นโยบายความมั่นคงปลอดภัย
ของระบบเทคโนโลยีสารสนเทศ
กลุ่มบริษัท อาปิโก
พุทธศักราช 2566

โดย

แผนกเทคโนโลยีสารสนเทศ
บริษัท อาปิโก ไฮเทค จำกัด (มหาชน)
วันที่มีผลบังคับใช้ 1 สิงหาคม 2566

จัดทำโดย/ IT	ทบทวนโดย/ IT Mgr.	ทบทวนโดย/ IT GM.	อนุมัติโดย/ CEO
วันที่ 12/08/23	Witthaya วันที่ 13/08/23	Somwang T. วันที่ 13/08/23	วันที่ 1/08/23

สารบัญ

เรื่อง	หน้า
นโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	1
หลักการและเหตุผล	1
วัตถุประสงค์	1
เจตนารมณ์ของนโยบาย	2
ขอบเขต	2
นิยามศัพท์	2
ส่วนที่ 1 การใช้งานทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ (Information security infrastructure)	4
ส่วนที่ 2 การเข้าถึงระบบเครือข่ายไร้สาย (Wireless)	9
ส่วนที่ 3 การใช้งานไฟร์วอลล์ (Firewall)	11
ส่วนที่ 4 การใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail)	12
ส่วนที่ 5 การใช้งานอินเทอร์เน็ต (Internet Security)	14
ส่วนที่ 6 การควบคุมการเข้าถึงข้อมูล (Access Control)	15
ส่วนที่ 7 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)	20
ส่วนที่ 8 การสำรองข้อมูลและการกู้คืนระบบ (Backup and Recovery)	22
ส่วนที่ 9 ความมั่นคงทางกายภาพห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย (Physical and Environmental Security)	24

นโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

กลุ่มบริษัท อาปิโก พุทธศักราช 2566

หลักการและเหตุผล

กลุ่มบริษัท อาปิโก ได้จัดทำนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยมีวัตถุประสงค์ เพื่อให้สารสนเทศของกลุ่มบริษัท อาปิโก มีความมั่นคงปลอดภัย อยู่ในระดับมาตรฐานสากล เป็นไปอย่างถูกต้องตามกฎหมาย การใช้งานทรัพยากรระบบสารสนเทศให้เกิดประโยชน์สูงสุด เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของกลุ่มบริษัท อาปิโก โดยเอกสารฉบับนี้จัดทำขึ้นตามกรอบมาตรฐาน ISO 17799-2005 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ โดยมีเนื้อหาครอบคลุมเรื่องดังต่อไปนี้

1. วัตถุประสงค์และความจำเป็นของการปกป้องสารสนเทศของกลุ่มบริษัทอาปิโก
2. สารสนเทศที่จำเป็นต้องปกป้องให้มีความมั่นคงปลอดภัย
3. หลักการและแนวทางการปกป้องสารสนเทศ
4. บทบาทหน้าที่และความรับผิดชอบของบุคลากรในกลุ่มบริษัท อาปิโก และบุคคลภายนอกที่เกี่ยวข้อง

วัตถุประสงค์

1. สร้างความมั่นใจว่าการใช้และการรักษาความมั่นคงปลอดภัยสารสนเทศภายในกลุ่มบริษัท อาปิโก เป็นไปอย่างถูกต้องตามกฎหมายและข้อบังคับที่เกี่ยวข้อง

2. ให้บุคลากรในกลุ่มบริษัท อาปิโก ตลอดจนบุคคลอื่นใดที่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศทราบและเข้าใจถึงข้อปฏิบัติ ข้อห้าม และความรับผิดชอบถึงการใช้งานนั้น ๆ ที่จะส่งผลให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศ และเกิดการใช้งานตรงตามวัตถุประสงค์ของการใช้งานระบบสารสนเทศของกลุ่มบริษัท อาปิโก รวมทั้งไม่ละเมิดระเบียบกฎหมาย หรือทำให้เกิดความเสียหายในการปฏิบัติงาน

3. ปกป้องสารสนเทศให้ปลอดภัยจากความสูญเสียในรูปแบบใด ๆ เช่น การสูญหายการถูกทำลาย การแก้ไขโดยไม่ได้รับอนุญาต การลักลอบนำข้อมูลไปใช้หรือเปิดเผย ตลอดจนสร้างความมั่นใจว่าสารสนเทศมีความถูกต้อง น่าเชื่อถือ และสามารถให้บริการได้

เจตนารมณ์ของนโยบาย

กลุ่มบริษัท อาปิโก ถือว่าการรักษาความมั่นคงปลอดภัยระบบสารสนเทศเป็นสิ่งสำคัญเพื่อให้กลุ่มบริษัท อาปิโก สามารถดำเนินงานได้อย่างสอดคล้องกับวิสัยทัศน์ พันธกิจ และภารกิจ

1. การเข้าถึงทรัพยากรสารสนเทศของกลุ่มบริษัท อาปิโก ต้องมีระบบควบคุมและตรวจสอบได้ภายใต้กรอบกฎหมาย และจะต้องใช้เพื่อภารกิจงานของบริษัทเท่านั้น
2. สารสนเทศที่มีระดับชั้นความลับต้องมีการปกป้องจาการเข้าถึงและแก้ไขโดยไม่ได้รับอนุญาต
3. ข้อมูลที่มีความสำคัญต่อภารกิจงานของบริษัท จะต้องมีการปกป้องไม่ให้เกิดความเสียหายหรือถูกทำลายหรือแก้ไขดัดแปลง
4. กลุ่มบริษัท อาปิโก จะต้องมีขีดความสามารถในการกู้ฟื้นระบบสารสนเทศและการสื่อสารที่เป็นหัวใจของระบบงานภายในระยะเวลาที่เหมาะสมเมื่อเกิดกรณีพิบัติภัย
5. การรักษาความมั่นคงปลอดภัยถือเป็นข้อปฏิบัติสำคัญที่ต้องพิจารณาและคำนึงถึงในทุกขั้นตอนของการพัฒนาหรือจัดซื้อระบบสารสนเทศใหม่ใด ๆ
6. กลุ่มบริษัท อาปิโก จะสร้างความตระหนักให้กับบุคลากรทุกระดับ ให้เห็นถึงความสำคัญในเรื่องความมั่นคงปลอดภัยอย่างต่อเนื่อง
7. นโยบายความมั่นคงปลอดภัยของกลุ่มบริษัท อาปิโก ต้องสามารถปรับเปลี่ยนให้สอดคล้องกับปัญหาความมั่นคงปลอดภัยและเทคโนโลยีได้อย่างเหมาะสม

ขอบเขต

นโยบายนี้มีผลบังคับใช้กับผู้ใช้งานระบบสารสนเทศของบริษัททุกระดับ ทุกตำแหน่ง โดยไม่มีการยกเว้น โดยผู้ใช้งานรวมถึง ลูกจ้าง สัญญาจ้าง ที่ต้องใช้งานระบบสารสนเทศของบริษัท ตลอดถึงบุคคลภายนอกหรือผู้ใช้งานที่ได้รับอนุญาตเข้าถึงทรัพยากรสารสนเทศของกลุ่มบริษัท อาปิโก โดยให้ถือว่านโยบายนี้ครอบคลุมสถานที่ปฏิบัติงานทั้งที่ทำการในและนอกราชอาจักรไทย สารสนเทศที่อยู่ภายใต้การปกป้องคุ้มครองอาจเป็นสารสนเทศที่จัดเก็บอยู่ในคอมพิวเตอร์ส่วนบุคคลหรือเซิร์ฟเวอร์หรืออุปกรณ์สื่อสารโทรคมนาคม ตลอดจนสารสนเทศที่ส่งผ่านระบบเครือข่าย รวมทั้งสารสนเทศที่บันทึกไว้ในสื่อบันทึกข้อมูลใด ๆ

คำนิยาม

ผู้ใช้งาน หมายถึง พนักงาน ลูกจ้าง ผู้ดูแลระบบ ผู้บริหาร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้งานระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท อาปิโก

ผู้ดูแลระบบ หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของบริษัท

ทรัพย์สิน หมายถึง อุปกรณ์หรือข้อมูลที่อยู่ในระบบเทคโนโลยีสารสนเทศ

ทรัพยากร หมายถึง สารสนเทศที่เกี่ยวข้องและอยู่ในระบบเทคโนโลยีสารสนเทศ

บริษัท หมายถึง บริษัทที่อยู่ในกลุ่มบริษัท อาปิโก

หน่วยงาน หมายถึง ฝ่ายหรือแผนกของบริษัทหรือส่วนงานที่ผู้บริหารได้มีคำสั่งจัดตั้งขึ้นเพื่อปฏิบัติงานตามที่ได้รับมอบหมาย

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของบริษัทได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

ระบบแลน (LAN) และ ระบบอินทราเน็ต (Intranet) หมายถึงระบบเครือข่ายอิเล็กทรอนิกส์ที่ชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต (Internet) หมายถึงระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของบริษัทที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่บริษัทสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่นระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

ส่วนที่ 1

การใช้งานทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

การใช้งานทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของกลุ่มบริษัท อาปิโก ต้องมีการวางระเบียบแนวทางปฏิบัติทั้งทางด้านจริยธรรม จรรยาบรรณ และให้ถูกต้องตามกฎหมายเพื่อป้องกันความเสียหายอันเกิดจากกระทำที่ไม่ถูกต้อง เพื่อรักษาภาพลักษณ์ขององค์กร เพื่อให้บุคลากรในองค์กรใช้เป็นแนวทางในการปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพ โดยมีรายละเอียดดังต่อไปนี้

หมวด 1 ว่าด้วยบัญชีผู้ใช้งานและรหัสผ่าน (User Accounts and Password)

ผู้ดูแลระบบ ต้องกำหนดนโยบายการจัดการบัญชีผู้ใช้งานและรหัสผ่านเพื่อให้เกิดความปลอดภัย โดยมีหัวข้อดังนี้

1. ผู้ดูแลระบบ ต้องกำหนดจำนวนหลักของรหัสผ่านไม่น้อยกว่า 8 หลัก ซึ่งต้องประกอบด้วย ตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)
2. ผู้ดูแลระบบ ต้องกำหนดไม่ให้ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย 3 รหัสผ่าน
3. ผู้ดูแลระบบ ต้องกำหนดให้แจ้งเปลี่ยนรหัสผ่าน (Password) ทุกๆ 90 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
4. ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง
5. ผู้ดูแลระบบ ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้ใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการทดสอบตัวตนจริงของผู้ใช้ระบบ
6. ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้รายใหม่หลังจากที่ได้รับรหัสผ่านครั้งแรก (default password) ในการเข้าใช้งานระบบ ให้ทำการเปลี่ยนรหัสผ่านโดยทันที
7. ผู้ดูแลระบบ ต้องกำหนดให้ระบบมีการล๊อกเอ้าท์ออกจากหน้าจอตัดการใช้งานผู้ใช้ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้ และรหัสผ่านอีกครั้ง

หมวด 2 ว่าด้วยการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

8. ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้แพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

9. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

10. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของบริษัท และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การถูกล็อคก็ดี หรือเกิดจาความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

หมวด 3 ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

11. ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) บริษัทที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

12. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

13. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

14. ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

15. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

16. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งาน การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ ที่บริษัทมอบหมาย

17. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของบริษัทที่ได้รับมอบหมาย

18. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทเลินเล่อของผู้ใช้งาน

19. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมทรัพย์สินไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

20. ทรัพย์สินและระบบสารสนเทศต่างๆ ที่บริษัทจัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้ในการดำเนินงานขององค์กร การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่

21. ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่บริษัทไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อบริษัท ความเสียหายใดๆ ที่เกิดขึ้นให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายนั้น

หมวด 4 ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

22. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของบริษัท หรือเป็นข้อมูลของบุคคลภายนอก

23. ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของบริษัท ถือเป็นทรัพย์สินของบริษัท ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

24. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัทหรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย การเผยแพร่โดยไม่ได้รับอนุญาตหรือนำไปใช้ในทางที่ผิดผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

25. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

26. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร บริษัทจะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่บริษัทต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับบริษัท ซึ่งบริษัทอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด 5 ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

27. ห้ามผู้ใช้งานพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ เว้นแต่ได้รับการพิจารณาและอนุมัติจากสารสนเทศของบริษัทเป็นลายลักษณ์อักษร

28. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent)

29. ห้ามเปิดหรือใช้งาน (Run) โปรแกรม ออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติงาน

30. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของบริษัท

31. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัท เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของบริษัท

32. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัทเพื่อประโยชน์ทางการค้า

33. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัท โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

34. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัทต้องหยุดชะงัก

35. ห้ามใช้ระบบสารสนเทศของบริษัท เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากแผนกเทคโนโลยีสารสนเทศ

36. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

37. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัท

หมวด 6 ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

38. บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของบริษัท ที่กำหนดหรือออกกฎระเบียบโดยอาศัยนโยบายดังกล่าวข้างต้น ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด 7 ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

~~39.~~ บริษัท ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัท อนุญาตให้ใช้งานหรือที่บริษัทมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และบริษัทห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบซอฟต์แวร์ที่ไม่มีลิขสิทธิ์แผนกเทคโนโลยีสารสนเทศมีสิทธิ์ที่จะถอดถอนโปรแกรมหรือซอฟต์แวร์นั้นโดยทันที และหากมีความผิดฐานละเมิดลิขสิทธิ์ บริษัทถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบ

40. ซอฟต์แวร์ (Software) ที่บริษัทได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด 7 ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

41. เครื่องคอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus) ตามที่บริษัทได้จัดหาหรือได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาพัฒนาระบบป้องกัน โดยต้องได้รับอนุญาตจากแผนกเทคโนโลยีสารสนเทศ

42. ข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

43. ผู้ดูแลระบบต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

44. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบทันที

45. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบทันที

46. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของบริษัท หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

47. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของบริษัท

ส่วนที่ 2
การเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)

ผู้ดูแลระบบและผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของบริษัทมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

1. การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูง และต้องมีการกำหนดรหัสผ่านในการเข้าใช้งาน

2. ห้ามผู้ใช้งาน (User) นำอุปกรณ์ระบบเครือข่ายไร้สายทุกชนิดมาติดตั้งหรือเปิดใช้งานเองในบริษัท ไม่ว่าจะเป็น Access point ,Wireless Routers, Wireless USB client หรือ Wireless card หรืออุปกรณ์อื่นใดที่มีคุณสมบัติการทำงานลักษณะเดียวกัน

3. ห้ามผู้ใช้งาน (User) เปิดระบบเครือข่ายไร้สายแบบจุดต่อจุด (ad-hoc) หรือ peer-to-peer Network

4. ผู้ใช้งาน ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของบริษัท จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากแผนกเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

5. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

6. ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

7. ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์กระจายออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

8. ผู้ดูแลระบบ ต้องแยกการเชื่อมต่อระบบเครือข่ายไร้สายจากบุคคลภายนอกออกจากระบบเครือข่ายไร้สายภายในองค์กร

9. ผู้ดูแลระบบ ต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณกระจายออกไปภายนอกหรือไม่ นอกจากนี้ การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

10. ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (Default) มาจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

11. ผู้ดูแลระบบ ต้องกำหนด ชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

12. ผู้ดูแลระบบ ต้องกำหนดค่าให้ WPA2 ในการเข้ารหัสข้อมูลระหว่างAccess Point และ Wireless LAN Client เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

13. ผู้ดูแลระบบ ต้องเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้งาน(Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address ชื่อผู้ใช้งานและรหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้

14. ผู้ดูแลระบบ ต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

ส่วนที่ 3
การใช้งานไฟร์วอลล์ (Firewall Policy)

ไฟร์วอลล์เป็นอุปกรณ์ที่มีความสำคัญในการบริหารความปลอดภัยของบริษัทเนื่องจากไฟร์วอลล์จะทำหน้าที่ควบคุมข้อมูลที่ผ่านเข้าออก เพื่อสร้างความปลอดภัยให้กับเครือข่ายขององค์กร ทั้งในด้านของการจำกัดการเชื่อมต่อ และการจำกัดการใช้งาน ไฟร์วอลล์จะทำหน้าที่กำหนดขอบเขตที่ควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ข้อมูลที่ผ่านเข้าออกไฟร์วอลล์ จะเป็นข้อมูลที่ตรงตามที่นโยบายขององค์กรกำหนดเท่านั้น นโยบายการใช้งานไฟร์วอลล์ มีไว้เพื่อใช้เป็นแนวทางปฏิบัติในการบริหาร และดูแลรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท

1. ไฟร์วอลล์ต้องกำหนดเงื่อนไขของการเชื่อมต่อหรือการให้บริการที่ได้รับอนุญาตเท่านั้น โดยกำหนดเงื่อนไขของกฎเป็น Deny All Allow Some คือ ห้ามทุกการเชื่อมต่อผ่านไฟร์วอลล์
2. กฎการเชื่อมต่อหรือการให้บริการที่กำหนดว่าได้รับอนุญาตให้ผ่านไฟร์วอลล์ได้จะต้องบันทึกเป็นเอกสาร และสำเนาให้กับผู้ดูแลระบบเครือข่ายทุกคนรับทราบ โดยเงื่อนไขของการอนุญาตจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบ และรายงานให้หัวหน้าแผนกเทคโนโลยีสารสนเทศทราบ
3. ในทุกเส้นทางการสื่อสารคอมพิวเตอร์ที่เข้าและออกจากบริษัท จะต้องได้รับการติดตั้งไฟร์วอลล์ในทุกเส้นทาง
4. เครื่องคอมพิวเตอร์แม่ข่ายที่มีการเชื่อมต่อไปยังภายนอกองค์กร จะต้องจัดให้อยู่ในDMZ (De-Militarize Zone) เสมอ
5. ต้องไม่มีกฎที่อนุญาตให้การสื่อสารจากภายนอกองค์กรใด ผ่านเข้าไปในองค์กรได้โดยจะยอมให้เข้ามาในส่วน DMZ ได้เท่านั้น
6. ผู้ดูแลระบบจะต้องตรวจสอบการทำงานของไฟร์วอลล์ จากบันทึกการทำงาน (log file) อย่างสม่ำเสมอ

ส่วนที่ 4
การใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail Policy)

1. ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงจดหมายอิเล็กทรอนิกส์ของบริษัทให้เหมาะสมกับการใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออกเป็นต้น
2. ผู้ใช้งาน ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อบริษัทหรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัท
3. ผู้ใช้งาน ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นจะได้รับยินยอมจากเจ้าของผู้ใช้ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
4. ผู้ใช้งานควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อการทำงานของบริษัท เท่านั้น
5. ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น
6. ผู้ใช้งาน ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
7. ผู้ใช้งาน ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม อันอาจทำให้เสียชื่อเสียงของบริษัท ทำให้เกิดความแตกแยกระหว่างบริษัทผ่านทางจดหมายอิเล็กทรอนิกส์
8. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
9. ห้ามไม่ให้ผู้ใช้งานใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเพื่อส่งจดหมายอิเล็กทรอนิกส์ที่ไม่ได้มีวัตถุประสงค์ในภารกิจของบริษัท หรือส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาในลักษณะขัดต่อศีลธรรม ความมั่นคงและกฎหมาย ของประเทศ
10. ห้ามไม่ให้ผู้ใช้งานนำบัญชีจดหมายอิเล็กทรอนิกส์ (email account) ซึ่งเป็นของบริษัท ไปเผยแพร่สู่บุคคลอื่น ไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในเว็บบอร์ดในชุดคำถามหรือแบบสอบถามจากผู้ค้า เป็นต้น เว้นแต่การเผยแพร่นั้นเป็นไปเพื่อผลประโยชน์ของบริษัท หรือได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
11. ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
12. ผู้ใช้งาน ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบหรือโอนย้ายจดหมายอิเล็กทรอนิกส์เก็บไว้ที่เครื่องพิวเตอร์ของบริษัท

13. จดหมายอิเล็กทรอนิกส์ที่มีวัตถุประสงค์พิเศษ เช่น hr@aapico.com อาจได้รับการสร้างขึ้นเพื่อเป็นจดหมายอิเล็กทรอนิกส์กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป ซึ่งต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของจดหมายอิเล็กทรอนิกส์นั้น

14. จดหมายอิเล็กทรอนิกส์ทั้งหมด และเนื้อหาภายในทุกฉบับ (รวมถึงจดหมายอิเล็กทรอนิกส์ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายขององค์บริษัท ถือเป็นสินทรัพย์ของบริษัท

15. ผู้ใช้งาน ไม่ควรส่งหรือตอบกลับหรือส่งต่อจดหมายอิเล็กทรอนิกส์ไปยังผู้รับหลายคนที่ไม่มีส่วนเกี่ยวข้อง หากมีความจำเป็นให้แจ้งแผนกเทคโนโลยีสารสนเทศ

ส่วนที่ 5

การใช้งานอินเทอร์เน็ต (Internet Security Policy)

1. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่บริษัทจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น

2. ห้ามผู้ใช้ ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เว้นแต่มีเหตุความจำเป็นในการทำงาน ต้องได้รับการอนุญาตจากผู้บังคับบัญชาและแจ้งแผนกเทคโนโลยีสารสนเทศรับทราบเป็นลายลักษณ์อักษร

3. ผู้ใช้งาน ห้ามใช้เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อหาประโยชน์ในเชิงธุรกิจ ส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่มีผลกระทบต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

4. ผู้ใช้งาน จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัท

5. ผู้ใช้งาน ห้ามเผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายต่อบริษัท

6. ห้ามผู้ใช้งาน เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านทางอินเทอร์เน็ต

7. ห้ามผู้ใช้งาน นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

8. ห้ามผู้ใช้งาน นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้ จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

9. ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

10. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดข้อมูล รูปภาพหรือสื่ออิเล็กทรอนิกส์ใดๆจากอินเทอร์เน็ตมาใช้งาน ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

11. การแสดงความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัท รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

12. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

13. ผู้ดูแลระบบสามารถนำข้อมูลการใช้งานอินเตอร์เน็ทของของผู้ใช้งานมาวิเคราะห์ เมื่อมีการใช้งานหรือเหตุอันเกิดความสงสัยที่ผิดปกติได้

ส่วนที่ 6
การควบคุมการเข้าถึงข้อมูล (Access Control Policy)

สำหรับการควบคุมการเข้าถึงระบบสารสนเทศ หมายถึง การเข้าถึงระบบของผู้ใช้ และรวมความถึงการกำหนดหน้าที่ของผู้ใช้ การเข้าถึงเครือข่าย การใช้งานระบบที่ให้บริการ และระบบสารสนเทศการเฝ้าดูการใช้งานระบบคอมพิวเตอร์ประเภทพกพา และการปฏิบัติงานนอกสถานที่ เป็นต้น ซึ่งการออกนโยบายนี้ควรครอบคลุมหัวข้อหลักดังต่อไปนี้ โดยมีจุดประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

หมวด 1 ข้อกำหนดสำหรับการควบคุมการเข้าถึงสารสนเทศ (Access Control)

1. ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งานในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน
2. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
3. ผู้ใช้งาน จะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

หมวด 2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

4. การลงทะเบียนผู้ใช้งานใหม่ หัวหน้างานสารสนเทศ/ผู้ดูแลระบบสารสนเทศต้องร่วมกันจัดทำระเบียบปฏิบัติ ในการลงทะเบียนผู้ใช้ใหม่เพื่อให้สามารถใช้งานระบบสารสนเทศ หรือโครงสร้างสนับสนุนระบบสารสนเทศอื่น ๆ ทั้งหมดได้ นอกจากนี้ ต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้ทันที ในกรณีที่มีการลาออกจากงานหรือเกษียณอายุ
5. กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
6. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของผู้ใช้งานดังนี้

(1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(2) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน ผู้ดูแลระบบจะเก็บรักษาบัญชีชื่อผู้ใช้งานอย่างน้อย 30 วันก่อนลบออกจากระบบ หรือตามที่ผู้บังคับบัญชา ผู้บริหารระดับสูง เห็นสมควรเป็นอย่างอื่น โดยให้แจ้งผู้ดูแลระบบเป็นลายลักษณ์อักษร

(3) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(4) ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(5) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(6) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง

หมวด 3 หน้าที่ความรับผิดชอบของผู้ใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

7. เพื่อให้การกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านมีคุณภาพ ผู้ใช้งานควรปฏิบัติ ดังนี้

(1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username)และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

(2) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(3) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา

(4) ควรกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติตัวเลข และสัญลักษณ์เข้าด้วยกัน

(5) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(6) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(7) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(8) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(9) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(10) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(11) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(12) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(13) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(14) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

(15) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(16) ผู้ดูแลระบบต้องเปลี่ยนรหัสถี่กว่าผู้ใช้งานทั่วไป

หมวด 4 การควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ (Network Access Control)

กำหนดขึ้นด้วยวัตถุประสงค์ เพื่อควบคุมการใช้บริการบนเครือข่ายคอมพิวเตอร์ของกลุ่มบริษัทอาปิโก

8. ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

9. การเข้าสู่ระบบเครือข่ายภายในบริษัทโดยผ่านทางเครื่อข่ายสาธารณะจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากฝ่ายเทคโนโลยีสารสนเทศก่อนที่จะสามารถใช้งานได้ในทุกกรณีและจะต้องใช้เครือข่ายเสมือนส่วนตัว (Virtual Private Network) เท่านั้น

10. การเข้าสู่ระบบเครือข่ายภายในบริษัทโดยผ่านทางเครือข่ายสาธารณะจะต้องใช้เครือข่ายเสมือนส่วนตัว (Virtual Private Network) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องเท่านั้น

11. ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

12. ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

13. ผู้ดูแลระบบ ควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้

14. ระบบเครือข่ายทั้งหมดของสำหนักงานใหญ่ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ในกลุ่มบริษัทอาปิโกหรือระบบเครื่อข่ายภายนอก จะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์(Malware) ด้วย

15. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของบริษัทในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

16. IP address ภายในของระบบงานเครือข่ายบริษัท ต้องมีการป้องกันมิให้หน่วยงานหรือบุคคลภายนอกที่เชื่อมต่อสามารถมองเห็นได้

17. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

18. การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

19. การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

หมวด 5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

กำหนดขึ้นด้วยวัตถุประสงค์เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติดังนี้

20. ผู้ดูแลระบบ ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (domain controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของบริษัทและกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของบริษัท

21. การเข้าถึงระบบปฏิบัติการผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง

22. ระบบจำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

23. ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

24. เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์จะต้องทำการล็อคหน้าจอ (Lock Screen) และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

25. เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) เมื่อไม่ใช้งานเป็นเวลา 10 นาที และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

26. ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

27. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

ส่วนที่ 7
การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)

กำหนดขึ้นด้วยวัตถุประสงค์เพื่อช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่ ความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ผู้ใช้งานควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของบริษัท ให้มีความลับ ความถูกต้อง ปลอดภัยและมีความพร้อมใช้งานอยู่เสมอ

1. เครื่องคอมพิวเตอร์ที่บริษัทอนุญาตให้ผู้ใช้งาน ใช้งานเป็นทรัพย์สินของบริษัท ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของบริษัท
2. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัท ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
3. ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้ง แก้ไขเปลี่ยนแปลงหรือถอนการติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์ของบริษัท
4. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่เทคโนโลยีสารสนเทศของบริษัทหรือได้รับอนุญาตจากเจ้าหน้าที่เทคโนโลยีสารสนเทศของบริษัทเท่านั้น
5. ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
6. ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่
7. ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
8. ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive
9. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น
10. การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
11. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
12. ไม่วางสิ่งของทับบนเครื่องคอมพิวเตอร์ หน้าจอหรือแป้นพิมพ์
13. การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

14. ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

15. ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล๊อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

16. ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (sub component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

17. ห้ามผู้ใช้งานนำคอมพิวเตอร์หรืออุปกรณ์สื่อสารส่วนตัว เข้ามาใช้งานหรือเชื่อมต่อระบบสารสนเทศของบริษัท เว้นแต่มีเหตุความจำเป็นในการทำงานต้องได้รับการอนุญาตจากผู้บังคับบัญชาและแจ้งแผนกเทคโนโลยีสารสนเทศรับทราบเป็นลายลักษณ์อักษร

ส่วนที่ 8
การสำรองข้อมูลและการกู้คืนระบบ (Backup and Recovery)

หมวด 1 การจัดให้มีระบบสำรองข้อมูล

นโยบายนี้จัดทำขึ้นด้วยวัตถุประสงค์เพื่อจัดทำระบบสำรองข้อมูล เพื่อให้มีข้อมูลสารสนเทศและระบบคอมพิวเตอร์ ระบบเครือข่าย สำหรับการใช้งานได้อย่างต่อเนื่องอย่างมีประสิทธิภาพและใช้งานได้ในเวลาที่ต้องการ (availability risk)

1. ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของบริษัท

2. การสำรองข้อมูลภายในองค์กร หมายถึง การทำสำรองข้อมูลทั้งหมด (Full backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องสำรองข้อมูลที่สำคัญไว้ตามระยะเวลาที่เหมาะสมและกำหนดไว้ชัดเจน เช่น สำรองข้อมูลอย่างน้อย ๑ ครั้งในรอบทุก ๆ สัปดาห์ เป็นต้น

3. ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการสำรองข้อมูลถูกต้องสมบูรณ์หรือไม่

4. การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นต่อหัวหน้าแผนกเทคโนโลยีสารสนเทศ

5. ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

6. ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและรายงานต่อหัวหน้าแผนกเทคโนโลยีสารสนเทศ

7. ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม

8. การสำรองข้อมูลภายนอกสำนักงาน (Off-site backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมของหน่วยงาน เพื่อให้สามารถกู้ระบบกลับคืนได้อย่างรวดเร็ว และเพื่อป้องกันระบบจากการถูกโจมตี หรือความเสียหานที่อาจเกิดขึ้น

9. นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy)ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

หมวด 2 การกู้คืนระบบ

10. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่าย ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อหัวหน้าแผนกเทคโนโลยีสารสนเทศทราบโดยเร็ว

11. ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

12. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

ส่วนที่ 9

ความมั่นคงทางกายภาพห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

(Physical and Environmental Security)

1. มีการกำหนดห้องควบคุมระบบและพื้นที่ควบคุม (Control Area) ชัดเจน
2. ข้อกำหนดทางด้านกายภาพของห้องควบคุมระบบ
    (1) แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไปโดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้เช่น Server, Router, Network Switch ต่าง ๆ
    (2) การติดตั้งอุปกรณ์ควรติดตั้งภายในตู้ Rack ที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา
    (3) ตำแหน่งของการวางอุปกรณ์ต่าง ๆ ไม่ควรวางใกล้ประตู หน้าต่างเพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น ไม่ควรวางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรงเพื่อหลีกเลี่ยงความชื้น
    (4) การจัดวางสายเครือข่ายและสายไฟฟ้าควรมีการเก็บสายให้เรียบร้อยเพื่อป้องกันการเดินสะดุด
    (5) ติดประกาศบันทึกการบำรุงรักษา ชื่อและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด
    (6) ระบบการเข้าออกห้องโดยระบบตรวจสอบลายนิ้วมือ (Fingerprint Scan) หรือบัตรผ่านเข้าออก (RFID)
    (7) มีระบบป้องกันอัคคีภัย
    (8) มีระบบไฟฟ้าสำรองเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบไฟฟ้าสำรอง เป็นต้น
    (9) มีระบบป้องกันไฟฟ้าจากฟ้าผ่า
    (10) ระบบปรับอากาศแบบควบคุมอุณหภูมิ (15 - 26°C) และความชื้น (20 – 80%)
    (11) มีตารางการเข้าตรวจสอบและบำรุงรักษาอุปกรณ์ชัดเจน
3. ข้อกำหนดการเข้าไปในพื้นที่ควบคุม
    (1) ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ ผู้บริหารหน่วยงานหรือบุคคลที่ผู้บริหารหน่วยงานนำเข้าเยี่ยมชม
    (2) บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชมในพื้นที่ควบคุมต้องได้รับอนุญาตจากหัวหน้าแผนกเทคโนโลยีสารสนเทศและต้องมีเจ้าหน้าที่นำเยี่ยมชมอยู่ด้วยตลอดเวลา

(3) ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของหน่วยงานจะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ

(4) ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

Information Technology Systems Security Policy

AAPICO Group

2023

By

Information Technology Department

AAPICO Hitech Public Company Limited

Effective date 1 August 2023

Prepared by / IT	Reviewed by / IT Mgr.	Reviewed by / IT GM.	Approved by /CEO
date 12/07/23	Wittaya date 13/07/23	Somwang T. date 13/07/23	date 4/9/2023

Table of Contents

Subject	Page
Information Technology Security Policy	1
Principles and Reasons	1
Objective	1
Policy Intents	2
Scope	2
Definition	2
Part 1	4
Use of computer network resources and information systems	4
Part 2	9
Access to wireless networks	9
Part 3	11
Firewall Policy	11
Part 4	12
E-Mail Policy	12
Part 5	14
Internet Security Policy	14
Part 6	16
Access Control Policy	16
Part 7	21
Use of Personal Computer	21
Part 8	23
Backup and Recovery	23
Part 9	25
Physical and Environmental Security	25

Information Technology Security Policy

AAPICO Group of Companies 2023

Principles and Reasons

AAPICO Group has established a security policy for information technology systems with the objectives to (1) have AAPICO Group's information safe and secure at the international standard level and legally abided, (2) optimize the use of information system resources, and (3) be a guideline for users of information systems of the AAPICO Group. This document has been prepared in accordance with the ISO 17799-2005 standard framework, Computer Crime Act B.E. 2550, and the Computer Crimes Act (No. 2) B.E. 2560, covering the following matters:

1. Objectives and necessity of AAPICO group information protection
2. Information that needs to be protected to be secure
3. Information Protection Principles and Guidelines
4. Roles, duties and responsibilities of personnel in the AAPICO Group and related third parties.

Objective

1. Ensure that the use and security of information within the AAPICO Group is in accordance with relevant laws and regulations.

2. Provide AAPICO group personnel as well as other persons authorized to access the information system with knowledge and understanding of good practices, prohibitions, and responsibilities of such use that will result in the security of the information system. And the use is consistent with the purpose of using the AAPICO Group's information system, including not violating the law, or causing damage to the operation

3. Protect information from any forms of losses, e.g., loss, destruction, unauthorized editing, and illegal use or disclosure of information; including to ensure that information is accurate, reliable and serviceable.

Policy Intents

The AAPICO Group considers the security of information systems as high importance to enable the AAPICO Group to operate in accordance with the vision and mission.

1. Access to information resources of AAPICO Group must be controlled and auditable under the legal framework, and must be used for the mission of the company only.
2. Confidential information must be protected from unauthorized access and alteration.
3. Information that is important to the mission of the company must be protected from damage, destruction, or alteration.
4. The AAPICO Group must have the ability to recover the information and communication systems that are the core of the system within a reasonable time in the event of a disaster.
5. Security is an important aspect that must be considered and taken into account at every stage of the development or purchase of any new information system.
6. AAPICO Group will raise awareness to personnel at all levels to continuously maintain the importance of information security.
7. The security policy of the AAPICO Group must be adaptable to appropriate with security and technology issues.

Scope

This policy is applicable to users of the company's information systems at all levels and positions without exception. Users are employees and contractors who use the company's information system, including third parties or authorized persons granted access to the information resources of the AAPICO Group. This policy covers the operations both within and outside the Kingdom of Thailand. Protected information may be information stored in personal computers, servers, or telecommunications equipment, including information being sent through the network system, and information recorded in any storage media

Definition

User means employees, workers, system administrators, administrators, service users, or those authorized to use the information technology systems of the AAPICO group of companies.

Administrator means a person assigned by the head of the department to be responsible for maintaining or managing the computer system and network system in any part.

Supervisor means a person who are authorized to give orders according to the management structure of the company.

Assets means equipment or data contained in information technology systems.

Resources means information related to and contained in the information technology system.

Company means a company in the AAPICO group of companies.

Working Unit means department or section of the company or business unit established by the executives to perform tasks as assigned.

Computer data means data, messages, commands, set of instructions or anything else residing in the computer system in a condition that being able to be processed. This includes electronic data under the law of electronic transactions.

Information refers to the facts obtained from the data processing and data organizing, which may be in the form of numbers, text, or graphics. Forming into a system that users can easily understand, and can be used for the benefit of management, planning, decision-making and others.

Computer system means a computer device or a set of computer equipment that are linked together. This linked equipment automatically processes data according to its operation guidelines, sets of commands, instructions, or anything else.

Network system means a system that can be used to communicate or send data and information between the company's information technology systems, such as a local area network (LAN), intranet system, Internet system, and etc.

Local Area Network (LAN) and intranet (Intranet) refer to electronic network systems that connect various computer systems within the department together. It is a network that aims to communicate and exchange data and information within the organization.

The Internet refers to an electronic network that connects various computer networks of the organization to the Global Internet network

Information Technology System means a system of computers and networks being used to create information that companies can use for planning, administration, supporting operation, and developing and controlling communication service. The system contains elements such as computer systems, network systems, programs, data and information, etc.

Part 1

Use of computer network resources and information systems

The use of computer network resources and information systems of the AAPICO group must be established in terms of ethical, and legal guidelines to prevent damage caused by improper actions, to maintain the image of the organization, and to set a guideline for the personnel in the organization to have the efficient operation. The details are as follows.

Section 1 User Accounts and Passwords

Administrator must establish user account and password management policy to ensure system security. The topics are as follows.

1. The administrator must specify that password must not less than 8 digits of which must contain numerical character, alphabet and special character.
2. Administrator must prohibit the reuse of password that have already been used in the last 3 passwords.
3. Administrator must notify users to change the password every 90 days or when there is a warning to change the password.
4. Administrator must set the maximum of 3 times that a user is allowed to enter a wrong password.
5. Administrator must assign new user account with a first time password for the new use to log in and verify identity of the system user.
6. Administrator must request the new user to change the password immediately after the first successful log in.
7. Administrator must set the system to log out when the user has not used the system for a specified period of time such as 15 minutes. User must re-log in with username and password to continue accessing the system.

Section 2 Proof of identity (Accountability, Identification and Authentication)

8. Users are responsible for protection of their own account information (Username) and password. Each user must have their own account (Username). Users are not allowed to share or let others know their password or use their account.
9. Users are responsible for any actions executed with the users' account (username), whether the action is done by the users or not.
10. Users must authenticate themselve before using company assets or information systems. If the authentication fails whether it is caused by a password issue, system locked up, or any other error, the user must notify the administrator immediately.

Section 3 Asset Management

11. User must not enter the server room which is a restrict area, unless authorized by the administrator.
12. User must not move any equipment or parts out of the server room, unless authorized by the administrator.
13. User must not connect tools or any other device to the network for personal business.
14. User must not use or delete other people's data or files in any case.
15. User must not copy or duplicate any copyright protected material before getting approval.
16. User is responsible for the property entrusted by the company for use as if it were the property of the user. The receipt or return of the property will be recorded and checked every time by the staff assigned by the company
17. In case of working outside the premises, the user must take care and be responsible for the assigned company's assets.
18. Users are obligated to pay for the damage or loss of the property according to the property value, if the damage or loss caused by the negligence of the user
19. Users must not lend their property to others under any circumstances, unless the borrowing has been approved in writing by an authorized person.
20. Assets and information systems that the company provides for use is intended for use in the operation of the organization. Any use of the systems and devices for personal business is allowed to a limited extent and as appropriate on the condition that it must not interfere or hinder the work according to the duties and responsibilities of the staff.

21. Users are forbidden to use assets and information systems in activities that the company has not specified or cause damage to the company. Any damage incurred shall be considered a personal fault, with the user responsible for the damage.

Section 4 Corporate Data Management

22. Users must be aware and careful in the use of information whether that information belongs to the company or a third party.
23. All information contained within the company's assets are considered the assets of the company. Dissemination, modification, duplication or destroying of these assets is prohibited, without the permission of the superior.
24. The user is sharing responsibility in taking care of the integrity of the company's and service receivers' information. In case of information loss, unauthorized distribution, or misusage, the relevant user bears responsibility for such damage as well.
25. User must protect, keep secret, and take care of accuracy and availability of the information.
26. Users have the right to keep, use, and protect personal information as appropriate. The Company supports and respects individual rights, and will not allow any person to infringe personal information without the permission of the user who possesses that information. As an exception, in the case that the company has to verify the information or suspects that the information is relevant to the company, the company may appoint an auditor to verify that information at any time without prior notifying the user.

Section 5 IT Infrastructure Management

27. Users are prohibited from developing any program or hardware, unless it has been considered and approved in writing from the company's information department.
28. Users are not allowed to open or use (run) Peer-to-Peer programs or programs that have the same level of risk such as Bittorrent.
29. Users are not allowed to open or use (run) any online entertainment program such as program for watching movies, listening to music, playing games, etc. during working hours.

30. Users are not allowed to use resources, communication systems, and any other equipment provided by the company to disseminate information, message, picture or anything else that will violate morality, national security, and laws, or will affect the mission of the company.
31. Users are not allowed to use resources, communication systems, and any other equipment provided by the company to disturb, cause damage, steal information, or do anything else that is against the law and morals, or affects the mission of the company.
32. Users are not allowed to use the company's resources for commercial purposes.
33. Users are not allowed to intercept data whether it is a message, picture, sound, or anything else in the company's information system network.
34. Users are not allowed to disturb, destroy, or cause any disruption to the company's information system.
35. Users are not allowed to use company information systems to control computers or external information systems without permission from the information technology department.
36. Users are not allowed to hack into the system or steal other personal passcodes for the benefit of accessing information or for the use of resources.
37. It is forbidden to install any equipment or perform any action to gain access to the company's information system.

Section 6 Compliance with Laws and Regulations

38. The users must abide by any laws promulgated and enacted in Thailand and the company's regulations. It is important that users are aware and strictly follow those laws and regulations. Any violation of such laws and regulations is considered a personal crime for which the user is responsible for the incurred penalty.

Section 7 Software Licensing and intellectual Property

39. The company has given importance to intellectual property, Therefore, the company's acquired software licenses for users to use per request and as necessary. The company prohibits users from installing or using any unlicensed software. If unlicensed software is found, the IT department has the right to immediately uninstall the program or software. If there is any copyright

infringement, the company considers it a personal offense, and the user will take the responsibility.

40. Software that the company has provided to users considered essential for work. Users are forbidden to install, uninstall, modify, or make a copy for use elsewhere.

Section 8 Preventing Malware

41. The user's computer must be equipped with a computer virus protection program as provided by the company or as announced for use. For exception, the computer is used for studying or developing protection systems with permission from the Information Technology Department.
42. Data, file, software or anything else received from other users must be scanned for computer viruses and malicious programs before being used or stored every time.
43. The administrator must check and update the operating system (patch update) in order to prevent damage that may occur.
44. Users must beware of viruses and malicious programs at all times. When an abnormality is found, the user must notify the system administrator immediately.
45. When users find that their computers are infected with a virus, the users must not connect their computers to the network, and must notify the administrator immediately.
46. Users must not copy, change, or delete information, message, document, or other things that is the asset of the company or of others without the permission of the superior.
47. Users must not disseminate computer viruses, malware, or any malicious programs that may cause damage to the company's assets.

Part 2

Access to wireless networks

Administrators and users of the company's wireless network have duties and responsibilities that must be performed. as follows

1. The installation of a wireless network must be authorized in writing from senior management, and must have a password to access.

2. Users are forbidden to bring all types of wireless network equipment to install or activate in the company, whether it is an Access Point, Wireless Routers, Wireless USB client, Wireless card, or any other equipment that has the ability to work the same way.

3. Users are prohibited to deploy the wireless network system, point to point (ad-hoc), or peer-to-peer Network.

4. Users who want to access the company's wireless network must be registered with the administrator and must be authorized in writting by the information and technology department information.

5. Administrator must registor and set user rights to access the wireless network system according to the user's responsibilities. The administrator shall regularly review users' access rights.

6. Administrator must registor all devices connected to the wireless network.

7. Administrator must properly assign location of the Access Point (AP) to prevent the device's signal from spreading outside the controlled area. This will prevent attackers from being able to transmit signals from outside the building or the controlled area

8. Administrator must separate third party wireless network connections from internal wireless networks.

9. Administrator must select the transmission power that suit the service area, and should explore whether the signal spreads out or not. In addition, considering using a special antenna that can direct signal propagation may help reduce signal spreading out.

10. Administrator must change the SSID (Service Set Identifier) from the manufacturer default ID when deploy the access point.

11. Administrator needs to set log in name and password for wireless device configuration settings. The login names and passwords must be difficult to guess to prevent attackers from easily guessing or breaking into the system.

12. Administrator must use WPA2 to encrypt the data exchanging between the Access Point and the Wireless LAN Client to make it difficult to intercept, and make the system more secure.

13. Administrator must use MAC Address together with Username and Password of the user to control the right to access the wireless network. Only devices with the specified MAC address, username and password are allowed to access the wireless network.

14. Administrator must keep the wireless network secured, and regularly monitor and record suspicious events occurring in the wireless network.

Part 3

Firewall Policy

A firewall is a device that is important in managing the security of a company 's networks because it controls the information that goes in and out. To make the corporate networks secured both in terms of limiting the connection and restrictions on use right, a firewall sets perimeters and controls access to a computer network. Information passing through the firewall will be complied with the policy of the organization. Firewall policy is intended to be used as a guideline for management, to maintain the security of the company's information technology system

1. The firewall must be set with the conditions for the connections or services that are allowed only. The setting condition should utilize the rule of Deny All Allow Some.
2. Rules to allow the connections or services to pass through the firewall must be documented and sent to all network administrators to acknowledge. The terms of these permission must be agreed by the administrator, and report to the head of the information technology department.
3. For all computer communication paths that go in and out of the company, a firewall must be installed on all routes.
4. The host computer that is connected to the outside of the organization must always be placed in the DMZ (De-Militarize Zone).
5. All communications from outside of any organization must pass through the DMZ only.
6. The administrator must monitor the functionality of the firewall from log file regularly.

Part 4

E-Mail Policy

1. Administrator must set the appropriate right for the users to access the company's e-mail service according to their responsibilities. Administrator must regularly review access rights such as when there is a user resignation, etc.
2. The users must be careful when using e-mail in order not to cause damage to the company, violate rights of or cause annoyance to others, perform illegal activity, or violate morals. The users must not seek benefits or allow others to seek business benefits from the use of e-mail through the Company's network system.
3. The user should not use other e-mail address to read, send, and receive messages, unless grant the consent from the account owner. The owner of such e-mail address shall be deemed responsible for the use of the e-mail address.
4. Users should use the company's electronic mail for the work of the company only.
5. Users should check the e-mail attachment with an anti-virus program before opening it. Users should avoid opening executable files such as files with extension .exe .com etc.
6. Users must not open or forward electronic mail or messages received from unknown senders.
7. Users must not use inappropriate messages or subscribe for inappropriate e-mail services, which may damage the reputation of the company, or cause conflicts in companies through electronic mail.
8. In case of sending confidential information, the importance of information should not be stated in the subject of the e-mail.
9. Users are prohibited from using the company's electronic mail system to send electronic mail that is not related to company's mission and objectives, or send electronic mail that contains content in a manner that is against morality, security, and laws of the country.
10. Users are prohibited from using company's email account to publish to other persons such as posting on forums in webborad, etc.; unless the dissemination is for the benefit of the company and already get permission from the supervisor.
11. Users should check e-mailbox every day, and should store data, files, and e-mails to the smallest amount.
12. The unwanted e-mail should be deleted from the system or transferred to the company's computer.

13. Electronic mail with special purpose e.g., hr@ aapico.com may be created as the department's central electronic mail and / or to be shared by more than one user. There must be one user appointed to act as the owner of the electronic mail.

14. All e-mail and all content therein (including personal e-mails) created and stored on the computer system or the company's network system are considered the assets of the company.

15. Users should not send, reply, or forward electronic mail to multiple unrelated recipients. If necessary, inform the Information Technology Department.

Part 5

Internet Security Policy

1. Administrator must set computer system connections routing for Internet access through the security system allocated by the company's Proxy, Firewall, IPS-IDS, etc.

2. Users are prohibited from connecting computer system through other channels. In case of necessity to work using other channels, permission from the supervisor and a notification in writing to the Information Technology Department are required.

3. Uuser must not use the company's internet network for personal business benefits, or entering inappropriate websites such as immoral websites, websites with content of negative impact to nation, religion, and monarchy institutions, or a website that is a threat to society etc.

4. Users will be assigned access rights to the data source based on their responsibility for the efficiency of the company's network and information security.

5. Users must not disseminate information for personal exploitation, morally inappropriate information, information that infringes the rights of others, or information that may cause damage to the company.

6. Users must not disclose important confidential information about the company's work that has not been officially announced over the Internet.

7. Users must not bring in computer information which contains false information, offense relating to the security of the Kingdom, offense related to terrorism, or obscene images, and not disseminating or forwarding such computer information through the Internet.

8. Users must not bring in other people's computer images that are created, edited, modified by electronic means or any other method, that cause others to lose their reputation, be insulted, hated, or get humiliated.

9. Users are responsible for verifying the accuracy and reliability of computer information on the Internet before using the information.

10. Users must be careful when downloading data, images, or any electronic media from the Internet to use, and make sure that it is not violating intellectual property.

11. When commenting, users must not use provocative messages, or slander that will cause damage to the reputation of the company, or destruction of relations with officials of other agencies.

12. Users must close out web browser after finished using the internet to prevent access by other people.

13. Administrators can analyze the user's internet usage data, when there is an unusual use or suspicious event.

Part 6

Access Control Policy

The access control of information systems is covering the control of user access to the system, the assignment of the user's role, network accessing, the use of the service system and information systems, monitoring the use of portable computer systems, and monitoring of off-site work etc. The issuance of this policy should cover the following main topics, with the purpose of securing and controlling access to information systems as follows

Section 1 Requirements for controlling access to information

1. Administrators are responsible for reviewing approvals and assigning permissions to access to the system for users. The permission request must be documented, and the signed approval document must be kept as evidence.

2. Administrators must assign access rights to data and information systems that are suitable for access by system users and responsibilities of staff in operation before accessing the information technology system. Therefore, permissions to access the work system must be specified only as minimum necessity, and should be regularly reviewed.

3. Users must obtain permission from the staff responsible for information and work systems as necessary for the use of information technology systems.

Section 2 User access management

4. The Information Supervisor / Information Administrator must work together to formulate a set of regulations to register new users to be able to use the information system or other structure supporting information systems. In addition, procedures must be in place to terminate users' rights immediately when users resigned or retired.

5. Administrator must determine the right to use important information technology systems such as computer systems, applications, electronic mail, wireless network, Internet system, etc., with specific rights to perform duties and written approval of the administrator is required. Administrator must review such rights regularly.

6. Administrators must manage system privileges and user passwords as follows.

(1) Change and cancellation of the password when the user resigned, retired, or cancelled.

(2) When a user resigned, retired, or cancelled, administrator will keep user account for at least 30 days before deleting from the system, or according to the supervisor or senior management deems appropriate and then inform the administrator in writing.

(3) Deliver temporary passwords to users in a secure way. Avoid using other people or sending unprotected electronic mail to send passwords.

(4) Users must not record or store passwords in a computer system in an unprotected form.

(5) The username or password must be unique.

(6) In case it is necessary to grant special privileges to users with the highest privileges, users must be authorized and approved by supervisors. There is a specified period of use and suspension of use immediately after the expiration of such period or upon user retirement. The special privileges must be clearly specified the right to access to what levels.

Section 3 Duties and Responsibilities of Users of Information Systems and Computer Networks

To prevent unauthorized access, disclosure, knowing, or copying of information, there should be at least the following practices:

7. To effectively set, use, and change the password, users should act as follows.

(1) Users are responsible for protecting and maintaining account information, username and password. Each user must have their own account (Username) , do not share with others. Users must not disseminate, distribute, or make others know the password.

(2) Users must change their temporary password immediately when log in to the system for the first time.

(3) A password must be difficult to guess.

(4) A password should be at least 8 characters with a combination of normal case letters, numbers, and symbols.

(5) The passwords should not be set based on one's name, surname, or those of one's family or someone close to the user, or from the words in the dictionary.

(6) Do not set a password from a sequence of characters or any similar group.

(7) Do not use personal passwords for sharing data files with others over a computer network.

(8) Keep one's own and group passwords confidential.

(9) Do not write down or save personal password in a place where it can be easily noticed by others, or stored in the computer system.

(10) Must not use option to save or remember passwords.

(11) Do not share password with others.

(12) In cases where it is necessary to give the password to others due to the work required, after completing the process, change the password immediately.

(13) Passwords should be changed at specified intervals, or change the password immediately when aware that it may have been disclosed or known.

(14) Avoid using the same password for different systems.

(15) Avoid using old passwords.

(16) Administrators have to change passwords more often than normal users.

Section 4 Computer Network Access Control

This policy established to control the use of services on the computer network of AAPICO Group

8. Administrators must design a network based on the group of information and communications technology services used, group of users, and group of information systems such as internal zones, external zones, etc., in order to systematically control and prevent intrusion.

9. Access to the company's internal network over a public network must be approved in writing by the IT department before it can be used in all cases and must use a virtual private only.

10. Access to the company's internal network via a public network will require a virtual private network and authentication is required to verify authenticity.

11. Administrators must have a way to limit permissions to control users to use only authorized networks.

12. Administrators should have a way to restrict shared network access routes.

13. Administrators should provide a way to restrict the use of paths on the network (Enforced path) from the client to the server so that users cannot use other routes

14. The entire network of the head office that is connected to other networks in AAPICO Group or external network system must be connected through an intrusion prevention device or a packet filtering program , such as using a firewall or other hardware. The device or program should have ability to detect malware as well.

15. IPS/IDS must be installed to monitor the use of individuals who have unusual access to the company network through the network. The monitoring includes intrusion detection through the network system, abnormal use, and alteration of the network by unauthorized persons.

16. Internal IP address of the company network system must be prevented from being seen by connected entities or third parties.

17. Administrator must prepare a network diagram, which contains details about the boundaries of the internal network and external networks, and equipment. The diagram should always be up to date.

18. The use of various tools to monitor the network system should be approved by the administrator and limited only to the extent necessary.

19. Installation and connection of network equipment must be performed by the staff of the information and communication technology center only.

Section 5 Operating System Access Control

This policy is established with the aim of preventing unauthorized access to the system, with the following guidelines:

20. Administrators must install a management program (domain controller) to manage all computers of the company, and assign a username and password for each users to access the operating system of the company's computers.

21. Every user access to operating system must be authenticated.

22. The system has a time limit for entering a password.

23. The system can disconnect from the terminal, when detecting that an attempt is made to guess the password from the terminal

24. When the user is away from the computer, the screen must be locked and the user must re-log in and be authenticated before allowing to use the computer.

25. Every computer must set a screen saver time. When not in use for 10 minutes, the user must re-log in and be authenticated before allowing to use the computer.

26. Users must log out immediately when they stop using it or not being on the screen for a long time.

27. Users must not allow others to use their username and password to access the computer of the organization.

Part 7

Use of Personal Computer

This policy is established with the purpose of helping users to be aware of their duties and responsibilities when using personal computers and portable computers. Users should understand and strictly follow the ploicy, to protect the company's valuable resources and information to be confidential, accurate, secure and always available.

1. Computers that the company allows users use are company assets. Therefore, users should use computers efficiently for company work.

2. The program installed on the company's computer, must be a program that the company has legally purchased with a license for use. Therefore, users are prohibited from copying programs and installing them on their personal computers or modifying or allowing others to use illegally.

3. Users are not allowed to install, modify, or uninstall programs on company computers.

4. Moving or sending computers for repair must only be carried out by the company's IT staff or authorized by the company's IT staff.

5. Before using portable media, it must be checked for viruses by an antivirus program.

6. Do not store important information of the company on the computer in use.

7. Do not bring food or drinks near the computer.

8. Do not place magnetic media near computer screens or disk drives.

9. In the case of moving a portable computer, it should be put in a bag for a portable computer, to prevent damage caused by concussion such as falling from a desk or slipping from the hand, etc.

10. When using a portable computer for a long period of time in extremely hot weather, it is recommended to shut down the computer for a short period of time before turning it back on.

11. Avoid using fingers or a hard object, such as the tip of a pen, to press against the LCD screen as it will scratch or shatter the LCD screen of the portable computer.

12. Do not place objects on top of the computer, screen, or keyboard.

13. To move the machine while it is on, lift it from the base under the keyboard. Do not move the machine by pulling up the screen.

14. Do not use or place the portable computer near liquids, moisture, such as food, water, coffee, or beverages, etc.

15. It is the user's responsibility to prevent loss, for example, the device should be locked when not in use, and not left it unattended in a public place or in areas where there is a risk of loss.

16. The user is prohibited from making any changes to the built-in sub-components, including the battery.

17. Users are prohibited from bringing personal computers or communication devices to use or connect to the company's information system, unless there is a necessity to work, permission from the supervisor must be obtained and notified in writing to the Information Technology Department is required.

Part 8

Backup and Recovery

Section 1 Providing a Backup System

This policy is established for the purpose of having a backup system to ensure that the information and computer systems network are continuously usable, efficient, and always available.

1. Administrator must regularly backup and verify the backup data in accordance with the company's backup policy.

2. On-premise backup means the full backup of important data. Administrator must perform the full backup at appropriate and well-defined intervals and storage duration, e.g., to backup data every week etc.

3. Administrator must verify the backup results whether the backup is complete or not.

4. The administrator must report any backup errors (fault logging) that occurred to the IT department head.

5. The administrator should delegate backup duties to another staff member, if computer administrators and/or network administrators are unable to perform their duties.

6. If there is a problem in the backup process resulting in the incomplete backup operation. The administrator has to solve the problem and report to the head of the information technology department.

7. Computer administrators and network administrators determine the appropriate backup type and interval.

8. Administrator must perform the off-site backups as appropriate for the organization, in order to be able to restore the system quickly and to protect the system from attack or damage that may occur.

9. Administrator must strictly follow the backup procedure and the related backup policy.

Section 2 System Recovery

10. In the event that a problem causes damage to the computer system and/or the network system and a system restore is needed, the computer administrator and/or network administrator must take corrective action, record the results of corrections, and then summarize and report the results of operations to the head of the information technology department as soon as possible.

11. The most up-to-date backup data or the most appropriate backup must be used to restore the system.

12. If damage occurs to the computer system or the network system affecting the service or the use of system users, the administrator must notify the user immediately, and periodically report the progress of system recovery until the operation is completely recovered.

Part 9

Physical and Environmental Security

1. The system control room and control area must be clearly defined.
2. Control Room Physical Requirements
    (1) Separate devices that are very important from general devices by setting the priority of each device such as Server, Router, Network Switch, etc.
    (2) Equipment should be installed in a suitable rack cabinet to facilitate maintenance.
    (3) The device should not be placed near the door or windows to prevent possible accidents. The device should not be placed directly in the venting area of air conditioner to avoid moisture.
    (4) The arrangement of network cables and power cables should be neatly stored to prevent tripping.
    (5) Post maintenance records including name and phone number of the person responsible for each device.
    (6) Room access system may use fingerprint verification system or access card.
    (7) Fire protection system must be installed.
    (8) There must be a backup power system to prevent power outages, such as installation of automatic generator system and backup power system etc.
    (9) There must be a surge protection system preventing damage from lightning.
    (10) There must be air conditioning system with temperature (15 - 26°C) and humidity control (20 - 80%)
    (11) There must be a clear schedule for equipment inspection and maintenance.
3. Requirements for entering the controlled area
    (1) No person is allowed entering the controlled area, except for the system control room staff, company executives, or persons escorted by company executives.
    (2) Any other persons necessary for operations or visitors must obtain permission from the head of information technology department and must be accompanied by a responsible staff at all times.

(3) In the event of an urgent need or emergency that may result in damage to the company's assets, entry into the controlled area is permitted with the approval of the head of information technology department.

(4) Food or drinks are not allowed inside the restricted area.