มาตรการรักษาความมั่นคงปลอดภัยข้อมูลในระบบสารสนเทศ

(Information Security Management System-ISMS)

บริษัท เมืองใหม่ กัตทรี จำกัด (มหาชน) และบริษัทในเครือ

ความมั่นคงปลอดภัยสารสนเทศให้มีผลบังคับใช้กับทรัพย์สินสารสนเทศที่ได้กำหนดไว้ในขอบเขต ผู้ทำหน้าที่ดูแลสินทรัพย์ ผู้ใช้สินทรัพย์ และผู้บริหารหรือฝ่ายบริหาร มีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามนโยบายอย่างเคร่งครัด ผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลสินทรัพย์จะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ ผู้ฝ่าฝืนนโยบายนี้มีความผิดและจะต้องได้รับการดำเนินการ ตามระเบียบของบริษัท เมืองใหม่ กัตทรี จำกัด (มหาชน) และบริษัทในเครือ

ทั้งนี้ทางบริษัท แจ้งกระบวนการคุ้มครองข้อมูลสารสนเทศ เอาไว้ดังต่อไปนี้

(1) กำกับดูแลรับผิดชอบด้านสารสนเทศของเมืองใหม่ กัตทรี จำกัด (มหาชน) และบริษัทในเครือ และรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นจากการละเลยการควบคุมความมั่นคงปลอดภัยสารสนเทศ

(2) สร้างความเข้าใจและให้การสนับสนุนการปฏิบัติงานของพนักงานภายในบริษัท ตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

(3) จัดให้มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงและแนวโน้มของความเสียงในอนาคตที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศของบริษัท

(4) จัดให้มีการประเมินแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ เพื่อนำไปปรับปรุงให้มีประสิทธิภาพในปีถัดไป

(5) นโยบายความมั่นคงปลอดภัยสารสนเทศต้องจัดทำเป็นลายลักษณ์อักษรตามวัตถุประสงค์ และขอบเขตงาน ที่ได้รับการอนุมัติจากผู้บริหารระดับสูงสุด (CEO) หรือผู้จัดการเทคโนโลยีสารสนเทศ (IT Manager) เพื่อประกาศใช้และถือปฏิบัติในบริษัท ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและสินทรัพย์สารสนเทศของบริษัท

(6) จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่พอเพียงต่อการบริหารจัดการด้านความมั่นคงปลอดภัยในแต่ละปีงบประมาณ ซึ่งรวมถึงแผนความมั่นคงปลอดภัยสารสนเทศที่จะดำเนินการในปีงบประมาณนั้นด้วย

(7) จัดให้มีการอบรมให้ความรู้ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้กับพนักงานในบริษัทและเจ้าหน้าที่ เพื่อสร้างความตระหนักและความเข้าใจภัยและผลกระทบที่เกิดขึ้นจากการใช้ระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์อย่างน้อยปีละ 1 ครั้ง

(8) จัดให้มีการตรวจสอบและประเมินความเสี่ยงในการปฏิบัติ ปีละ 1 ครั้ง และจัดให้มีการทำแผนการปรับปรุงฯ เพื่อทบทวนหรือแก้ไขปัญหาที่พบ

(10) กำหนดหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศและแผนฉุกเฉินภัยพิบัติของระบบเทคโนโลยีสารสนเทศของบริษัท

ความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Security)

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษา ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้อยู่ระดับมาตรฐานสากลโดย อ้างอิงจากกรอบมาตรฐานสากล ISO/IEC ๒๗๐๐๑ อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืน ระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศขององค์กร นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ ประกอบด้วย รายละเอียดดังต่อไปนี้

ความมั่นคงปลอดภัยของครือข่ายไร้สาย (Security of wireless networks)

(1) ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(2) ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point)

(3) ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือ องค์กรภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ขององค์กร

ความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall security)

(1) ฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของไฟร์วอลล์ภายในส่วนกลาง

(2) การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

(3) ทุกเส้นทางเชื่อมต่ออินเตอร์เน็ตผ่านระบบเครือข่ายขององค์กร ที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

3.1 การใช้งาน Web

3.2 การใช้งาน E-mail

3.3 การใช้งาน Instant Messaging

3.4 การใช้งาน Video Conference/Streaming

บริการอื่นนอกจากที่ระบุไว้ข้างต้นนี้ บริษัท ไม่อนุญาตให้ใช้งาน

(4) ข้อมูลจราจรทางคอมพิวเตอร์ที่ เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

(5) การกำหนดนโยบายในการให้บริการอินเตอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางองค์กรอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความความยินยอมจาก ฝ่ายเทคโนโลยีสารสนเทศและฝ่ายบริหารก่อน

(6) การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์ แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

(7) จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกเดือน หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

(8) ฝ่ายเทคโนโลยีสารสนเทศ มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่อง คอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

(9) ข้อกำหนดการลงโทษผู้ซึ่งมิได้ปฏิบัติตามนโยบายด้านความปลอดภัยของไฟร์วอลล์

12.1 ให้ดำเนินการกล่าวตักเตือนด้วยวาจากับผู้ใช้งาน

12.2 ในกรณีที่ผู้ใช้งานยังคงไม่ปฏิบัติตามนโยบายและยังคงปฏิบัติอยู่เช่นเดิม ให้ดำเนินการตักเตือนเป็นลายลักษณ์อักษรถึงผู้บังคับบัญชา

ความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (Email security)

(1) ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่ดูแลฝ่ายสารสนเทศ

(2) ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท มีวัตถุประสงค์เพื่อการใช้งาน ของบริษัทเท่านั้น ห้ามไม่ให้ผู้ใช้งานนำบัญชีจดหมายอิเล็กทรอนิกส์ (Email Account) ไปใช้นอกเหนือจากวัตถุประสงค์ที่บริษัทกำหนด

(3) เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (E-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ต้องเปลี่ยนรหัสผ่าน (Password) โดยทันที

(4) ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ หรือติดรหัสไว้หน้าเครื่องคอมพิวเตอร์

(5) ควรเปลี่ยนรหัสผ่าน (Password) อย่างน้อยทุก ๑ ปี

(6) ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-mail) ของตน

(7) การส่งจดหมายอิเล็กทรอนิกส์ จะต้องระบุชื่อ หัวข้อ ให้ชัดเจน ทั้งนี้เนื้อหาข้อความของจดหมายอิเล็กทรอนิกส์จะต้องสุภาพ ไม่ขัดต่อจริยธรรม ไม่เป็นการปลุกปั่น ยั่วยุ เสียดสี หรือส่อไปในทางผิดกฎหมาย

(8) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

(9) ไม่อนุญาตให้ผู้ใช้งาน จดหมายอิเล็กทรอนิกส์ (E-mail) ทุกคนนำข้อมูลที่เป็นความลับหรือข้อมูลที่มีความสำคัญขององค์กรส่งไปยังบุคคลที่ไม่เกี่ยวข้อง

(10) ห้ามส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของบริษัทฯ หรือก่อให้เกิดความเสียหายต่อบริษัทฯ

(11) ไม่อนุญาตให้ผู้ใช้งาน จดหมายอิเล็กทรอนิกส์ (E-mail) ทุกคนส่งข้อมูลหรือเผยแพร่ข้อมูล ข้อความ รูปภาพหรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคง หรือภาระกิจของทางบริษัท อันเป็นข้อมูลที่ผิดหรือขัดต่อกฎหมาย

(12) ไม่อนุญาตให้ผู้ใช้งาน จดหมายอิเล็กทรอนิกส์ (E-mail) ทุกคนส่งข้อมูลหรือข้อความที่เป็นในรูปแบบของ Junk Mail หรือ Spam Mail หรือการโฆษณา หรือชี้นำ หรือให้มีการซื้อขายสิ่งของหรือบริการ

ความมั่นคงปลอดภัยของอินเตอร์เน็ต (Internet security)

(1) ห้ามใช้ระบบอินเตอร์เน็ต (Internet) ของหน่วยงานเพื่อแสวงหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับบริษัทฯ

(2) ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัท บอสฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

(3) หลังจากใช้งานระบบอินเตอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

(4) ผู้ที่ถูกตรวจสอบว่าพยายามกระทำ การอันใดที่เป็นการละเมิดนโยบายขององค์กร การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำ ความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือพ.ร.บ.ข้อมูลส่วนบุคคล เป็นการ กระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของบริษัท บอสฯ จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

ทางบริษัทจัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการ ทำงานโดยกำหนดกลุ่มผู้ใช้งานหรือสิทธิของกลุ่มผู้ใช้งาน และกำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการ กำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

1.1 อ่านอย่างเดียว

1.2 สร้างข้อมูล

1.3 ป้อนข้อมูล

1.4 แก้ไข

1.5 อนุมัติ

1.6 ไม่มีสิทธิ

(2) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย

จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

(1) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(2) ข้อมูลที่มีระดับความสำคัญปานกลาง

(3) ข้อมูลที่มีระดับความสำคัญน้อย

จัดแบ่งลำดับชั้นความลับของข้อมูล

(1) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย อย่างร้ายแรงที่สุด
(2) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย อย่างร้ายแรง
(3) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
(4) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

เกณฑ์ในการกำหนดชั้นความลับของข้อมูล

(1) ประเภทลับ หมายถึง ข้อมูลที่รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง
(2) ประเภทใช้ภายในเท่านั้น หมายถึง ข้อมูลที่สื่อสารกันในกลุ่มย่อย/หน่วยงาน หรือข้อมูลที่เผยแพร่เฉพาะภายในบริษัท
(3) ประเภทส่วนบุคคล หมายถึง ข้อมูลที่ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแลข้อมูลนั้น
(4) ประเภทเปิดเผยได้ หมายถึง ข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกองค์กร

จัดแบ่งระดับชั้นการเข้าถึง

(1) ระดับชั้นสำหรับผู้บริหาร
(2) ระดับชั้นสำหรับผู้ใช้งานทั่วไป
(3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

เกณฑ์การแบ่งระดับชั้นการเข้าถึงข้อมูลและสารสนเทศ

(1) ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น
(2) ผู้ปฏิบัติงาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย
(3) ผู้ดูแลระบบ มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่
(4) บุคคล เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้
(5) ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น
(6) การกำหนดสิทธิ์พิเศษสามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูลเท่านั้น
(7) การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิ์ หรือหน่วยงานหลักเท่านั้น

การควบคุมการเปลี่ยนแปลง

การเปลี่ยนแปลงใดๆ ที่อาจส่งผลกระทบต่อข้อมูลและสารสนเทศที่ใช้งานอยู่ให้ดำเนินการดังนี้

(1) พิจารณาวางแผนดำเนินการเปลี่ยนแปลง รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในการเปลี่ยนแปลง
(2) แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับการเปลี่ยนแปลงนั้นๆ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการเตรียมความพร้อมก่อนที่จะดำเนินการเปลี่ยนแปลง
(3) ต้องตรวจสอบความสมบูรณ์ของข้อมูลและสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลง

ต้องจัดเก็บซอร์สโค้ดและไลบรารี่ของระบบสารสนเทศทั้งเวอร์ชั่นปัจจุบันและเวอร์ชั่นเก่าไว้ ในสถานที่ที่มีความมั่นคงปลอดภัย เพื่อให้สามารถนำกลับมาใช้ได้เมื่อจำเป็น

ข้อกำหนดการควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ

(1) ต้องควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบ สารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(2) ต้องปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความ มั่นคงปลอดภัย

การทบทวนและตรวจสอบสิทธิ์การเข้าถึงและการใช้งานข้อมูล สารสนเทศ และระบบสารสนเทศ

(1) ทบทวนและตรวจสอบสิทธิ์การเข้าถึงและใช้งานระบบสารสนเทศ ปีละ ๑ ครั้ง โดยผู้ดูแลระบบพิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงานที่ขอสิทธิ์ จัดส่งรายชื่อนั้นให้กับหน่วยงานที่ขอสิทธิ์เพื่อดำเนินการทบทวนว่า มีรายชื่อที่ลาออกหรือไม่ หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้แก้ไขสิทธิ์การเข้าถึงให้ถูกต้องหรือไม่

(2) หน่วยงานผู้ขอสิทธิ์แจ้งกลับผู้ดูแลระบบเพื่อดำเนินการแก้ไขให้ถูกต้อง

(3) หน่วยงานที่เป็นเจ้าของระบบสารสนเทศต้องตรวจสอบคุณสมบัติและสิทธิ์ของผู้ใช้อย่างสม่ำเสมอ หากมีการ

การทบทวนสิทธิ์การเข้าถึง

(1) ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้อย่างน้อยปีละ ๑ ครั้ง

(2) บัญชีผู้ใช้จะหมดอายุ ดังนี้

1) กรณีบุคลากร หมดอายุเมื่อพ้นสภาพการเป็นบุคลากรของบริษัท

2) กรณีพนักงาน หมดอายุหลังพ้นสภาพการเป็นพนักงานและจะไม่สามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าคอมพิวเตอร์ได้

การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

(1) จัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่มั่นคงปลอดภัย

(2) ต้องควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยผู้เป็นเจ้าของหรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น

(3) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญ ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญได้

(4) สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(5) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางบริษัทฯ

(6) จัดทำแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสารตอบโต้ และแนวทางต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่มหาวิทยาลัยต้องปฏิบัติตาม

(7) โปรแกรมต่างๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่ห้ามนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานเพราะเป็นการกระทำที่ผิดกฎหมาย

(8) ไม่เก็บข้อมูลสำคัญของบริษัทไว้บนเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลที่เป็นสมบัติส่วนบุคคล

(9) ต้องทำการล้างข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์

(10) ต้องลบหรือฟอร์แมต (Format) ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำลายหรือเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์

(11) ต้องลบข้อมูลที่ไม่มีการใช้งานตั้งแต่ 5 ปีขึ้นไปออกจากฐานข้อมูล และสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และ จัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล ทั้งนี้ การลบหรือทำลายข้อมูลอิเล็กทรอนิกส์ดังกล่าว ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติให้ทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูลทุกครั้ง

คำนิยาม

การรักษาความมั่นคงปลอดภัย หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท บอสฯ

มาตรฐาน (Standard) หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติงานเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

ผู้ใช้งาน หมายความว่า เจ้าหน้าที่ พนักงาน ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับผิดชอบ ผู้ใช้งานทั่วไป ได้แก่

- **ผู้บริหารระดับสูงสุด** (Chief Executive Officer : CEO) หมายความว่า กรรมการผู้จัดการบริษัทฯ มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น
- **บุคคลภายนอก** หมายความว่า บุคคลที่บริษัท บอสฯ อนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศ ของบริษัท บอสฯ ได้ชั่วคราวเพื่อประโยชน์ในการดำเนินงานของบริษัท บอสฯ เช่น พนักงาน หรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับบริษัท บอสฯ หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง
- **สิทธิผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ ของหน่วยงาน
- **สินทรัพย์** (Asset) หรือ ทรัพย์สินสารสนเทศ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่
    - ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
    - ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด
    - ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** (Access Control) หมายความว่า การอนุญาตการกำหนดสิทธิ หรือ การมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ เอาไว้ด้วยก็ได้
- **ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ** (Information Security) หมายความว่า การธำรงไว้ซึ่ง ความลับ (Confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธ ความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึงการป้องกัน ทรัพย์สิน
- สารสนเทศจากการเข้าถึงใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ
- **สารสนเทศ** (Information) หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถ นำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ โดยในที่นี้เรียกรวมว่า “ข้อมูล”
- **ระบบคอมพิวเตอร์** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดย ได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผล ข้อมูลโดยอัตโนมัติ

- **ระบบเครือข่าย** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์สื่อสารหรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัท บอสฯ ได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet)
- **ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายความว่า ระบบงานของหน่วยงานที่นำเอา เทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถ นำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย แอพพลิเคชั่นข้อมูล และสารสนเทศ เป็นต้น
- **เจ้าของข้อมูล** หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของ ข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- **รหัสผ่าน** (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยัน ตรวจตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบ เทคโนโลยีสารสนเทศ
- **ระยะเวลาที่ยอมให้การดำเนินงานหยุดชะงักได้** (Maximum Tolerable Period of Disruption: MTPD) หมายความว่า ระยะเวลานานที่สุดที่ยังสามารถปฏิบัติงานได้ หากการดำเนินงานที่สำคัญหยุดชะงัก
- **ระบบและอุปกรณ์เครือข่าย** หมายความว่า ระบบและอุปกรณ์ที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของ บริษัท บอสฯ
- **โครงสร้างพื้นฐานสารสนเทศ** หมายความว่า ระบบคอมพิวเตอร์ และระบบเครือข่าย ในการสนับสนุนการให้บริการ ควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย แอพพลิเคชั่นข้อมูล และ สารสนเทศ เป็นต้น
- **ความมั่นคงปลอดภัยด้านการบริหารจัดการ** (Administrative Security) หมายความว่า การกระทำในระดับบริหารโดยการจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในกระบวนการคัดเลือก การพัฒนา การนำไปใช้ หรือการบำรุงรักษาทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัย
- **ความมั่นคงปลอดภัยทางด้านกายภาพ**. (Physical Security) หมายความว่า การจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์อื่นใด จากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

มาตรการรักษานี้ให้ใช้บังคับตั้งแต่วันที่ 1 ตุลาคม 2565

ลงชื่อ .....

(นายพิทยา ตันติพิริยะกิจ)

ตำแหน่ง ประธานกรรมการ

วันที่ 17 กุมภาพันธ์ 2568