

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy)

เพื่อเป็นระเบียบปฏิบัติสำหรับการบริหารจัดการระบบสารสนเทศของ บริษัท เค.เอ็ม. แพคเกจจิ้ง จำกัด ให้มีความสอดคล้องกับข้อกำหนดของมาตรฐานสากลที่บริษัทมีการประยุกต์ใช้ และเป็นไปอย่างมีประสิทธิภาพ ปลอดภัย สอดคล้องกับกฎหมายและความต้องการในการใช้งาน เพื่อให้มั่นใจว่ามีการจัดเก็บและควบคุมข้อมูลทางอิเล็กทรอนิกส์เป็นไปตามนโยบายของบริษัทฯ จึงประกาศใช้นโยบาย ความมั่นคงปลอดภัยทางสารสนเทศให้เป็นปัจจุบัน สอดคล้องกับสถานการณ์ดังนี้

หมวด 1 ว่าด้วยการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

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

1.1 กรณีที่ พนักงานเริ่มงานใหม่ ที่มีสิทธิ์ ตามตารางสิทธิ์ซึ่งฝ่ายทรัพยากรมนุษย์ จะต้องร้องขอ Username / Password ใหม่ละเมิดการใช้งานโดยระบุ ชื่อ รหัสพนักงาน ตำแหน่ง และการอนุมัติสิทธิ์การใช้งานระบบสารสนเทศ

1.2 กรณีที่มีการ โยกย้าย เปลี่ยนตำแหน่งหน้าที่รับผิดชอบ จะต้องมีการแจ้งฝ่ายสารสนเทศ เพื่อทำการ ยกเลิก/กำหนด สิทธิ์ใหม่ ตามหน้าที่รับผิดชอบใหม่

ข้อ 2 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username/Login) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ 3 ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า 6 ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

ข้อ 4 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ 90 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน โดยจะต้องไม่ซ้ำกับที่เคยใช้งานก่อนหน้าอย่างน้อย 3 ครั้งย้อนหลัง

ข้อ 5 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพยากรหรือระบบสารสนเทศของบริษัทฯ และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อกกั๊ก หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

(1) คอมพิวเตอร์โน้ตบุ๊ก (Notebook) ต้องทำการพิสูจน์ตัวตน ก่อนการใช้งานทุกครั้ง

(2) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(3) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(4) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูล ซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

บริษัท เค.เอ็ม. แพคเกจจิง จำกัด

เลขประจำตัวผู้เสียภาษี 0105527032801 (สำนักงานใหญ่)
99/99 ม.11 ต.บางเสาธง อ.บางเสาธง จ.สมุทรปราการ 10570
Email : saleadmin@kmp.co.th ; www.kmp.co.th



Tel : +66-(0)2397-9449 Fax : +66-(0)2397-9448

K.M. PACKAGING CO., LTD.

TAX ID NO. 0105527032801 (HEAD OFFICE)
99/99 MOO.11 T.BANGSAOTHONG
A.BANGSAOTHONG SAMUTPRAKARN 10570

(5) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

ข้อ 6 การตัดสินใจ การเข้าถึงระบบสารสนเทศของบริษัท สิทธิการเข้าถึงจะถูกยกเลิกในกรณีต่อไปนี้

6.1 พนักงาน พ้นสภาพการเป็นพนักงานของบริษัทฯ

6.2 กรณีเครื่องสูญหาย/ถูกโจรกรรม

6.3 ต้องสงสัยหรือถูกสอบสวนเรื่องการทุจริตในการนำออกข้อมูลที่ไม่ได้รับอนุญาตออกภายนอก

6.4 การระบุตัวตนหรือรหัสผ่านไม่ถูกต้อง

หมวด 2 ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

2.1 ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ของบริษัทโดยเด็ดขาด และต้องพิสูจน์ตัวตนทุกครั้ง รวมทั้งต้องลงบันทึกรายละเอียดการเข้าออกทุกครั้ง บุคคลภายนอกหรือผู้รับจ้างช่วงห้ามเข้าเว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ หรือผู้มีสิทธิ์เป็นผู้พาเข้าไป

2.2 ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

2.3 ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

2.4 ผู้ใช้งานต้องไม่ใช่ หรือลบเพิ่มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

2.5 ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาเพิ่มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

2.6 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทฯ ไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยบรรดารายการทรัพย์สิน (Fix Asset) ที่ผู้ใช้งานต้องรับผิดชอบจะอยู่แนบท้ายเอกสารข้อบังคับนี้การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ ฝ่ายสารสนเทศ

2.7 กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของบริษัทที่ได้รับมอบหมายให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

2.8 ผู้ใช้งานมีหน้าที่ต้องชดเชยค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

2.9 ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน้ตบุ๊ก ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้น ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

2.10 ทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่บริษัทฯ จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของบริษัทเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่บริษัทฯ ไม่ได้กำหนด หรือทำให้เกิดความเสียหายบริษัท ความเสียหายใด ๆ ที่เกิดจากการละเมิด ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

2.10(1) กรณีทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่ทางบริษัทฯ จัดเตรียมไว้ให้ใช้งาน ถูกโจรกรรม ผู้ถือครองจะต้องแจ้งความลงบันทึกประจำวันเพื่อเป็นหลักฐาน โดยทางบริษัทจะพิจารณาสั่งรองอุปกรณ์หรือให้ชดเชยค่าเสียหาย ตามสมควร

2.10 (2) กรณีที่สูญหาย และมีการแจ้งความดำเนินคดีแล้ว ทางบริษัทจะดำเนินการตัดทรัพย์สินดังกล่าวออกจากระบบทันที รวมทั้ง Username/Password ต่าง ๆ ต้องมีการตั้งใหม่เพื่อความปลอดภัยของข้อมูลภายในบริษัทฯ

หมวด 3 ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

การจัดเก็บและสำรองข้อมูลเพื่อการใช้งานภายในบริษัทฯ ให้มีการจัดเก็บจากส่วนกลางได้สองรูปแบบคือ 1. การจัดเก็บที่เครื่องแม่ข่ายภายในบริษัท (File Server) 2. จัดเก็บบน Cloud storage (One Drive) บนบริการที่ทางบริษัทจัดหาให้เท่านั้น

3.1(1) การสำรองข้อมูลภายในบริษัทฯ ให้อ้างอิงตาม WI-ITD-001-04 การสำรองข้อมูล (Back up) ของเครื่องแม่ข่าย

3.1 (2) การสำรองข้อมูลที่จัดเก็บบน Cloud storage ให้อ้างอิงตามผู้ให้บริการ

3.2 การเรียกคืนข้อมูล Recovery

3.2 (1) การเรียกคืนข้อมูลของผู้ใช้งาน จากข้อมูลที่มีการ Back up ไว้ ตาม ข้อ 3.1(1) กรณีที่มีการร้องขอข้อมูลย้อนหลัง ผู้ใช้งานต้องแจ้งความต้องการมายังฝ่ายสารสนเทศเพื่อกู้คืน (Recovery File) โดยมีระยะเวลาย้อนหลังไม่เกิน 5 วันหรือ Revision ล่าสุด กรณี ตามข้อ 3.1 (2) ให้เรียกคืนได้ตามที่มีการแก้ไขก่อนหน้าที่มีการบันทึกไว้ตามคู่มือผู้ให้บริการ

3.2(2) การเรียกคืน ระบบ (Recovery Systems)ให้อ้างอิงตาม WI-ITD-001-03 โดยเรียกคืนระบบที่ Back up ไว้ล่าสุด โดย Recovery point ไม่เกิน 6 ชั่วโมงสำหรับ File Server.

3.3 ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของบริษัทฯ ถือเป็นทรัพย์สินของบริษัทฯ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากฝ่ายสารสนเทศ หรือบริษัทผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของบริษัทฯ หรือเป็นข้อมูลของบุคคลภายนอก

3.4 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัทฯ หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิดต่อจริยธรรมหรือกฎหมาย การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายนั้น และข้อมูลสารสนเทศที่ไม่เป็นที่เปิดเผยแก่บุคคลทั่วไป เกี่ยวกับธุรกรรมและข้อมูลอื่นใดที่เป็นของ “บริษัทฯ” กำหนดให้ “พนักงาน” ต้องเก็บรักษาเป็นความลับ หรือโดยสภาพ “พนักงาน” ต้องเก็บรักษาข้อมูลนั้นเป็นความลับรวมทั้ง

3.4.1 ข้อมูลไม่ว่าจะปรากฏในรูปของเอกสาร หรือรูปแบบอื่นใด ซึ่งได้รับโดยตรงจาก “บริษัทฯ” หรือตัวแทนของ “บริษัทฯ” โดยมีเนื้อหาที่ไม่พึงเปิดเผยแก่สาธารณชนทั่วไป หรือเป็นความลับทางการค้า หรือผลการวิจัย หรือที่เป็นข้อมูลความลับอื่นใดของคู่สัญญาฝ่ายที่เปิดเผยมูลรวมทั้งข้อมูลลูกค้าและคู่ค้าของ “บริษัทฯ”

3.4.2 การวิเคราะห์ ศึกษา รายงาน บันทึก หรือเอกสารอื่นใดที่ “บริษัทฯ” จัดทำขึ้น หรือที่ “บริษัทฯ” จัดทำขึ้นเกี่ยวกับการดำเนินธุรกิจ

3.4.3 ภาพถ่าย หรือสิ่งที่เป็นข้อมูลลับดังกล่าวข้างต้น (3.4.1-3.4.2)

3.5 ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

3.6 ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร บริษัทฯ จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคลตามกฎหมาย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลหรือผู้ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่อยู่ภายใต้เงื่อนไขที่อนุญาตให้ใช้งานได้

3.7 ข้อมูลส่วนบุคคลหรือลูกค้าเป็นความลับทางธุรกิจหรือการค้า ให้ถือว่าเป็นความลับทางการค้าของบริษัทฯ ห้ามนำไปใช้งานที่ขัดต่อกฎหมาย หรือนโยบายบริษัทฯ

หมวด 4 ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

4.1 ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ แต่ต้องไม่ดำเนินการดังนี้

4.1(1) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

4.1(2) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้อื่น

4.1(3) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฟ้มตัวโปรแกรมไปกับโปรแกรมอื่นใน ลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

4.1(4) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

4.1(5) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

4.2 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิททอร์เรนท์ (Bit torrent), Streaming ต่าง ๆ ที่ไม่เกี่ยวกับงาน เป็นต้น เว้นแต่จะได้รับอนุญาตจากฝ่ายสารสนเทศ หรือบริษัทฯ ตามแต่กรณี

4.3 ห้ามมิให้เปิดหรือใช้งาน (Run) โปรแกรม ออนไลน์ที่ไม่เกี่ยวข้องกับงาน ภายบริษัทฯ ในระหว่างเวลาปฏิบัติงาน เว้นแต่เป็นผู้จะได้รับอนุญาตเป็นลายลักษณ์อักษร ผู้บังคับบัญชาดังต่อไปนี้

4.3(1) Social Media เช่น Facebook line twitter Instagram Tiktok Etc. สำหรับพนักงานทั่วไป ที่ไม่ได้มีส่วนเกี่ยวข้องกับการทำงานผ่าน Application เหล่านี้ ยกเว้นเจ้าหน้าที่ฝ่ายสารสนเทศและพนักงานตั้งแต่ระดับผู้จัดการฝ่ายขึ้นไป สำหรับพนักงานที่ระดับต่ำกว่าผู้จัดการฝ่ายต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารระดับผู้ช่วยผู้อำนวยการ (Asst. Director) ขึ้นไป

4.3(2) การเข้าถึงบริการ ฟรี E-mail / ที่เก็บข้อมูลบน Cloud Storage ที่ไม่ใช่ของบริษัทฯ ต้องได้รับอนุมัติจากผู้บริหารระดับผู้ช่วยผู้อำนวยการ (Asst. Director) ขึ้นไป

4.3(3) การกำหนดสิทธิ์การเข้าถึงต่าง ๆ จะต้องถูกระบบไว้ใน ทะเบียนสิทธิ์การเข้าถึงระบบสารสนเทศของบริษัทฯ

4.4 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทฯ ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภาพลักษณ์ด้านลบของบริษัทฯ

บริษัท เค.เอ็ม. แพคเกจจิ้ง จำกัด

เลขประจำตัวผู้เสียภาษี 0105527032801 (สำนักงานใหญ่)
99/99 ม.11 ต.บางเสาธง อ.บางเสาธง จ.สมุทรปราการ 10570
Email : saleadmin@kmp.co.th ; www.kmp.co.th



Tel : +66-(0)2397-9449 Fax : +66-(0)2397-9448

K.M. PACKAGING CO., LTD.

TAX ID NO. 0105527032801 (HEAD OFFICE)
99/99 MOO.11 T.BANGSAOTHONG
A.BANGSAOTHONG SAMUTPRAKARN 10570

4.5 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทฯ เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูลบุคคลอื่นหรือลูกค้า หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อความลับทางการค้าของบริษัทฯ

4.6 ห้ามใช้ทรัพยากรของบริษัทฯทุกประเภทที่เป็นเพื่อประโยชน์ทางการค้าส่วนบุคคล

4.7 ห้ามกระทำการใด ๆ เพื่อการเผยแพร่ข้อมูล ความลับทางการค้า ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัทฯ ก่อนได้รับอนุญาตจากฝ่ายสารสนเทศ หรือบริษัทโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

4.8 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัทฯ ต้องหยุดชะงัก

4.9 ห้ามใช้ระบบสารสนเทศของบริษัทฯ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากเจ้าของผู้มีอำนาจ

4.10 ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

4.11 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัทฯ โดยไม่ได้รับอนุญาตจากผู้จัดการฝ่ายสารสนเทศ เช่นการติดต่อกับผู้ให้บริการหรือที่ปรึกษาที่เกี่ยวข้องกับระบบสารสนเทศ

หมวด 5 ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

5.1 บริษัทฯ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัทฯ อนุญาตให้ใช้งานหรือที่บริษัทฯ มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และบริษัทฯ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัทฯถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

5.2 ซอฟต์แวร์ (Software) ที่บริษัทฯ ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลงโดยไม่ได้รับอนุญาต

5.3 ซอฟต์แวร์ประเภททดลองใช้ (Shared ware / Trial version) จะต้องถูกอนุมัติให้ติดตั้งได้จาก ผู้จัดการฝ่ายสารสนเทศเท่านั้น เมื่อสิ้นสุดระยะเวลาทดลองใช้งาน กรณีที่ไม่ได้ซื้อลิขสิทธิ์การใช้งานต่อ จะต้องแจ้งถอนการติดตั้งออกจากเครื่องคอมพิวเตอร์ทันที

5.4 การขอใช้และติดตั้งซอฟต์แวร์เฉพาะทาง ดันสังกัดจะต้องแจ้งเรื่องและให้เหตุผลจำเป็นในการขอใช้งาน และต้องทำเรื่องนำเสนอความเห็นชอบให้จัดซื้อ-จัดหาโดยผู้จัดการฝ่ายสารสนเทศ และอนุมัติงบประมาณ โดยประธานเจ้าหน้าที่บริหารหรือสูงกว่าตามอำนาจการอนุมัติ

หมวด 6 ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

บริษัท เค.เอ็ม. แพคเกจจิ้ง จำกัด

เลขประจำตัวผู้เสียภาษี 0105527032801 (สำนักงานใหญ่)
99/99 ม.11 ต.บางเสาธง อ.บางเสาธง จ.สมุทรปราการ 10570
Email : saleadmin@kmp.co.th ; www.kmp.co.th



Tel : +66-(0)2397-9449 Fax : +66-(0)2397-9448

K.M. PACKAGING CO., LTD.

TAX ID NO. 0105527032801 (HEAD OFFICE)
99/99 MOO.11 T.BANGSAOTHONG
A.BANGSAOTHONG SAMUTPRAKARN 10570

- 6.1 คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus) ตามที่บริษัทฯ ได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกัน โดยต้องได้รับอนุญาตจากฝ่ายสารสนเทศ หรือบริษัทฯ
- 6.2 ข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งใด ๆ ที่ได้รับจากผู้ใช้งานอื่นหรือภายนอกบริษัทต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง
- 6.3 ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น
- 6.4 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุฝ่ายสารสนเทศ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส หรือต้องสงสัยว่าติดไวรัสคอมพิวเตอร์ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และ ต้องแจ้งแก่ผู้ดูแลระบบ / ฝ่ายสารสนเทศตรวจสอบโดยทันที
- 6.5 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของบริษัทฯ หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ
- 6.6 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หนอนคอมพิวเตอร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของบริษัทฯ
- 6.7 ห้ามใช้คอมพิวเตอร์หรือสารสนเทศอื่นใดของบริษัทฯ เข้าเว็บไซต์ที่มีความเสี่ยงที่จะเผยแพร่ไวรัสคอมพิวเตอร์ โทรจัน หรือมัลแวร์ Ransomware เช่น เว็บไซต์การพนัน หรือลามกอนาจาร เป็นต้น

หมวด 7 ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ ว่าด้วยการใช้งานระบบอีเมล (Email) ของบริษัทฯ

- 7.1 ผู้มีสิทธิ์ใช้ อีเมลของบริษัท (Username@kmp.co.th) จะต้องเป็นพนักงาน หรือผู้ที่ได้รับอนุญาตหรือมีสิทธิ์ตามตารางสิทธิ์การใช้งานระบบสารสนเทศของบริษัทเท่านั้น
- 7.2 ผู้ใช้งานอีเมลของบริษัท จะต้องใช้งานภายใต้ขอบเขตหรือในนามบริษัทเท่านั้น ไม่ใช่เพื่อเป็นการส่วนบุคคล
- 7.3 ผู้ใช้งานอีเมลต้องไม่ทำการส่งอีเมลในลักษณะ รบกวนผู้อื่น เช่น การส่งแบบ Reply All ให้กับทุกคนทั้ง ๆ ที่ไม่เกี่ยวข้อง
- 7.4 ผู้ใช้งานต้องไม่เปิด ส่งต่อ อีเมลที่ไม่รู้จักหรือต้องสงสัยว่า มีไวรัส หรือมัลแวร์ ถ้าสงสัยให้ทำการลบทิ้งหรือแจ้งฝ่ายสารสนเทศ เพื่อตรวจสอบโดยทันที
- 7.5 กรณีที่พนักงานลาออก หรือพ้นสภาพการเป็นพนักงาน จะต้องถูกการระงับการเข้าถึงโดยทันที
- 7.6 ผู้ใช้งานต้องไม่ใช้อีเมลของบริษัทฯ ส่ง/ส่งต่อ อีเมลที่มีเนื้อหา กระบอบต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ และ กระบอบต่อความสงบเรียบร้อยของบ้านเมือง

บริษัท เค.เอ็ม. แพคเกจจิ้ง จำกัด

เลขประจำตัวผู้เสียภาษี 0105527032801 (สำนักงานใหญ่)
99/99 ม.11 ต.บางเสาธง อ.บางเสาธง จ.สมุทรปราการ 10570
Email : saleadmin@kmp.co.th ; www.kmp.co.th



Tel : +66-(0)2397-9449 Fax : +66-(0)2397-9448

K.M. PACKAGING CO., LTD.

TAX ID NO. 0105527032801 (HEAD OFFICE)
99/99 MOO.11 T.BANGSAOTHONG
A.BANGSAOTHONG SAMUTPRAKARN 10570

7.7 ผู้ใช้งานจะต้องไม่ใช้อีเมลของบริษัทในการใช้ลงทะเบียนหรือทำธุรกรรมส่วนบุคคล

ผู้จัดทำ _____

(นายศรสุพรรณ ลีนลาด)

ตำแหน่ง ผู้จัดการฝ่ายสารสนเทศ

ผู้ตรวจสอบ _____

(น.ส.สุตาภัทร ทบผา)

ตำแหน่ง ผู้ช่วยผู้อำนวยการการปฏิบัติการ

ผู้อนุมัติ _____

(นายพัศกร กมลสุวรรณ)

ตำแหน่ง ประธานเจ้าหน้าที่บริหาร

(นายพศิน กมลสุวรรณ)

ตำแหน่ง ประธานเจ้าหน้าที่บริหารอาวุโส