



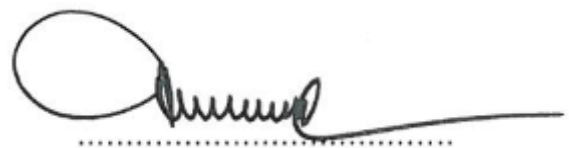
นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

(Information Technology Security Policy)

## ประวัติเปลี่ยนแปลง / เพิ่มเติมนโยบาย

วันที่	เวอร์ชัน	เนื้อหาที่เปลี่ยนแปลงเพิ่มเติม
23 พ.ค. 65	1.0	ประกาศนโยบาย และข้อกำหนดด้านระบบสารสนเทศ
02 ก.ค. 66	1.1	1.ปรับปรุงข้อกำหนดด้านระบบสารสนเทศ ข้อกำหนดการใช้งานระบบ จากภายนอกบริษัทผ่านระบบ Virtual Private Network (VPN)

ผู้อนุมัติ



( นายศิริพงษ์ อุ๋นทรพันธุ์ )

กรรมการผู้จัดการใหญ่

## นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ (Information Technology Security Policy)

ด้วยบริษัท แอ็ดวานซ์ อินฟอร์เมชันเทคโนโลยี จำกัด (มหาชน) ได้จัดให้มีการใช้งานระบบเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวก เพิ่มประสิทธิภาพ และให้ประสิทธิผลต่อการทำงานทั้งระบบ ทั้งนี้เพื่อให้การให้บริการ และการให้บริการสามารถดำเนินการใช้งานร่วมกันได้อย่างเหมาะสม สอดคล้องกับนโยบายทางธุรกิจ และป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องทั้งจากผู้ใช้งาน และภัยคุกคามต่าง ๆ ซึ่งอาจส่งผลกระทบต่อระบบธุรกิจของบริษัทให้ได้รับความเสียหายได้ จึงเห็นสมควรกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อให้ถือเป็นแนวทางในการปฏิบัติเดียวกัน นอกจากนี้ยังเป็นหลักปฏิบัติเพื่อให้การสนับสนุนต่อพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550

### วัตถุประสงค์

1. เพื่อกำหนดทิศทางหลักการ และข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
2. เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ รวมถึงกฎหมายที่เกี่ยวข้องกับระบบคอมพิวเตอร์ได้อย่างถูกต้อง และเหมาะสม
3. เพื่อให้พนักงาน และผู้ที่ต้องใช้หรือเชื่อมต่อระบบคอมพิวเตอร์ของบริษัท ให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม
4. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลายหรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

### ขอบเขตนโยบาย

นโยบายฉบับนี้ใช้กับบริษัท แอ็ดวานซ์ อินฟอร์เมชันเทคโนโลยี จำกัด (มหาชน) และบริษัทย่อย ทั้งนี้ครอบคลุมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้ระบบเครือข่าย คอมพิวเตอร์แม่ข่าย ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ คอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสารแบบพกพาหรืออุปกรณ์สื่อสารอื่นๆ เพื่อเข้าถึงสารสนเทศของบริษัท โดยให้ยกเลิกประกาศนโยบายการใช้งานระบบสารสนเทศและการรักษาความปลอดภัยข้อมูลฉบับเดิม

## คำจำกัดความ

“บริษัท” หมายความว่า บริษัท แอ็ดวานซ์ อินฟอร์เมชันเทคโนโลยี จำกัด (มหาชน) และบริษัทย่อย

“เครื่องคอมพิวเตอร์” หมายความว่า อุปกรณ์ประมวลผลข้อมูลทำงานด้วยระบบอิเล็กทรอนิกส์ที่มีความเร็วสูง โดยทำงานตามคำสั่งผ่านทางซอฟต์แวร์ให้ได้ผลตามที่ต้องการ ได้แก่ คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) และคอมพิวเตอร์แบบพกพา (Notebook Computer)

“อุปกรณ์คอมพิวเตอร์” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ทำงานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ รวมถึงเครื่องสมาร์ทโฟน โทรศัพท์มือถือ แท็บเล็ต

“เครือข่ายคอมพิวเตอร์” หมายความว่า เครือข่ายคอมพิวเตอร์ของบริษัท เครือข่ายคอมพิวเตอร์

“ผู้บังคับบัญชา” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างองค์กรของบริษัท

“ผู้ใช้งาน” (User) หมายความว่า พนักงานบริษัทหรือบุคคลภายนอก รวมถึงลูกจ้างทดลองงาน ลูกจ้างชั่วคราวของบริษัท หรือบุคคลอื่นที่ได้รับมอบหมายให้ปฏิบัติงานตามสัญญาหรือข้อตกลงของบริษัทที่ได้รับสิทธิให้ใช้งานระบบคอมพิวเตอร์ของบริษัท

“บัญชีผู้ใช้งาน” (User account) หมายความว่า บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบคอมพิวเตอร์ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบคอมพิวเตอร์

“ข้อมูล” หมายความว่า สิ่งสื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะทำในรูปแบบเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งนั้นบันทึกไว้ปรากฏได้

“การพิสูจน์ตัวตน” หมายความว่า ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

“ผู้ดูแลระบบ” หมายความว่า ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ที่ได้รับมอบหมายจากบริษัท

“Virtual Private Network (VPN)” หมายถึง การเข้าสู่ระบบสารสนเทศของบริษัทจากระยะไกล

## หลักปฏิบัติการรักษาความมั่นคงปลอดภัย

- การรักษาความมั่นคงปลอดภัยถือว่าเป็นหน้าที่ของพนักงานและบุคคลภายนอกทุกคนที่ใช้งานระบบสารสนเทศของบริษัท
- การบริหาร และการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา

- การมีจิตสำนึกผู้ใช้งานที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนดไว้ ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่างๆ ถือเป็นสิ่งสำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบาย ให้พนักงานและบุคคลภายนอกทราบอย่างชัดเจน เพื่อให้มีความเข้าใจในหน้าที่และความรับผิดชอบในการรักษาความปลอดภัย ที่ตนเองรับผิดชอบเป็นสิ่งที่ทำให้การรักษาความ มั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิภาพ

## ข้อบังคับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

ผู้ใช้งานระบบสารสนเทศของบริษัท มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

### 1. การบริหารบัญชีผู้ใช้และการพิสูจน์ตัวตน

บริษัทกำหนดให้ใช้ชื่อบัญชี (User Account Name) และ รหัสผ่าน (Password) เป็นตัวกำหนดสิทธิ์การใช้งาน ระบบงานต่างๆ สำหรับพนักงาน ซึ่งถือเป็นข้อปฏิบัติพื้นฐานสำหรับการรักษาความปลอดภัยข้อมูลคอมพิวเตอร์ โดยมีรายละเอียด ดังนี้

- 1.1. ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)
- 1.2. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีชื่อผู้ใช้งาน (Username) ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ยกเว้นการกระทำที่เกิดจากบัญชีชื่อผู้ใช้งาน (Username) โดยบุคคลอื่นซึ่งไม่ได้เกิดจากความตั้งใจ หรือความประมาทของผู้ใช้งาน
- 1.3. การดำเนินการใดๆ เกี่ยวกับบัญชีผู้ใช้ระบบคอมพิวเตอร์ เช่น การขอชื่อบัญชี การขอเปลี่ยนแปลงสิทธิ์ ในการเข้าระบบ เป็นต้น จะต้องมีการขอและได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาหรือหน่วยงานที่เกี่ยวข้อง
- 1.4. ผู้ใช้งานจะต้องตั้งรหัสผ่านและดำเนินการใดๆ ที่เกี่ยวข้องกับรหัสผ่าน ตาม **ข้อกำหนดด้านสารสนเทศ**

### 2. การบริหารจัดการทรัพย์สิน

- 2.1 ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กับการใช้งาน ก่อนได้รับอนุญาต
- 2.2 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้ง

- 2.3 ผู้ใช้งานมีหน้าที่ต้องชดเชยค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน
- 2.4 ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม Computer หรือ Notebook ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ
- 2.5 ทรัพย์สินและระบบสารสนเทศต่างๆ ที่บริษัท จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์ เพื่อการใช้งานของบริษัทเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่บริษัทไม่ได้กำหนดหรือทำให้เกิดความเสียหายต่อบริษัท
- 2.6 ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ 2.5 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น
- 2.7 การรับเครื่องคอมพิวเตอร์ใหม่ทดแทนเครื่องเก่าอายุ 5 ปี ต้องทำตามข้อกำหนดด้านสารสนเทศ

### 3. การบริหารจัดการข้อมูลองค์กร

- 3.1 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของบริษัทหรือเป็นข้อมูลของบุคคลภายนอก
- 3.2 ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของบริษัท ถือเป็นทรัพย์สินของบริษัท ห้ามมิให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
- 3.3 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัท หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย
- 3.4 ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล
- 3.5 ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร บริษัทจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่บริษัท ต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับบริษัท ซึ่งบริษัทอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

#### 4. การบริหารจัดการระบบสารสนเทศ

- 4.1 ผู้ใช้งานห้ามนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพ็จนบนเครือข่ายคอมพิวเตอร์
- 4.2 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent), อีมูเล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา
- 4.3 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของบริษัท
- 4.4 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัท เพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อ กฎหมายและศีลธรรม หรือกระทบต่อภารกิจของบริษัท
- 4.5 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัทเพื่อประโยชน์ทางการค้าส่วนตัว
- 4.6 ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดใน เครือข่ายระบบสารสนเทศของบริษัท โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม
- 4.7 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัท ต้องหยุดชะงัก
- 4.8 ห้ามใช้ระบบสารสนเทศของบริษัท เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศ ภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ
- 4.9 ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม
- 4.10 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัท โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

#### 5. การปฏิบัติตามกฎหมายและข้อบังคับ

บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของบริษัท ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

## 6. ซอฟต์แวร์และลิขสิทธิ์

- 6.1 บริษัท ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัท อนุญาตให้ใช้งานหรือที่บริษัท มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและบริษัท ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์บริษัท ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งาน จะต้องรับผิดชอบแต่เพียงผู้เดียว
- 6.2 ซอฟต์แวร์ ที่บริษัท ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น
- 6.3 ผู้ใช้งานต้องตรวจสอบความถูกต้องของซอฟต์แวร์ที่ใช้งาน รวมถึงข้อตกลงและขอบเขตในการใช้งานเครื่องคอมพิวเตอร์ของบริษัท ใน **แบบฟอร์มรับคอมพิวเตอร์และซอฟต์แวร์ลิขสิทธิ์** ทุกครั้ง ก่อนทำการเซ็นรับเครื่องคอมพิวเตอร์

## 7. การป้องกันโปรแกรมอันตรายมัลแวร์

- 7.1 บริษัท และหน่วยงานเทคโนโลยีสารสนเทศจะต้องใช้ซอฟต์แวร์ที่มีกระบวนการ ในการจัดการและป้องกันโปรแกรมไม่ประสงค์ดีหรือเรียกว่ามัลแวร์ พนักงานทุกคนต้องให้ความร่วมมือปฏิบัติตามนโยบายดังกล่าวรวมทั้งไม่ติดตั้งซอฟต์แวร์เอง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายให้ทำงานแทน
- 7.2 คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus) ตามที่บริษัท ได้ติดตั้งให้ใช้งาน
- 7.3 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาให้ใช้งานหรือเก็บบันทึกทุกครั้ง
- 7.4 ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น
- 7.5 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ
- 7.6 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ
- 7.7 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของบริษัท



## 8. การใช้งานระบบจดหมายอิเล็กทรอนิกส์

ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตาม “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550” หมวด 1 มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

- 8.1 ห้ามใช้ E-Mail เพื่อการค้าหรือธุรกิจอื่น ที่ไม่ใช่ธุรกิจของบริษัท อันเป็นการขัดต่อกฎหมายและศีลธรรมอันดีงาม หรือกระทบต่อภารกิจของบริษัท
- 8.2 ไม่ควรใช้ E-Mail Address ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ E-Mail และให้ถือว่าเจ้าของ E-Mail เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ
- 8.3 ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง
- 8.4 ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
- 8.5 ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
- 8.6 ห้ามส่ง E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น
- 8.7 ห้ามส่ง E-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
- 8.8
- 8.9 ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
- 8.10 ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของบริษัท ทำให้เกิดความแตกแยกระหว่างบริษัทผ่านทางจดหมายอิเล็กทรอนิกส์
- 8.11 ผู้ที่ไม่ใช่พนักงานของบริษัท ที่ต้องการใช้งาน E-Mail ต้องทำการกรอกข้อมูลคำขอเข้าใช้งาน และยื่นคำขอกับแผนก IT เพื่อดำเนินการกำหนดสิทธิ์ชื่อผู้ใช้งานรายใหม่และรหัสผ่าน

## 9. การควบคุมการให้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น

- 9.1 ต้องมีสัญญาการรักษาข้อมูลเป็นความลับที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล NDA (Non-disclosure agreement) ขอบเขตงานและเงื่อนไขในการให้บริการอย่างชัดเจน
- 9.2 ต้องให้เจ้าหน้าที่ IT ควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติงานที่บริษัทฯ (onsite service) และให้เจ้าหน้าที่ IT ตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ Remote Access และเปิด VPN Service หรือ Remote Access Service ทันทีที่การให้บริการเสร็จสิ้น

- 9.3 ดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ
- 9.4 ต้องกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข
- 9.5 ต้องมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ จากผู้มีใช้งานที่เกี่ยวข้อง และมีการรองรับการตรวจรับงานจากผู้มีอำนาจหน้าที่

## 10. การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

- 10.1 ต้องกำหนดให้มีขั้นตอนสำหรับการลงทะเบียนต่างๆ เพื่อให้มีสิทธิและควบคุมสิทธิในการเข้าถึงระบบสารสนเทศของบริษัทตามความจำเป็นรวมถึงขั้นตอนการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกหรือเปลี่ยนแปลงตำแหน่ง เป็นต้น
- 10.2 การเข้าถึงระบบสารสนเทศทุกระบบต้องได้รับการพิสูจน์ และยืนยันตัวตนทุกครั้งอย่างน้อยด้วย Username และ Password ที่ได้รับจากผู้ดูแลระบบ ก่อนที่จะเข้าใช้งานตามสิทธิที่ได้รับ และหากเป็นระบบสำคัญ หรือการใช้งานจากภายนอกบริษัทผ่านระบบ Virtual Private Network (VPN) จะต้องปฏิบัติตาม**ข้อกำหนดด้านสารสนเทศ**
- 10.3 ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบโดยมาตรการ ต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย
- 10.4 การเข้าถึงแอปพลิเคชันใดๆ ต้องถูกควบคุมและจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับ อนุญาต หรือได้รับมอบหมายให้มีสิทธิ์ เช่น ผู้ดูแลระบบ เป็นต้น รวมถึงการใช้ ซอฟต์แวร์ที่มีลิขสิทธิ์ ต้อง อนุญาตเฉพาะผู้ที่มีสิทธิ์ตามจำนวนที่ซื้อเท่านั้น
- 10.5 ต้องมีการแบ่งแยกระบบเครือข่ายตามกลุ่มที่ให้บริการ เช่น โซนภายในบริษัท โซนระบบสำคัญ โซนภายนอกบริษัท เป็นต้น เพื่อให้สามารถป้องกันการบุกรุกได้อย่างเป็นระบบ
- 10.6 ผู้ใช้งานต้องใช้หมายเลข IP Address ที่กำหนดให้โดยแผนกเทคโนโลยีสารสนเทศ ห้ามพนักงานทำการ ตั้งค่าหมายเลข IP Address เอง

## 11. การรักษาความปลอดภัยระบบเครือข่ายไร้สาย

- 11.1 การเชื่อมโยงระบบเครือข่ายไร้สาย จะอนุญาตให้เฉพาะอุปกรณ์ที่มี MAC Address ตามที่ได้ขึ้นทะเบียนไว้
- 11.2 พนักงานที่จะใช้งานระบบเครือข่ายไร้สาย (Wireless LAN) จะต้องลงทะเบียน Wireless Network Interface Card (MAC Address) ของอุปกรณ์ที่จะใช้งานกับแผนก Information Technology สำหรับบุคคลอื่นที่ไม่ใช่ พนักงาน (Guest) หากมีความจำเป็นต้องใช้งาน

ระบบเครือข่ายไร้สาย จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่เกี่ยวข้อง และอนุญาตให้ใช้งานเฉพาะการออก Internet เท่านั้น

11.3 ห้ามพนักงานนำ Wireless Access Point มาติดตั้งใช้งานเพิ่มเติมเข้ากับระบบเครือข่ายของบริษัทโดยเด็ดขาด หากมีความจำเป็นต้องจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาและแผนก Information Technology

11.4 กลุ่มผู้ใช้ที่มีพนักงานของบริษัทฯ เช่น ลูกค้า ผู้ขาย หรือ ผู้รับช่วงงาน (Sub-contractor) เป็นต้น สามารถเข้าถึงระบบเครือข่ายของบริษัทฯได้ผ่านระบบ Wireless LAN และจะได้รับสิทธิเฉพาะการใช้งาน Internet อย่างเดียวเท่านั้น โดยต้องทำการลงทะเบียนใช้งานตามข้อกำหนดด้านสารสนเทศ

## 12. การรักษาความปลอดภัยด้านกายภาพห้องแม่ข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

12.1 เครื่องแม่ข่ายจะต้องตั้งอยู่ในสถานที่ที่มีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) พนักงานที่มีหน้าที่ดูแลระบบและผู้ได้รับอนุญาตเท่านั้น เป็นผู้ที่มีสิทธิ์เข้า-ออก มีระบบการพิสูจน์ตัวตนและจัดเก็บบันทึกการเข้าออก เช่น ระบบ Access Control ในกรณีที่มีความจำเป็นสำหรับบุคคลภายนอกที่จะต้องเข้าถึงสถานที่ดังกล่าวเพื่อทำการบำรุงรักษาหรือซ่อมแซม อุปกรณ์ต่างๆ จะต้องอยู่ในความดูแลของผู้ดูแลระบบและต้องบันทึกรายการ เข้า-ออก ทุกครั้งเป็นลายลักษณ์อักษร

12.2 มีระบบกล้องวงจรปิด ภายในห้องคอมพิวเตอร์แม่ข่าย และทางเข้าออก และมีการตรวจสอบสภาพให้พร้อมใช้งานเสมอ

12.3 มีระบบสำรองไฟและระบบปรับอากาศ จะต้องมีความปลอดภัยและเหมาะสม โดยจัดให้มีระบบสำรองไฟและระบบปรับอากาศสำรอง เพื่อใช้งานเมื่อไฟฟ้าขัดข้องและรักษาอุณหภูมิในห้อง

12.4 ต้องมีมาตรการป้องกันอัคคีภัย ภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย ต้องมีการติดตั้งอุปกรณ์ดับเพลิงสำหรับใช้กรณีฉุกเฉินเมื่อเกิดอัคคีภัย

12.5 เครื่องแม่ข่ายจะต้องได้รับการติดตั้ง Security Patch ตามคำแนะนำ ของผู้ผลิตเพื่อปิดช่องโหว่ที่เกี่ยวกับปัญหาความปลอดภัย เว้นแต่การติดตั้ง Security Patch นั้นส่งผลกระทบกับการทำงานส่วนอื่นๆของระบบ ซึ่ง Security Patch นี้จะต้องได้รับการทดสอบโดยผู้ดูแลระบบ (System Administrator) ก่อนที่จะนำไปติดตั้งใช้งานจริง

- 12.6 เครื่องแม่ข่ายจะต้องได้รับการติดตั้งโปรแกรม Anti-Virus มีการอัปเดต (patch) และโปรแกรมประยุกต์ต่าง ๆ ให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ
- 12.7 ต้องทำการยกเลิกบัญชีผู้ใช้ที่ติดตั้งมาจากผู้ผลิตหรือทำการเปลี่ยนรหัสผ่านของบัญชีผู้ใช้ที่ติดตั้งจากผู้ผลิต
- 12.8 จะต้องตั้งค่าให้มีการบันทึก Audit Log ของการใช้งานเครื่องแม่ข่าย และเก็บไว้เป็นเวลานานไม่น้อยกว่า 90 วัน และให้มีการตรวจสอบ Audit Log ต่างๆ ของเครื่องแม่ข่ายเป็นประจำเพื่อตรวจสอบการถูกบุกรุก หรือความผิดปกติอื่นๆ
- 12.9 ต้องจัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดครอบคลุม เครือข่ายภายใน เครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- 12.10 ต้องมีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ของระบบเครือข่าย ( Log ) อย่างน้อย 90 วัน

### 13. ความปลอดภัยของการสำรองข้อมูลและความต่อเนื่องในการดำเนินการ

- 13.1 จัดทำระบบสำรองข้อมูลของระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของ บริษัทสามารถให้บริการได้อย่างต่อเนื่อง และมีเสถียรภาพ ต้องจัดทำระบบ สารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของผู้ดูแลระบบในการสำรองข้อมูล และ จัดทำแผนเตรียมความพร้อมในกรณีฉุกเฉิน หรือในกรณีที่ไม่สามารถดำเนินการ ได้อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่าง
- 13.2 จัดทำแผนบริหารความต่อเนื่องทางธุรกิจสำหรับระบบงานที่มีความสำคัญ มีการทดสอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเมื่อเกิดเหตุฉุกเฉินสามารถนำแผนมาใช้งานได้จริง
- 13.3 ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจเพื่อให้ แผนทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ

### วิธีการปฏิบัติให้เป็นไปตามนโยบาย

ผู้ใช้งานและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทจำเป็นต้องตระหนักรู้ และให้ความสำคัญในการรักษาความมั่นคงปลอดภัยด้านข้อมูล เพื่อให้ระบบสารสนเทศของบริษัท สามารถดำเนินการหรือให้บริการต่าง ๆ ได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัยและเชื่อถือได้ ทาง

บริษัทได้จัดทำนโยบายฉบับนี้ขึ้น เพื่อให้ผู้ใช้งาน และผู้ดูแลระบบสารสนเทศในบริษัททราบ และยึดถือปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดอย่างเคร่งครัด และประกาศบนเว็บไซต์อินเทอร์เน็ตของบริษัท เพื่อให้การดำเนินงานด้วยวิธีการระบบสารสนเทศของบริษัทมีความมั่นคงปลอดภัยและเชื่อถือได้

และเพื่อให้การใช้งานในระบบสารสนเทศเกิดความปลอดภัยสูงสุด บริษัทจะจัดให้มีการอบรมอย่าง น้อยปีละ 1 ครั้ง เพื่อสร้างความรู้ความเข้าใจกับผู้ใช้งาน และสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ ( information security awareness training ) อันจะเกิดจากความรู้อะไรก็ตามถึงการฉ้อโกงหรือความไม่ระมัดระวัง

## บทลงโทษและการบังคับใช้

การใช้งานที่มีเจตนาฝ่าฝืนนโยบาย เกี่ยวกับความปลอดภัยระบบสารสนเทศของบริษัท แม้ว่าการฝ่าฝืนนั้นจะกระทำไม่บรรลุผลโดยสมบูรณ์ก็ถือว่ามีความผิดโดยสมบูรณ์

## การลงโทษทางวินัย

1. หากพนักงานกระทำผิดทางวินัย หรือกระทำการใดๆ ที่เป็นการฝ่าฝืนประกาศ ระเบียบ คำสั่ง หนังสือเวียนของบริษัทฯ จะต้องถูกลงโทษตามความหนักเบาหรือชนิดของการกระทำผิด โดยจะพิจารณาจากเจตนา สภาพแวดล้อม ผลจากการกระทำผิด หรือโอกาสจะเกิดผลดังกล่าว การให้ความร่วมมือในการทำงาน และคุณงามความดีในอดีตตลอดจนประโยชน์ที่บริษัทจะได้รับในอนาคตเป็นรายๆ ไป โดยพนักงานอาจได้รับโทษประการใดประการหนึ่ง หรือหลายประการ พร้อมกันโดยไม่ต้องเรียงลำดับ ดังต่อไปนี้

- 1.1 ตักเตือนด้วยวาจา
- 1.2 ตักเตือนเป็นหนังสือ
- 1.3 พักงานโดยไม่ได้รับค่าจ้าง
- 1.4 ตัดสิทธิประโยชน์ หรือเงินได้อื่นๆ ที่ไม่ใช่ค่าจ้าง
- 1.5 เลิกจ้าง

ทั้งนี้ บริษัทฯอาจลดโทษให้แก่ผู้มีเหตุอันควรลดโทษให้ โดยเปลี่ยนโทษเลิกจ้าง เป็นตัดโบนัส งดโบนัส ลดค่าจ้าง และ/หรือ ลดตำแหน่ง ซึ่งเป็นคุณต่อลูกจ้างยิ่งกว่าการเลิกจ้าง โดยยังคงจ้างงานต่อไปก็ได้

2. ให้ผู้บังคับบัญชาในระดับหัวหน้างาน หรือผู้มีตำแหน่งเทียบเท่าตำแหน่งดังกล่าวขึ้นไป มีอำนาจสั่งลงโทษตามข้อ 1.1 ได้

3. ให้ผู้บังคับบัญชาในระดับผู้จัดการแผนก หรือผู้มีตำแหน่งเทียบเท่าตำแหน่งดังกล่าวขึ้นไปมีอำนาจสั่งลงโทษได้ ตามข้อ 1.1-1.4
4. ให้กรรมการผู้จัดการใหญ่ หรือผู้ที่ได้รับมอบหมายจากกรรมการผู้จัดการใหญ่เป็นผู้มีอำนาจใช้ดุลพินิจในการสั่งลงโทษพนักงานคนใดในระดับโทษอย่างไรที่เห็นสมควรก็ได้ตามข้อ 1.1-1.5 รวมทั้งการสั่งให้ชดใช้ความเสียหายในทางแพ่ง

อนึ่ง ในการลงโทษพนักงานนั้น ผู้บังคับบัญชาต้องทำการสอบสวนให้ได้ความจริงเป็นที่ยุติก่อนว่ามีพยานหลักฐานที่มีน้ำหนักความน่าเชื่อถือ มากกว่าพยานหลักฐานหรือคำชี้แจงแก้ข้อกล่าวหาผู้ที่ถูกสงสัยว่าได้กระทำความผิดจึงค่อยสั่งลงโทษ

### การบังคับใช้

ประธานเจ้าหน้าที่บริหาร ผู้จัดการฝ่าย ผู้จัดการแผนก หัวหน้าฝ่าย หัวหน้าแผนก มีหน้าที่ควบคุมผู้ใต้บังคับบัญชา ให้ปฏิบัติตามนโยบาย และข้อบังคับ อย่างเคร่งครัด หากพบว่าผู้ใต้บังคับบัญชากระทำความผิด ให้ผู้บังคับบัญชารายงานตามลำดับชั้นเพื่อเอาโทษต่อผู้กระทำความผิดอย่างเคร่งครัด การละเว้นการปฏิบัติหน้าที่ถือเป็นความผิดเช่นเดียวกับผู้กระทำผิด

### การทบทวนนโยบาย

บริษัทฯ ตั้งเป้าหมายในการทบทวนนโยบายระบบสารสนเทศเพื่อให้ทันสมัย และมีความสอดคล้องกับบริษัทฯ โดยกำหนดให้มีการทบทวนทุก ๆ 1 ปี หรือหากมีกรณีเร่งด่วนจะนำมาทบทวนปรับปรุงก่อนครบกำหนดระยะเวลาดังกล่าว

## ข้อกำหนดด้านระบบสารสนเทศ

### 1. ข้อกำหนดการจัดการรหัสผ่าน

นโยบายรหัสผ่านให้เป็นไปตามข้อกำหนดของฝ่ายเทคโนโลยีสารสนเทศ โดยฝ่ายเทคโนโลยีสารสนเทศจะต้องทำการทบทวนข้อกำหนดอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง รหัสผ่านครอบคลุมบัญชีชื่อผู้ใช้งานดังนี้ คือ

13.4 Computer User ทั้งที่เป็น Domain User และ Local User, E-mail, Internet, Oracle หรือบัญชีผู้ใช้งานระดับบริหารจัดการระบบสารสนเทศต่างๆ

13.5 การตั้งรหัสผ่าน จะต้องมีความยาวอย่างน้อย 8 ตัวอักษร และยากต่อการคาดเดา ( Strong Password ) ซึ่งมีแนวทางการตั้งรหัสผ่าน ดังนี้

- ประกอบด้วยตัวอักษรภาษาอังกฤษ (Alphabet) ใหญ่และเล็ก ( A-Z, a-z ) ตัวเลข ( 0-9 ) ตัวอักขระพิเศษ(Special character) เช่น !@#\$ โดยจัดเรียงแบบไหนก็ได้
- ไม่ใช่ค่า default password ที่ระบบตั้งมาให้

13.6 รหัสผ่านต้องไม่เป็นลักษณะตัวเลขหรืออักขระที่เรียงกันหรือซ้ำเกิน 3 ตัวอักษร หรือตัวอักขระ ที่เหมือนกับบัญชีชื่อผู้ใช้งาน เกิน 3 ตัวอักษร เช่น aaabbbb, abcdef, 123456 เป็นต้น

13.7 ต้องไม่ใช้รหัสผ่านซ้ำกับรหัสผ่านที่เคยใช้มาแล้ว 2 ครั้ง

13.8 Password age อายุหรือความถี่ในการเปลี่ยนรหัสผ่าน

- รหัสผ่านผู้ใช้งานทั่วไป ต้องเปลี่ยนรหัสผ่านทุกๆ 90 วัน
- รหัสผ่านผู้บริหารระบบ (system administrator) ต้องเปลี่ยนรหัสผ่านทุกๆ 60 วัน

13.9 ห้ามเลือกใช้คุณสมบัติที่มีหน้าที่ในการจดจำรหัสผ่านในโปรแกรมต่างๆ เช่น Outlook , Web Browser เป็นต้น

13.10 หากใส่รหัสผ่านผิดเกิน 10 ครั้ง บัญชีผู้ใช้งาน (User account) จะถูกล็อกโดยอัตโนมัติ ต้องติดต่อแผนก IT เพื่อทำการปลดล็อก

13.11 ผู้ใช้งานต้องยินยอมให้ทางเจ้าหน้าที่หรือตัวแทนบริษัทเข้าตรวจสอบการพิสูจน์ตัวตนโดยไม่ต้องบอกล่วงหน้า

### 2. ข้อกำหนดการใช้งานระบบ จากภายนอกบริษัทผ่านระบบ Virtual Private Network (VPN)

2.1 กำหนดให้ใช้ User และ Password Active Directory (AD) ในการ Connect พนักงานต้องเก็บ User และ Password ไว้เป็นความลับห้ามใช้ร่วมกับผู้อื่น

2.2 กำหนดให้ใช้งานโปรแกรม VPN Client ด้วย Cisco AnyConnect และสามารถใช้งานได้เฉพาะในประเทศไทยเท่านั้น

2.3 กำหนดให้ใช้งาน 1 User ต่อ 1 Connection เท่านั้น

2.4 เครื่องคอมพิวเตอร์ที่ต้องการใช้งาน VPN ต้องได้รับอนุญาตและลงทะเบียน MAC Address อุปกรณ์ที่จะใช้งาน กับแผนก IT เพื่อยืนยันตัวตนก่อนการใช้งาน

2.5 อุปกรณ์มือถือทุกชนิดต้องลงทะเบียน UID (Device ID) ของ Application AnyConnect

2.6 เครื่องคอมพิวเตอร์ที่ต้องการใช้งาน VPN ต้องติดตั้งโปรแกรม Anti Virus ของบริษัทหรือของส่วนตัว และได้รับการตรวจสอบโดยแผนก IT ก่อน

### 3. ข้อกำหนดในการใช้งานระบบเครือข่ายไร้สาย Wireless LAN

- พนักงานที่จะใช้งานระบบเครือข่ายไร้สาย (Wireless LAN) จะต้องลงทะเบียน Wireless Network Interface Card (MAC Address) ของอุปกรณ์ที่จะใช้งาน กับแผนก Information Technology สำหรับบุคคลอื่นที่ไม่ใช่ พนักงาน (Guest) หากมีความจำเป็นต้องใช้งานระบบเครือข่ายไร้สาย จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่เกี่ยวข้อง และอนุญาตให้ใช้งานเฉพาะการออก Internet เท่านั้น

### 4. ข้อกำหนดในการรับเครื่องคอมพิวเตอร์ใหม่ทดแทนเครื่องเก่า

- หลังจากได้รับเครื่องคอมพิวเตอร์จากทาง Admin-CA ให้นำเครื่องมาที่แผนก IT เพื่อทำการ Create User Profile Domain ,Setup Email MS-Outlook , และ Setup การใช้งานต่างๆ เช่น Map Drive , Printer , เปลี่ยนภาษา การตั้งค่าดังกล่าวควรทำที่ Network AIT เพื่อความสะดวกรวดเร็ว
- กรุณาตรวจสอบ ความถูกต้องของชื่อและซอฟต์แวร์ที่ใช้งาน รวมถึงข้อตกลงและขอบเขตในการใช้งานเครื่องคอมพิวเตอร์ของบริษัท ในแบบฟอร์มรับคอมพิวเตอร์และซอฟต์แวร์ลิขสิทธิ์ทุกครั้ง ก่อนทำการเซ็นรับ
- ในกรณีที่ผู้ใช้ลิขสิทธิ์ซื้อเครื่องเก่าที่หมดอายุการใช้งาน ต้องนำเครื่องมาให้ทาง IT ทำการตรวจสอบเครื่อง และถอนการติดตั้งโปรแกรมลิขสิทธิ์ของบริษัทก่อนทุกครั้ง ทางแผนก IT จะไม่ทำการเซ็นรับรองเอกสารตัดจำหน่ายทรัพย์สินในทุกกรณีหากยังไม่มีตรวจสอบเครื่อง