นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security Policy)

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ให้อยู่ระดับมาตรฐานสากลอีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากเกิดปัญหา เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของพนักงานบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน)

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ประกอบไปด้วย 8 หมวด โดยมีรายละเอียดดังนี้

หมวด 1 ว่าด้วยการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

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

ข้อ 2 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ 3 ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านควรมีความยาวไม่น้อยกว่า 8 ตัวอักษรซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษรที่เป็นตัวพิมพ์ใหญ่ (Alphabet) และตัวอักษรพิเศษ (Special character)

ข้อ 4 ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิม 5 ครั้งสุดท้าย

ข้อ 5 ผู้ใช้งานควรเปลี่ยนรหัสผ่าน (Password) ครั้งแรกที่ Login เข้าใช้งาน และควรเปลี่ยนรหัสผ่าน (Password) ทุกๆ 90 วันหรือเมื่อมีสัญญาณบอกเหตุว่าข้อมูลอาจรั่วไหลหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยน

ข้อ 6 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) และหากพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อค หรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

(1) คอมพิวเตอร์โน๊ตบุ๊ค (Notebook) ที่เชื่อมต่อด้วย wifi ต้องทำการพิสูจน์ตัวตนก่อนการใช้งาน

(2) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(3) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(4) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(5) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(6) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย 15 นาที

หมวด 2 ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

ข้อ 7 ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบโดยต้องลงชื่อในสมุดบันทึกการเข้า-ออกห้อง Server ทุกครั้ง

ข้อ 8 ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 9 ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ 10 ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

ข้อ 11 ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

ข้อ 12 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยบรรดารายการทรัพย์สิน (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบจะอยู่ในแบบฟอร์มใบทะเบียนประวัติอุปกรณ์คอมพิวเตอร์ FM-IT-01/02 การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ ที่บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) มอบหมาย

ข้อ 13 กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ที่ได้รับมอบหมาย

ข้อ 14 ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ 15 ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊ค ไม่ว่ากรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารสูงสุดของฝ่ายเท่านั้น

ข้อ 16 ทรัพย์สินและระบบสารสนเทศต่างๆ ที่บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) จัดเตรียมไว้ให้ใช้งานมีวัตุประสงค์เพื่อการใช้งานของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน)

ข้อ 17 ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ 16 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด 3 ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ 18 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ 19 ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ถือเป็นทรัพย์สินของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 20 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ 21 ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ 22 ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) จะให้การสนับสนุนและเคราพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ซึ่งบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด 4 ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ 23 ผู้ใช้งานห้ามพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ และต้องไม่ดำเนินการดังนี้

(1) พัฒนาโปรแกรมหรือฮาร์แวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(2) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

(3) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(4) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) สิทธิ์การใช้ (License) ซฮฟต์แวร์

(5) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ 24 ห้ามเปิดใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent), Utorrent เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 25 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เล่นเกมส์ เป็นต้น ในระหว่างปฏิบัติงาน

ข้อ 26 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ที่จัดเตรียมไว้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน)

ข้อ 27 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใด เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน)

ข้อ 28 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) เพื่อประโยชน์ทางการค้า

ข้อ 29 ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) โดยเด็ดขาด ไม่ว่าจะด้วยวิธีใดๆ ก็ตาม

ข้อ 30 ห้ามกระทำการรบกวน ทำลายหรือทำให้ระบบสารสนเทศของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ต้องหยุดชะงัก

ข้อ 31 ห้ามใช้ระบบสารสนเทศของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ 32 ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ 33 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด 5 ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

ข้อ 34 บรรดากฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบ ของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน)ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้นหากผู้ใช้งานกระทำผิดกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด 6 ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

ข้อ 35 บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) อนุญาตให้ใช้งาน หรือที่บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ถือว่าเป็นความผดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ 36 ซอฟต์แวร์ (Software) ที่บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด 7 ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

ข้อ 37 คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) ได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 38 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 39 ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเปิดขึ้น

ข้อ 40 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบทันที

ข้อ 41 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายและ ต้องแจ้งแก่ผู้ดูแลระบบทันที

ข้อ 42 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆที่เป็นทรัพย์สินของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) หรือของผู้อื่น โดยไม่ได้รับอนุญาติจากผู้มีอำนาจ

ข้อ 43 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของบริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน)

หมวด 8 ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

ข้อ 44 ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ข้อ 1 ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ 2 ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access point) มาใช้งาน

ข้อ 3 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP(Wired Equivalent Privacy) หรือ WPA (Wi-fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless Lan Client และอุปกรณ์กระจายสัญญาณ (Access Point)

ข้อ 4 ผู้ดูแลระบบ (System Administrator) ควรเลือกใช้วิธีการควบคุม Mac address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี Mac address (Media Access Control Address) และชื่อผู้ใช้(Username) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ 5 ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ 6 ผู้ดูแลระบบ (System Administrator) ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารกับระบบ Server ภายในได้

ข้อ 7 ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย ในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บริหารสูงสุดของฝ่ายทันที

ข้อ 8 ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

ข้อ 1 ผู้ดูแลระบบ (System Administrator) บริษัท ที.เอ.ซี คอนซูเมอร์ จำกัด (มหาชน) มีหน้าที่ในการบริหารจัดการ และติดต่อผู้ให้บริการติดตั้งและกำหนดค่าของไฟร์วอลล์ทั้งหมด

ข้อ 2 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ 3 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

ข้อ 4 ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนใช้งานทุกครั้ง

ข้อ 5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ 6 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ 7 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุแกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

ข้อ 8 การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางบริษัท ที.เอ.ซี คอนซูเมอร์ จำกัด (มหาชน) อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากบริษัท ที.เอ.ซี คอนซูเมอร์ จำกัด (มหาชน) ก่อน

ข้อ 9 การกำหนดค่าให้บริการเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ 10 จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์ทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ 11 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ 12 ผู้ดูแลระบบ (System Administrator) บริษัท ที.เอ.ซี คอนซูเมอร์ จำกัด (มหาชน) มีสิทธิจะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ 13 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจาก บริษัท ที.เอ.ซี คอนซูเมอร์ จำกัด (มหาชน) ก่อนในกรณีที่อนุญาตให้บุคคลภายนอกบริษัท Remote Login จากภายนอก ผู้ดูแลระบบจะต้องควบคุมเฝ้าหน้าจอเครื่อง Server ตลอดการ Remote Login จากภายนอก

ข้อ 14 ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

นโยบายความมั่นคงปลอดภัยของอีเมลล์ (Email Policy)

ข้อ 1 ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ในใบ ICT Request From โดยมีการเซ็นส์อนุมัติตามลำดับ และยื่นคำขอกับเจ้าหน้าที่เทคโนโลยีสารสนเทศ

ข้อ 2 เมื่อได้รับรหัสผ่าน (Password) ต้องเก็บรหัสผ่านที่รับไว้เป็นความลับ เพื่อป้องกันไม่ให้ผู้อื่นที่ไม่เกี่ยวข้องเข้าสู่ระบบ เพื่อกระทำการใด ๆ อันอาจจะก่อให้เกิดความเสียหายแก่ผู้ใช้ และ/หรือ ระบบของเซิร์ฟเวอร์โดยรวม

ข้อ 3 ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ 4 ควรเปลี่ยนรหัส (Password) ทุก 1 ปี

ข้อ 5 ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ให้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

ข้อ 6 การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลในหัวจดหมายอิเล็กทรอนิกส์ (e-mail)

ข้อ 7 ห้ามใช้บริการอีเมล์ที่ได้รับในทางที่ก่อให้เกิดความเดือดร้อนแก่ผู้อื่น เช่น โพสต์ข้อความที่ไม่สุภาพ โฆษณา ประชาสัมพันธ์ข้อมูล ข่าวสาร ที่ก่อให้เกิดความรำคาญแก่บุคคลอื่น หรือก่อให้เกิดความเข้าใจผิด ลงในแหล่งข้อมูลที่เป็นสาธารณะ เช่น ตามกระดานข่าวของเว็ปไซต์สาธารณะต่าง ๆ (Message Board) เพราะอาจเป็นสาเหตุทำให้ระบบเมล์ของบริษัทโดนโจมตีได้

ข้อ 8 ไม่ควรเปิดเมล์หรือไฟล์แนบจากผู้ส่งหรือบุคคลที่ไม่รู้จัก เพราะอาจมี Link หรือไวรัสหรือมัลแวร์ที่แนบมากับ E-mail

ข้อ 9 ไม่ควรใช้อีเมลล์ของบริษัทในการสมัครบริการออนไลน์ต่าง ๆ ที่ใช้งานส่วนตัว เช่น Zalora , Line , Facebook รวมทั้งเว็ปจอง หรือซื้อขายของ และบริการต่าง ๆ เป็นต้น เพราะจะทำให้ได้รับจดหมายโฆษณา และจดหมายขยะต่าง ๆ เข้ามาใน Sever Mail และจะเกิดปัญหาเวลาที่ท่านไม่ได้ใช้อีเมลล์ของบริษัทแล้ว ควรใช้อีเมลล์ส่วนตัวในการสมัครบริการต่าง ๆ ที่เข้าข่ายดังที่กล่าวมาทั้งหมด

ข้อ 10 การใช้อีเมลล์จากเครื่องมือสื่อสารส่วนบุคคลเมื่อลาออกจากบริษัทต้องนำเครื่องมือสื่อสารส่วนบุคคลมาให้เจ้าหน้าที่เทคโนโลยีสารสนเทศทำการลบข้อมูลอีเมลล์จากเครื่องทั้งหมดก่อนถึงกำหนดลาออก 3-7 วัน

นโยบายความมั่นคงปลอดภัยอินเทอร์เน็ต (internet Security Policy)

ข้อ 1 ไม่ใช้ระบบอินเทอร์เน็ต (internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็ปไซต์ที่ไม่เหมาะสม เช่น เว็ปไซต์ที่ขัดต่อศีลธรรม เว็ปไซต์ที่มีเนื้อหาอันอาจกระทบกรเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็ปไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายต่อหน่วยงาน

ข้อ 2 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (internet)

ข้อ 3 ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (internet) การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ 4 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ไม่เปิดข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ 5 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

ข้อ 6 หลังจากใช้งานระบบอินเทอร์เน็ต (internet) เสร็จแล้ว และไม่อยู่ที่เครื่องคอมพิวเตอร์ ให้ล็อคหน้าจอทุกครั้ง เพื่อป้องกันการเข้าใช้งานจากบุคคลอื่น

นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access control Policy)

ข้อ 1 บริษัท ที.เอ.ซี คอนซูเมอร์ จำกัด (มหาชน) กำหนดมาตรการควบคุมการเข้าใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการขอใช้งานเครื่องคอมพิวเตอร์และเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรโดยใช้แบบฟอร์มขอใช้เครื่องคอมพิวเตอร์และอินเทอร์เน็ตจากบุคคลภายนอก

ข้อ 2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบใน firewall ก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ 3 ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการเข้าใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลในระบบ firewall และบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบเพื่อเป็นหลักฐานในการตรวจสอบ

นโยบายความมั่นคงปลอดภัยของการควบคุมการใช้งาน Onedrive และ Sharepoint

ข้อ 1 การกำหนดสิทธิ์การเข้าถึงข้อมูล บริษัทกำหนดให้ OneDrive ใช้สำหรับการจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้งาน โดยผู้ใช้งานแต่ละรายจะได้รับพื้นที่จัดเก็บเฉพาะตนไม่สามารถเข้าถึงข้อมูลของผู้ใช้งานรายอื่นได้ ยกเว้นในกรณีที่มีการแชร์สิทธิ์โดยเจ้าของไฟล์เท่านั้น สำหรับ SharePoint บริษัทกำหนดให้ใช้เป็นพื้นที่จัดเก็บและแลกเปลี่ยนข้อมูลในระดับแผนก โดยมีการกำหนดสิทธิ์การเข้าถึงตามกลุ่มผู้ใช้งานในแต่ละแผนกข้อมูลและเอกสารภายใน SharePoint จะสามารถเข้าถึงได้เฉพาะบุคลากรที่ได้รับสิทธิ์ตามที่กำหนดไว้การเข้าถึงข้ามแผนกจะต้องได้รับการอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูล

ข้อ 2 การกำหนดสิทธิ์การเข้าถึงข้อมูลใน SharePoint ของแต่ละหน่วยงาน จะดำเนินการโดย ผู้ดูแลระบบ (System Administrator) ภายใต้กระบวนการควบคุมสิทธิ์การเข้าถึงจะต้องได้รับการ อนุมัติจากผู้บริหารสูงสุดของฝ่าย หลังจากได้รับการอนุมัติ ผู้ดูแลระบบดำเนินการปรับสิทธิ์ในระบบ SharePoint ให้ตรงตามที่ได้รับอนุมัติ

ข้อ 3 ผู้ใช้งานหน่วยงานอื่นต้องขออนุญาติเข้าถึงข้อมูลใน Sharepoint ของหน่วยงานใดๆ ต้องกรอกใบ IT Request Form และได้รับอนุญาตจากผู้บริหารสูงสุดของฝ่ายที่ดูแล Sharepoint นั้น

ข้อ 4 ห้ามผู้ใช้งานจัดเก็บข้อมูลที่ไม่เกี่ยวข้องกับการทำงานในบริษัท เช่น รูปภาพ เพลง วีดีโอ หนัง เป็นต้นใน Sharepoint ทั้งหมด หากผู้ดูแลระบบ (System Administrator) ตรวจสอบพบสามารถลบข้อมูลนั้นได้ทันที โดยมิต้องแจ้งให้ทราบล้วงหน้า และรายงานต่อผู้บริหารระดับสูงทราบ

การฝ่าฝืน

ในกรณีที่บริษัทฯ ตรวจพบการกระทำละเมิดจริยธรรมและศีลธรรมอันดีของผู้ใช้บริการ บริษัทฯ จะพิจารณาดำเนินการมาตรการทางวินัยตามนโยบายและระเบียบวิธีปฏิบัติด้านการบุคคลแก่ผู้ถือครอง และ/หรือ ผู้ใช้บริการที่ฝ่าฝืนนโยบายและระเบียบวิธีปฏิบัติฯ ซึ่งอาจรวมถึงการยกเลิกสิทธ์การใช้บริการระบบเทคโนโลยีสารสนเทศอีกด้วย

ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของบริษัท ที.เอ.ซี คอนซูเมอร์ จำกัด (มหาชน) การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศจะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของบริษัท ที.เอ.ซี คอนซูเมอร์ จำกัด (มหาชน) จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ผู้ดูแลระบบ (System Administrator) บริษัท ที.เอ.ซี. คอนซูเมอร์ จำกัด (มหาชน) มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า