นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ

(Acceptable Use Policy)

บริษัท นามยง เทอร์มินัล จำกัด (มหาชน)

Namyong Terminal Public Company Limited

18 -02-2565

บริษัท นามยง เทอร์มินัล จำกัด (มหาชน) ได้จัดให้มีการใช้ระบบเครือข่ายคอมพิวเตอร์ เพื่อให้การปฏิบัติงานของพนักงานมีความสะดวกรวดเร็ว และให้บริการที่มีประสิทธิภาพต่อลูกค้า นอกจากนี้ยังมีการเชื่อมต่อระบบเครือข่ายจากภายในบริษัทฯ กับหน่วยงานด้านนอก หรือ เชื่อมต่อกับบริษัทของลูกค้าโดยตรง เพื่อสร้างความสะดวกต่อลูกค้าผู้มาใช้บริการ ดังนั้น เพื่อให้การใช้เครือข่ายคอมพิวเตอร์เป็นไปด้วยความเรียบร้อยและเหมาะสมต่อการใช้งานและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเครือข่ายอย่างไม่ถูกต้อง จึงเห็นสมควรวางระเบียบไว้ดังนี้

<u>บทที่ 1 คำนิยาม</u>

" องค์กร หรือ บริษัท "	หมายถึง บริษัท นามยง เทอร์มินัล จำกัด (มหาชน) (สำนักงานแหลมฉบัง และ สำนักงานกรุงเทพ)
" เครือข่ายคอมพิวเตอร์ "	หมายถึงระบบการเชื่อมโยงคอมพิวเตอร์ภายในบริษัทฯ และการเชื่อมโยงคอมพิวเตอร์จากภายในบริษัทฯ กับ หน่วยงานภายนอกบริษัทฯ
" ผู้บังคับบัญชา "	หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของบริษัทฯ
" ผู้รับจ้างช่วง "	หมายถึง บริษัท ที่ได้ทำสัญญาข้อตกลงกับบริษัทฯ ในการปฏิบัติงานตามที่ได้รับมอบหมาย
" พนักงาน "	หมายถึง บุคคลที่บริษัทฯ ได้รับเข้าทำงานตามหน่วยงานต่าง ๆ ซึ่งประกอบด้วยพนักงานประจำและพนักงานชั่วคราว พนักงานรายวัน
" ข้อมูล "	หมายถึง สิ่งที่สื่อความหมายให้รับรู้ถึงเรื่องราว ข้อเท็จจริง อันประกอบด้วย เอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยใช้เครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
" ผู้ดูแลระบบคอมพิวเตอร์ "	หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ดูแล รักษาเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อจัดการฐานข้อมูล (Database) ระบบเชื่อมโยงเครือข่าย (Network)

บทที่ 2 ข้อปฏิบัติของพนักงานที่ใช้งานเครือข่ายคอมพิวเตอร์

1. พนักงานผู้ใช้งานระบบเครือข่ายจะต้องได้รับอนุญาตจากผู้ดูแลระบบคอมพิวเตอร์ โดยกำหนดให้มีชื่อผู้ใช้งาน (User Name) รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนมีบัญชีผู้ใช้งาน (User Name) เป็นของตัวเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามนำมาเผยแพร่ แจกจ่าย ทำให้ผู้อื่นได้รับรู้รหัสผ่าน (Password)
2. ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Name) ไม่ว่าการกระทำนั้นเกิดจากผู้ใช้งานเองหรือไม่ก็ตาม
3. ผู้ใช้งานจะต้องใช้บัญชีรายชื่อ (User Name) และรหัสผ่าน (Password) ทุกครั้งเมื่อเข้าใช้ระบบสารสนเทศของบริษัทฯ หากมีปัญหาการใช้งานผู้ใช้งานจะต้องแจ้งให้ผู้ดูแลระบบคอมพิวเตอร์ทราบทันที
4. เมื่อพนักงาน หรือ ผู้รับจ้างช่วง ลาออกจากการปฏิบัติงานกับบริษัทฯ ฝ่ายบุคคลจะต้องทำหนังสือแจ้ง ผู้ดูแลระบบคอมพิวเตอร์ทันที เพื่อทำการยกเลิกบัญชีชื่อผู้ใช้งาน (User Name) ออกจากระบบเครือข่าย
5. เมื่อผู้ใช้งานเลิกใช้งานจะต้องทำการล็อคออกจากหน้าจอทุกครั้ง (Log Out)
6. พนักงานควรใช้ระบบเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ Download, Upload ไฟล์ข้อมูลที่มีขนาดใหญ่ที่ไม่จำเป็นต่อบริษัทฯ และไม่ควรปฏิบัติในเวลาทำงานซึ่งมีการใช้เครือข่ายอย่างหนาแน่น
7. พนักงานต้องใช้คำสุภาพ และถูกต้องตามข้อปฏิบัติการใช้เครือข่าย เช่น ไม่ส่ง E-Mail แบบกระจายไปถึงบุคคลอื่นที่ไม่เกี่ยวข้อง หรือไม่ส่ง E-Mail ที่ไม่เกี่ยวข้องกับการทำงาน เป็นต้น
8. พนักงานผู้ใช้ระบบเครือข่ายคอมพิวเตอร์ต้องไม่ปฏิบัติดังต่อไปนี้
   - การกระทำผิดกฎหมาย หรือ ก่อให้เกิดความเสียหายต่อผู้อื่น
   - การกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดี
   - เปิดเผยข้อมูลที่เป็นความลับแก่บุคคลหรือองค์กรอื่น ๆ ไม่ว่าจะเป็นข้อมูลของบริษัทฯ หรือ บุคคลภายนอก
   - การกระทำการอันมีลักษณะละเมิดทรัพย์สินทางปัญญาขององค์กร หรือ บุคคลอื่น
   - การรับหรือส่งข้อมูลที่ก่อให้เกิดความเสียหายแก่บริษัทฯ เช่น ข้อมูลที่มีลักษณะเป็นการละเมิดหรือขัดต่อกฎหมาย หรือ ละเมิดสิทธิของบุคคลอื่น
   - แสดงความคิดเห็นส่วนบุคคลในเรื่องเกี่ยวข้องกับการดำเนินงานบริษัทฯ ไปยังที่อยู่เว็บ (Website) ใด ๆในลักษณะที่ก่อให้เกิดความคาดเคลื่อนจากความเป็นจริง หรือ ทำให้บริษัทฯ เสียหาย
9. พนักงานผู้ใช้ระบบเครือข่ายภายใต้กฎระเบียบนี้ฝ่าฝืนข้อกำหนดซึ่งอาจก่อให้เกิดความเสียหายต่อบริษัทฯ หรือ บุคคลอื่นใด ทางบริษัทฯ จะดำเนินการทางวินัยและกฎหมายแก่พนักงานที่ฝ่าฝืนตามความเหมาะสม

บทที่ 3 การป้องกันโปรแกรมไม่ประสงค์ดี (Preventive Malwares)

1. เพื่อความปลอดภัยในการใช้เครือข่ายคอมพิวเตอร์โดยส่วนรวม พนักงานจะต้อง
   - ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาต้นสังกัด
   - ไม่ติดตั้งอุปกรณ์คอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัทฯ เพื่อให้บุคคลอื่นใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครือข่ายคอมพิวเตอร์ของบริษัทฯได้
   - ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองดูแลอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือ ยุติการใช้งาน เว้นแต่เครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ต้องให้บริการตลอด 24 ชั่วโมง
   - ข้อมูล ไฟล์ ซอฟต์แวร์ ที่ได้รับจากผู้ใช้งานอื่น หรือหน่วยงานภายนอกต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งาน หรือเก็บบันทึกทุกครั้ง เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น
   - ผู้ใช้งานต้องพึงระวังไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ
   - เมื่อพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ เพื่อตรวจสอบและกำจัดไวรัสคอมพิวเตอร์โดยเร็วที่สุด
   - ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลอย่างสม่ำเสมอ
   - ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล
2. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่ผู้ดูแลระบบจัดหาอย่างถูกต้อง
3. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่ก่อให้เกิดความเสียหายต่อบริษัทฯ
4. ผู้ดูแลระบบ (System Administrator) มีการติดตั้งระบบไฟร์วอลล์ (Firewall) ระหว่างการเชื่อมต่อเครือข่ายของบริษัทฯ กับหน่วยงานภายนอก
5. ผู้ดูแลระบบ (System Administrator) ต้องควบคุมไม่ให้บุคคลหรือหน่วยงานข้างนอกที่ไม่ได้รับอนุญาต ใช้เครือข่ายเข้าสู่ระบบ Internet, E-Mail เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา
6. ผู้ดูแลระบบมีสิทธิที่จะระงับหรือ หยุดการใช้งานเครื่องคอมพิวเตอร์เครือข่าย ที่มีพฤติกรรมการใช้งานผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข
7. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครือข่ายบริษัทฯ จะต้องบันทึกรายการของการดำเนินงาน และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาก่อน
8. ผู้ละเมิดนโยบายการป้องกันโปรแกรมไม่ประสงค์ดี จะถูกระงับการใช้งานทันที

บทที่ 4 นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

1. กำหนดให้มีมาตรการควบคุมการเข้าและออกห้องคอมพิวเตอร์แม่ข่าย (Server) ต้องมีการจดบันทึกไว้ทุกครั้ง กรณีบุคคลภายนอกเข้าและออกจะต้องมีเจ้าหน้าที่สารสนเทศดูแลอย่างใกล้ชิด
2. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการการใช้งานเพื่อควบคุมให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น
3. ทุกเส้นทางเชื่อมต่อ Internet และ บริการ Internet ที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์ (Firewall)
4. ผู้ดูแลระบบจะต้องทำการตรวจสอบข้อมูลการใช้งานหรือเชื่อมต่อทางคอมพิวเตอร์ (Log) เป็นประจำและต้องเก็บรักษาข้อมูล (Log) ไว้ตามกฎหมายที่กำหนดไว้อย่างน้อย 90 วัน
5. เครื่องคอมพิวเตอร์เครือข่ายส่วนบุคคล แต่ละเครื่องกำหนดให้มีผู้รับผิดชอบประจำเครื่อง ห้ามบุคคลภายนอก หรือ ผู้ที่ไม่เกี่ยวข้องใช้งาน
6. ไม่อนุญาตให้บุคคลใดทำการเคลื่อนย้ายคอมพิวเตอร์ หรือ อุปกรณ์ต่อพ่วงโดยพลการ เพราะอาจทำความเสียหายต่ออุปกรณ์อื่น ๆ ได้หากต้องการเคลื่อนย้ายต้องแจ้งผู้ดูแลระบบให้อนุญาตก่อน
7. ห้ามผู้ใช้ระบบเครือข่ายนำบุคคลภายนอก หรือ ผู้ที่ไม่เกี่ยวข้อง ทำการแก้ไข ติดตั้งอุปกรณ์ คอมพิวเตอร์ Software หรือ Hardware โดยเด็ดขาด หากไม่ได้รับอนุญาตจากผู้ดูแลระบบ
8. ไม่อนุญาตให้ผู้ใช้งานคอมพิวเตอร์เครือข่าย ทำการเชื่อมต่อเครือข่าย Internet นอกเหนือจากเครือข่ายที่ผู้ดูแลระบบกำหนดไว้
9. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

บทที่ 5 นโยบายความปลอดภัยการสำรองข้อมูล (Backup Policy)

1. ให้มีการจัดเก็บสำรองข้อมูล (Backup Data) และ ซอฟต์แวร์ (Backup Software) ให้ทันสมัยอยู่ตลอดเวลา และจัดเก็บไว้ในที่ปลอดภัย ไม่เสี่ยงต่อการรั่วไหลของข้อมูล
2. กำหนดให้มีขั้นตอนการปฏิบัติการสำรองข้อมูล และ การกู้คืนข้อมูล อย่างเป็นระบบและถูกต้อง
3. การสำรองข้อมูลจะต้องมีการจดบันทึกรายละเอียดการสำรองให้ชัดเจนเพื่อความสะดวกในการเรียกใช้งาน เช่น วันที่, เวลา, ผู้สำรองข้อมูล
4. กำหนดให้มีการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าสามารถใช้งานได้
5. ต้องกำหนดแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับมาได้ภายในระยะเวลาที่เหมาะสม

บทที่ 6 นโยบายความปลอดภัยของอินเตอร์เน็ต และ อีเมล์ (Internet Security and E-Mail Policy)

1. ผู้ที่มีสิทธิ์ใช้ระบบ Internet หรือ E-Mail ต้องทำเรื่องขออนุญาตผู้จัดการฝ่ายต้นสังกัดก่อน จากนั้นจึงส่งเรื่องต่อให้ผู้จัดการฝ่ายสารสนเทศอนุญาตต่อไป เพื่อกำหนดบัญชีชื่อผู้ใช้งาน (User Name) และ รหัสผ่าน (Password)
2. ไม่อนุญาตให้ใช้ Internet ของบริษัทฯ หาประโยชน์เชิงพาณิชย์เป็นการส่วนบุคคล
3. ไม่อนุญาตให้เข้าสู่เว็บไซต์ (Website) ที่ขัดต่อศีลธรรม หรือ เว็บไซต์ที่เป็นภัยต่อสังคม หรือ ละเมิดสิทธิผู้อื่น หรือข้อมูลที่ก่อให้เกิดความเสียหายต่อบริษัทฯ
4. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับบริษัทฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)
5. การดาวน์โหลดข้อมูล (Download) จากระบบ Internet ต้องไม่ละเมิดลิขสิทธิ์ผู้อื่น และ อนุญาตให้ดาวน์โหลดข้อมูล (Download) เฉพาะที่เกี่ยวข้องกับการทำงาน หรือ เพื่อหาความรู้ทั่วไปเท่านั้น
6. การใช้งานโปรแกรมสนทนาทาง Internet ต้องไม่เปิดเผยข้อมูลสำคัญของบริษัทฯ และไม่ละเมิดสิทธิ์ผู้อื่น ไม่ใช้ถ้อยคำที่ไม่สุภาพ ไม่ใช้ถ้อยคำที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อหน่วยงาน หรือ ทำลายความสัมพันธ์กับบุคคลในบริษัทฯ
7. ไม่อนุญาตให้พนักงาน Download โปรแกรม ผ่านทาง Internet หากไม่ได้รับอนุญาตจากผู้ดูแลระบบ
8. หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้วให้ปิดเว็บเบราว์เซอร์ (Web Browser) เพื่อป้องกันบุคคลอื่นเข้าไปใช้งาน
9. ไม่ควรส่ง E-Mail ให้กับผู้ที่ไม่เกี่ยวข้อง, หรือ E-Mail ที่มีรูปภาพ ข้อความที่ผิดต่อกฎหมาย
10. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวจดหมายอิเล็กทรอนิกส์ (E-mail)
11. ไม่ควรใช้ที่อยู่จดหมายอิเล็คทรอนิคส์ (E-mail address) ของผู้อื่น เพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่ได้รับการยินยอมจากเจ้าของ และให้ถือว่าเจ้าของ E-mail เป็นผู้รับผิดชอบต่อการใช้งาน E-mail ของตน
12. ควรทำการตรวจสอบเอกสารแนบจาก E-mail ก่อนทำการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น
13. ควรลบ E-mail ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ในระบบ E-mail
12. ผู้ละเมิดนโยบายความปลอดภัยของอินเตอร์เน็ต และ อีเมล์ (Internet Security and E-Mail Policy) จะถูกระงับการใช้งาน Internet หรือ E-Mail ทันที

บทที่ 7 นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

1. ให้มีการใช้งานเครื่องมือหรืออุปกรณ์ในการควบคุมการเข้าออกห้องแม่ข่าย (Server) ด้วย เครื่องสแกนลายนิ้วมือหรืออย่างอื่นที่เหมาะสม
2. ให้มีการเก็บบันทึกการเข้าออกห้องแม่ข่าย (Server) เพื่อเป็นหลักฐานในการตรวจสอบ
3. เมื่อมีบุคคลภายนอกต้องการเข้ามายังห้องแม่ข่าย ต้องมีการขออนุญาตจากผู้มีหน้าที่รับผิดชอบ และมีเจ้าที่หน้าที่สารสนเทศอยู่ด้วย
4. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
5. ผู้ดูแลระบบ (System Administrator) เท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้
5. ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ
6. รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย ห้ามใช้ Account ร่วมกันหรือให้ผู้อื่นเข้าใช้งาน Account ของตนโดยเด็ดขาด ทั้งนี้ รวมถึงสมาชิกใน ครอบครัวเมื่อผู้ใช้งานนำงานกลับไปทำที่บ้านด้วย
7. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่าน User ID และรหัสผ่านของตนทั้งหมด
8. หากผู้ใช้งานสงสัยว่า User ID หรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อผู้ดูแลระบบ (System Administrator) และทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที
9. การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนด ให้มีระเบียบปฏิบัติอย่างเป็นทางการเพื่อให้สามารถใช้งาน ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ ในกรณีที่ผู้ใช้งานสิ้นสุดสถานภาพต้องยกเลิกสิทธิ์การใช้งานออกจากระบบทันที

บทที่ 8 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

1. ให้มีการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ เช่น คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์, ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ , ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข , เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
2. เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่าง ๆ จะต้อง ตรวจสอบและทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย
3. จัดเก็บโปรแกรม Version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับสู่สภาพเดิมของระบบงาน ในกรณีระบบงานผิดพลาด หรือไม่สามารถใช้งานได้

บทที่ 9 ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ (Security of System Files)

1. การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ใช้อยู่เดิม โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็น อย่างดีว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ใช้อยู่
2. การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code) ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย และต้องไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริง แล้ว

บทที่ 10 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

1. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง
2. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อการประเมินความเสี่ยงนั้นๆ
3. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น
4. ติดตามการดำเนินการตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานที่ได้กำหนดไว้
5. ทบทวนและปรับปรุงแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง ให้สอดคล้องกับสถานการณ์

ลงชื่อ  ผู้อนุมัตินโยบาย

(นายพงศ์เทพ เหลืองสุวรรณ)

ประธานเจ้าหน้าด้านบริหารจัดการ

18 กุมภาพันธ์ 2565