บริษัท เมืองไทย แคปปิตอล จำกัด (มหาชน)
332/1 ถนนจรัญสนิทวงศ์ แขวงบางพลัด เขตบางพลัด กรุงเทพฯ 10700 โทร. 02 483 8888

นโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ
(Information Security Policy)

1. วัตถุประสงค์

บริษัท เมืองไทย แคปปิตอล จำกัด (มหาชน) และ บริษัทในเครือเมืองไทย แคปปิตอล (“บริษัท”) มีความมุ่งหมายเพื่อให้การใช้บริการ และการให้บริการสามารถดำเนินการใช้งานร่วมกันอย่างเหมาะสมสอดคล้องกับนโยบายทางธุรกิจ และป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องจากผู้ใช้งาน และภัยคุกคามต่าง ๆ บริษัทจึงได้จัดทำนโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศฉบับนี้ขึ้นเพื่อใช้เป็นแนวทางกำหนดวิธีปฏิบัติในการตรวจสอบและรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้มีความมั่นคงปลอดภัย และสามารถให้บริการได้อย่างต่อเนื่อง อีกทั้งเพื่อเป็นการลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์ เพื่อให้เกิดความเชื่อมั่นของผู้ใช้บริการ

บริษัทได้กำหนดนโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศเพื่อให้ผู้บริหาร พนักงานของบริษัทรวมถึงบุคคลภายนอกที่เกี่ยวข้องกับบริษัทใช้เป็นแนวทางในการปฏิบัติงานให้สอดคล้องกับกฎหมาย และกฎเกณฑ์ทางการที่กล่าวมาข้างต้น โดยให้ยกเลิกประกาศนโยบายความมั่นคงปลอดภัย (Information Security Policy) ฉบับวันที่ 9 พฤษภาคม 2557

2. หน้าที่และความรับผิดชอบในการปฏิบัติตามนโยบาย

2.1. คณะกรรมการบริษัทฯ มีหน้าที่อนุมัตินโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ และให้ความสำคัญในการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องจากผู้ใช้งาน และภัยคุกคามต่าง ๆ อีกทั้งมอบหมายให้มีการประเมินความเสี่ยงด้านสารสนเทศภายใต้การกำกับบริหารความเสี่ยง

2.2. ผู้บริหารระดับสูงมีหน้าที่ควบคุมดูแลการปฏิบัติงานให้ถูกต้องตามกฎหมาย และกฎเกณฑ์ทางการอื่น ๆ ที่เกี่ยวข้อง

2.3. พนักงานมีหน้าที่ต้องปฏิบัติตามนโยบายฉบับนี้ ระเบียบปฏิบัติ คำสั่ง และคู่มือปฏิบัติงานเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

บริษัท เมืองไทย แคปปิตอล จำกัด (มหาชน)
332/1 ถนนจรัญสนิทวงศ์ แขวงบางพลัด เขตบางพลัด กรุงเทพฯ 10700 โทร. 02 483 8888

3. คำจำกัดความ

“บริษัท” หมายถึง บริษัท เมืองไทย แคปปิตอล จำกัด (มหาชน) และ บริษัทในเครือเมืองไทย แคปปิตอล

“ฝ่ายเทคโนโลยีสารเทศ” หมายถึง หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศของบริษัท

“พนักงาน” หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานฝึกงาน พนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท

“ผู้ใช้งาน” หมายถึง พนักงานของบริษัท รวมไปถึงบุคคลภายนอกบริษัทที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งานเพื่อใช้งานอุปกรณ์สารสนเทศของบริษัท

“ผู้ใช้สิทธิสูง” หมายถึง ผู้ใช้งานที่มีสิทธิสูงกว่าผู้ดูแลระบบและผู้ใช้งานทั่วไป โดยได้รับมอบหมายให้สามารถเปลี่ยนแปลงแก้ไขในส่วนของระบบงานและฐานข้อมูลซึ่งมีสิทธิสูงสุดในแต่ละระบบงาน

“ผู้ดูแลระบบสารสนเทศ” หมายถึง หน่วยงานสารสนเทศภายในซึ่งเป็นเจ้าของระบบคอมพิวเตอร์ และมีความรับผิดชอบในระบบคอมพิวเตอร์นั้น ๆ

“ผู้ดูแล” หมายถึง ผู้ที่ได้รับมอบให้ดูแล ใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สารสนเทศ

“บุคคลภายนอก” หมายถึง บุคคล นิติบุคคล ซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิในการเข้าถึงข้อมูลหรือระบบสารสนเทศ โดยได้รับสิทธิตามประเภทการใช้งาน และต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทโดยไม่ได้รับอนุญาต

“ผู้จัดการฝ่าย” หมายถึง พนักงานซึ่งเป็นผู้ดูแลรับผิดชอบของหน่วยงานภายในตามโครงสร้างบริษัทของบริษัท

"ระบบคอมพิวเตอร์" หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุอุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิด ต่าง ๆ ระบบ Internet และระบบ Intranet รวมถึงอุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่าง ๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัท ของบริษัทคู่ค้า และบริษัทอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของพนักงานที่นำเข้ามาติดตั้ง หรือใช้งานภายในสถานประกอบการของบริษัท

“ข้อมูล” หมายถึง ข้อมูล ข่าวสารบันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรืออุปกรณ์ใด ๆ

“ทรัพย์สินสารสนเทศ” หมายถึง ทรัพย์สินด้านฮาร์ดแวร์ เช่น เครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ อุปกรณ์สื่อสาร เป็นต้น และทรัพย์สินด้านข้อมูลทั้งที่อยู่ในรูปอิเล็กทรอนิกส์และรูปเอกสาร เช่น ฐานข้อมูล,

บริษัท เมืองไทย แคปปิตอล จำกัด (มหาชน)
332/1 ถนนจรัญสนิทวงศ์ แขวงบางพลัด เขตบางพลัด กรุงเทพฯ 10700 โทร. 02 483 8888

แฟ้มข้อมูล ในระบบที่ใช้งานจริง ข้อมูลสำรอง คู่มือการใช้งานระบบ เอกสารประกอบการพัฒนาระบบ และสัญญาต่าง ๆ เป็นต้น
“เจ้าของข้อมูล” หมายถึง บริษัท หรือบุคคลที่ได้รับมอบหมายให้ดำเนินการดูแลรักษาข้อมูลตามนโยบายฉบับนี้

4. เนื้อหานโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ประกอบด้วยหมวดต่าง ๆ ดังต่อไปนี้

<u>หมวดที่ 1</u> การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้

บริษัทได้มีการกำหนดบทบาทและหน้าที่ของแต่ละหน่วยงานอย่างชัดเจน อีกทั้งมีการควบคุมการเข้าถึงระบบสารสนเทศ การพิสูจน์ตัวตนผู้ใช้ และการป้องกันการปฏิเสธความรับผิดตามนโยบายดังต่อไปนี้

1.1 การกำหนดบุคลากรหรือหน่วยงานทางระบบสารสนเทศ และการแบ่งแยกอำนาจหน้าที่ที่เหมาะสมในการบริหารจัดการทางระบบสารสนเทศ

พนักงานทุกคนมีบทบาทหน้าที่รับผิดชอบในการรักษาความปลอดภัยสารสนเทศ รวมถึงการปฏิบัติตามนโยบายและระเบียบปฏิบัติด้านความปลอดภัยสารสนเทศ โดยแบ่งแยกหน้าที่ของแต่ละฝ่ายโดยชัดเจนเพื่อเป็นการถ่วงดุลในการปฏิบัติงาน

1) กรณีที่พนักงานมีหน้าที่เกี่ยวข้องกับข้อมูลที่มีความสำคัญหรือความลับ ต้องมีการกำหนดหน้าที่และความรับผิดชอบด้านความปลอดภัยสารสนเทศที่มีลักษณะเฉพาะกับหน้าที่งานนั้นในคำอธิบายหน้าที่งาน
2) หน่วยงานทรัพยากรบุคคล ต้องสร้างความตระหนักถึงความรับผิดชอบด้านความปลอดภัยสารสนเทศตั้งแต่การจ้างพนักงาน รวมทั้งระบุความรับผิดชอบดังกล่าวในสัญญาว่าจ้าง
3) เงื่อนไขการจ้างงาน ควรกำหนดถึงหน้าที่ความรับผิดชอบด้านความปลอดภัยสารสนเทศและการปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ การฝ่าฝืนหรือละเลยต่อหน้าที่และนโยบายความปลอดภัยสารสนเทศของบริษัทถือว่ามีความผิด ต้องพิจารณาตามบทลงโทษของบริษัทซึ่งขึ้นอยู่กับความรุนแรงของผลกระทบที่เกิดขึ้นกับบริษัท
4) หน่วยงานหรือบุคคลจากหน่วยงานภายนอกซึ่งบริษัทว่าจ้างจะต้องทำความเข้าใจและรับทราบนโยบายความปลอดภัยสารสนเทศในสาระสำคัญ โดยเฉพาะอย่างยิ่งในเรื่องการไม่เปิดเผยข้อมูล ก่อนการเริ่มปฏิบัติงานจริงในบริษัท
5) พนักงานมีหน้าที่และความรับผิดชอบในการดูแลรักษาความลับของข้อมูล แม้ว่าเมื่อนำข้อมูลไปทำงานภายนอกอาคารสำนักงาน นำข้อมูลไปทำงานที่บ้าน หรือการเข้าสู่ระบบของบริษัทจากภายนอก (Remote Access)
6) ผู้ใช้งาน พนักงาน หน่วยงานภายนอกต้องปฏิบัติตามนโยบายและระเบียบปฏิบัติทางด้านความปลอดภัยสารสนเทศของบริษัท พนักงานทุกคนควรเข้ารับฟังการอบรมให้ตระหนักถึงความปลอดภัยสารสนเทศเพิ่มเติมเป็นระยะ ๆ เพื่อรับทราบถึงนโยบายความปลอดภัยเพิ่มเติมของบริษัท เหตุการณ์ละเมิดความปลอดภัยและกรณีศึกษาใหม่ๆ เพื่อเป็นการเน้นย้ำในนโยบายความปลอดภัยสารสนเทศของบริษัท
7) หน่วยงานทรัพยากรบุคคล และหน่วยงานด้านกฎหมายต้องกำหนดบทลงโทษสำหรับพนักงานซึ่งละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้อง

1.2 การควบคุมการเข้าถึงระบบสารสนเทศ

ทุกฝ่ายของบริษัทที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศจะต้องดำเนินการจัดทำบัญชีทรัพย์สินสารสนเทศของบริษัท

1) ผู้ดูแลทรัพย์สินสารสนเทศต้องตรวจทาน และปรับปรุงบัญชีทรัพย์สินสารสนเทศอย่างสม่ำเสมอตลอดจนถึงการแจ้งถึงการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นกับทรัพย์สินให้ผู้ดูแลทรัพย์สินสารสนเทศทราบอย่างน้อยปีละ 1 ครั้ง
2) ในการจัดทำทะเบียนทรัพย์สินสารสนเทศ แต่ละหน่วยงานจะต้องกำหนดเจ้าของทรัพย์สินสารสนเทศที่มีหน้าที่รับผิดชอบในการรักษาทรัพย์สินสารสนเทศนั้น สำหรับในกรณีที่เป็นทรัพย์สินด้านข้อมูล ซึ่งอาจมีเจ้าของข้อมูลได้หลายคน ผู้บริหารระดับสูงขึ้นไปต้องมอบหมายความรับผิดชอบความเป็นเจ้าของข้อมูลให้กับบุคคลที่ใช้หรือเกี่ยวข้องกับข้อมูลนั้นมากที่สุด
3) ข้อมูลเกี่ยวกับบัญชีทรัพย์สินถือว่าเป็นข้อมูลลับที่อาจอนุญาตให้เปิดเผย หรือเข้าใช้งานได้ เฉพาะบุคคลที่เกี่ยวข้องและมีความจำเป็นต้องทราบเท่านั้น
4) ผู้ใช้งาน พนักงาน รวมทั้งบุคคลภายนอกต้องยินยอมทำตามข้อกำหนดในการใช้งานข้อมูลและทรัพย์สินสารสนเทศ
5) การอนุญาตให้เข้าใช้ข้อมูลที่จัดอยู่ในชั้นลับขึ้นไป ต้องกระทำโดยเจ้าของข้อมูลนั้น ในการกำหนดสิทธิการเข้าใช้ข้อมูลโดยยึดถือตามความจำเป็นทางธุรกิจ
6) พนักงานต้องตระหนักถึงหน้าที่ และความรับผิดชอบในการเปิดเผย และแบ่งปันข้อมูล ทั้งในบริษัทและกับหน่วยงานภายนอก
7) ฝ่ายงานทรัพยากรบุคคลต้องแจ้งฝ่ายงานด้านเทคโนโลยีสารสนเทศและฝ่ายงานที่เกี่ยวข้องทราบทันทีที่มีการโอนย้าย ลาออก หรือพ้นสภาพการเป็นพนักงานของบริษัท เพื่อทำการถอดถอนสิทธิการเข้าใช้ระบบงาน ต่างๆ และการเข้า-ออกพื้นที่ของบริษัท อีกทั้งต้องทำการคืนทรัพย์สินของบริษัทให้ฝ่ายที่ดูแลทรัพย์สินนั้น ๆ
8) กำหนดพื้นที่ควบคุมความมั่นคงปลอดภัยภายในบริษัท และกำหนดมาตรการป้องกันที่เหมาะสมตามระดับของความเสี่ยงในแต่ละพื้นที่ โดยการควบคุมดังกล่าวเป็นการป้องกันสารสนเทศ และระบบประมวลผลสารสนเทศของบริษัทขั้นพื้นฐานจากการเข้าถึงโดยไม่ได้รับการอนุญาต ความเสียหายที่อาจเกิดขึ้นจากภัยคุกคาม และการรบกวนไม่ว่าโดยตั้งใจหรือจากภัยธรรมชาติ
9) จัดระดับความสำคัญของพื้นที่ในอาคารสำนักงานของบริษัท และกำหนดให้มีพื้นที่ควบคุมโดยใช้การประเมินความเสี่ยง ซึ่งการจัดทำการประเมินความเสี่ยงในพื้นที่อาคารสำนักงานของบริษัท เพื่อกำหนดหาพื้นที่ควบคุมความปลอดภัย และหามาตรการควบคุมที่เหมาะสมกับพื้นที่ดังกล่าว
10) สิทธิในการผ่านเข้า-ออกพื้นที่ของพนักงานทุกคนในเวลาทำการต้องติดบัตรพนักงานให้เห็นอย่างชัดเจนขณะอยู่ในอาคารสำนักงานของบริษัท ทั้งนี้สิทธิดังกล่าวจะต้องถูกยกเลิกทันทีเมื่อพนักงานลาออกหรือสิ้นสุดการเป็นพนักงาน
11) ผู้ที่มาติดต่อต้องติดต่อเจ้าหน้าที่รักษาความปลอดภัยเพื่อทำการแลกบัตรอนุญาตให้เข้าสถานที่ และต้องติดบัตรให้เห็นอย่างชัดเจนตลอดเวลาที่อยู่ในอาคารสำนักงานของบริษัท
12) อาคารที่มีศูนย์คอมพิวเตอร์ ห้องระบบคอมพิวเตอร์หรือระบบสื่อสารต้องมีมาตรการความมั่นคงปลอดภัยที่เข้มงวด เพื่อป้องกันการผ่านเข้า-ออกของผู้ที่ไม่ได้รับอนุญาต

13) พื้นที่ที่มีการติดตั้งอุปกรณ์ควบคุมการเข้า-ออก ห้ามพนักงานทำการหลีกเลี่ยงหรืองดเว้นการทำงานของอุปกรณ์ควบคุมการผ่านเข้า-ออก เช่น การเปิดจากภายในและอนุญาตให้บุคคลจากด้านนอกเข้าโดยมิได้มีการควบคุม ติดตามหรือสอบถาม เป็นต้น
14) ห้องประมวลผลในศูนย์คอมพิวเตอร์เป็นพื้นที่หวงห้าม โปรแกรมเมอร์และผู้ใช้งานทั่วไปไม่มีสิทธิที่จะเข้าไปในพื้นที่ดังกล่าวโดยไม่มีการควบคุม อีกทั้งไม่ควรมีป้ายหรือสัญลักษณ์ที่แสดงถึงที่ตั้งสถานที่ของศูนย์คอมพิวเตอร์
15) อุปกรณ์และสื่อที่ใช้สำรองข้อมูล ต้องจัดเก็บไว้ในสถานที่ปลอดภัยห่างจากอุปกรณ์ที่เก็บข้อมูลหลักในระยะที่สามารถป้องกันความเสียหายเมื่อมีเหตุเกิดขึ้นกับสถานที่จัดเก็บอุปกรณ์หลัก
16) ศูนย์คอมพิวเตอร์ต้องมีการควบคุมความปลอดภัยที่อาจเกิดจากน้ำท่วม แผ่นดินไหว อัคคีภัย อีกทั้งยังต้องมีระบบปรับอากาศและความชื้น ระบบกระแสไฟฟ้า รวมถึงต้องมีการติดตั้งระบบป้องกันฟ้าผ่าในทุกอาคาร เป็นต้น

    อุปกรณ์ต้องมีการจัดวางเพื่อลดการเข้าถึงบริเวณทำงานโดยไม่จำเป็นเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต อีกทั้งต้องมีการจัดวางอุปกรณ์ในมุมที่เหมาะสม เพื่อลดความเสี่ยงในการมองเห็นข้อมูลโดยบุคคลที่ไม่เกี่ยวข้องและไม่ได้รับอนุญาตระหว่างการใช้งาน โดยอุปกรณ์ดังกล่าวต้องมีการควบคุมดูแลสภาพแวดล้อม เช่น อุณหภูมิและความชื้น ซึ่งสามารถทำให้เกิดการทำงานที่ผิดพลาดของอุปกรณ์ประมวลผลสารสนเทศ อุปกรณ์คอมพิวเตอร์และเครือข่ายที่สำคัญต้องมีอุปกรณ์สำรองไฟฟ้าฉุกเฉิน (UPS) ระบบเครื่องกำเนิดไฟฟ้าสำรอง (Power Generator) เพื่อให้ระบบทำงานต่อเนื่องหรือสิ้นสุดการทำงานอย่างเหมาะสมเมื่อระบบไฟฟ้าขัดข้อง และต้องมีการตรวจสอบอุปกรณ์สำรองไฟฟ้าฉุกเฉินตามขั้นตอนของผู้ผลิตอย่างสม่ำเสมอ

1.2 การตรวจสอบตัวตน และการป้องกันการปฏิเสธความรับผิด

เพื่อลดความเสี่ยงและป้องกันการเข้าใช้ระบบโดยไม่ได้รับอนุญาต จำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมเพื่อการจำกัดสิทธิการเข้าใช้งานระบบจากความจำเป็นและความต้องการทางธุรกิจประกอบกับข้อกำหนดด้านความปลอดภัย โดยต้องมีวิธีการควบคุมสิทธิในกระบวนการที่เกี่ยวข้องกับผู้ใช้งานระบบเริ่มตั้งแต่การขอจดทะเบียนไปจนถึงการยกเลิกสิทธิในกรณีที่ผู้ใช้งานนั้นไม่มีความจำเป็นต้องใช้อีกต่อไป รวมไปถึงการควบคุมสิทธิของผู้ใช้ซึ่งมีสิทธิสูงที่สามารถแก้ไขสิทธิต่าง ๆ ของระบบได้

1) ผู้ใช้ทุกคนต้องมีรหัสผู้ใช้เฉพาะบุคคล เพื่อสามารถระบุและติดตามการใช้งานของผู้ใช้แต่ละคนได้
2) พนักงานทุกคนที่มีสิทธิเข้าใช้งานระบบข้อมูลต้องมีรหัสผู้ใช้เฉพาะบุคคลในการเข้าสู่ระบบ โดยรหัสดังกล่าวต้องเป็นของผู้ที่ร้องขอเท่านั้น
3) ผู้ใช้ระบบของบริษัททุกคนต้องลงนามรับทราบถึงกฎระเบียบและเงื่อนไขในการใช้งานระบบของบริษัทและยินยอมปฏิบัติตามระเบียบการใช้งานของระบบนั้น ๆ
4) ผู้ใช้งานซึ่งมีรหัสผู้ใช้ที่มีสิทธิสูงต้องมีรหัสผู้ใช้ส่วนตัวสำหรับการปฏิบัติงานปกติด้วย โดยให้ใช้สิทธิในการปฏิบัติงานตามหน้าที่ความรับผิดชอบและความจำเป็นของงานเท่านั้น ทั้งนี้ผู้ดูแลระบบสารสนเทศจะเป็นผู้พิจารณาในการอนุญาตให้หรือถอดถอนสิทธิสูง

5) ผู้ดูแลระบบสารสนเทศต้องกำหนดความถี่ในการตรวจทานสิทธิการเข้าใช้งานของผู้ใช้ รวมถึงเพิกถอนการเข้าใช้งานของผู้ใช้ซึ่งไม่มีสิทธิดังกล่าวให้ออกจากระบบทันที เพื่อป้องกันการลักลอบใช้งานโดยไม่ได้รับอนุญาต
6) ผู้ใช้มีหน้าที่ต้องกำหนดและใช้รหัสผ่านที่มีความปลอดภัยและยากแก่การคาดเดา เป็นความลับ และไม่แบ่งปันหรือเปิดเผยรหัสดังกล่าวแก่บุคคลอื่น โดยผู้ใช้ต้องเปลี่ยนรหัสผ่านของตนเป็นประจำ
7) ผู้ใช้ต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับทันทีที่เข้าระบบครั้งแรก เพื่อป้องกันบุคคลอื่นลักลอบใช้งาน
8) ผู้ใช้ควรออกจากระบบเครือข่าย (Log-off) ทันทีเมื่อใช้งานเสร็จหรือไม่มีความจำเป็นต้องใช้งานอีก และหากไม่มีการใช้งานเป็นเวลานานผู้ใช้ควรปิดเครื่องคอมพิวเตอร์หรือเครื่องปลายทางให้เรียบร้อย ทั้งนี้การเชื่อมต่อเข้าสู่ระบบจากเครื่องปลายทาง หากพบว่าไม่มีการใช้งานระบบภายในระยะเวลาที่กำหนด ระบบต้องทำการยกเลิกการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ
9) การอนุญาตให้ใช้รหัสผู้ใช้ร่วมกันหรือใช้รหัสผู้ใช้ “GUEST” ต้องขึ้นอยู่กับเหตุผลความจำเป็นทางด้านธุรกิจหรือด้านเทคนิคที่สำคัญ ต้องมีการควบคุมเพิ่มเติมเพื่อสามารถระบุและติดตามการใช้งานของผู้ใช้แต่ละคนได้
10) บริษัทได้ดำเนินการให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication สำหรับผู้ใช้งานที่มีสิทธิสูง (Privileged User) ทุกบัญชีของระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย และผู้ใช้งาน (User) ทุกบัญชีที่สามารถเข้าถึงข้อมูลลูกค้าของระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายที่เชื่อมต่อกับเครือข่ายสาธารณะ (Internet facing)

หมวด 2 การรักษาชั้นความลับของข้อมูล และความถูกต้องเชื่อถือได้ของระบบสารสนเทศ

บริษัทได้มีมาตรการในการรักษาความลับของข้อมูลและการรักษาความถูกต้องเชื่อถือได้ของระบบสารสนเทศที่ให้บริการตามนโยบายดังต่อไปนี้

1. การรักษาความลับของข้อมูล

บริษัทได้กำหนดขั้นตอน วิธีการในการรับส่ง ประมวลผล การจัดเก็บ และการทำลายข้อมูลอย่างเหมาะสมเพื่อรักษาความลับ ความถูกต้องสมบูรณ์ของข้อมูล

1) บริษัทจะต้องมีการพิจารณาถึงลำดับชั้นของข้อมูลและแนวทางในการจัดการข้อมูลในลำดับชั้นดังกล่าวประกอบการพิจารณาในการใช้งานการเข้ารหัส โดยมีลำดับชั้นความลับดังนี้
   1.1) ชั้นที่ 1 ข้อมูลทั่วไป (เปิดเผยได้)
   ข้อมูลที่บุคคลภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้นซึ่งเป็นข้อมูลที่ไม่มีผลต่อการปฏิบัติงาน สามารถนำเสนอต่อสาธารณะชน และไม่เป็นประโยชน์โดยตรงในเชิงการค้าต่อคู่แข่ง หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย ทั้งนี้การทำลายเอกสารทำโดยการฉีกหรือเผาทำลาย ส่วนสื่ออิเล็กทรอนิกส์ทำลายโดยการลบข้อมูล
   1.2) ชั้นที่ 2 ข้อมูลใช้ภายใน
   เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่าสามารถเปิดเผยให้พนักงานทุกคนภายในบริษัททราบได้ แต่ไม่สามารถเปิดเผยต่อบุคคลภายนอกบริษัทได้ เนื่องจากอาจสร้างความเสียหายให้กับบริษัทได้ หากมีการร้องของบุคคลภายนอก เจ้าของข้อมูลต้องใช้ดุลยพินิจในการเปิดเผย โดยยึดหลักความจำเป็นใน

การใช้งาน ทั้งนี้การทำลายเอกสารทำโดยการฉีกหรือเผาทำลาย ส่วนสื่ออิเล็กทรอนิกส์ทำลายโดยการลบแฟ้มข้อมูล หรือทำลายสื่อบันทึกข้อมูลด้วยมาตรการที่เหมาะสม

1.3) ชั้นที่ 3 ข้อมูลลับ

เป็นข้อมูลใช้ภายในบริษัทที่เจ้าของข้อมูลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้พนักงานทุกคนทราบ ข้อมูลประเภทนี้จะถูกกำหนดให้ผู้ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานได้ทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่ควรทราบเพื่อให้เพียงพอต่อการปฏิบัติงาน ทั้งนี้การทำลายเอกสารทำโดยการฉีกหรือเผาทำลาย ส่วนสื่ออิเล็กทรอนิกส์ทำลายโดยการลบข้อมูล และเขียนทับข้อมูล หรือทำลายข้อมูลด้วยชุดคำสั่งของโปรแกรม หรือทำลายข้อมูลโดยสนามแม่เหล็ก หรือทุบทำลาย

2) เจ้าของข้อมูลต้องรับผิดชอบในการกำหนดลำดับชั้นของข้อมูลนั้น โดยคำนึงถึงความต้องการและผลกระทบด้านธุรกิจเป็นหลัก

3) เนื่องจากลำดับชั้นของข้อมูลอาจมีการเปลี่ยนแปลงตามระยะเวลา เจ้าของข้อมูลต้องสอบทานลำดับชั้นของข้อมูลที่รับผิดชอบอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับสภาพปัจจุบันของข้อมูลนั้น

4) ข้อมูลที่สำคัญต้องมีผู้ดูแลรับผิดชอบข้อมูล โดยผู้ดูแลข้อมูลต้องปกป้องข้อมูลตามแนวทางการปฏิบัติที่สอดคล้องกับลำดับชั้นของข้อมูล

5) การเปลี่ยนแปลงระดับการป้องกันข้อมูลและลำดับชั้นข้อมูล จำเป็นต้องได้รับความเห็นชอบและอนุมัติจากเจ้าของข้อมูล

การรับส่ง การประมวลผลและการจัดเก็บข้อมูลลับในลักษณะที่มั่นคงปลอดภัยตามระดับความสำคัญ เพื่อป้องกันการเข้าแก้ไขเปลี่ยนแปลงโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต บริษัทได้จัดให้มีการรับส่งข้อมูลผ่านระบบเครือข่าย Intranet รวมทั้งการประมวลผลข้อมูลโดยใช้เซิร์ฟเวอร์ที่มีความปลอดภัยมั่นคง และสถานที่ที่จัดเก็บข้อมูลได้รับมาตรฐานตามนโยบายนี้

2. การพัฒนาระบบ การควบคุมการเปลี่ยนแปลง การปรับปรุงแก้ไขระบบสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศ

บริษัทได้กำหนดนโยบายการปฏิบัติและการควบคุมภายในสำหรับการพัฒนา การควบคุมการเปลี่ยนแปลง การปรับปรุงแก้ไขระบบสารสนเทศ เพื่อลดการทำงานที่ผิดปกติหรือความเสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบสารสนเทศ

2.1 การรักษาความลับของข้อมูล

1) ผู้ดูแลระบบสารสนเทศต้องกำหนดความต้องการด้านความปลอดภัยสารสนเทศก่อนที่จะพัฒนาหรือจัดหาระบบงาน โดยจะต้องจัดทำเป็นลายลักษณ์อักษรและต้องปฏิบัติตามนโยบายและมาตรฐานต่าง ๆ ของบริษัทในการพัฒนาระบบงาน

2) ระบบประมวลผลต้องออกแบบให้มีความสามารถในการสอบทาน เพื่อตรวจจับกรณีประมวลผลข้อมูลมีความผิดพลาดหรือเสียหาย รวมถึงให้มีความสามารถแจ้งถึงความผิดพลาดต่าง ๆ จากการประมวลผล เช่น ข้อความแจ้งเมื่อระบบขัดข้อง เป็นต้น

บริษัท เมืองไทย แคปปิตอล จำกัด (มหาชน)
332/1 ถนนจรัญสนิทวงศ์ แขวงบางพลัด เขตบางพลัด กรุงเทพฯ 10700 โทร. 02 483 8888

3) กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์ เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องสมบูรณ์
4) ในการประมวลผลที่สำคัญต้องกำหนดให้มีระเบียบปฏิบัติในกรณีที่ตรวจพบข้อผิดพลาดของข้อมูลผลลัพธ์ รวมถึงกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการข้อมูลผลลัพธ์ไปใช้
5) กำหนดให้มีระเบียบปฏิบัติในเรื่องการใช้การเข้ารหัส รวมถึงซอฟต์แวร์และมาตรฐานวิธีการเข้ารหัสที่อนุญาตให้ใช้งานสำหรับข้อมูลในลำดับชั้นต่าง ๆ อีกทั้งต้องมีการปรับปรุงรายชื่อซอฟต์แวร์และมาตรฐานในด้านการเข้ารหัสให้ทันสมัยอยู่เสมอ
6) ก่อนมีการปรับปรุงเวอร์ชันใหม่ในระบบใช้งานจริงจะต้องได้รับเอกสารการอนุมัติการใช้โปรแกรมเวอร์ชันใหม่และหลักฐานประกอบอื่น ๆ เช่น รายงานผลการทดสอบเพื่อการรับรองความถูกต้องจากผู้ใช้งาน เป็นต้น และต้องปรับเปลี่ยน Source Code ในสมุดทะเบียน (Library) ให้สอดคล้องกัน โดยให้มีการสำรองและจัดเก็บโปรแกรมเวอร์ชันก่อนการแก้ไข เพื่อนำกลับมาใช้เมื่อมีความจำเป็น โดยมีรายละเอียดต่าง ๆ เช่น วัน-เดือน-ปี ที่ใช้งาน เป็นต้น
7) ไม่จัดเก็บ Source Code ของโปรแกรมไว้ในระบบใช้งานจริง โดยจะต้องมีการจัดเก็บรายการบันทึกเพื่อการตรวจสอบต่าง ๆ ของการแก้ไข Source Code และโปรแกรม
8) ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงไปใช้เพื่อการทดสอบระบบงานที่พัฒนาใหม่ ต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง โดยต้องได้รับอนุญาตก่อนการนำสำเนาข้อมูลจริงไปใช้ในระบบงานทดสอบในแต่ละครั้ง มีการควบคุมในการเข้าถึงข้อมูลที่ใช้ในการทดสอบระบบ และทำการลบข้อมูลทดสอบออกจากระบบทันทีเมื่อเสร็จสิ้นการทดสอบและมีการจัดเก็บบันทึกการทำรายการในระบบ (Audit Log) เพื่อตรวจสอบกิจกรรมการทดสอบ
9) แต่งตั้งผู้ดูแลสมุดทะเบียน (Library) ที่เก็บ Source Code และมีการจำกัดสิทธิในการเข้าถึงที่เก็บ Source Code ของโปรแกรม

2.2 การพัฒนาระบบ การควบคุมการเปลี่ยนแปลง การปรับปรุงแก้ไขระบบสารสนเทศ หรืออุปกรณ์ประมวลผลสารสนเทศ

บริษัทได้กำหนดมาตรฐานการรักษาความปลอดภัยขั้นต่ำและตั้งค่าการรักษาความมั่นคงปลอดภัยของระบบและอุปกรณ์ประมวลผลสารสนเทศให้สอดคล้องกับการให้บริการโดยอ้างอิงจากมาตรฐาน ISO-IEC 27001:2013 Information Security Management Systems รวมถึงมาตรการและกฎเกณฑ์ตามกฎหมายที่เกี่ยวข้อง เพื่อให้เกิดความมั่นคงปลอดภัยแก่ระบบสารสนเทศ อีกทั้งบริษัทได้มีการจัดการพัฒนาระบบและสอบทาน อย่างสม่ำเสมอ

1) การปรับปรุงแก้ไขระบบงานหรือโปรแกรมต่าง ๆ ต้องปฏิบัติตามระเบียบว่าด้วยเรื่องการปรับปรุงแก้ไขระบบงานหรือโปรแกรม โดยต้องจัดทำเป็นลายลักษณ์อักษรและสามารถติดตามสถานะได้ เช่น แผนการทดสอบการปรับปรุงแก้ไขโปรแกรมระบบ และผลการทดสอบ เป็นต้น
2) การปรับปรุงแก้ไขระบบงาน ผู้ดูแลแต่ละระบบงานต้องจัดทำเป็นหนังสือขออนุมัติในการแก้ไขระบบงานหรือโปรแกรมจากผู้ดูแลระบบสารสนเทศ การระบุถึงเครื่องคอมพิวเตอร์ ซอฟต์แวร์ ฐานข้อมูล ที่จะต้องเปลี่ยนแปลง การป้องกันผลกระทบที่อาจเกิดขึ้นกับการทำงาน การสำรองข้อมูลก่อนการปรับปรุงหรือบำรุงรักษาระบบ การจัดทำเอกสารประกอบการเปลี่ยนแปลงให้ทันสมัย การควบคุมเวอร์ชันที่เปลี่ยนแปลง และการจัดเก็บบันทึกเพื่อการตรวจสอบการแก้ไข เป็นต้น

2.3 การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก

1) ต้องมีการทำสัญญาทำเป็นลายลักษณ์อักษร พร้อมทั้งระบุขอบเขตการดำเนินงานหน้าที่และความรับผิดชอบของคู่สัญญาให้ชัดเจน
2) ต้องมีการบริหารความเสี่ยงในการใช้บริการจากผู้ให้บริการภายนอก โดยพิจารณาถึงการคัดเลือก การติดตาม การประเมิน และการตรวจสอบการให้บริการอย่างเหมาะสม
3) ต้องมีสัญญาเป็นลายลักษณ์อักษรในการรักษาความมั่นคงปลอดภัยของข้อมูล ซึ่งรวมถึงการรักษาความลับและกฎหมายที่เกี่ยวข้อง
4) ต้องมีการดำเนินการให้ผู้ให้บริการภายนอกทำแผนฉุกเฉินสำหรับการดำเนินการด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของบริษัท

2.4 การจัดการเครือข่ายที่เกี่ยวกับการให้บริการ

บริษัทได้มีการกำหนดมาตรการป้องกันการเข้าถึงระบบที่ให้บริการเครือข่ายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

1) ผู้ดูแลระบบสารสนเทศมีหน้าที่กำหนดมาตรการควบคุมการเชื่อมต่อทางเครือข่าย การอนุญาตการเชื่อมต่อโดยอุปกรณ์จากภายนอก
2) ต้องมีการลงทะเบียนเพื่อยืนยันตัวตนในการเข้าใช้งานเครือข่ายผ่านระบบรักษาความปลอดภัยของบริษัท
3) ต้องมีการแบ่งแยกประเภทเครือข่ายที่ชัดเจนตามประเภทของกลุ่มบริการสารสนเทศ และระดับความสำคัญของข้อมูล
4) บริษัทได้มีการกำหนดห้ามนำซอฟต์แวร์ หรือข้อมูลจากภายนอกมาใช้งาน เว้นแต่ ได้รับอนุญาตจากผู้ดูแลระบบสารสนเทศ และต้องมีการตรวจสอบซอฟต์แวร์ หรือข้อมูลดังกล่าวให้แน่ใจว่าไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่
5) บริษัทจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัสและมัลแวร์ รวมทั้งมีการอัปเดตตลอดเวลาในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และเครื่องเซิร์ฟเวอร์ เพื่อลดความเสี่ยงจากการถูกโจมตีจากไวรัสและมัลแวร์

หมวดที่ 3 การรักษาสภาพความพร้อมใช้งานของการให้บริการ

บริษัทได้มีมาตรการในการให้บริการที่มีประสิทธิภาพและมีสภาพความพร้อมใช้งานในการให้บริการตลอดเวลา เพื่อให้สามารถรองรับการทำธุรกรรมตามความต้องการของธุรกิจได้อย่างต่อเนื่อง รวมทั้งมีการสำรองข้อมูลอย่างเหมาะสม เพื่อให้สามารถกู้ระบบให้กลับมาทำงานได้ตามปกติ ในกรณีที่ระบบเกิดความเสียหายตามนโยบายดังต่อไปนี้

1. การประเมิน และจัดการความเสี่ยงของระบบที่ให้บริการ

บริษัทจัดให้มีการประเมิน และจัดการความเสี่ยงโดยกำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรม วิเคราะห์และประเมินผลกระทบที่มีต่อธุรกิจที่อาจเป็นผลจากความล้มเหลวของการรักษาความมั่นคงปลอดภัย กำหนดเกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้ ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงในการดำเนินการที่อาจเกิดขึ้นได้ เพื่อหลีกเลี่ยงความเสี่ยงและลดความเสียหายที่จะเกิดขึ้น ทั้งนี้บริษัทจะจัดให้มีการทบทวนความเสี่ยงอยู่เสมอ

2. การติดตามตรวจสอบความผิดปกติและช่องโหว่ของระบบสารสนเทศ

บริษัทจัดให้มีการติดตามตรวจสอบรายที่ไม่ปกติ และโอกาสที่จะเกิดภัยคุกคาม หรือการลักลอบเข้าถึงระบบสารสนเทศ กระบวนการบริหารจัดการ Security Patch สำหรับทุกระบบงานและอุปกรณ์ ประเมินช่องโหว่ของระบบ (Vulnerability Assessment) จัดเตรียมแนวทางการแก้ไขหรือปิดช่องโหว่จากความล่อแหลมของระบบ โดยเฉพาะในส่วนของระบบเครือข่ายที่เกี่ยวกับการให้บริการ รวมถึงโปรแกรมระบบงานและฐานข้อมูล กรณีระบบมีความเสี่ยงสูง เช่น ระบบที่ให้บริการผ่านเครือข่ายสาธารณะควรจัดให้มีการทดสอบเจาะระบบ (Penetration Test) เพื่อทดสอบประสิทธิภาพของเทคโนโลยีการรักษาความมั่นคงปลอดภัย โดยบริษัทจะมีการดำเนินการติดตั้งอุปกรณ์และปรับปรุง พัฒนาระบบซอฟต์แวร์เพื่อให้สอดคล้องกับนโยบาย

3. การแก้ไขปัญหา บันทึกเหตุการณ์ และการรายงาน กรณีระบบสารสนเทศได้รับความเสียหาย

บริษัทจัดให้มีการกำหนดขั้นตอนการแก้ไขปัญหา ทีมงานหรือผู้รับผิดชอบ รวมถึงวิธีการรายงานปัญหาให้กับผู้บริหาร และแจ้งให้ผู้เกี่ยวข้องทราบ เก็บรวบรวมหลักฐานต่าง ๆ ที่เป็นประโยชน์ บันทึกเหตุการณ์ หรือจัดทำรายงานที่เป็นลายลักษณ์อักษรเพื่อเก็บไว้เป็นแนวทางในการแก้ปัญหา

4. การสำรองข้อมูล

บริษัทจัดให้มีการสำรองข้อมูลที่สำคัญและข้อมูลอื่นที่จำเป็นต่อการปฏิบัติงาน เพื่อให้มีข้อมูลพร้อมใช้ภายในประเทศ สำหรับการดำเนินธุรกิจและการให้บริการแก่ลูกค้าอย่างต่อเนื่อง กำหนดวิธีปฏิบัติ หรือขั้นตอนในการสำรองข้อมูลให้เหมาะสมและสอดคล้องกับความเสี่ยงของรูปแบบหรือลักษณะการให้บริการระบบการชำระเงินที่มีความสำคัญ การประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และบริการการชำระเงินภายใต้กำกับ แล้วแต่กรณี เช่น ข้อมูลที่จะสำรอง ความถี่ในการสำรองข้อมูล สื่อที่ใช้ สถานที่เก็บ วิธีการเก็บรักษา และการนำมาใช้งานทดสอบข้อมูลที่เก็บสำรองไว้อย่างสม่ำเสมอ อย่างน้อย ปีละ 1 ครั้ง และให้เป็นไปตามนโยบายการสำรองข้อมูลของบริษัท

5. การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง หรือแผนฉุกเฉินของระบบสารสนเทศ

บริษัทจัดให้มีการวิเคราะห์และระบุความเสี่ยง และการดำเนินงานที่สำคัญของการให้บริการ กำหนดระยะเวลาหยุดดำเนินงานที่ยอมรับได้ (Recovery Time Objectives) จัดทำแผนเป็นลายลักษณ์อักษร กำหนดขั้นตอนรายละเอียดการดำเนินการเมื่อมีการหยุดชะงักของการดำเนินงานที่สำคัญ เพื่อให้สามารถกลับมาดำเนินงานได้ตามระยะเวลาที่กำหนด ตามรายละเอียดและข้อกำหนดที่ระบุไว้ในนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ อีกทั้งยังมีการจัดการฝึกอบรม ทดสอบและทบทวนแผนสำหรับการดำเนินการงานที่สำคัญอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงปัจจัยที่มีผลต่อความเสี่ยง

หมวดที่ 4 การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ

เพื่อให้มั่นใจได้ว่านโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการเป็นไปอย่างมีประสิทธิภาพ มั่นคงปลอดภัยสามารถให้บริการได้อย่างต่อเนื่อง บริษัทจัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และจัดทำรายงานผลการตรวจสอบเสนอคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย และแจ้งให้หน่วยงานภายในที่เกี่ยวข้องทราบเพื่อนำไปปฏิบัติ พร้อมจัดส่งสำเนาผลการตรวจสอบให้ธนาคารแห่งประเทศไทยภายใน 45 วัน นับแต่วันที่ทำการตรวจสอบแล้วเสร็จ รวมถึงติดตาม ตรวจสอบการให้บริการระบบชำระเงินภายใต้การกำกับพร้อมส่งรายงานต่าง ๆ ให้เป็นไปตามกฎระเบียบข้อบังคับที่เกี่ยวข้องทั้งหมด เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดตามกฎหมาย

บริษัท เมืองไทย แคปปิตอล จำกัด (มหาชน)
332/1 ถนนจรัญสนิทวงศ์ แขวงบางพลัด เขตบางพลัด กรุงเทพฯ 10700 โทร. 02 483 8888

หมวด 5 การทบทวนหรือปรับปรุงมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

บริษัทหรือผู้ที่ได้รับมอบหมายต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำอย่างน้อยปีละ 1 ครั้ง และต้องเสนอให้คณะกรรมการบริษัทอนุมัติหากมีการเปลี่ยนแปลง

นโยบายฉบับนี้ได้รับการพิจารณาและอนุมัติโดยคณะกรรมการของบริษัท มีผลตั้งแต่วันที่ 9 พฤษภาคม พ.ศ. 2566

ลงชื่อ .....
(พลเรือเอกอภิชาติ เพ็งศรีทอง)
ประธานกรรมการบริษัท