บริษัท เอเชียน มารีน เซอร์วิสส์ จำกัด (มหาชน)

ASIAN MARINE SERVICES PUBLIC COMPANY LIMITED

ประกาศที่ EXC-A67054
เรื่อง นโยบายการรักษาความมั่นคงความปลอดภัยไซเบอร์
Cyber Security Policy

วัตถุประสงค์

1.เพื่อกำหนดนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ บริษัท เอเชียน มารีน เซอร์วิสส์ จำกัด(มหาชน) ตระหนักถึงความสำคัญของการรักษาความมั่นคงและความปลอดภัยด้านสารสนเทศ และปฏิบัติตามอย่างเหมาะสม

2.เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศของ องค์กร ว่าสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีความพร้อมใช้งาน (Availability)

3.เพื่อเผยแพร่ให้เจ้าหน้าที่และผู้ใช้งานสารสนเทศของ บริษัท เอเชียน มารีน เซอร์วิสส์ จำกัด (มหาชน) ได้รับทราบและปฏิบัติอย่างเคร่งครัด

ขอบเขต

1.จัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติในการรักษาความมั่นคงและความปลอดภัยด้านสารสนเทศ เป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.จัดให้ข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ สถานที่และสิ่งแวดล้อมที่เกี่ยวข้องกับ สารสนเทศ การพัฒนาและบำรุงรักษาระบบสารสนเทศ และสิ่งใดๆที่เกี่ยวข้องกับสารสนเทศ มีการรักษาความมั่นคงปลอดภัยอย่าง เหมาะสมและเพียงพอ และมีการควบคุมการเข้าถึงที่กำหนดอย่างชัดเจนตามหลักการของความต้องการในการใช้งานที่เหมาะสม และมั่นคงปลอดภัย

3.จัดให้มีระบบสำรองข้อมูล ระบบกู้คืนข้อมูล และระบบสำรองที่ใช้ทดแทนระบบเทคโนโลยีสารสนเทศหลักในกรณีฉุกเฉิน โดยระบบสำรองต้องอยู่ในสภาพพร้อมใช้งาน และมีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

4.จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยมีแนวทางสอดคล้องกับการบริหารความเสี่ยงของทางแผนก IT

5.จัดให้มีการตรวจสอบและกำเนินการแก้ไข เมื่อมีเหตุการละเมิดความมั่นคงปลอดภัยเกิดขึ้น พร้อมทั้งดำเนินการป้องกันไม่ให้เกิดซ้ำ และให้รายงานและบันทึกไว้อย่างชัดเจน

6.จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย แนวทางปฏิบัติ มาตรฐาน และระเบียบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

คำจำกัดความ

1. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การรักษาไว้ซึ่งความลับ ความถูกต้องครบถ้วน และความพร้อมใช้ตามความต้องการด้านความมั่นคงปลอดภัยของสารสนเทศนั้นๆรวมถึงความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

2. แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ควรปฏิบัติตาม เพื่อให้สามารถบรรลุวัตถุประสงค์ได้ง่ายขึ้น

3. ข้อกำหนด (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์

4. ขั้นตอนปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้บรรลุวัตถุประสงค์ที่ได้กำหนดไว้

5. ผู้ใช้งาน (User) หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ องค์กร ตามสิทธิและหน้าที่ของผู้ใช้งาน

6. เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ หรือ "เจ้าหน้าที่สารสนเทศ" หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายให้สามารถเข้าใช้งานและบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของ องค์กร โดยแบ่งออกได้ดังนี้

- "ผู้ดูแลระบบ" (System Administrator) หมายถึง บุคคลที่ได้รับมอบหมายจากผู้บังคับชาให้มีหน้าที่รับผิดชอบในการดูแลรักษา ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านฮาร์ดแวร์และซอฟต์แวร์ ซึ่งสามารถเข้าถึงระบบงานหรือระบบจัดการ ฐานข้อมูลของ องค์กร เช่น การกำหนดสิทธิ์ของผู้ใช้ เป็นต้น
- "ผู้พัฒนาระบบ" (System Developer) หมายถึง บุคคลที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนา ระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- "บุคคลภายนอก" ที่มาดำเนินการติดตั้ง หรือบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งให้คำปรึกษาหรือ ปฏิบัติตามสัญญาจ้าง

7. ข้อมูลคอมพิวเตอร์ (Data) หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

8. "ข้อมูลจราจรทางคอมพิวเตอร์" (Log) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง วันที่ เวลา ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆที่เกี่ยวข้องกับการสื่อสารของระบบคอมพิวเตอร์นั้น

9. "สารสนเทศ" (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ใน รูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ โดยหมายรวมถึงสารสนเทศที่อยู่ในรูปแบบของอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์

10. "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน และ หน่วยงานภายนอก เข้าถึงหรือใช้งานระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบเครือข่าย ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

11. "ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่ทำให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลและจัดเก็บข้อมูลโดยอัตโนมัติ

12. "ระบบเครือข่าย" (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่าง ระบบเทคโนโลยีสารสนเทศต่างๆของ องค์กร เช่น ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

— "ระบบอินทราเน็ต" (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงาน เข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

— "ระบบอินเทอร์เน็ต" (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ขององค์กร เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

13. "ระบบเทคโนโลยีสารสนเทศ" (Information Technology System) หมายถึง ระบบงานขององค์กร ที่นำเอาเทคโนโลยี สารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่องค์กร สามารถนำมาใช้ประโยชน์ในการวางแผนการบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบ คอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

14. “ห้องควบคุมระบบคอมพิวเตอร์” หรือ “ห้องเครื่องแม่ข่าย” หมายถึง ห้องที่จัดเตรียมพื้นที่ไว้สำหรับการติดตั้งเครื่องมือที่เป็น อุปกรณ์หลัก ของระบบคอมพิวเตอร์และระบบการสื่อสารขององค์กร อาทิเช่น เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องจัดเก็บ ข้อมูลคอมพิวเตอร์ (Data Storage) อุปกรณ์เครือข่าย เป็นต้น

15. “เจ้าของข้อมูล” หมายถึง บุคคลหรือหน่วยงานที่รับผิดชอบในสินทรัพย์ข้อมูลและเอกสาร (information and Document Asset) โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย

16. “เจ้าของระบบ” หมายถึง บุคคลหรือหน่วยงานที่รับผิดชอบในระบบ (System Owner) โดยเจ้าระบบเป็นผู้รับผิดชอบระบบงาน นั้นๆ หรือได้รับผลกระทบโดยตรงหากระบบนั้นเสียหาย

17. “สินทรัพย์สารสนเทศ” หมายถึง สินทรัพย์ข้อมูลและเอกสาร (information and Document Asset) สินทรัพย์ซอฟต์แวร์และ โปรแกรมประยุกต์ (Software and Application Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) ที่เกี่ยวข้องกับงานสารสนเทศ

18. “จดหมายอิเล็กทรอนิกส์” (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และ เครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่ง ข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail Box) ที่กำหนดไว้สำหรับผู้ใช้ในเครือข่าย ผู้รับสามารถเปิดอ่านข่าวสาร พิมพ์ลงกระดาษ หรือลบทิ้งได้

19. “ชื่อผู้ใช้งาน” (Username) หมายถึง ชุดตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นมาเพื่อใช้ในการเข้าใช้งานในระบบสารสนเทศที่ กำหนดสิทธิการใช้งานไว้

20. “รหัสผ่าน” (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุม การเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

21. “โปรแกรมไม่พึงประสงค์” หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

22. “เหตุการณ์ที่ละเมิดความมั่นคงปลอดภัย” (IT Security Incident) หมายถึง เหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งอาจทำาให้ระบบสารสนเทศขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

23. “ระบบที่มีผลกระทบและมีความสำคัญสูงต่อองค์กร” ได้แก่ ระบบบริหารโครงการออนไลน์และระบบบัญชีการเงินและพัสดุ

หน้าที่และความรับผิดชอบ

<u>ระดับนโยบาย</u>

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

ตำแหน่ง ผู้จัดการแผนกเทคโนโลยีสารสนเทศ

<u>ระดับปฏิบัติ</u>

รับผิดชอบ กำกับดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษาทบทวนวางแผน ติดตาม การบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่

ตำแหน่ง IT SUPPORT

รับผิดชอบดูแลบำรุงรักษา ระบบเครื่อง ระบบเครือข่าย โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่างๆ ของระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งการทำสำเนาฐานข้อมูล ผู้รับผิดชอบ ได้แก่

ตำแหน่ง IT SUPPORT

ตำแหน่ง IT SUPPORT

รับผิดชอบในการรักษาความปลอดภัย ของแต่ละระบบฐานข้อมูล ผู้รับผิดชอบ ได้แก่

ตำแหน่ง Programmer

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

บริษัท เอเชียน มารีน เซอร์วิสส์ จำกัด(มหาชน) มีการควบคุมการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เพื่อ กำหนดมาตรการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศโดยไม่ได้รับอนุญาต ป้องกันการบุกรุกทั้งด้านกายภาพ ผ่านระบบเครือข่าย และจากโปรแกรม ที่จะสร้างความเสียหายแก่ข้อมูลหรือทำให้ระบบหยุดชะงัก และสามารถตรวจสอบติดตามการพิสูจน์ตัวบุคคลที่ใช้งาน ข้อมูลหรือระบบสารสนเทศขององค์กรได้อย่างถูกต้องโดยยึดหลักดังนี้

1. การรักษาความลับ (Confidentiality) ให้บุคคลผู้มีสิทธิ์เท่านั้น เข้าถึงข้อมูลได้ และมีการควบคุมการเข้าถึงโดยข้อมูลที่เป็นความลับ จะได้ไม่ถูกเปิดเผยกับผู้ไม่มีสิทธิ์

2. ความถูกต้องครบถ้วน (Integrity) ให้มีการรักษาความถูกต้องครบถ้วนของข้อมูล และควบคุมความผิดพลาด ไม่ให้ข้อมูลถูกแก้ไข ลบทิ้ง เปลี่ยนแปลงโดยผู้ไม่มีสิทธิ

3. ความสามารถในการเข้าถึงและใช้งานได้ (Availability) ให้ผู้มีสิทธิ์ใช้ข้อมูลเท่านั้นสามารถที่จะเข้าถึงข้อมูลได้ตามเวลาที่ตกลงไว้ ผู้รับผิดชอบต้องควบคุมไม่ให้ระบบหยุดชะงัก มีสมรรถภาพในการทำงานต่อเนื่อง และมีการป้องกันไม่ให้มีสิ่งใดทำให้ระบบหยุดทำงาน

1.การควบคุมการเข้าถึงข้อมูลสารสนเทศ (Folder/File Shared)

1.1. อนุญาตให้ผู้ใช้งานเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจาก ผู้บังคับบัญชา/ เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น โดยมีการกำหนดขั้นตอนและแบบฟอร์มในการขออนุญาตเข้าถึง

1.2. การลงทะเบียนผู้ใช้งาน (User Registration) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน โดยต้องระบุข้อมูลพื้นฐานเป็นอย่างน้อย ดังนี้ ชื่อและนามสกุล ตำแหน่ง หน่วยงาน ระยะเวลาในการใช้งาน

1.3. ตัดผู้ใช้งานออกจากทะเบียนโดยปฏิบัติตามขั้นตอนปฏิบัติของการตัดผู้ใช้งาน เมื่อสิ้นสุดหน้าที่ตามงานที่รับผิดชอบ เช่น การโอนย้ายงาน การลาออก

1.4. กำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application System) สิทธิ การใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่ และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การ ปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

1.5. ต้องให้สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น กรณีมีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิ์ผู้ใช้งานรายอื่น ให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การแบ่งปันแฟ้มข้อมูล (Share Files) รวมถึงกำหนดระยะเวลา การใช้งานและยกเลิกการให้สิทธิ์ดังกล่าวทันทีที่ไม่มีความจำเป็นแล้วหรือพ้นระยะเวลาที่กำหนด

1.6. ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง และทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้าย หน่วยงาน หรือสิ้นสุดการจ้างงาน

2.การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

2.1. ผู้ใช้งานควรออกจากระบบเทคโนโลยีสารสนเทศขององค์กร โดยทันที เมื่อเสร็จสิ้นการใช้งาน เช่น ออกจากระบบงาน ออกจาก เครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้งาน (Log out)

2.2. ผู้ใช้งานควรป้องกันไม่ให้ผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศ โดยการกำหนดให้ต้องใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

2.3. ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอ หลังจากที่ไม่ได้ใช้งานมาช่วงระยะเวลาหนึ่งโดยอัตโนมัติ เช่น 15 นาที หลังจากที่มีการล็อคหน้าจอแล้วนั้น ต้องใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบงานได้

2.4. ผู้ใช้งานควรปิดเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือไม่มีการใช้งาน นานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ซึ่งต้องใช้งานตลอด 24 ชั่วโมง ให้ ผู้ดูแลระบบออกจากระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายหรือล็อคหน้าจอ

3.การเข้าถึงระบบเครือข่าย

3.1. จัดระบบเครือข่ายเพื่อให้บริการแก่บุคลากรขององค์กร และผู้ที่ได้รับอนุญาตเท่านั้น

3.2. ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานต้องรับรองว่า หากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบขององค์กร

3.3. ไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การ ให้บริการโฆษณาสินค้า

3.4. ห้ามผู้ใช้งานละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่ไม่ใช่ของตน การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่ สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียวองค์กร ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

3.5. ห้ามผู้ใดเข้าใช้งานโดยไม่ได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามกระทำผิด

3.6. ห้ามผู้ใช้งานกระทำการโอนหรือจ่ายแจกบัญชีผู้ใช้งานนี้ให้กับผู้อื่น เนื่องจากบัญชีผู้ใช้งาน (User Account) เป็นการมอบให้เฉพาะ บุคคลเท่านั้น

3.7. กำหนดให้ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ ที่อาจจะเกิดขึ้น รวมถึงผลเสียหายที่เกิดจากการใช้บัญชีผู้ใช้งาน (User Account) ที่องค์กร มอบให้ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น โดยไม่ได้เกิดจากความประมาทเลินเล่อของ ผู้ใช้งาน

3.8. กำหนดให้ผู้ใช้งานระบบเครือข่ายขององค์กร ต้องผ่านพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้บริการ

3.9. กำหนดให้ผู้ใช้งานระบบเครือข่ายไร้สายขององค์กร ใช้งานด้วยชื่อเครือข่าย หรือ SSID (Sub Station Identifier) และ มีระยะเวลาการ ใช้งาน ตามสถานภาพ สิทธิ์หรือประเภทของผู้ใช้งาน

3.10. การนำอุปกรณ์เทคโนโลยีสารสนเทศส่วนตัวมาใช้งาน (BYOD : Bring Your Own Device) และเชื่อมต่อกับระบบเครือข่าย ต้องผ่านการตรวจสอบความปลอดภัยบนอุปกรณ์นั้นๆ จึงสามารถอนุญาตให้เข้าใช้บริการเชื่อมต่อกับระบบเครือข่ายองค์กร ได้

3.11. กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายเพื่อใช้สารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

3.12. ห้ามเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงทุกประเภท ในระหว่างปฏิบัติงาน เว้นแต่บุคคลนั้นจะได้รับการพิจารณายกเว้นว่า เป็นการกระทำในหน้าที่การปฏิบัติงาน จากผู้บังคับบัญชา

4.การควบคุมการจัดเส้นทางบนเครือข่าย

4.1. ใช้อุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์เครือข่ายคอมพิวเตอร์เพื่อตรวจสอบเลขที่อยู่ไอพี (IP Address) ของทั้งต้นทางและ ปลายทาง ทำให้เครือข่ายที่แตกต่างกันสามารถสื่อสารกันได้ และควบคุมการถ่ายโอนของข้อมูลผ่านเครือข่ายต่างๆ จากเครือข่าย หนึ่งไปสู่อีกเครือข่ายหนึ่ง

4.2. ควบคุมไม่ให้มีการเปิดเผยแผนการใช้งานเลขที่อยู่ไอพี

4.3. กำหนดให้มีการแปลงเลขที่อยู่ไอพีและชื่อโดเมน เพื่อแยกเครือข่ายย่อย หรือแยกเครือข่ายภายในและภายนอก

4.4. จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์หนึ่งเครื่องใด ไปยังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่าย โดยไม่ อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

4.5. กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้หรือจำกัดสิทธิ์ในการ เข้าใช้บริการระบบเครือข่ายตามสิทธิ์ที่ได้รับ

4.6. ไม่อนุญาตให้บุคคลใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใดๆ ต่ออุปกรณ์เครือข่ายส่วนกลาง ได้แก่ อุปกรณ์จัด เส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย โดยไม่ได้รับอนุญาตจากผู้ดูแล ระบบ (System Administrator)

4.7. ไม่อนุญาตผู้ใช้งานทำการเปลี่ยนแปลงเลขที่อยู่ไอพี หรือกำหนดค่าเลขที่อยู่ไอพีของเครื่องคอมพิวเตอร์ภายในหน่วยงาน โดยไม่ได้ รับอนุญาตจากผู้ดูแลระบบ

4.8. ต้องดำเนินการใดๆ เพื่อยุติการกระทำของผู้ใช้งานที่ไม่เป็นไปตามแนวปฏิบัตินี้และในกรณีที่จำเป็นให้ระงับการใช้ระบบเครือข่าย ของผู้ใช้งานดังกล่าว เพื่อป้องกันหรือบรรเทาความเสียหายที่อาจเกิดขึ้นแก่องค์กร

5.การเข้าถึงระบบปฏิบัติการ

5.1. จัดให้มีระบบปฏิบัติการ (Operating System) ไว้เพื่อรองรับการปฏิบัติงานที่เกี่ยวข้องกับองค์กร เท่านั้น

5.2. ควบคุมการแก้ไขหรือปรับแต่งค่าในระบบปฏิบัติการ ต้องผ่านการอนุมัติจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร

5.3. กำหนดให้ผู้ใช้งานแต่ละบุคคลมี ชื่อผู้ใช้และ รหัสผ่าน ในการใช้งานระบบปฏิบัติการหรือเครื่องคอมพิวเตอร์ตามบทบาทหน้าที่ที่ บุคคลนั้นได้รับเท่านั้น

5.4. ต้องระบุชื่อผู้ใช้และ รหัสผ่าน ทุกครั้งก่อนการเข้าใช้ระบบปฏิบัติการ

5.5. ต้องตั้งค่าการใช้งานโปรแกรมรักษาหน้าจอ (Screen saver) ทำการล็อคหน้าจอภาพ เมื่อไม่มีการใช้งาน หรือลงบันทึกออก (Log out) จากระบบปฏิบัติการทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน หลังจากนั้นเมื่อต้องการใช้งานระบบปฏิบัติการอีก ต้องใส่รหัสผ่านอีกครั้งเพื่อเข้าใช้งาน

5.6. ควบคุมการใช้งาน ชื่อผู้ใช้ และ รหัสผ่าน ของระบบปฏิบัติการของตน ไม่นำชื่อผู้ใช้ และ รหัสผ่าน ของตนไปมอบให้บุคคลอื่น

5.7. ควบคุมการนำ ชื่อผู้ใช้ และ รหัสผ่าน ของผู้ใช้คนหนึ่งๆ ไปเพิ่มสิทธิ์ให้เข้าใช้งานกับระบบปฏิบัติการของเครื่องคอมพิวเตอร์เครื่อง อื่น ให้ดำเนินการโดยผู้ดูแลระบบเท่านั้น โดยกำหนดสภาพแวดล้อมพื้นฐานของระบบปฏิบัติการเครื่องนั้นๆ แยกบัญชีผู้ใช้จากผู้ใช้ รายอื่น (Multi-User/Multi-Identity Profiles) และกำหนดสิทธิ์ตามบทบาทหน้าที่สำหรับระบบปฏิบัติการนั้น

5.8. ควบคุมการติดตั้งซอฟต์แวร์คอมพิวเตอร์ที่มีลิขสิทธิ์ขององค์กร ลงบนระบบปฏิบัติการ โดยผู้ใช้งานขออนุมัติต่อผู้บังคับบัญชาและ ผู้บริหารองค์กร เพื่อขอใช้งานเพิ่มเติมได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้ งานซอฟต์แวร์อื่นใดที่ละเมิดลิขสิทธิ์ลงบนระบบปฏิบัติการที่องค์กร ใช้งาน หากตรวจพบให้ผู้ดูแลระบบลบทิ้ง และนับเป็นความผิด ที่ผู้ใช้งานผู้นั้นต้องรับผิดชอบต่อความผิด

5.9. ควบคุมการติดตั้งโปรแกรมประยุกต์สำหรับการใช้งานทั่วไป โดยผู้ใช้งานขออนุมัติต่อผู้บังคับบัญชาและผู้จัดการฝ่ายและผู้บริหาร เพื่อขอใช้งานเพิ่มเติมได้ตามความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งโปรแกรมประยุกต์อื่นใดที่ละเมิดลิขสิทธิ์ ลงบนระบบปฏิบัติการที่องค์กร ใช้งานด้วยตนเองหากตรวจพบให้ผู้ดูแลระบบลบทิ้งและนับเป็นความผิดที่ผู้ใช้งานผู้นั้นต้อง รับผิดชอบต่อความผิด

5.10. ควบคุมการติดตั้ง ถอนการติดตั้ง หรือปรับเปลี่ยนการกำหนดค่าการทำงานของซอฟต์แวร์หรือโปรแกรมประยุกต์ โดยให้ผู้ดูแล ระบบพิจารณาผลกระทบกับระบบปฏิบัติการก่อนการดำเนินการ

5.11. ห้ามใช้ซอฟต์แวร์ระบบปฏิบัติการขององค์กร เพื่อประโยชน์ทางการค้าใดๆ หรือเพื่อผลประโยชน์ส่วนตัว

5.12. ห้ามผู้ใช้งานระบบปฏิบัติการ กระทำการใดๆ เพื่อควบคุมคอมพิวเตอร์เครื่องอื่น โดยเชื่อมต่อทั้งจากภายในไปสู่ภายนอก หรือจาก ภายนอกเข้ามาสู่ระบบปฏิบัติการภายใน โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

5.13. ควบคุมโดยตัดการใช้งานเมื่อไม่ได้มีการใช้งานเกินกว่าระยะเวลาที่กำหนด และล็อคหน้าจอสำหรับระบบปฏิบัติการที่มีความสำคัญ

5.14. ควบคุมระยะเวลาการเชื่อมต่อเพื่อเข้าถึงระบบปฏิบัติการที่มีความสำคัญหรือมีความเสี่ยงสูง ให้เข้าถึงได้ในระยะเวลาที่กำหนด หรือเป็นไปตามที่ผู้ดูแลระบบกำหนดไว้

5.15. จัดให้มีระบบบันทึกการเข้าใช้งานระบบปฏิบัติการ ที่ระบุถึงชื่อผู้ใช้ วันที่และเวลาที่เข้า/ออกระบบปฏิบัติการ

5.16. ห้ามมิให้ผู้ใช้งานกระทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไขระบบปฏิบัติการหรือทำสำเนา เพื่อนำไปใช้งานที่อื่นโดยไม่ได้รับ อนุญาต เนื่องจากระบบปฏิบัติการที่องค์กร จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นและสำคัญ

5.17. ห้ามทำการปรับแต่งไบออส (BIOS) โดยมิได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ เนื่องจากส่งผลกระทบกับการทำงานของ คอมพิวเตอร์และระบบปฏิบัติการ

5.18. กำหนดให้มีการจัดทำและประกาศใช้มาตรการดำเนินการสำหรับผู้กระทำผิด

6.การเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์ (โปรแกรมระบบ ERP)

6.1.กำหนดให้ผู้ดูแลระบบต้องควบคุม จำกัด หรือให้สิทธิ์การเข้าถึงสารสนเทศ ข้อมูลและฟังก์ชั่นต่าง ๆ ของระบบสารสนเทศและ โปรแกรมประยุกต์ ดังนี้

- ต้องลงทะเบียนการเข้าใช้งานเพื่อทำการระบุตัวตน
- ให้เข้าถึงได้เฉพาะส่วนระบบงานและฟังก์ชั่นที่จำเป็นต่อการทำงานและที่ได้รับอนุญาตเท่านั้น
- ให้เข้าถึงได้เฉพาะข้อมูลที่จำเป็นต่อการใช้งานและที่ได้รับอนุญาตเท่านั้น
- ห้ามไม่ให้กระทำการโอนย้ายสิทธิ์แก่ผู้อื่น โดยสิทธิ์การเข้าใช้งานให้เป็นสิทธิ์เฉพาะบุคคลเท่านั้น
- ให้ทำการยกเลิกสิทธิ์การเข้าใช้งานทันทีที่ผู้ได้รับสิทธิ์นั้น ไม่ได้รับสิทธิ์การเข้าใช้งานอีกต่อไป

6.2.กำหนดให้ผู้ดูแลระบบต้องทำการควบคุมหรือจำกัดสิทธิ์การเข้าถึงระบบงานซึ่งถูกเข้าถึงจากอีกระบบงานหนึ่งดังนี้

- ให้เข้าถึงได้เฉพาะส่วนฟังก์ชั่นที่จำเป็นต่อการใช้งานและที่ได้รับอนุญาตเท่านั้น
- ให้เข้าถึงได้เฉพาะข้อมูลที่จำเป็นต่อการใช้งานและที่ได้รับอนุญาตเท่านั้น
- กำหนดให้มีการพิสูจน์ตัวตน (Authentication) ก่อนการเข้าถึงระบบงานทุกครั้ง

— กำหนดให้มีการจำกัดเส้นทางและวิธีการในการเข้าถึงระบบงานจากอีกระบบงานหนึ่ง

— กำหนดให้มีการทบทวนสิทธิ์ในการเข้าถึงอย่างน้อยปีละ 1 ครั้ง

6.3.กำหนดให้ผู้ดูแลระบบต้องทำการควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงานหนึ่ง โดยให้นำข้อมูลออกได้เฉพาะที่เกี่ยวข้อง และจำเป็นสำหรับการนำไปใช้งานเท่านั้น

6.4.กำหนดให้ระบบที่ใช้งานต้องมีการแสดงเฉพาะข้อมูลพื้นฐานเพื่อให้ผู้ใช้งานได้รับทราบข้อมูลเฉพาะที่จำเป็นและตามสิทธิ์การใช้ งานเท่านั้น

6.5.กำหนดให้ระบบที่ใช้งานต้องมีข้อจำกัดไม่ให้ระบบแสดงความช่วยเหลือใด ๆ กรณีที่มีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นในระบบ

6.6.กำหนดให้ระบบที่ใช้งานต้องมีฟังก์ชั่นที่สามารถทำการตรวจสอบและควบคุมการลงบันทึกเข้า (Login) ดังนี้

— แสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่ลงบันทึกเข้า (Login) เสร็จแล้ว

— จำกัดไม่ให้ระบบแสดงข้อความผิดพลาดจากการทำงานหรือการใช้งานในลักษณะที่เปิดเผยข้อมูลภายในของระบบ

— กำหนดให้มีการบันทึกข้อมูลลงบันทึกเข้า (Login) ทั้งที่สำเร็จและไม่สำเร็จ

— แสดงวันที่/เวลาที่ลงบันทึกเข้า (Login) ครั้งที่แล้ว (ทั้งที่สำเร็จและไม่สำเร็จ)

แนวทางป้องกันการโจมตีจากภัยคุกคาม

ทางแผนกเทคโนโลยีสารสนเทศได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานและให้พนักงานได้รับความสะดวกขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตีจากไวรัสคอมพิวเตอร์ จากบุคลากร หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ส่งผลกระทบต่อการดำเนินงานของบริษัท ทางแผนกเทคโนโลยีสารสนเทศ จึงมีแนวทางการป้องกัน ดังนี้

1.ป้องกันเหตุเกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน hardware และ software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศ ในเบื้องต้น จึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรม สัมมนา ให้มีความรู้ความเข้าใจ ในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน human error ให้น้อยที่สุด

2.ป้องกันเหตุเกิดจากไวรัสคอมพิวเตอร์ (Computer Virus)

2.1.ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัส ที่เครื่องให้บริการ (server) และเครื่องลูกข่าย (client) ซึ่งทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ 1 ครั้ง

2.2.ติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ของบริษัทได้ โดยบน Firewall จะมีการเปิดใช้งานระบบ “Intrusion Prevention System” หรือ “IPS” ตลอดเวลา เพื่อทำหน้าที่ตรวจสอบภัยคุกคามจากภายนอก โดยถ้าระบบตรวจพบผู้บุกรุกหรืออาชญากรทางไซเบอร์ก็จะทำการยับยั้งการบุกรุกในทันที

2.3.แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านเครือข่าย internet รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากไวรัสต่างๆ ให้กับผู้ใช้งาน ได้ศึกษาและสามารถปฏิบัติการป้องกันในเบื้องต้นได้ เช่น

2.3.1.ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ เช่น external harddisk แผ่นซีดี Flash disk เป็นต้น

- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จัก หรือน่าสงสัย
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

2.3.2.ใช้ความระมัดระวังในการเปิด E-mail

- อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
- ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

2.3.3.ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet

- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น ICQ MSN เป็นต้น
- ไม่ควรเข้าไปเปิด website ที่แนะนำมาทาง E-mail ที่ไม่ทราบแหล่งที่มา
- ไม่ ดาวน์โหลด ไฟล์ จาก website ที่ไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

3.มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของแผนกเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้าออก มีการใช้การล็อกแบบเข้ารหัส และ ติดตั้งกล้องวงจรปิดเพื่อป้องกันการโจรกรรม

4.การสำรองข้อมูล เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลถูกทำลายโดยไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล เป็นต้น โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยมีแนวทาง โดยมีการตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย เป็นประจำทุกวัน โดยสำรองข้อมูลไว้ใน Harddisk ของเครื่องคอมพิวเตอร์ในแผนกเทคโนโลยีสารสนเทศ นอกเหนือจากการสำรองข้อมูลไว้ในห้อง Server แล้ว ทางแผนกได้ดำเนินการสำรองข้อมูลไว้ที่ สาขาสุราษฎร์ธานี เพื่อเอาไว้ใช้เป็นสถานที่สำรองข้อมูล (Backup site) ซึ่งจะช่วยให้การสำรองข้อมูล และ การกู้ข้อมูลในสถานการณ์ฉุกเฉินเป็นไปอย่างมีประสิทธิภาพยิ่งขึ้น

จึงประกาศมาให้พนักงานทราบโดยทั่วกัน

ประกาศ ณ วันที่ 10 ธันวาคม 2567

(นายสุรเดช ตัณฑ์ไพบูลย์)
ประธานเจ้าหน้าที่บริหาร

SCI
Board up to date: 31 January 2025
CC: SRD, NP, RPP
CC: ASS, JYK, KKP, PSP, WWP, NWK, SLW, SMK, TTT, TWT, SLS, NKP, PSJ, TWL, AKN, TLK, KAT, TPS, SSP, ACL, PYN, NTP, ECO, คสส.