นโยบายการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ

บริษัท พริมา มารีน จำกัด (มหาชน) และบริษัทย่อย

ฉบับ 2568

PRIMA MARINE
PUBLIC COMPANY LIMITED

นโยบายการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ

บริษัท พริมา มารีน จำกัด (มหาชน) (“**บริษัทฯ**”) ตระหนักถึงความสำคัญของการนำระบบเทคโนโลยีสารสนเทศเข้ามาสนับสนุนเพื่อเพิ่มประสิทธิภาพในการดำเนินงานได้เป็นอย่างดี แต่เมื่อระบบสารสนเทศไม่สามารถให้บริการได้หรือมีความผิดพลาดในการให้บริการไม่ว่าด้วยสาเหตุใดก็ตาม อาจส่งผลให้การดำเนินงานด้านระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ไม่สามารถทำงานได้อย่างต่อเนื่อง และไม่มีความปลอดภัย ซึ่งอาจส่งผลกระทบต่อชื่อเสียงหรือความน่าเชื่อถือ ผู้ใช้งานทุกคนต้องร่วมมือกันป้องกันไม่ให้เกิดความเสียหายหรือลดโอกาสที่จะเกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ ดังนั้น บริษัทฯ จึงได้กำหนดข้อตกลงว่าด้วยการรักษาความมั่นคงปลอดภัย ดังนี้

1. การวางแผนและจัดการเรื่องความปลอดภัยของข้อมูล

บริษัทฯ ทำการวางแผนการจัดการความปลอดภัยของข้อมูล เครื่องมือ อุปกรณ์ของระบบสารสนเทศ และโครงข่ายคอมพิวเตอร์ของบริษัทฯ ให้อยู่ในระบบมาตรฐานซึ่งเป็นที่ยอมรับในระดับสากล เชื่อถือได้ โดยมีการเฝ้าติดตาม ตรวจสอบความสามารถของระบบอยู่สม่ำเสมอ

2. การเก็บรักษาความปลอดภัยของข้อมูล

บริษัทฯ เล็งเห็นความสำคัญของการรักษาความปลอดภัยของข้อมูล โดยระบุการรักษาความลับและการรักษาความปลอดภัยของข้อมูลแต่ละการให้บริการกับลูกค้าไว้เป็นส่วนหนึ่งของสัญญาการให้บริการที่บริษัทฯ จัดทำกับลูกค้า ไม่ว่าจะเป็นการบริการประเภทใด ซึ่งทางบริษัทฯ และพนักงานทุกคนจะต้องถือปฏิบัติตามโดยเคร่งครัด

3. มาตรการเกี่ยวกับการจัดการความปลอดภัยของข้อมูล

พนักงานทุกระดับชั้นที่มีส่วนเกี่ยวข้องกับขอบข่ายการรับรองระบบมาตรฐานความมั่นคงปลอดภัยสาระสนเทศมีหน้าที่ต้องปฏิบัติตามกฎระเบียบและ/หรือนโยบายของบริษัทฯ หากมีการฝ่าฝืนให้ถือว่าเป็นการกระทำผิดวินัยอย่างร้ายแรง โดยบริษัทฯ ถือว่าเป็นหน้าที่ที่พนักงานทุกคนจะต้องทราบถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล และมีการจัดอบรมสื่อสารให้พนักงานใหม่รับทราบด้วย

4. การอนุญาตให้ใช้งานระบบเครือข่าย/อินเทอร์เน็ต

4.1 ผู้ใช้งานต้องใช้งานระบบเครือข่าย/อินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัทฯ และบุคคลผู้ที่เกี่ยวข้องเสื่อมเสียชื่อเสียงหรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย โดยการใช้งานระบบเครือข่าย/อินเทอร์เน็ตในทางที่ผิด จัดถือว่าเป็นความผิดทางวินัยและอาจถูกดำเนินคดีตามกฎหมาย

4.2 ไม่อนุญาตให้ใช้เครื่องส่วนตัวของพนักงานเข้ามาใช้ระบบอินเทอร์เน็ตของบริษัทฯ ในกรณีที่มีความให้ขอความยินยอมจากหัวหน้างาน

4.3 ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสม หรือผิดกฎหมาย โดยเฉพาะการใช้งานระบบเครือข่าย/ อินเทอร์เน็ตในทางที่ผิด จัดถือได้ว่าเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมายขึ้นมาตามลำดับ

4.4 เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า Website ที่เข้าถึงมีความไม่ปลอดภัย ผู้ใช้งานต้องระงับการเข้าถึง Website ดังกล่าวโดยทันที หรือถ้ามีความจำเป็นต้องเข้าให้แจ้งหน่วยงานที่รับผิดชอบ

4.5 บริษัทไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบเว็บบอร์ด หรือบล็อกของผู้ใช้งาน โดยความเสียหายใดๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือว่าเป็นความรับผิดชอบของผู้ใช้งานผู้นั้นๆ (เฉพาะรายบุคคล)

5. การอนุญาตให้ใช้อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล

เพื่อเป็นแนวทางการป้องกัน ควบคุม และคุ้มครองผู้ใช้งานจากการใช้งานระบบซอฟแวร์ ข้อมูลและอุปกรณ์สื่อสารอิเลคทรอนิคส์แบบไร้สายสารสนเทศ อาทิ โทรศัพท์มือถือ สมาร์ทโฟน แท็บเล็ต เครื่องคอมพิวเตอร์แบบพกพา ผิดจากวัตถุประสงค์การใช้งานที่กำหนดหรือกิจกรรมที่ไม่ประสงค์

5.1 คอมพิวเตอร์แบบพกพา

5.1.1 ใช้งานจะต้องดูแลรักษาคอมพิวเตอร์แบบพกพาอย่างใกล้ชิด ผู้ใช้งานควรพึงระลึกไว้เสมอว่าความเสียหายที่เกิดขึ้นเมื่อมีการสูญหาย หรือโดนขโมยคอมพิวเตอร์แบบพกพาไป จะส่งผลกระทบทั้งในแง่ของทรัพย์สินและข้อมูลที่อยู่ในคอมพิวเตอร์แบบพกพา ยิ่งมีการเก็บข้อมูลสำคัญในคอมพิวเตอร์แบบพกพามากเท่าไหร่ยิ่งมีโอกาสก่อให้เกิดปัญหาตามมามากขึ้นเท่านั้น ยังไม่รวมถึงการเก็บข้อมูลที่เกี่ยวข้องกับองค์กร เช่น อีเมลซึ่งจะส่งผลกระทบกับองค์กรโดยตรง เพราะฉะนั้นผู้ใช้งานควรมีความรอบคอบและระวังรักษาคอมพิวเตอร์แบบพกพาอย่างใกล้ชิด

5.1.2 ผู้ใช้งานจะต้องตั้งค่าการล็อกคอมพิวเตอร์แบบพกพาเมื่อไม่ใช้งาน แม้การล็อกการใช้งานคอมพิวเตอร์แบบพกพา จะไม่ได้เป็นการป้องกันการเข้าถึงข้อมูลที่ได้ผลร้อยเปอร์เซ็นต์ แต่ก็สามารถเป็นแนวทางเบื้องต้นในการชะลอหรือป้องกันการเข้าถึงข้อมูลสำคัญบนโทรศัพท์มือถือจากผู้ไม่หวังดี ซึ่งอาจจะเกิดจากการถูกขโมย หรือผู้ใช้หลงลืม คอมพิวเตอร์แบบพกพา และยังเป็นแนวทางที่ผู้ใช้งานสามารถทำได้การใส่ Password เข้าเครื่องโดยต้องปฏิบัติตามข้อกำหนดของบริษัทฯ

5.1.3 ผู้ใช้งานจะต้องเก็บเฉพาะข้อมูลที่จำเป็นในคอมพิวเตอร์แบบพกพา การเก็บข้อมูลควรพิจารณาถึงความสำคัญและความเหมาะสมของข้อมูลที่จะจัดเก็บ ไม่ควรเก็บข้อมูลที่มีความสำคัญมากๆ เช่น ข้อมูลบัตรเครดิต หรือข้อมูลรหัสผ่านสำหรับล็อกอินเข้าใช้งานระบบ เนื่องจากหากโทรศัพท์เกิดสูญหาย หรือโดนผู้ประสงค์ร้ายลักลอบขโมยไปได้ อาจทำให้เกิดความเสียหายที่รุนแรงมากกว่าเดิม

5.1.4 เมื่อผู้ใช้งานทำคอมพิวเตอร์แบบพกพาหาย หรือ ถูกโจรกรรม ให้รีบแจ้งหน่วยงานที่รับผิดชอบภายใน 24 ชั่วโมง เพื่อดำเนินการป้องกันการรั่วไหลของข้อมูล หรือการถูกคุกคามจากภายนอก

5.1.5 ห้ามผู้ใช้งานขัดขวางหรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส หรืออื่นๆ ที่เกี่ยวข้อง

5.1.6 ผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Notebook Palmtops Laptop) และอุปกรณ์สื่อสารอื่นๆ อาทิ เมื่อปฏิบัติงานอยู่นอกสถานที่ ได้แก่ ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง ต้องใส่รหัสผ่านป้องกันข้อมูลที่สำคัญ

5.2 การอนุญาตให้ใช้งานมือถือ

5.2.1 ผู้ใช้งานจะต้องดูแลรักษาโทรศัพท์มือถืออย่างใกล้ชิด ผู้ใช้งานควรพึงระลึกไว้เสมอว่าความเสียหายที่เกิดขึ้นเมื่อมีการสูญหาย หรือโดนขโมยโทรศัพท์มือถือไป จะส่งผลกระทบทั้งในแง่ของทรัพย์สินและข้อมูลที่อยู่ในโทรศัพท์มือถือ ยิ่งมีการเก็บข้อมูลสำคัญในโทรศัพท์มือถือมากเท่าไหร่ยิ่งมีโอกาสก่อให้เกิดปัญหาตามมามากขึ้นเท่ากัน ยังไม่รวมถึงการเก็บข้อมูลที่เกี่ยวข้องกับองค์กร เช่น อีเมลซึ่งจะส่งผลกระทบกับองค์กรโดยตรง เพราะฉะนั้นผู้ใช้งานควรมีความรอบคอบและระวังรักษาโทรศัพท์มือถืออย่างใกล้ชิด

5.2.2 ผู้ใช้งานจะต้องตั้งค่าการล็อกโทรศัพท์มือถือเมื่อไม่ใช้งาน แม้การล็อกการใช้งาน โทรศัพท์มือถือ จะไม่ได้เป็นการป้องกันการเข้าถึงข้อมูลที่ได้ผลร้อยเปอร์เซ็นต์ แต่ก็สามารถเป็นแนวทางเบื้องต้นในการชะลอหรือป้องกันการเข้าถึงข้อมูลสำคัญบนโทรศัพท์มือถือจากผู้ไม่หวังดี ซึ่งอาจจะเกิดจากการถูกขโมยโทรศัพท์มือถือ และยังเป็นแนวทางที่ผู้ใช้งานสามารถทำได้โดยง่าย ซึ่งกระบวนการดังกล่าวสามารถทำได้โดยการตั้งค่า Pin หรือรหัสผ่านบนโทรศัพท์มือถือนั้นๆ โดยการล็อคนั่นสามารถทำได้หลายวิธี เช่น การใส่ Password เข้าเครื่อง การตั้งค่า รูปแบบ เส้นต่อเส้น (Line Pattern) ใช้ Bio Authentication ลายนิ้วมือ หรือเรตินาหรืออย่างใดอย่างหนึ่ง

5.2.3 ผู้ใช้งานจะต้องติดตั้งโปรแกรมในโทรศัพท์มือถือเท่าที่จำเป็นและจากแหล่งที่มาที่น่าเชื่อถือ แม้ระบบปฏิบัติการบนโทรศัพท์มือถือทั่วไปจะอนุญาตให้สามารถติดตั้งโปรแกรมเสริมเพื่ออำนวยความสะดวกในการใช้งานมากขึ้น แต่ก็มีความเสี่ยงที่ผู้ใช้งานจะเจอกับโปรแกรมที่มีความสามารถในการขโมยข้อมูลหรือโปรแกรมไม่พึงประสงค์ต่างๆ ตามที่ได้กล่าวไว้ในหัวข้อภัยคุกคาม เพราะฉะนั้นทางป้องกันที่ดีที่สุดคือดาวน์โหลดเฉพาะโปรแกรมที่จำเป็นจริงๆ และพิจารณาดาวน์โหลดจากเว็บไซต์ของผู้พัฒนาเท่านั้น หรือดาวน์โหลดจากแหล่งดาวน์โหลดที่ได้รับการควบคุมและรับรองความปลอดภัยจากผู้พัฒนาระบบปฏิบัติการเช่น Android Market สำหรับระบบปฏิบัติการ Android หรือ App Store สำหรับระบบปฏิบัติการ iOS

5.3 การปฏิบัติงานจากระยะไกล (Teleworking)

ในการทำงานจากระยะไกล Remote Working บริษัทฯ อนุญาตให้ใช้ผ่านระบบ VPN และ Remote Desktop เท่านั้น โดยสามารถเข้าถึงระบบได้ตามที่บริษัทฯ กำหนด โดยสืบเนื่องจากการป้องกันภัยคุกคามจากภายนอก ซึ่งมีความเสี่ยงที่จะทำให้เกิดความไม่ปลอดภัยในการบริการของบริษัทฯ ซึ่งประกอบไปด้วย การป้องกันความลับการเป็นส่วนบุคคล, การถูกต้องของข้อมูล และความพร้อมใช้ของระบบบริษัทฯ จึงได้พัฒนาระบบการเข้าถึงการให้บริการภายในซึ่งได้แก่ ระบบ ERP Microsoft Dynamic AX BassNet HRMS และ ระบบ File Sharing โดยสามารถเข้าใช้งานผ่านระบบ VPN ซึ่งมีความมั่นคงปลอดภัยสูง

6. การอนุญาตให้ใช้งานซอฟต์แวร์ประยุกต์ทางด้านธุรกิจ (Core Business Software)

6.1 ผู้ใช้งานซอฟต์แวร์ทั้งหมดของบริษัทฯ ต้องมี User Login เป็นของตนเอง

6.2 ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นใช้สิทธิ (User/Password Login) ของตนโดยเด็ดขาด ถ้ามีความผิดพลาดเกิดขึ้นเจ้าของสิทธิต้องเป็นผู้รับผิดชอบ

6.3 ผู้ใช้งานห้ามนำข้อมูลในระบบซอฟต์แวร์ไปเปิดเผยโดยไม่ได้รับอนุญาต

6.4 ห้ามผู้ใช้งานใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัทฯ กระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม

6.5 ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

6.6 ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่

6.7 ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัท โดยเด็ดขาด

6.8 เพื่อที่จะให้เกิดความแน่ใจว่าพนักงานและเจ้าหน้าที่ มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือพลั้งเผลอ จึงไม่ควรจะทำสำเนาซอฟต์แวร์ใดๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัทฯ เพื่อจุดประสงค์ใดๆ ก็ตาม โดยที่ไม่ได้รับอนุญาต

7. มาตรฐานรูปแบบการกำหนดการตั้งค่ารหัสส่วนตัว

7.1 รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย ห้ามใช้ บัญชีรายชื่อ (Account) ร่วมกันหรือให้ผู้อื่นเข้าใช้งานบัญชีรายชื่อ (Account) ของตนโดยเด็ดขาด ทั้งนี้รวมถึงสมาชิกในครอบครัวเมื่อผู้ใช้งานนำงานกลับไปทำที่บ้านด้วย

7.2 รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้ใน “เอกสารขั้นตอนการปฏิบัติงานมาตรฐานการใช้รหัสผ่าน (Password Standard)”

7.3 รหัสผ่านต้องมีความมั่นคงปลอดภัยตามที่ได้กำหนดไว้ใน “เอกสารขั้นตอนการปฏิบัติงานมาตรฐานการใช้รหัสผ่าน (Password Standard)”

7.4 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่กระทำผ่าน User ID และรหัสผ่านของตนทั้งหมด

7.5 หากผู้ใช้งานสงสัยว่า User ID หรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อหน่วยงานที่รับผิดชอบและทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที

7.6 วิธีการตั้งค่ารหัสผ่านมีแนวทางในการดำเนินการดังต่อไปนี้

8. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

8.1 ต้องจัดหาที่ตั้งห้อง Server หรือ Data Center Room ที่มีสภาพแวดล้อมภายนอกปลอดภัยจากภัยคุกคามภายนอก คืออยู่ในสถานที่ๆ เข้าถึงได้โดยยากจากบุคคลภายนอก อยู่บนอาคารสูงที่สามารถป้องกันเหตุจากน้ำท่วมได้พื้นที่โดยรอบโปร่ง และสามารถมองเห็นได้ชัดหากมีการเข้าถึงห้อง Server

8.2 จัดห้อง Server หรือ Data Center Room ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ส่วนเครื่องสำรองไฟฟ้า (UPS Zone) ส่วนแบตเตอรี่เครื่องสำรองไฟฟ้า (Battery UPS Zone) เป็นต้น เพื่อความสะดวกในการปฏิบัติงานและทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น

8.3 หน่วยงานที่ดูแลพื้นที่ ต้องควบคุมการเข้า-ออกทางกายภาพของพื้นที่ที่กำหนดให้เป็นพื้นที่ควบคุมพิเศษ เช่น ห้อง Server โดยอนุญาตให้บุคคลผ่านเข้า-ออกพื้นที่ควบคุมพิเศษได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยมีการจัดเตรียมอุปกรณ์รักษาความปลอดภัยในการเข้าถึงห้อง Server ดังนี้

1) มีการติดตั้งกล้องวงจรปิด และบันทึกภาพภายในห้องตลอดเวลา โดยสามารถดูข้อมูลย้อนหลังได้

2) ห้อง Server หรือ Data Center เป็นห้องระบบล็อคที่มีระบบที่สามารถตรวจสอบการระบุตัวตน ซึ่งจำกัดสิทธิการเข้าถึงเฉพาะผู้ที่ได้รับการอนุญาตเท่านั้น

8.4 การป้องกันความเสียหาย

8.4.1 ระบบป้องกันไฟไหม้

ต้องมีระบบป้องกันอัคคีภัย เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลาร

8.4.2 ระบบป้องกันไฟฟ้าขัดข้อง

ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า มีระบบสำรองไฟฟ้าสำหรับระบบงานคอมพิวเตอร์ที่สำคัญ และระบบเครือข่ายคอมพิวเตอร์ เพื่อให้การดำเนินงานมีความต่อเนื่อง

8.4.3 ระบบควบคุมอุณหภูมิและความชื้น

ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

8.4.4 ระบบเตือนภัยน้ำรั่ว

ในกรณีที่มีการยกระดับพื้นของ ห้อง Server หรือ Data Center Room เพื่อติดตั้งระบบปรับอากาศ รวมทั้งเดินสายไฟและ/หรือ สายเครือข่ายด้านล่าง ควรติดตั้งระบบเตือนภัยน้ำรั่วบริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่ว

ทั้งนี้ ให้มีผลใช้บังคับตั้งแต่วันที่ 14 พฤษภาคม 2568 เป็นต้นไป

(นายบวร วงศ์สินอุดม)

ประธานกรรมการ

บริษัท พริมา มารีน จำกัด (มหาชน)