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร
6. หากมีการยกเลิกบัญชีชื่อผู้ใช้งาน (Account) ให้พนักงานแจ้งกับผู้บังคับบัญชา และทำเรื่องขอยกเลิกบัญชีผู้ใช้งานโดยจะต้องกระทำทันทีที่เลิกใช้งาน

.../9

7. พนักงานพึงใช้ทรัพยากรระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ อย่างมีประสิทธิภาพ ไม่ก่อให้เกิดความหนาแน่นของระบบเครือข่ายและคอมพิวเตอร์ และไม่ดาวน์โหลด (Download) หรืออัปโหลด (Upload) ข้อมูลหรือสิ่งอื่นใดที่ไม่เกี่ยวข้องกับการทำงาน หรือใช้ Website ที่ไม่เกี่ยวข้องกับการทำงานหรือการดำเนินงานของบริษัทฯ
8. พนักงานพึงใช้ข้อความสุภาพ และ/หรือใช้ข้อความที่วิญญูชนพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น รวมทั้งปฏิบัติให้ถูกต้องตามธรรมเนียมปฏิบัติของการใช้ระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ
9. พนักงานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้ระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ โดยเฉพาะอย่างยิ่งไม่พึงอนุญาตให้บุคคลอื่นเข้าใช้ระบบเครือข่ายและคอมพิวเตอร์จากบัญชีชื่อผู้ใช้งาน (Account) ของตนเอง
10. เพื่อป้องกันหากมีบุคคลอื่นล่วงรู้และนำรหัสผ่าน (Password) ของพนักงานไปใช้ในทางที่ผิดและเกิดความเสียหายต่อบริษัทฯ พนักงานจะต้องเก็บรหัสผ่าน (Password) ไว้เป็นความลับ ไม่จดบันทึกรหัสผ่าน (Password) ไว้ในที่สามารถมองเห็นได้ง่าย และไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่
11. เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ ถือเป็นสินทรัพย์ของบริษัทฯ พนักงานมีหน้าที่ดูแลรักษาให้อยู่ในสภาพที่สมบูรณ์และสามารถใช้งานได้ปกติ และไม่กระทำการใด ๆ ที่สุ่มเสี่ยงให้เกิดความเสียหาย หรือไม่มั่นใจว่าจะปลอดภัย
12. ห้ามพนักงานติดตั้ง หรือดัดแปลงเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ หรือพัฒนาโปรแกรมซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมถึงทรัพยากรระบบ เพื่อใช้ในการลดขีดความสามารถระบบ หรือทำลายกลไกรักษาความปลอดภัย หรือเพื่อทำให้ได้ใช้ทรัพยากรเพิ่มขึ้น หรือพยายามที่จะเปลี่ยนข้อจำกัดของสิทธิในการเข้าใช้ทรัพยากรระบบไปจากที่ได้รับอนุญาต
13. เพื่อความปลอดภัยในการใช้ระบบเครือข่ายคอมพิวเตอร์ หากพนักงานพบไวรัสคอมพิวเตอร์ (Computer Virus) จะต้องแจ้งให้เจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศดำเนินการกำจัดไวรัสคอมพิวเตอร์ (Computer Virus) โดยเร็ว
14. พนักงานพึงลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน เพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล
15. พนักงานพึงให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์ ในการตรวจสอบความปลอดภัยของระบบเครือข่ายและคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำที่เกี่ยวข้องกับความปลอดภัยในระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ

.../10

16. ห้ามพนักงานใช้ระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ เพื่อการดังต่อไปนี้

16.1 การกระทำเพื่อการอื่นใดนอกเหนือจากวัตถุประสงค์ในการปฏิบัติงาน หรือตามที่ได้รับอนุญาตจากบริษัทฯ เช่น ใช้เพื่อประโยชน์ธุรกิจของตนเองหรือบุคคลอื่น

16.2 การกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

16.3 การกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

16.4 การค้าหรือแสวงหาผลกำไร หรือผลประโยชน์ส่วนตัว

16.5 การเปิดเผยข้อมูลที่เป็นความลับ ซึ่งได้มาจากการปฏิบัติงานให้บริษัทฯ ไม่ว่าจะเป็นข้อมูลของบริษัทฯ พนักงาน หรือบุคคลภายนอกก็ตาม

16.6 การกระทำอันมีลักษณะเป็นการละเมิดสิทธิ์ หรือเข้าไปใช้ทรัพยากรคอมพิวเตอร์ของบุคคลอื่นที่เชื่อมต่อกับระบบเครือข่ายและคอมพิวเตอร์ หรือระบบอินเตอร์เน็ต (Internet)

16.7 การกระทำอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของบริษัทฯ หรือบุคคลอื่น

16.8 การกระทำเพื่อให้ได้มาซึ่งข้อมูลข่าวสารของบุคคลอื่น โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูลหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

16.9 การรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายแก่บริษัทฯ หรือบุคคลอื่น เช่น การนำเข้าหรือส่งต่อข้อมูลอันเป็นเท็จ การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ การรับหรือส่งข้อมูลอันมีลักษณะเป็นการละเมิดต่อกฎหมาย หรือละเมิดสิทธิของบุคคลอื่น เป็นต้น

16.10 การกระทำเพื่อการเผยแพร่ภาพ ตัดต่อ หรือดัดแปลงด้วยวิธีการอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่ทำให้บริษัทฯ หรือบุคคลอื่นเสียหายหรือเสียชื่อเสียง หรือให้ได้รับความอับอาย

16.11 การขัดขวางการใช้งานระบบเครือข่ายและคอมพิวเตอร์ของพนักงานอื่น หรือทำให้ระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ ไม่สามารถใช้งานได้ตามปกติ

16.12 การแสดงความเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของบริษัทฯ ไปยังที่อยู่เว็บไซต์ (Website) ใด ๆ ในลักษณะที่อาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง หรือก่อให้เกิดความเสียหายแก่บริษัทฯ หรือบุคคลอื่น

16.13 การอื่นใดที่อาจขัดต่อผลประโยชน์ของบริษัทฯ หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่บริษัทฯ

17. การเข้าใช้งานซอฟต์แวร์ (Software) โปรแกรมหรือแอปพลิเคชัน (Application) ต่าง ๆ จะต้องได้รับอนุญาตและความเห็นชอบจากผู้บังคับบัญชาของพนักงาน และต้องเป็นซอฟต์แวร์ (Software) โปรแกรมหรือแอปพลิเคชัน (Application) ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

.../11

18. ห้ามมิให้พนักงานนำซอฟต์แวร์ (Software) โปรแกรมหรือแอปพลิเคชัน (Application) ใด ๆ มาติดตั้งบนเครื่องคอมพิวเตอร์รวมถึงอุปกรณ์ประกอบอื่น ๆ นอกเหนือจากที่บริษัทฯ ได้จัดไว้ให้ กรณีมีความจำเป็นต้องใช้งานเพิ่มเติม ให้แจ้งเจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศเป็นผู้ดำเนินการ โดยได้รับอนุญาตและความเห็นชอบจากผู้บังคับบัญชาโดยตรงของพนักงาน
19. จดหมายอิเล็กทรอนิกส์ (e-mail) ของบริษัทฯ (@wacoal.co.th) ให้ใช้เพื่อกิจการงานของบริษัทฯ เท่านั้น ห้ามมิให้พนักงานส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ก่อให้เกิดการรบกวน (Spam/Junk) ระบบเครือข่ายและคอมพิวเตอร์ของบุคคลอื่น หรือการแนบไฟล์ที่มีไวรัสคอมพิวเตอร์ (Computer Virus) แอบแฝงหรือส่งแบบกระจายถึงบุคคลอื่นโดยไม่จำเป็น อันจะก่อให้เกิดความเสียหายต่อผู้รับ หรือส่งผลกระทบโดยรวมกับระบบเครือข่ายและคอมพิวเตอร์ หากพนักงานฝ่าฝืนใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ไปในทางที่ไม่ถูกต้องนอกเหนือจากการใช้งานสำหรับการดำเนินงานของบริษัทฯ ถ้าเป็นการกระทำที่ขัดต่อกฎหมายที่กำหนดไว้ และมีความผิดตามระเบียบข้อบังคับของบริษัทฯ พนักงานต้องเป็นผู้รับผิดชอบต่อความเสียหายที่เกิดขึ้น
20. การสืบค้นและเรียกใช้ทรัพยากรของระบบข้อมูล และระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ เป็นสิทธิที่จัดเตรียมไว้เฉพาะพนักงาน ทั้งนี้ สิทธิดังกล่าวอาจมอบให้กับบุคคลภายนอก โดยให้เป็นไปตามดุลพินิจของผู้บังคับบัญชาเท่านั้น
21. การใช้ระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ ต้องเป็นไปตามนโยบายความมั่นคงปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ของบริษัทฯ และกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง
22. พนักงานที่มีสิทธิเข้าใช้ระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ จำเป็นต้องปฏิบัติตามข้อกำหนด ขั้นตอน วิธีปฏิบัติในการใช้งานระบบเครือข่ายและคอมพิวเตอร์อย่างเคร่งครัดโดยทั่วกัน
23. หากพบว่ามีการส่งข้อมูลที่ผิดต่อกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง ให้แจ้งต่อผู้บังคับบัญชา และผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์ หรือเจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศ

.../ 12

หมวดที่ 4

ข้อปฏิบัติสำหรับเจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศ

1. ข้อปฏิบัติสำหรับผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์

1.1 มีหน้าที่ในการควบคุมดูแลบำรุงรักษาและปรับปรุงพัฒนาระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ กรณีพบความผิดปกติเกิดขึ้นในระบบฯ ผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์มีอำนาจระงับการใช้งานระบบเครือข่ายและคอมพิวเตอร์ เพื่อป้องกันความเสียหายได้

1.2 ตรวจสอบการใช้งานระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ เพื่อให้เป็นไปตามนโยบายความมั่นคงปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ หรือปฏิบัติตามคำสั่งของผู้บังคับบัญชาระดับฝ่ายของศูนย์เทคโนโลยีสารสนเทศในการระงับการใช้งานระบบเครือข่ายและคอมพิวเตอร์ของพนักงาน ในกรณีที่อาจจะก่อให้เกิดความเสียหายต่อบริษัทฯ

1.3 ไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึง รับหรือส่งข้อมูลที่รับผ่านระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ได้รับอนุญาตเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

1.4 จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยถือปฏิบัติตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง

1.5 จัดเทียบเวลามาตรฐานสำหรับระบบคอมพิวเตอร์ให้เป็นไปตามที่กฎหมายกำหนด

1.6 ควบคุมดูแลซอฟต์แวร์ (Software) และโปรแกรมต่างๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ส่วนของพนักงานให้ถูกต้องตามลิขสิทธิ์ของซอฟต์แวร์ (Software) หรือโปรแกรมที่ติดตั้งอยู่

1.7 ปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ ตามที่ผู้บังคับบัญชาระดับฝ่ายของศูนย์เทคโนโลยีสารสนเทศมอบหมาย

1.8 บริษัทฯ เคารพในสิทธิความเป็นส่วนตัวของพนักงานทุกคน และบริษัทฯ ขอสงวนสิทธิให้ผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์ที่ได้รับมอบหมาย ดูแลตรวจสอบการใช้งานระบบเครือข่ายและคอมพิวเตอร์ของพนักงาน เพื่อให้เป็นไปตามนโยบายนี้

2. ข้อปฏิบัติสำหรับผู้ดูแลระบบข้อมูล

2.1 พัฒนา ปรับปรุง และบำรุงรักษาระบบข้อมูล รวมทั้งระบุข้อกำหนดความปลอดภัย

2.2 กำหนดสิทธิการใช้งานของระบบข้อมูล ก่อนการใช้งาน

.../13

2.3 ควบคุมการติดตั้งซอฟต์แวร์ (Software) ต่าง ๆ ลงในระบบข้อมูล หรือในเครื่องคอมพิวเตอร์ของพนักงาน โดยไม่ให้กระทบต่อระบบหลัก หรือก่อให้เกิดความเสียหายต่อระบบรวม

2.4 ระงับการใช้งานระบบข้อมูลของพนักงาน เมื่อมีการตรวจสอบพบว่าใช้งานไม่ถูกต้องหรือละเมิดข้อตกลงการใช้งาน หรือไม่ถูกต้องตามกฎหมาย

2.5 ปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับระบบข้อมูลตามที่ผู้บังคับบัญชาระดับฝ่ายของศูนย์เทคโนโลยีสารสนเทศมอบหมาย

3. ข้อปฏิบัติสำหรับผู้พัฒนาซอฟต์แวร์และฮาร์ดแวร์

3.1 บริษัทฯ สนับสนุนการวิจัยและการค้นคว้า เพื่อสร้างความรู้ทางวิชาการทางด้านซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) แก่ผู้พัฒนาซอฟต์แวร์และฮาร์ดแวร์ หากว่าซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) นั้นไม่ส่งผลกระทบหรือสร้างปัญหาต่อระบบเครือข่ายและคอมพิวเตอร์ และบริษัทฯ เป็นเจ้าของลิขสิทธิ์ในโปรแกรม ชุดคำสั่ง ซอฟต์แวร์ (Software) หรือฮาร์ดแวร์ (Hardware) ที่ผู้พัฒนาซอฟต์แวร์และฮาร์ดแวร์พัฒนาขึ้นในระหว่างที่เป็นพนักงานของบริษัทฯ

3.2 ไม่พัฒนาโปรแกรม ชุดคำสั่ง ซอฟต์แวร์ (Software) หรือฮาร์ดแวร์ (Hardware) ใด ๆ เพื่อทำลายระบบรักษาความปลอดภัยสำหรับระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ ทำให้ไม่สามารถใช้งานได้ตามปกติ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน (Password) ลักลอบทำสำเนาข้อมูลของบุคคลอื่น หรือแกะรหัสผ่าน (Password) ของบุคคลอื่น หรือทำให้มีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรในระบบเครือข่ายและคอมพิวเตอร์ รวมถึงการควบคุมหน้าจอ แป้นพิมพ์ เมาส์ และข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์อื่นของบริษัทฯ

3.3 ไม่พัฒนาโปรแกรม ชุดคำสั่ง ซอฟต์แวร์ (Software) หรือฮาร์ดแวร์ (Hardware) ใด ๆ ที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่น ในลักษณะเช่นเดียวกับ โปรแกรมประสงค์ร้าย (Malware) หรือไวรัสคอมพิวเตอร์ (Computer Virus) หรือตัวโปรแกรมที่จะทำลายระบบข้อมูลและระบบเครือข่ายและคอมพิวเตอร์ หรือจำกัดสิทธิในการใช้ซอฟต์แวร์ (Software) ของบริษัทฯ

3.4 เจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศที่มีหน้าที่พัฒนาเว็บไซต์ (Website) ต้องไม่นำเสนอข้อมูลที่ผิดกฎหมาย หรือละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา หรือแสดงข้อความ รูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงาม

3.5 เจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศที่มีหน้าที่พัฒนาเว็บไซต์ (Website) ที่เกี่ยวข้องกับ Web Board หรือ Web Blog ต้องตรวจสอบการเข้าใช้งานและจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตามที่กฎหมายกำหนด

.../14

นโยบายความมั่นคงปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ฉบับนี้ ให้ถือเป็นส่วนหนึ่งของข้อบังคับเกี่ยวกับการทำงานของ บริษัท ไทยวาโก้ จำกัด (มหาชน) และดำเนินการประกาศให้พนักงานรับทราบและปฏิบัติตาม รวมถึงให้มีการตรวจสอบและควบคุมให้มีการปฏิบัติตามนโยบายนี้อย่างเคร่งครัด หากมีการฝ่าฝืน เพิกเฉย ไม่ปฏิบัติตาม ให้ดำเนินมาตรการทางวินัยตามข้อบังคับเกี่ยวกับการทำงานต่อไป

นโยบายความมั่นคงปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ฉบับนี้ได้รับอนุมัติโดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2569 เมื่อวันที่ 28 มกราคม 2569 มีผลใช้บังคับตั้งแต่วันที่ 1 กุมภาพันธ์ 2569 เป็นต้นไป และให้ยกเลิกนโยบายความมั่นคงปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ ฉบับลงวันที่ 1 มกราคม 2568

(นายธรรมรัตน์ โชควัฒนา)
ประธานกรรมการบริษัท