นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ (0001-2562)

Policy used of Information Technology (IT)

ความเป็นมา

ในปัจจุบันมีการใช้ระบบเทคโนโลยีสารสนเทศในองค์กรมากขึ้น ในขณะเดียวกันก็ทำให้มีภัยคุกคามหลากหลายประเภทตามมา ดังนั้นองค์กรที่ไม่มีการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างรัดกุมจึงมีความเสี่ยงที่จะเกิดผลกระทบจากภัยคุกคามต่างๆ เหล่านั้น ทำให้องค์กรจำเป็นที่จะต้องยกระดับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและเครือข่ายขององค์กร เพื่อลดความเสี่ยงดังกล่าว โดยในปัจจุบันเป็นที่ยอมรับกันว่า “คอมพิวเตอร์” ได้กลายเป็นส่วนหนึ่งของชีวิตไปแล้ว “คอมพิวเตอร์” เข้ามามีบทบาทในงานต่างๆ เกือบทุกด้านในสังคมมนุษย์ การนำคอมพิวเตอร์มาใช้ในหน่วยงานนั้นจำเป็นจะต้องไปสัมพันธ์กับเจ้าหน้าที่และผู้ปฏิบัติจำนวนมาก บุคคลเหล่านี้มีแนวคิดและทัศนคติแตกต่างกันออกไป ดังนั้นเพื่อให้คนเหล่านี้ทำงานร่วมกันได้โดยไม่มีปัญหา จึงจำเป็นต้องมีระเบียบปฏิบัติที่ชัดเจน

วัตถุประสงค์

บริษัท แพลน บี มีเดีย จำกัด (มหาชน) ได้จัดให้มีเครือข่ายคอมพิวเตอร์เพื่ออำนวยความสะดวกแก่พนักงานในการปฏิบัติงานให้แก่องค์กร ให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาอันอาจจะเกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง อีกทั้งเพื่อให้พนักงานที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกเข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการงโมย การฉ้อโกง การใช้ข้อมูลอันเป็นความลับอย่างผิดวิธี และการใช้อุปกรณ์ผิดวัตถุประสงค์ องค์กรจึงสมควรวางระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์และระบบเครือข่ายขึ้นเพื่อให้พนักงานที่องค์กรทำสัญญาว่าจ้างและหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคาม ปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยและหน้าที่ความรับผิดชอบ ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย ให้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงความปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

ความสำคัญ

พนักงานมีสิทธิ์ใช้เครือข่ายคอมพิวเตอร์ได้ภายใต้ข้อกำหนดแห่งระเบียบนี้ การฝ่าฝืนข้อกำหนดนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศนี้ หรือกระทำการใดๆ อันก่อหรืออาจจะก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและทางกฎหมายขั้นสูงสุดแก่พนักงานที่ฝ่าฝืนทันที ดังนั้น องค์กรจำต้องกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน และปรับปรุงระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์และระบบเครือข่ายเพื่อให้รองรับกับเทคโนโลยีสารสนเทศที่ปรับเปลี่ยนไปอย่างรวดเร็วรวมทั้งรองรับกับกฎหมาย

ผู้รับผิดชอบหลัก

พนักงานทั้งหมดขององค์กร

คำนิยามที่เกี่ยวข้อง

“องค์กร” หมายถึง บริษัท แพลน บี มีเดีย จำกัด (มหาชน)

“เครือข่ายคอมพิวเตอร์” หมายถึง เครือข่ายคอมพิวเตอร์ของ บริษัท แพลน บี มีเดีย จำกัด (มหาชน)

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของ บริษัท แพลน บี มีเดีย จำกัด (มหาชน)

“พนักงาน” หมายถึง พนักงานและลูกจ้างของ บริษัท แพลน บี มีเดีย จำกัด (มหาชน) รวมถึงบุคคลอื่นที่องค์กรมอบหมายให้ปฏิบัติงานตามสัญญาข้อตกลง หรือใบสั่งซื้อ หรือผู้ที่องค์กรสามารถให้เข้าถึงเครือข่ายคอมพิวเตอร์ขององค์กรได้

“ผู้ดูแลเครือข่ายคอมพิวเตอร์” หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“ผู้บริหารองค์กร” หมายถึง พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับการดำเนินการทั้งหมดขององค์กร

“ผู้บริหารสารสนเทศ” หมายถึง พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับระบบเทคโนโลยีสารสนเทศภายในองค์กร

“ผู้ดูแลระบบ” หมายถึง พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

“หัวหน้างานสารสนเทศ” หมายถึง พนักงานที่มีหน้าที่ควบคุมดูแลการทำงานของผู้ดูแลระบบ พร้อมทั้งมีอำนาจสั่งการผู้ดูแลระบบเครือข่ายและสารสนเทศขององค์กร และรายงานต่อผู้บริหารสารสนเทศ

“หน่วยงานภายนอก” หมายถึง องค์กรอื่น ๆ ที่เกี่ยวข้อง เช่น บริษัทขายฮาร์ดแวร์หรือซอฟต์แวร์ บริษัทให้คำปรึกษาเกี่ยวกับระบบเทคโนโลยีสารสนเทศ เป็นต้น

“ข้อมูล” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย ได้แก่ ไฟล์ข้อความ ไฟล์ภาพ ไฟล์เสียง โปรแกรมคอมพิวเตอร์ เป็นต้น

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ได้แก่ คอมพิวเตอร์หรือเชื่อมต่อกันหรือไม่ก็ตาม โทรศัพท์เคลื่อนที่ เป็นต้น

“ผู้ให้บริการ” หมายถึง ผู้ให้บริการแก่บุคคลอื่นในการเข้าถึงอุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ได้แก่ คอมพิวเตอร์ (ไม่ว่าจะเชื่อมต่อกันหรือไม่ก็ตาม) โทรศัพท์เคลื่อนที่ เป็นต้น

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ได้แก่ ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย, ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อและเครื่องที่เข้ามาใช้บริการและเครื่องที่ให้บริการ เป็นต้น

หมวดที่ 1 ว่าด้วย ระเบียบปฏิบัติทั่วไป

ให้ผู้ถือครองเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นในกรณีที่เครื่องนั้นเกิดความเสียหายต่อตัวเครื่องหรือระบบปฏิบัติการจากการใช้งานผิดวิธี หรือสูญหายไป

- ห้ามพนักงานใหม่ใช้งานเครื่องคอมพิวเตอร์ขององค์กรจนกว่าจะได้รับการอนุมัติให้ใช้งานโดยผ่านการลงทะเบียนก่อน
- ให้ตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติ และ มีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ ต้องทำการตรวจสอบอย่างน้อยวันละ 1 ครั้ง หากพบว่าทำงานผิดปกติให้รีบแจ้งเจ้าหน้าที่เทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยทันที (ทางฝ่ายเทคโนโลยีสารสนเทศเปิดอบรมหลักสูตรวิธีการตรวจสอบโปรแกรม Anti-Virus)
- ให้ผู้ที่เป็นเจ้าของข้อมูลที่ต้องการนำข้อมูลนั้นเผยแพร่สู่สาธารณะ โดยช่องทางต่างๆ เช่น โดยผ่านทางเว็บไซต์ขององค์กร จะต้องทำการตรวจสอบความถูกต้องของข้อมูลก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหาจะต้องรับผิดชอบต่อความผิดพลาดนั้น
- ให้ผู้ที่มีหน้าที่รับผิดชอบในการนำข้อมูลเผยแพร่สู่สาธารณะโดยช่องทางต่างๆ เช่น โดยผ่านทางเว็บไซต์ขององค์กร จะต้องดำเนินการด้วยตนเอง โดย ห้ามมิให้ผู้อื่นดำเนินการแทน และจะต้องทำการเปิดเผยข้อมูลเท่าที่จำเป็นเท่านั้น
- ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง
- ทำการตั้งค่า Screen Server ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการ “การ Lock หน้าจอ” หลังจากที่ไม่ได้ใช้งานเกินกว่า 10 นาที
- ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน เพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล
- ระมัดระวังการใช้งาน และ สงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคล และระบบเครือข่ายเหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและระบบเครือข่าย แล้วแต่กรณี
- ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมที่นอกเหนือจากที่องค์กรได้ติดตั้งไว้ให้ใช้งาน
- ห้ามทำการเปลี่ยนแปลง หรือแก้ไขซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องที่องค์กรจัดซื้อมา
- ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น
- ห้ามพนักงานทั่วไปติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย
- ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้น หรือระบบเครือข่ายขององค์กรได้
- ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวของพนักงานมาใช้กับระบบเครือข่ายขององค์กร ยกเว้นจะได้รับการตรวจสอบจากฝ่ายเทคโนโลยีสารสนเทศก่อนการใช้งาน
- กรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกสำนักงานจะต้องได้รับอนุมัติจากผู้มีอำนาจในการนำทรัพย์สินออกก่อนทุกครั้ง
- ให้ทำการติดตั้ง UPS สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีการใช้งานข้อมูลเป็นปริมาณมากและมีความถี่ในการใช้งานสูง
- ห้ามทำการปรับแต่งค่าระบบที่ได้รับจากการติดตั้งแต่เริ่มแรกอย่างเด็ดขาด เพราะอาจทำให้เกิดความเสียหายต่อระบบการทำงานของเครื่องคอมพิวเตอร์
- ห้ามทำการถอดหรือเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ได้รับการติดตั้งไว้ โดยไม่ได้แจ้งให้กับฝ่ายเทคโนโลยีสารสนเทศที่รับผิดชอบทราบล่วงหน้า
- ห้ามติดตั้งเพิ่มเติมอุปกรณ์ต่อพ่วงใด ๆ ของคอมพิวเตอร์ เช่น หูฟัง, ไมโครโฟน, Printer โดยพละการ ให้แจ้งฝ่ายเทคโนโลยีสารสนเทศที่รับผิดชอบเพื่อดำเนินการติดตั้งให้
- ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ (Server room) ก่อนได้รับอนุญาต

ผู้ใช้งานคอมพิวเตอร์ต้องรับทราบรวมถึงทำความเข้าใจและปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ณ วันที่ 23 มกราคม 2560 อย่างเคร่งครัด

หมวดที่ 2 ว่าด้วย ระเบียบปฏิบัติสำหรับการใช้งานอินเตอร์เน็ต

- ห้ามทำการดาวน์โหลด หรือส่งไฟล์ประเภทสื่อลามก อนาจาร
- ห้ามทำการดาวน์โหลดไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็น
- ห้ามใช้อินเตอร์เน็ตโดยไม่เกี่ยวข้องกับงานที่รับผิดชอบ และไม่ควรใช้งานที่ไม่จำเป็นระหว่างเวลาที่มีการใช้เครือข่ายอย่างหนาแน่น
- ห้ามเล่นเกมส์ ดูภาพยนตร์ หรือฟังเพลง ผ่านทางอินเตอร์เน็ต
- ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

    1. การพนัน
    2. การประมูล
    3. วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และ พระมหากษัตริย์
    4. ลามก อนาจาร ผิด พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวคอมพิวเตอร์ (ฉบับที่ 2)พ.ศ. 2560 มาตรา 14
    5. อื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

- ห้ามใช้โปรแกรมสนทนาในห้องสนทนา (เช่น สังคมออนไลน์ (Facebook/Instagram/Line/We chat/whats app/Skype/Twitter ฯลฯ) และยกเว้นส่วนงานที่ได้รับอนุญาติให้ใช้งานเท่านั้น
- ห้ามใช้งานข้อมูลที่ได้รับโดยผ่านทางอินเตอร์เน็ตที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของข้อมูลนั้น
- ห้ามใช้อินเตอร์เน็ตเพื่อส่ง กระจาย หรือแจกจ่าย ดังต่อไปนี้

    1.สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของ
    2.ข้อมูลที่เป็นความลับขององค์กรไปยังบุคคลที่ไม่ได้รับอนุญาต
    3.ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

- ห้ามใช้อินเตอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ และชื่อเสียงขององค์กร

หมวดที่ 3 ว่าด้วย ระเบียบปฏิบัติสำหรับการใช้งาน E-mail

- ห้ามมิให้พนักงานหรือผู้ไม่มีสิทธิเข้าถึงข้อมูล E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต
- ห้ามลงทะเบียนด้วย E-mail Address ที่องค์กรมอบให้ ไว้ตามที่อยู่เว็บไซต์ต่าง ๆ ที่ไม่เกี่ยวข้องกับงานขององค์กร
- ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
- ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
- ห้ามส่ง E-mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น
- ห้ามส่ง E-mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
- ห้ามปลอมหรือปกปิดชื่อที่อยู่ E-mail ของตน เมื่อทำการส่งE-Mail ไปยังผู้อื่น
- ห้ามส่ง E-mail ที่มีลักษณะเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น
- ห้ามปลอมแปลง E-mail ของบุคคลอื่น
- ห้ามรับ หรือส่ง E-mail แทนบุคคลอื่นโดยไม่ได้รับอนุญาต
- ให้ใช้คำที่ไม่สุภาพในการส่ง E-mail
- ห้ามส่ง E-mail ที่มีขนาดไฟล์ใหญ่เกินกว่า 10 เมกกะไบต์ หรือตามที่องค์กรระบุไว้
- ห้ามส่ง E-mail ที่เป็นความลับขององค์กร เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล E-mail ที่องค์กรกำหนดไว้
- ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-mail ของผู้รับให้ถูกต้อง
- ให้ระบุชื่อของผู้ส่งใน E-mail ทุกฉบับที่ส่งไป
- ให้ใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับ E-mail เท่าที่มีความจำเป็นต้องรับรู้รับทราบ

หมายเหตุ: หมวดที่ 3 นี้ มีความผิดตาม พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มาตรา 4

หมวดที่ 4 ระเบียบปฏิบัติสำหรับการป้องกันการใช้ทรัพยากรผิดวัตถุประสงค์

พนักงานจะต้องไม่ใช้ระบบเครือข่าย โดยมีวัตถุประสงค์ดังต่อไปนี้

- เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ
- เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- เพื่อการพาณิชย์ การบันเทิง หรือเพื่อประโยชน์ส่วนตน
- เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงานให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กร หรือบุคคลภายนอกก็ตาม
- เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือของบุคคลอื่น
- เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่น โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

- เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กร ไปยังที่อยู่เว็บ (website) ใด ๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
- เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่องค์กร

- ฝ่ายเทคโนโลยีสารสนเทศจะทำการสุ่มตรวจเครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์แบบพกพารวมทั้งอุปกรณ์ต่อพ่วงต่างๆ ตามความเหมาะสม ผู้ถือครองทรัพย์สินคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่างๆ ต้องให้ความร่วมมือในการตรวจสอบอุปกรณ์ดังกล่าว
- เพื่อปลอมแปลงข้อมูลคอมพิวเตอร์อันจะก่อให้เกิดความเสียหายต่อผู้อื่นหรือประชาชน
- เพื่อเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ปลอมนั้นไปยังผู้อื่น
- เพื่อนำข้อมูลคอมพิวเตอร์เท็จอันจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน เข้าสู่ระบบคอมพิวเตอร์
- เพื่อเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์เท็จนั้นไปยังผู้อื่น
- เพื่อนำข้อมูลคอมพิวเตอร์ใด ๆ เข้าสู่ระบบคอมพิวเตอร์ โดยข้อมูลนั้นถือเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
- เพื่อนำข้อมูลคอมพิวเตอร์ใด ๆ เข้าสู่ระบบคอมพิวเตอร์ ที่มีลักษณะเป็นการลามกและข้อมูลคอมพิวเตอร์นั้นพนักงานอื่นหรือประชาชนทั่วไปอาจเข้าถึงได้
- เพื่อเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ที่มีลักษณะเป็นการลามกไปยังผู้อื่น
- เพื่อสร้าง ตัดต่อ เติมหรือดัดแปลงภาพด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่จะทำให้ผู้อื่นเกิดความเสียหายได้
- เพื่อเก็บข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่จะทำให้ผู้นั้นเกิดความเสียหายได้

หมวดที่ 5 ว่าด้วย ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน

- ต้องเก็บ และ รักษารหัสผ่านที่ได้รับมอบมาจากองค์กรให้เป็นความลับ
- ต้องตั้งรหัสผ่านให้มีคุณสมบัติ ดังต่อไปนี้
    - มีความยาวไม่น้อยกว่า 8 ตัวอักษร
    - มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ,ตัวพิมพ์ใหญ่,ตัวเลขและสัญลักษณ์เข้าด้วยกัน
    - ไม่กำหนดรหัสผ่านจากชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน
    - ไม่กำหนดรหัสผ่านจากคำศัพท์ที่ใช้ในพจนานุกรม
    - การตั้งชื่อผู้ใช้งานนั้น ต้องกำหนด การตั้งชื่อไม่ซ้ำกัน (Unique User ID)
- ต้องกำหนดรหัสผ่านสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านทางระบบเครือข่าย
- ห้ามใช้โปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำรหัสผ่านของตนโดยอัตโนมัติ (Save Password)
- ต้องไม่จด หรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- ไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง
- กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที
- ให้กลุ่มผู้ใช้งานที่มีการใช้งานบัญชีผู้ใช้งาน และ รหัสผ่านเดียวกัน จะต้องร่วมกันรับผิดชอบหากมีความเสียหาย หรือมีปัญหาเกิดขึ้นกับระบบที่เข้าถึง
- ผู้ใช้งานระบบต้องเปลี่ยนรหัสผ่านเข้าเครื่องคอมพิวเตอร์ทุก 90 วัน
- ห้ามกำหนดรหัสลับ (Set Password) ในส่วนของเครื่องคอมพิวเตอร์ (Hardware) ทั้งในระดับ BIOS และระดับแบบปฏิบัติการ (Operating System) ด้วยตนเอง นอกเหนือจากผู้บังคับบัญชาของส่วนเทคโนโลยีสารสนเทศ และผู้ที่ได้รับมอบหมาย
- รหัสผ่านของพนักงานถือเป็นทรัพย์สินของ บริษัท แพลน บี มีเดีย จำกัด (มหาชน) ทาง บริษัท แพลน บี มีเดีย จำกัด (มหาชน) ไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และพนักงานทุกคนมีหน้าที่ในการป้องกันรหัสผ่านของบริษัท แพลน บี มีเดีย จำกัด (มหาชน) อย่างเคร่งครัด
- หากจะต้องการยกเลิกชื่อผู้ใช้งาน(Username)และรหัสผ่าน(Password) ให้แจ้งกับผู้บังคับบัญชาโดยตรงเพื่อทำเรื่องขอยกเลิกใช้งาน โดยจะต้องกระทำทันทีที่จะเลิกใช้งาน และเจ้าหน้าที่เทคโนโลยีสารสนเทศที่ได้รับการมอบหมายต้องทำการยกเลิกผู้ใช้งานและรหัสผ่าน ทันทีที่ได้รับการแจ้งยกเลิก
- หากชื่อผู้ใช้งานและรหัสผ่านของพนักงานท่านใด ตรวจสอบมีการกระทำความผิดตาม พ.ร.บ.คอมพิวเตอร์ที่ก่อให้เกิดความเสียหายแก่ บริษัท แพลน บี มีเดีย จำกัด (มหาชน) ผู้ที่รับผิดชอบชื่อผู้ใช้งานและรหัสผ่านต้องยอมรับความผิดแต่เพียงผู้เดียว

หมวดที่ 6 ว่าด้วยการเข้าถึงและการใช้งาน เครื่องแม่ข่าย (Server)

- ห้ามเข้าไปในบริเวณห้องเครื่องแม่ข่าย (Server) ก่อนได้รับอนุญาต
- ห้ามพนักงานเข้าไปในบริเวณห้องเครื่องแม่ข่าย (Server) โดยไม่มีกิจที่เกี่ยวข้อง
- ห้ามนำอาหาร และ เครื่องดื่มเข้าไปในบริเวณห้องเครื่องแม่ข่าย (Server)
- บุคคลภายนอกที่เข้ามาติดต่อให้ติดบัตร Visitor ตลอดเวลาเพื่อให้สามารถสังเกตเห็นได้อย่างชัดเจน หากไม่ใช่พนักงานของบริษัท
- ให้ทำการลงบันทึกการเข้าออกห้องเครื่องแม่ข่าย (Server)โดยบุคคลภายนอกในสมุดบันทึกการเข้า - ออกห้องเครื่องแม่ข่าย (Server) ทุกครั้ง
- หากพบเห็นความผิดปกติในห้องเครื่องแม่ข่าย (Server)เช่น มีทรัพย์สินหาย มีร่องรอยการบุกรุก เป็นต้น ให้รีบแจ้งผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทันที
- ห้ามนำอุปกรณ์ที่สามารถบันทึกภาพได้เข้าไปภายในห้องเครื่องแม่ข่าย (Server)เช่น โทรศัพท์เคลื่อนที่, กล้องดิจิตอล กล้องวิดีโอ
- ให้ปฏิบัติตามคำแนะนำของพนักงานที่ดูแลห้องเครื่องแม่ข่าย (Server Room)อย่างเคร่งครัด

หมวดที่ 7 ว่าด้วย ระเบียบปฏิบัติสำหรับการจัดการสารสนเทศ

สำหรับสารสนเทศที่อยู่ในรูปแบบเอกสารกระดาษ

- ให้ใช้เครื่องทำลายเอกสารเพื่อทำลายเอกสารที่เป็นความลับ หรือที่มีระดับความสำคัญสูง
- ให้ป้องกันเอกสารที่เป็นความลับ หรือที่มีระดับความสำคัญสูงที่ถูกพิมพ์ออกมาทางเครื่องพิมพ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- ให้จัดหมวดหมู่เอกสารที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างพอเพียง
- ให้สำเนาเอกสารที่เป็นความลับ หรือที่มีระดับความสำคัญสูงได้ก็ต่อเมื่อได้รับอนุญาตจากผู้เป็นเจ้าของแล้ว
- ให้ระมัดระวังการกระจาย หรือแจกจ่ายเอกสารที่เป็นความลับขององค์กรไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้รับทราบในเอกสารนั้น
- ให้ทำการตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน
- ให้ผู้เป็นเจ้าของเอกสารกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างพอเพียงสำหรับเอกสารที่เป็นความลับ หรือที่มีระดับความสำคัญสูงที่จะถูกส่งไปทางไปรษณีย์

หมวดที่ 8 ว่าด้วย สารสนเทศที่เป็นข้อมูลอิเล็กทรอนิกส์
(เช่น ไฟล์อิเล็กทรอนิกส์, ข้อมูลบนเว็บ, E-mail, Voice-Mail, ข้อมูลมัลติมีเดีย)

- ให้จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างพอเพียง
- ให้สำเนาข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงได้ก็ต่อเมื่อได้รับอนุญาตจากผู้เป็นเจ้าของแล้ว
- ให้ระมัดระวังการกระจาย หรือแจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับขององค์กรไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้รับทราบในข้อมูลอิเล็กทรอนิกส์นั้น
- ให้ผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ ทำการตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน
- ห้ามผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูง ทำการส่งข้อมูลดังกล่าวไปทางไปรษณีย์ เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลที่องค์กรกำหนดไว้
- ให้ส่งเครื่องคอมพิวเตอร์ที่จะจำหน่ายออกให้กับฝ่ายเทคโนโลยีสารสนเทศเพื่อทำการฟอร์แมตข้อมูลอิเล็กทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์นั้น
- ห้ามมิให้ผู้ใดทำการคัดลอกสำเนา (Copy) ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ออกไปนอกบริษัทไม่ว่าจะด้วยวิธีการใดก็ตาม (เช่น การบันทึกลงในสื่อบันทึกต่างๆ อาทิ เช่น ฟล็อปปี้ดิสก์, ฮาร์ดดิสก์, แผ่น CD, แผ่นDVD, Handy Drive / Flash Drive เป็นต้น) ซึ่งการกระทำดังกล่าวผิด พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวคอมพิวเตอร์ (ฉบับที่ 2)พ.ศ. 2560 มาตรา 18

หมายเหตุ : หากผู้ใดมีความจำเป็นต้องนำข้อมูลเหล่านั้นออกนอกบริษัท ต้องแจ้งให้ผู้บังคับบัญชาทราบและอนุญาตก่อน มิฉะนั้นจะถือว่ามีเจตนามิชอบ

หมวดที่ 9 ว่าด้วย ระเบียบปฏิบัติสำหรับการเข้าถึงระบบงาน

- เมื่อพนักงานใหม่เข้ามาปฏิบัติหน้าที่ ให้ผู้บังคับบัญชาของพนักงานดังกล่าวส่งความประสงค์ขอเข้าใช้ระบบงานของ"บริษัท แพลน บี มีเดีย

จำกัด (มหาชน)" ในแบบฟอร์มขอสิทธิ์เข้าใช้ระบบงาน (FM-MIS-S-001) แจ้งขอรหัสเข้าใช้งานระบบงาน ของ"บริษัท แพลน บี มีเดีย จำกัด (มหาชน)" เพื่อนำเสนอต่อผู้บังคับบัญชาตามลำดับขั้นและแจ้งความประสงค์มายังส่วนเทคโนโลยีสารสนเทศ

- ต้องไม่เข้าถึงระบบงานอื่นที่ตนไม่ได้รับอนุมัติให้ใช้งาน

(การอนุมัติเข้าใช้งานในระบบงาน จะต้องกระทำโดยผ่าน "แบบฟอร์มขอสิทธิ์เข้าใช้ระบบงาน" ของบริษัทเท่านั้น)

- ต้องไม่เข้าถึงข้อมูลคอมพิวเตอร์ที่ได้มีการป้องกันเอาไว้ และไม่ได้รับอนุญาตการเข้าใช้งาน
- ต้องออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ
- ต้องไม่เปิดเผยข้อมูลที่เกี่ยวข้องกับมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ขององค์กรให้แก่บุคคลภายนอก
- ต้องไม่ใช้ทรัพยากรคอมพิวเตอร์ขององค์กรเพื่อดักรับข้อมูลคอมพิวเตอร์ขององค์กรหรือของผู้อื่นที่อยู่ระหว่างการส่งข้อมูลและไม่ได้รับสิทธิการเข้าถึงระบบงาน

หมวดที่ 10 ระเบียบปฏิบัติสำหรับการแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย

ให้เจ้าหน้าที่ทำการแจ้งไปยังฝ่ายเทคโนโลยีสารสนเทศ โดยทันที เมื่อพบเห็นเหตุการณ์ทางด้านความมั่นคงปลอดภัย ได้แก่

- โปรแกรมไม่ประสงค์ดี
- ระบบถูกบุกรุกทางเครือข่าย
- ข้อมูลสำคัญถูกเปลี่ยนแปลง หรือสูญหาย
- มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
- การนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์
- การใช้ทรัพยากรเทคโนโลยีสารสนเทศผิดวัตถุประสงค์
- การพบจุดอ่อนในซอฟต์แวร์ ระบบงาน หรือฮาร์ดแวร์ที่ใช้งาน
- ระบบถูกโจมตีจนไม่สามารถให้บริการได้
- ทรัพยากรเทคโนโลยีสารสนเทศถูกขโมย
- การอนุญาตให้บุคคลภายนอกเข้าใช้ระบบงานขององค์กร
- การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่าย หรือ
- เหตุการณ์อื่นๆ ที่เป็นการละเมิดนโยบายด้านความมั่นคงปลอดภัยขององค์กร

ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา หรือผู้ดูแลระบบเครือข่ายในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้น และ/หรือ ระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล และ ระบบเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา หรือผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด

หมวดที่ 11 บทลงโทษ

- ในกรณีที่พนักงานมีการฝ่าฝืนนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศฉบับนี้ จนเป็นเหตุให้องค์กรได้รับความเสียหายหรืออาจจะพิสูจน์ได้ว่าจะได้รับความเสียหายตามความเห็นของผู้บริหารองค์กร พนักงานที่กระทำความผิดดังกล่าวรับทราบและยินยอมให้องค์กรสามารถทำการให้โทษแก่พนักงานได้ตามความเหมาะสมของเหตุการณ์ที่เกิดขึ้นไม่ว่าจะเป็นการว่ากล่าวตักเตือน ออกหนังสือแจ้ง คาดโทษ หรือ ให้พ้นสภาพจากการเป็นพนักงานได้ ตามกฎระเบียบข้อบังคับขององค์กร
- ในกรณีที่เกิดความเสียหายอย่างร้ายแรง โดยการกระทำที่จงใจหรือประมาทเลินเล่ออย่างร้ายแรงจนเป็นเหตุให้องค์กรได้รับความเสียหาย พนักงานที่กระทำความผิดดังกล่าวรับทราบและยินยอมให้องค์กรสามารถกระทำการตามข้อข้างต้นได้ รวมถึงยินยอมที่จะชดใช้ความเสียหายที่เกิดขึ้นตามจริงให้แก่องค์กรในการกระทำผิดดังกล่าว

ทั้งนี้ให้มีผลตั้งแต่ วันที่ 1 กรกฎาคม พ.ศ. 2562 เป็นต้นไป
จึงประกาศมาเพื่อทราบโดยทั่วกัน

ประกาศ ณ วันที่ 15 กรกฎาคม 2562

(ดร.พินิจสรณ์ ลือชัยจรพันธ์)
กรรมการผู้จัดการ