ระเบียบ บริษัท ไออาร์พีซี จำกัด (มหาชน) และบริษัทในเครือ
ว่าด้วย การบริหารงานเทคโนโลยีสารสนเทศ
พ.ศ. 2562

เพื่อกำหนดทิศทาง นโยบาย การกำกับดูแล การบริหารจัดการงานด้านเทคโนโลยีสารสนเทศและการสื่อสารมีความชัดเจน ให้พนักงานมีความเข้าใจสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ สอดคล้องกับกฎระเบียบข้อบังคับทางกฎหมายต่างๆ และให้มีความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงอำนาจหน้าที่และความรับผิดชอบ กรรมการผู้จัดการใหญ่ จึงให้ออกระเบียบไว้ดังต่อไปนี้

1. ระเบียบนี้เรียกว่า "ระเบียบ บริษัท ไออาร์พีซี จำกัด (มหาชน) และบริษัทในเครือ ว่าด้วย การบริหารงานเทคโนโลยีสารสนเทศ พ.ศ. 2562" ระเบียบนี้ให้ใช้บังคับตั้งแต่วันที่ประกาศเป็นต้นไป

2. ให้ยกเลิกบรรดาระเบียบ ประกาศ หรือคำสั่งอื่นใดที่กำหนดไว้แล้วก่อนระเบียบนี้ ซึ่งขัดหรือแย้งกับระเบียบนี้ และให้ใช้ระเบียบนี้แทน

หมวดที่ 1
บททั่วไป

3. ขอบเขต

ระเบียบนี้มีผลบังคับใช้กับพนักงานของบริษัท ไออาร์พีซี จำกัด (มหาชน) และบริษัทในเครือ ทั้งพนักงานประจำ พนักงานตามสัญญาจ้าง พนักงานยืมตัวชั่วคราว รวมถึงบุคคลภายนอกที่เกี่ยวข้องโดยการว่าจ้างของบริษัททั้งหมด

4. นิยาม

"ระเบียบ" หมายถึง ระเบียบ บริษัท ไออาร์พีซี จำกัด (มหาชน) และบริษัทในเครือ ว่าด้วย การบริหารงานเทคโนโลยีสารสนเทศ พ.ศ. 2562

"บริษัท" หมายถึง บริษัท ไออาร์พีซี จำกัด (มหาชน) และบริษัทในเครือ

"ผู้บริหาร" หมายถึง กรรมการผู้จัดการใหญ่ รองกรรมการผู้จัดการใหญ่ ผู้ช่วยกรรมการผู้จัดการใหญ่ ผู้จัดการฝ่าย และ/หรือ ชื่อเรียกเป็นอย่างอื่นที่มีระดับตำแหน่งเทียบเท่า

"พนักงาน" หมายถึง ลูกจ้างของบริษัทตามความหมายของกฎหมายคุ้มครองแรงงาน และให้รวมถึงพนักงานทดลองงาน พนักงานประจำ พนักงานตามสัญญาจ้างงาน พนักงานยืมตัวชั่วคราว

"บุคคลภายนอก" (Third Party) หมายถึง บุคคลอื่นใด ซึ่งไม่ใช่พนักงานของบริษัท แต่มีความจำเป็น ต้องเข้าถึงหรือมีส่วนเกี่ยวข้องกับข้อมูล ทรัพย์สิน หรือระบบเทคโนโลยีสารสนเทศของบริษัท เช่น คู่สัญญา คู่ค้า ที่ปรึกษา ผู้ให้บริการ ผู้รับจ้าง ลูกค้า นักศึกษาฝึกงาน เป็นต้น

"ผู้ใช้งาน" (User) หมายถึง ผู้ที่สามารถเข้าถึงและใช้งานข้อมูล ทรัพย์สิน หรือระบบเทคโนโลยีสารสนเทศของบริษัท

"เทคโนโลยีสารสนเทศและการสื่อสาร" (Information and Communication Technology) หมายถึง การผสานเทคโนโลยีสารสนเทศเข้ากับระบบสื่อสารโทรคมนาคมที่ครอบคลุมระบบสื่อสารอันได้แก่ วิทยุ โทรทัศน์ โทรสาร โทรศัพท์ เครื่องมือการสื่อสารอื่นๆ กับระบบคอมพิวเตอร์ซอฟแวร์ ฐานข้อมูล และบริการสารสนเทศ ตลอดจนระบบเครือข่ายโทรคมนาคมจำนวนมากที่เชื่อมโยงติดต่อกันและใช้ร่วมกันได้

"ศูนย์คอมพิวเตอร์" (Data Center) หมายถึง สถานที่ที่ติดตั้งอุปกรณ์คอมพิวเตอร์หลักทุกแห่งขององค์กร โดยมีระบบไฟฟ้า ระบบสำรองไฟฟ้าอัตโนมัติ ระบบควบคุมอุณหภูมิความชื้น ระบบดับเพลิงอัตโนมัติที่มีประสิทธิภาพ ทั้งนี้ เพื่อการรักษาเสถียรภาพของระบบเทคโนโลยีสารสนเทศขององค์กร

"ระบบเทคโนโลยีสารสนเทศ" หมายถึง ฮาร์ดแวร์ ซอฟแวร์ เครือข่าย กระบวนการ หรือบริการต่างๆ ที่ใช้ในการประมวลผล จัดเก็บ และส่งต่อข้อมูล

"ICT Service Desk" หมายถึง ระบบ หรือช่องทางที่รับเรื่องการร้องขอการใช้บริการจากผู้ใช้งานด้านระบบเทคโนโลยีสารสนเทศ

"โปรแกรมมุ่งร้าย" (Malware) หมายถึง โปรแกรมมุ่งร้ายที่สร้างขึ้นมาโดยมุ่งหวังทำลายทั้งซอฟท์แวร์ โปรแกรม และระบบปฏิบัติการ ได้แก่ ไวรัส (Virus) หนอนอินเทอร์เน็ต (Worm) และม้าโทรจัน (Trojan Horse) เป็นต้น

"อุปกรณ์สารสนเทศ" หมายถึง อุปกรณ์ที่เกี่ยวกับสารสนเทศ เช่น เครื่องคอมพิวเตอร์ตั้งโต๊ะ (PC Desktop Computer) เครื่องคอมพิวเตอร์พกพา (Notebook) เครื่องพิมพ์ส่วนกลางที่ต้อง Login เพื่อสั่งพิมพ์ (Print on Demand) เครื่องพิมพ์สี ขาวดำ เครื่องสแกนเนอร์ อุปกรณ์เชื่อมต่อ Internet ไร้สาย (WiFi) เป็นต้น

"อุปกรณ์สารสนเทศแบบพกพา" หมายถึง อุปกรณ์สารสนเทศที่สามารถเคลื่อนย้ายหรือพกพาได้ เช่น Notebook, Tablet, Thumb Drive, External Hard Drive เป็นต้น

"เว็บบอร์ด" (Web board) หมายถึง เว็บไซต์ที่มีลักษณะเป็นชุมชนอิเล็กทรอนิกส์ มีการพูดคุย สนทนา แลกเปลี่ยนความคิดเห็นด้วยกระดานสนทนา

"เว็บบล็อก" (Web Blog) หมายถึง การบันทึกบทความของตนเอง ลงบนเว็บไซต์ โดยเนื้อหาของ blog นั้นจะครอบคลุมได้ทุกเรื่อง ไม่ว่าจะเป็นเรื่องส่วนตัว ความคิดเห็นต่อเรื่องต่าง ๆ หรือเป็นบทความเฉพาะด้าน เช่น เรื่องการเมือง เรื่องกล้องถ่ายรูป เรื่องกีฬา เรื่องธุรกิจ เป็นต้น

"เครือข่ายสังคมออนไลน์" (Social Network) หมายถึง ช่องทางการสื่อสาร โดยผ่าน Internet สิ่งที่สื่อสารกันอาจเป็นการรับรู้ข่าวสาร หรือแบ่งปันข้อมูลข่าวสาร ประสบการณ์หรือความคิดเห็นต่อเรื่องราวต่างๆ ซึ่งอาจส่ง

เป็นข้อความ รูปภาพ เสียง คลิปวีดิโอ โดยการใช้งานเทคโนโลยีประเภทสื่อสังคม (Social Media) ที่เป็นที่รู้จัก ได้แก่ Facebook, Twitter, Instagram, Google+, YouTube, LinkedIn เป็นต้น

"ข้อความแชท" (Instant Messaging) หมายถึง ระบบการสื่อสารข้อความสั้นๆ และไฟล์ข้อมูล ในระหว่างเพื่อน หรือกลุ่มคนที่อยู่ใน Internet แบบทันทีทันใด เช่น Facebook Messenger, Instagram, Microsoft Lync, Skype, LINE, WhatsApp เป็นต้น

"ข้อมูลสำคัญของบริษัท" หมายถึง ข้อมูลที่สำคัญต่อการดำเนินธุรกิจ หรือข้อมูลที่เป็นความลับทางการค้า เช่น ข้อมูลลูกค้า ข้อมูลสินค้า สูตรการผลิต ขั้นตอนการปฏิบัติงาน ข้อมูลการเงิน เอกสารสัญญา แผนงานลับที่ยังไม่เปิดเผยต่อสาธารณะ ข้อมูลพนักงาน ข้อมูลส่วนบุคคล นโยบาย เป็นต้น

"ข้อมูลลับ" (Secret) หมายถึง ข้อมูลที่มีความสำคัญต่อบริษัทในระดับสูง หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อบริษัทในระดับสูง เช่น รายชื่อลูกค้า และพันธมิตรทางธุรกิจ ข้อมูลการพัฒนาสินค้าระหว่างการทำวิจัย ข้อมูลบัญชีของบริษัท ข้อมูลเงินเดือน เป็นต้น

"ข้อมูลส่วนบุคคล" (Personal Data) หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม รวมถึงข้อมูลที่นำมารวมกันแล้วสามารถใช้ระบุอัตลักษณ์ของบุคคลได้

"เจ้าของข้อมูลส่วนบุคคล" (Data Subject) หมายถึง บุคคลที่เป็นเจ้าของข้อมูล ซึ่งมีสิทธิขั้นพื้นฐานที่ได้รับความคุ้มครอง

"ผู้กำกับดูแลข้อมูล" (Data Governance) หมายถึง พนักงานในหน่วยงานซึ่งได้รับมอบหมายให้มีอำนาจหน้าที่ในการกำกับดูแลข้อมูลสำคัญของบริษัท รวมถึงข้อมูลส่วนบุคคล ซึ่งมีอำนาจหน้าที่ในการประสานความร่วมมือกับหน่วยงานต่างๆ ที่เกี่ยวข้อง เพื่อกำหนดวัตถุประสงค์ วิธีการในการประมวลผลข้อมูล ตัดสินใจเกี่ยวกับการเก็บรวบรวม การใช้ การเปิดเผยข้อมูล และการลบ/ทำลายข้อมูล อย่างเหมาะสม

"เมทาดาต้า" (Metadata) หมายถึง ข้อมูลที่ใช้อธิบายข้อมูลหลักหรือข้อมูลอื่น เพื่อให้ผู้ใช้งานเข้าใจว่าข้อมูลชุดนี้คือข้อมูลที่เกี่ยวข้องกับอะไร สามารถนำไปใช้งานอย่างไร มีข้อจำกัดอะไร และมีฟิลด์ข้อมูลอะไรบ้าง

"คลังข้อมูล" (Data Warehouse) หมายถึง แหล่งเก็บข้อมูลกลางโดยอาศัยการบูรณาการข้อมูล (Data Integration) เพื่อรวบรวมข้อมูลจากแหล่งต่าง ๆ ข้อมูลที่อยู่ในคลังข้อมูลจะถูกจัดทำให้อยู่ในรูปแบบที่เหมาะสมสำหรับการนำไปวิเคราะห์ข้อมูล ทั้งในรูปแบบของรายงานอัจฉริยะ (Business Intelligence) และดาตาอนาไลติกส์ (Data Analytics)

"ทะเลสาบข้อมูล" (Data Lake) หมายถึง แหล่งเก็บรักษาข้อมูลหลายรูปแบบ โดยที่ข้อมูลเหล่านี้ถูกเก็บรักษาไว้ในรูปแบบที่ใกล้เคียง หรือเหมือนกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ และเป็นที่เก็บรักษาสำรองสำหรับข้อมูลต้นฉบับ

"ฟิชชิ่งเมล์" (Phishing Mail) หมายถึง การปลอมอีเมล์ หรือปลอมหน้าเว็บไซต์ ที่มีข้อความหลอกล่อให้ผู้เสียหาย เปิดเผยรหัสผ่าน หรือ คลิกที่ลิงก์ หรือ เปิดไฟล์เอกสาร หรือ ติดตั้งซอฟแวร์ที่เครื่องคอมพิวเตอร์

"ภัยคุกคามทางด้านไซเบอร์" (Cyber Threats) หมายถึง ภัยคุกคามที่ส่งผลกระทบในทุกภาคส่วน ไม่ว่าจะเป็นการให้บริการระบบเครือข่ายของภาคเอกชน ทางเศรษฐกิจ หรือความมั่นคงของประเทศ เกิดจากการกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

"ไซเบอร์" (Cyber) หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

"Asset Owner" หมายถึง เจ้าของงบประมาณที่ขอซื้อทรัพย์สินถาวรนั้นมาใช้งาน หรือได้รับโอนทรัพย์สินซึ่งมีหน้าที่ดูแลทรัพย์สินที่ใช้นั้น

"IT Asset Controller" หมายถึง หน่วยงานที่เป็นผู้ควบคุม ตรวจสอบ ประสานงาน สำหรับการทำรับทรัพย์สินถาวรใหม่จากผู้ขาย หรือรับโอนจากทรัพย์สินระหว่างก่อสร้างจากโครงการ การโอนย้าย การเลิกใช้งานกับหน่วยงานที่เกี่ยวข้อง ซึ่งดูแลในหมวดคอมพิวเตอร์และอุปกรณ์ และซอฟแวร์

5. อำนาจการอนุมัติและอำนาจการบริหารงาน

5.1 อำนาจในการบริหารงานเทคโนโลยีสารสนเทศให้เป็นไปตามตารางอำนาจที่บริษัทกำหนดในเรื่องที่เกี่ยวข้องกับการบริหารงานเทคโนโลยีสารสนเทศ เพื่อให้ผู้บังคับบัญชาได้ใช้เป็นแนวทางในการบริหารงานเทคโนโลยีสารสนเทศ กับผู้ใต้บังคับบัญชา ให้มีความโปร่งใส ยุติธรรมและเป็นไปตามข้อกำหนดต่างๆ ของบริษัท

5.2 ให้รองกรรมการผู้จัดการใหญ่ ผู้มีหน้าที่กำกับดูแลงานด้านการบริหารงานเทคโนโลยีสารสนเทศ มีอำนาจดำเนินการดังต่อไปนี้

5.2.1 ออกข้อกำหนด ประกาศและคำสั่ง เพื่อกำหนดหลักเกณฑ์ แนวทางบริหารและแนวทางปฏิบัติตามระเบียบนี้ โดยให้คำนึงถึงหลักเกณฑ์และมาตรฐาน ซึ่งเป็นที่ยอมรับและถือปฏิบัติกันในทางธุรกิจด้วย

5.2.2 มอบอำนาจให้พนักงานปฏิบัติงานตามระเบียบนี้แทนได้ ทั้งนี้ การมอบอำนาจดังกล่าวให้คำนึงถึงตำแหน่งหน้าที่และความรับผิดชอบของผู้รับมอบอำนาจด้วย

5.3 ในกรณีที่มีปัญหาเกี่ยวกับการดำเนินการตามระเบียบนี้ ให้กรรมการผู้จัดการใหญ่เป็นผู้วินิจฉัยชี้ขาดและสั่งการ

หมวดที่ 2
ข้อบังคับและการปฏิบัติตามกฎหมาย (Compliance)

6. การปฏิบัติตามกฎระเบียบและข้อบังคับทางกฎหมายที่เกี่ยวข้อง

6.1 พนักงาน บุคคลภายนอก ที่เกี่ยวข้องกับบริษัท ต้องใช้เทคโนโลยีสารสนเทศและการสื่อสารภายใต้กฎระเบียบ ข้อบังคับ กฎหมายที่เกี่ยวข้องทางด้านเทคโนโลยีสารสนเทศ และกฎหมายที่เกี่ยวข้อง รวมถึง

ระเบียบ ข้อกำหนด คำสั่งของบริษัท ที่อาจมีการเปลี่ยนแปลงแก้ไข หรือประกาศใช้เพิ่มเติมทั้งในปัจจุบันและอนาคตอย่างเคร่งครัด

6.2 พนักงาน บุคคลภายนอก ที่เกี่ยวข้องกับบริษัท มีหน้าที่รับผิดชอบในการป้องกันและดูแลให้ระบบสารสนเทศของบริษัท ที่อยู่ในความครอบครองหรือหน้าที่ความรับผิดชอบของตน เพื่อไม่ให้ถูกบุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลโดยมิชอบ และไม่เปิดเผยข้อมูลสำคัญของบริษัทต่อผู้ไม่เกี่ยวข้อง

6.3 พนักงาน บุคคลภายนอก ที่เกี่ยวข้องกับบริษัท ต้องมีวินัยในการใช้ระบบสารสนเทศและอุปกรณ์สื่อสารของบริษัท ไม่ให้ส่งผลกระทบในแง่ลบต่อบริษัทและต่อผู้อื่น เช่น ใช้เป็นเครื่องมือในการเข้าระบบสารสนเทศโดยมิชอบ สร้างความเสียหายต่อชื่อเสียงและทรัพย์สินของบริษัท รบกวน หรือก่อกวนต่อการทำงานของระบบสารสนเทศ ดักข้อมูล ลักลอบถอดรหัสผ่าน ปลอมแปลงข้อมูลคอมพิวเตอร์ เผยแพร่ภาพ ข้อความ หรือเสียงที่ไม่เหมาะสม รวมทั้งไม่ใช้ในเชิงธุรกิจส่วนตัว หรือการกระทำใดๆ ที่ผิดกฎหมาย

7. การปฏิบัติตามลิขสิทธิ์และทรัพย์สินทางปัญญา

7.1 เอกสาร ข้อความ เนื้อหา รูปภาพ หรือซอฟแวร์ของเครื่องคอมพิวเตอร์ ที่มีการใช้งานภายในบริษัทต้องได้มาโดยไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา

7.2 พนักงานต้องไม่ทำการผลิต คัดลอก ดัดแปลง ครอบครอง เผยแพร่ ทำซ้ำ จำหน่าย หรือกระทำการใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือข้อตกลงของเจ้าของสิทธิ หรือทรัพย์สินทางปัญญาโดยเด็ดขาด

7.3 ผู้ใช้งานที่ละเมิดลิขสิทธิ์ซอฟแวร์ของเครื่องคอมพิวเตอร์ หรือลิขสิทธิ์ หรือทรัพย์สินทางปัญญาใดๆ หากมีการฟ้องร้องจากผู้เสียหาย และตรวจสอบพบความผิดฐานละเมิดแล้ว บริษัทถือว่า เป็นความผิดส่วนบุคคล ผู้ใช้งานผู้นั้นต้องรับผิดชอบความเสียหายที่เกิดขึ้นทั้งหมด

8. การกำกับดูแลข้อมูลสำคัญของบริษัท

ข้อมูล (Data and Information) ถือเป็นทรัพย์สินที่สำคัญของบริษัท สามารถผลักดันธุรกิจให้มีศักยภาพในการแข่งขัน จึงควรได้รับการปกป้องไว้ซึ่ง ความถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย รักษาความเป็นส่วนบุคคล ความเชื่อมโยง และเป็นประโยชน์ รวมถึงมีการกำกับดูแลการใช้งาน ในการจัดเก็บ การใช้ การส่งต่อ การตรวจสอบคุณภาพ การลบ การทำลายอย่างเหมาะสม เพื่อป้องกันข้อมูลสูญหาย เสียหาย การเข้าถึง/การเผยแพร่โดยผู้ไม่ได้รับอนุญาต ซึ่งจะส่งผลกระทบกับธุรกิจ ชื่อเสียง ความน่าเชื่อถือของบริษัท เพื่อให้มั่นใจได้ว่าบริษัท ได้ดำเนินการบริหารจัดการข้อมูลอย่างมีความมั่นคงปลอดภัย มีคุณภาพ ดังนั้นผู้กำกับดูแลข้อมูล ร่วมกับทุกหน่วยงาน ต้องกำหนดกระบวนการบริหารจัดการข้อมูลที่ดี ตามแนวทางปฏิบัติสำคัญดังนี้

8.1 การจัดทำบัญชีข้อมูล การจัดกลุ่มข้อมูล (Data Classification) เพื่อให้ผู้ใช้งานได้เข้าใจข้อมูลและนำไปใช้ได้อย่างถูกต้อง เหมาะสม

8.2 การระบุชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ได้แก่

- ข้อมูลทั่วไป-เปิดเผยได้
- ข้อมูลใช้ภายใน-ควรปกปิด
- ข้อมูลลับ-มีการจำกัดการใช้งานหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลลับมาก-มีการจำกัดการใช้งาน หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

8.3 การจัดเก็บข้อมูล และการลบ/ทำลายข้อมูล ให้สอดคล้องกับชั้นความลับของข้อมูลที่กำหนดไว้ การจัดเก็บข้อมูล เป็นไปตามความต้องการและวัตถุประสงค์ในการดำเนินงาน มีการกำหนดสิทธิ์การเข้าถึงข้อมูลและเครื่องมือที่ใช้ในการเข้าถึงข้อมูล เพื่อให้ข้อมูลมีความมั่นคงปลอดภัยและรักษาคุณภาพของข้อมูล

8.4 การจัดการคุณภาพข้อมูล ให้มีความถูกต้อง ครบถ้วน พร้อมใช้ มีความเป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้

8.5 การประมวลผลให้ได้ข้อมูลที่มีประสิทธิภาพ หรือการใช้ข้อมูลให้เกิดประโยชน์ มีการจัดทำเมทาดาต้า (Metadata) สำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล (Data Warehouse) หรือทะเลสาบข้อมูล (Data Lake) เพื่อการวิเคราะห์ข้อมูลที่ซับซ้อน สนับสนุนการตัดสินใจทั้งในระดับปฏิบัติการและระดับบริหาร

8.6 การเปิดเผยข้อมูล โดยห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย นโยบาย คำสั่ง ระเบียบ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม และต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล

9. การรักษาปกป้องข้อมูลส่วนบุคคลของบริษัท

เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนบุคคล (Privacy Right) ที่ต้องได้รับการคุ้มครอง และต้องดำเนินการตามกฎหมายที่เกี่ยวข้อง ให้มีการบริหารจัดการข้อมูลส่วนบุคคลของบริษัท สร้างแนวทางการดำเนินการเกี่ยวกับการรักษาข้อมูลส่วนบุคคลที่ชัดเจนในการนำไปปฏิบัติได้อย่างมีประสิทธิภาพ ด้านการเก็บรวบรวม การใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้มีความมั่นคงปลอดภัย สอดคล้องกับกฎหมายที่เกี่ยวข้อง โดยให้ผู้บริหาร พนักงาน ผู้กำกับดูแลข้อมูล ปฏิบัติดังนี้

9.1 ระบุ กำหนดข้อมูลส่วนบุคคล การจัดแบ่งประเภท และวัตถุประสงค์ความจำเป็นในการเก็บข้อมูลนั้นๆ

9.2 ประเมินความเสี่ยง และวิเคราะห์กระบวนการ และกำหนดมาตรการรักษาข้อมูลส่วนบุคคล

9.3 จัดทำแนวปฏิบัติ การบริหารจัดการข้อมูลส่วนบุคคล ตลอดวงจรชีวิตของข้อมูล ให้สอดคล้องกับกฎหมายที่เกี่ยวข้อง ได้แก่

9.3.1 การเก็บรวบรวมข้อมูลส่วนบุคคล การใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์

9.3.2 การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็น มีการระบุวัตถุประสงค์การใช้อย่างเจาะจง ชัดเจน มีระยะเวลาในการเก็บรักษาข้อมูล และมีการแจ้งให้เจ้าของข้อมูลทราบ

9.3.3 ห้ามมิให้ทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

9.3.4 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

9.3.5 จัดการความยินยอม และกำหนดสิทธิ และวิธีการเข้าถึงข้อมูลส่วนบุคคลอย่างชัดเจน

9.3.6 ปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลในการขอเข้าถึง หรือขอรับสำเนาข้อมูลหรือโอนข้อมูลส่วนบุคคล ที่เกี่ยวกับตนที่ได้ให้ความยินยอมไว้

9.3.7 ปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลในการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ หรือระงับการใช้ข้อมูลส่วนบุคคล

9.3.8 เมื่อมีการว่าจ้างบริษัทภายนอกทำการประมวลผลข้อมูลส่วนบุคคลของบริษัท ต้องมีการคัดเลือกผู้ประมวลผลข้อมูลที่มีการคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูลอย่างเพียงพอตลอดกระบวนการพัฒนาระบบงาน และมีการทำข้อตกลงระหว่างกันอย่างชัดเจนเพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อมิให้บริษัทมีความเสี่ยงที่ข้อมูลส่วนบุคคลจะรั่วไหล

9.3.9 ต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลงแก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

9.3.10 จัดให้มีระบบการตรวจสอบข้อมูลส่วนบุคคลอย่างสม่ำเสมอ และดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น

9.4 สร้างความสำนึกรับผิดชอบ และความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลให้แก่พนักงานอย่างสม่ำเสมอ

9.5 จัดทำ Framework ที่ครอบคลุมนโยบาย แนวทาง โดยอาศัยกระบวนการทางเทคนิค สร้างระบบที่เป็นอัตโนมัติ เพื่อเป็นมาตรฐานให้กับการจัดการข้อมูล นำไปสู่การกำกับดูแลที่มีประสิทธิภาพมากขึ้น

หมวดที่ 3
การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

เพื่อกำหนดมาตรการควบคุมภายในที่ดี มีแนวทางปฏิบัติที่เป็นมาตรฐาน ทำให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย เชื่อถือได้ ป้องกันไม่ให้ระบบถูกบุกรุก ขโมย ทำลาย ที่อาจสร้างความเสียหายต่อบริษัทได้

10. การรักษาความมั่นคงปลอดภัยทางกายภาพของสำนักงาน

10.1 พนักงานต้องติดบัตรพนักงาน และบุคคลภายนอกต้องติดบัตรผู้มาติดต่อไว้ตลอดเวลาที่อยู่ในพื้นที่สำนักงาน ทั้งนี้บัตรพนักงานและบัตรผู้มาติดต่อไม่อนุญาตให้โอนกรรมสิทธิ์ หรือหยิบยืมกันใช้งาน

10.2 พนักงานต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

10.4 ห้ามพนักงานบอกตำแหน่งหรือสถานที่ตั้งของศูนย์คอมพิวเตอร์ให้กับบุคคลภายนอก ยกเว้นกรณีที่มีความจำเป็นในการปฏิบัติงานเท่านั้น

10.5 เจ้าหน้าที่ศูนย์คอมพิวเตอร์เท่านั้นที่มีสิทธิเข้าถึงพื้นที่ศูนย์คอมพิวเตอร์ บุคคลอื่นที่ไม่ใช่เจ้าหน้าที่ศูนย์คอมพิวเตอร์ ต้องผ่านกระบวนการพิจารณาอนุญาตที่เหมาะสมก่อนที่จะมีสิทธิเข้าถึงพื้นที่ศูนย์คอมพิวเตอร์ได้

10.6 เจ้าหน้าที่ศูนย์คอมพิวเตอร์ ต้องจัดทำระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ที่มีการควบคุมอย่างเคร่งครัด

10.7 ห้ามบุคคลภายนอกปฏิบัติงานภายในศูนย์คอมพิวเตอร์โดยลำพัง ต้องมีเจ้าหน้าที่ศูนย์คอมพิวเตอร์หรือเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศที่รับผิดชอบ เฝ้าติดตามการกระทำต่างๆ อย่างใกล้ชิด

10.8 เจ้าหน้าที่ศูนย์คอมพิวเตอร์ ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายคอมพิวเตอร์ หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นได้รับอนุญาตให้ดำเนินการได้

11. การรักษาความมั่นคงปลอดภัยของข้อมูลเทคโนโลยีสารสนเทศ

11.1 บริษัท ครองสิทธิความเป็นเจ้าของข้อมูลทั้งหมดที่ถูกเก็บรักษา หรือส่งผ่านบนระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัทโดยชอบธรรม และสงวนสิทธิในการเข้าถึงข้อมูลโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้าในกรณีที่มีเหตุจำเป็น อนึ่ง บริษัทไม่มีสิทธิในการเป็นเจ้าของข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอก

11.2 ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษในการใช้ข้อมูลประเภทข้อมูลสำคัญ และข้อมูลส่วนบุคคลของบริษัท เพื่อป้องกันการใช้ และการเผยแพร่ข้อมูลที่ไม่ถูกต้อง

11.3 สื่อบันทึกข้อมูลและอุปกรณ์สารสนเทศแบบพกพาที่มีข้อมูลของบริษัทบันทึกอยู่ ต้องได้รับการดูแลรักษา และการใช้อย่างระมัดระวังให้มีความปลอดภัยอย่างเหมาะสม

11.4 ข้อมูลสำคัญที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัททั้งหมด ทั้งที่มีการเก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน หรือเครื่องเซิร์ฟเวอร์ที่ดูแลโดยผู้ใช้งาน ต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหา เช่น การติดไวรัสคอมพิวเตอร์ ฮาร์ดดิสเสีย และควรเก็บรักษาสื่อบันทึกข้อมูลสำรอง ไว้ในสถานที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

11.5 ข้อมูลที่ถูกแสดงบนระบบที่เปิดเผยสู่สาธารณะ เช่น เว็บไซต์ของบริษัท, Social Network ของบริษัท ต้องได้รับการตรวจสอบความถูกต้อง และความเหมาะสมจากผู้มีอำนาจ ก่อนที่จะดำเนินการประกาศ (Publish) บนระบบที่เปิดเผยสู่สาธารณะ

11.6 เจ้าของข้อมูลมีหน้าที่ในการพิจารณาอนุมัติสิทธิในการเข้าใช้ข้อมูลนั้นๆ

11.7 การเข้าถึงฐานข้อมูลของระบบใช้งานจริง (Production) ต้องดำเนินการผ่านแอพลิเคชั่นเท่านั้น ยกเว้นผู้มีหน้าที่ดูแลรักษาระบบฐานข้อมูล

11.8 กรณีผู้ใช้งานต้องการขอใช้ข้อมูลสำรองที่เก็บไว้ เพื่อทำการกู้ข้อมูลหรือต้องการใช้ข้อมูลย้อนหลัง ต้องได้รับการอนุมัติจากเจ้าของข้อมูลทุกครั้ง

12. การรักษาความมั่นคงปลอดภัยของเครือข่ายคอมพิวเตอร์

12.1 ผู้ใช้งานต้องเชื่อมต่อคอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา กับเครือข่ายของบริษัทที่มีระบบรักษาความปลอดภัยที่จัดสรรไว้ให้เท่านั้น เช่น Proxy, Firewall

12.2 ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ จากภายนอกเข้ากับระบบเครือข่ายของบริษัทโดยเด็ดขาด หากจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

12.3 ห้ามพนักงานเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท หรือของผู้อื่นที่ตนไม่ได้รับอนุญาตให้ใช้งาน เพื่อแอบดักข้อมูลบนเครือข่าย หรือ ทำลาย แก้ไข เพิ่มเติมข้อมูลสารสนเทศ

12.4 ห้ามพนักงานเปิดเผยข้อมูลที่เกี่ยวข้องกับมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ และเครือข่ายขององค์กรให้แก่บุคคลภายนอก และพนักงานที่ไม่เกี่ยวข้อง เช่น วิธีการเข้าถึงรหัสผ่าน

12.5 ห้ามพนักงานทำให้ระบบคอมพิวเตอร์ขององค์กรหรือของผู้อื่น ถูกชะลอ ขัดขวาง ระงับ หรือรบกวนจนไม่สามารถทำงานตามปกติได้

12.6 ผู้ใช้งานที่ได้รับอนุญาตตามความจำเป็นให้เข้าถึงเครือข่ายของบริษัทจากระยะไกล ต้องมีการใช้งานอย่างระมัดระวัง มิให้บุคคลภายนอกร่วมใช้งาน และไม่เข้าถึงเครือข่ายโดยใช้เครื่องคอมพิวเตอร์สาธารณะ

12.7 หน่วยงานใดที่มีความจำเป็นต้องให้บุคคลภายนอก เข้าใช้ระบบคอมพิวเตอร์ และระบบเครือข่ายของบริษัท ต้องถือปฏิบัติดังนี้

12.7.1 บุคคลภายนอก ต้องปฏิบัติตามข้อตกลงตามนโยบายเกี่ยวกับการรักษาความมั่นคงความปลอดภัยของเครือข่ายคอมพิวเตอร์

12.7.2 หน่วยงานที่ดูแลบุคคลภายนอกต้องขอสิทธิในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ โดยอย่างน้อยต้องระบุชื่อนิติบุคคล ชื่อ-นามสกุลของบุคคล เหตุผลความจำเป็น ระยะเวลาการใช้งาน เลขที่บัตรประจำตัวประชาชน

12.7.3 หน่วยงานที่ดูแลบุคคลภายนอก ต้องควบคุมการใช้งาน รับผิดชอบต่อความเสียหายที่เกิดขึ้น และแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีที่เลิกการปฏิบัติงานก่อนกำหนด

12.8 บริษัทมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานให้ทราบล่วงหน้า

13. การรักษาความมั่นคงปลอดภัยของอุปกรณ์สารสนเทศ

13.1 ผู้ใช้งานสามารถนำอุปกรณ์สารสนเทศและสื่อบันทึกข้อมูล ที่จำเป็นต่อการปฏิบัติงานเข้าใช้งานในสถานที่ทำงานของบริษัทได้ โดยต้องมีการตรวจสอบให้มั่นใจว่าไม่มีไวรัสและโปรแกรมมุ่งร้ายก่อนนำเข้าใช้งาน

13.2 ห้ามใช้อุปกรณ์สารสนเทศของบริษัท ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือทำการรบกวนก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม ความมั่นคงของประเทศหรือกระทบต่อภารกิจของบริษัท

13.3 กรณีพนักงานนำอุปกรณ์สารสนเทศหรือสื่อบันทึกข้อมูลส่วนบุคคล ที่ไม่ใช่อุปกรณ์ของบริษัท หรือที่บริษัทจัดหาให้เข้าใช้งานในบริษัท จะไม่ได้รับการสนับสนุนและแก้ไขปัญหาจากฝ่ายเทคโนโลยีสารสนเทศ

13.4 เครื่องคอมพิวเตอร์ของพนักงานที่พ้นสภาพการเป็นพนักงานบริษัท ต้องถูกแยกออกจากระบบเครือข่ายทั้งภายในและภายนอกโดยทันที และก่อนนำกลับมาใช้ใหม่ ต้องมีการสำรองข้อมูลจากฮาร์ดดิสก์ (Hard disk) เสียก่อน แล้วจึงทำการฟอร์แมท (Format) เครื่องคอมพิวเตอร์นั้น เพื่อป้องกันการแพร่กระจายของซอฟแวร์มุ่งร้ายที่มีอยู่ในเครื่อง และเพื่อกำจัดซอฟแวร์ที่ไม่ได้รับอนุญาตซึ่งอาจถูกติดตั้งไว้ในเครื่อง

14. การป้องกันไวรัสและโปรแกรมมุ่งร้าย

14.1 เครื่องเซิร์ฟเวอร์และเครื่องคอมพิวเตอร์ของพนักงาน ที่เชื่อมต่อกับระบบเครือข่ายของบริษัททุกเครื่อง ต้องได้รับการติดตั้งซอฟแวร์ป้องกันไวรัส (Anti-Virus) และโปรแกรมมุ่งร้าย (Malware) ที่มีประสิทธิภาพ และต้องได้รับการปรับปรุง (Update) ให้เป็นปัจจุบันอยู่เสมอโดยฝ่ายเทคโนโลยีสารสนเทศ

14.2 พนักงานต้องไม่ปรับแต่งหรือยกเลิกการทำงานของซอฟแวร์ป้องกันไวรัส ที่ติดตั้งในเครื่องคอมพิวเตอร์ของตน

14.3 ห้ามพนักงานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใดๆ เช่น ไวรัส หนอนอินเตอร์เน็ท ม้าโทรจัน เป็นต้น เข้าสู่ระบบเทคโนโลยีสารสนเทศของบริษัทโดยเด็ดขาด

14.4 พนักงานควรตรวจสอบหาไวรัสจากสื่อบันทึกข้อมูลต่างๆ เช่น Thumb Drive, External Hard Drive, Data storage ต่างๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของบริษัท

14.5 หากพนักงานสงสัยว่า เครื่องคอมพิวเตอร์ของตนติดไวรัสหรือได้รับการแจ้งเตือนจากซอฟแวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ถูกโจมตี พนักงานต้องหยุดการทำงานทั้งหมด และแจ้งเหตุต่อ ICT Service Desk ทันที

15. การใช้งานรหัสผ่านอย่างปลอดภัย

15.1 ผู้ใช้งานแต่ละคนต้องได้รับรหัสผู้ใช้งาน (User ID) และรหัสผ่าน (Password) เพื่อใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท ตามความจำเป็นในหน้าที่การทำงานที่รับผิดชอบ

15.2 การตั้งรหัสผ่าน ควรตั้งให้มีความยากแก่การคาดเดา แต่ตนเองจำได้ง่าย โดยมีหลักเกณฑ์ดังนี้

15.2.1 รหัสผ่านมีความยาว อย่างน้อย 8 ตัวอักษร

15.2.2 ประกอบด้วยอักษรอย่างน้อย 3 ชนิด จาก 4 ชนิด ดังนี้

- ตัวอักษรใหญ่ (A-Z)
- ตัวอักษรเล็ก (a-z)
- ตัวเลข (0-9)
- ตัวอักขระพิเศษ (~ ! $ % ^ & * ( ) _ = , . / : [ ] " < > { } \ | -)
  โดยห้ามใช้อักขระ เว้นวรรค @ ? ' + :

15.2.3 รหัสผ่านที่ตั้งใหม่ อย่างน้อย 1 วัน จึงจะสามารถเปลี่ยนรหัสผ่านได้อีกครั้ง

15.2.4 รหัสผ่าน จะตั้งซ้ำกับของเดิมที่เคยถูกตั้งมาแล้วล่าสุด 5 ครั้งไม่ได้

15.3 การตั้งรหัสผ่านที่ปลอดภัย เดาได้ยากนั้น ไม่ควรใช้ชื่อจริง ชื่อเล่น วันเดือนปีเกิด โทรศัพท์ หมายเลขบัตรประชาชน ชื่อคนในครอบครัว คำที่มีในพจนานุกรม หรือ รหัสผ่านที่ง่ายเกินไป เช่น 1234 เป็นต้น

15.4 ผู้ใช้งานต้องเปลี่ยนรหัสผ่านที่เข้าถึงเครือข่ายเป็นประจำทุก 90 วัน หรือตามระยะเวลาการเปลี่ยนรหัสผ่านตามที่บริษัทกำหนด

15.5 การขอ Reset รหัสผ่านโดยผู้ใช้งาน ต้องแสดงตัวตนและสิทธิความเป็นเจ้าของรหัสผู้ใช้งานนั้นๆ เจ้าหน้าที่ที่ดำเนินการมีสิทธิในการขอข้อมูลและพิสูจน์ตัวตนของผู้ใช้งานตามความเหมาะสม

15.6 ผู้ใช้งานต้องรับผิดชอบไม่เปิดเผยรหัสผู้ใช้งานและรหัสผ่านแก่ผู้อื่น รวมถึงสมาชิกในครอบครัวโดยเด็ดขาด ยกเว้นกรณีที่ได้รับอนุญาตจากผู้บังคับบัญชาให้มีการใช้รหัสผ่านร่วมกัน ผู้ใช้รหัสผ่านร่วมกันต้องเก็บรักษารหัสผ่านไว้เป็นความลับเฉพาะกลุ่ม และต้องร่วมกันรับผิดชอบต่อการกระทำที่ทำให้เกิดความเสียหายนั้นทั้งหมด

15.7 ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นที่ไม่มีส่วนเกี่ยวข้องกับการใช้งานของรหัสผู้ใช้งาน เข้ากระทำการใดแทนตนโดยเด็ดขาด

15.8 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่กระทำผ่านรหัสผู้ใช้งานและรหัสผ่านทั้งหมด

15.9 ในกรณีที่มีความจำเป็นต้องใช้รหัสผู้ใช้งานที่มีสิทธิพิเศษหรือสิทธิสูงสุด ต้องมีการควบคุมการใช้งานอย่างรัดกุม และได้รับความเห็นชอบในการใช้งานจากผู้มีอำนาจหน้าที่ มีการกำหนดระยะเวลาการใช้งาน พร้อมทั้งระงับการใช้งาน และต้องเปลี่ยนรหัสผ่านทันทีเมื่อพ้นระยะเวลาดังกล่าว

15.10 หากผู้ใช้งานสงสัยว่ารหัสผ่านของตนถูกล่วงละเมิด ให้ดำเนินการเปลี่ยนรหัสผ่านของตนทั้งหมดทันที

หมวดที่ 4
การจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

เพื่อกำหนดมาตรฐานการใช้ทรัพย์สินด้านเทคโนโลยีสารสนเทศ ช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ทรัพย์สินด้านเทคโนโลยีสารสนเทศ และผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพย์สินและข้อมูลที่มีค่าขององค์กร ให้มีความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

16. การจัดสรรเครื่องคอมพิวเตอร์/อุปกรณ์สารสนเทศ

16.1 บริษัทจะจัดสรรเครื่องคอมพิวเตอร์ที่มีคุณสมบัติเหมาะสมเพียงพอต่อการทำงาน และเกิดประโยชน์สูงสุดให้แก่พนักงานของบริษัท ตามหน้าที่และความจำเป็นในการใช้งาน ทั้งนี้จำกัดคนละไม่เกิน 1 เครื่อง

16.2 บริษัทจะไม่พิจารณาอนุมัติการขอใช้อุปกรณ์สารสนเทศแก่บุคคลภายนอก ที่ทำงานให้แก่บริษัท

16.3 พนักงานที่มีสิทธิใช้เครื่องคอมพิวเตอร์พกพา ต้องมีลักษณะงานไม่ประจำที่ หรือปฏิบัตงานนอกสำนักงานอยู่เป็นประจำในงานที่มีความสำคัญ เช่น การตรวจสอบ การอนุมัติ ที่ต้องรีบดำเนินการทันที เพื่อมิให้กระทบต่อการดำเนินการธุรกิจ

16.4 การขอเปลี่ยนการใช้คอมพิวเตอร์ตั้งโต๊ะเป็นคอมพิวเตอร์พกพา สามารถเปลี่ยนได้เมื่อหมดระยะเวลาการเช่าแต่ละงวดเท่านั้น ทั้งนี้ ต้องได้รับอนุมัติงบประมาณในการจัดหา พร้อมทั้งต้องผ่านการพิจารณาอนุมัติถึงลักษณะงานตามความจำเป็นข้อ 16.3

16.5 เครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศที่เกี่ยวข้องทั้งหมดที่บริษัทเป็นผู้จัดหา มีวัตถุประสงค์ เพื่อให้ใช้ในการดำเนินงานของบริษัทเท่านั้น

16.6 ผู้ใช้งานมีหน้าที่ดูแลรักษาเครื่องคอมพิวเตอร์ที่บริษัทจัดหาให้ใช้งานอย่างระมัดระวังมิให้เกิดความเสียหายหรือสูญหายแต่อย่างใด หากเครื่องคอมพิวเตอร์สูญหาย เสียหาย เนื่องจากเจนตนา หรือความประมาทเลินเล่อของผู้ใช้งาน ผู้ใช้งานต้องเป็นผู้รับผิดชอบค่าใช้จ่ายในความเสียหายนั้น

17. สิทธิการขอใช้อุปกรณ์สารสนเทศ

17.1 พนักงานมีสิทธิขอใช้อุปกรณ์สารสนเทศได้ตามหน้าที่และความจำเป็น เพื่อการปฏิบัติงานได้ตามหลักเกณฑ์ที่บริษัทกำหนด ดังนี้

	ITEM	CEO/SEVP PG 16 up	MD/EVP/VP/ Expertise PG 13-15	DM/Specialist PG 11-12	SM Down PG 1-10
1	PC Desktop Computer	PC and/or NB	PC or NB ขอใช้ตามความจำเป็นในการทำงาน		
2	Notebook Computer				
3	Shared Printer	ใช้ Print on Demand			
4	Air Card	ขอใช้ตามความจำเป็นในการทำงาน			
5	Mail box	ไม่เกิน 5 GB		ไม่เกิน 4 GB	PG 9 - 10 ไม่เกิน 4 GB PG 6 - 8 ไม่เกิน 3 GB PG 1 – 5 ไม่เกิน 2 GB
6	Internet	ได้สิทธิการใช้อัตโนมัติ		ขอใช้ตามความจำเป็นในการทำงาน	
7	VPN	ขอใช้ตามความจำเป็นในการทำงาน			
8	WiFi	ขอใช้ตามความจำเป็นในการทำงาน			

17.2 การขอใช้อุปกรณ์สารสนเทศให้ดำเนินการขอใช้ในระบบ ICT Service Desk

18. อำนาจอนุมัติการขอใช้อุปกรณ์สารสนเทศ

18.1 ให้ผู้บังคับบัญชาผู้มีอำนาจในการอนุมัติ พิจารณาตามข้อ 16 การจัดสรรเครื่องคอมพิวเตอร์/อุปกรณ์สารสนเทศตามความรับผิดชอบอย่างเหมาะสม

	รายการ/ผู้ขอใช้	CEO/SEVP PG 16 up	MD/EVP/VP/ Expertise PG 13-15	DM/Specialist PG 11-12	SM Down PG 1-10
1	PC Desktop Computer	-	-	VP อนุมัติ	VP อนุมัติ และได้รับอนุมัติงบประมาณ
2	Notebook Computer				กรณีใช้ NB แทน PC VP อนุมัติ และได้รับอนุมัติงบประมาณ
3	Air Card	-	EVP ขึ้นไป อนุมัติ	VP อนุมัติ	
4	Mail box	-			
5	Internet	-			SM อนุมัติ
6	VPN	-			SM อนุมัติ
7	WiFi	-			SM อนุมัติ

<u>หมายเหตุ</u> : บริษัทในเครือใดที่ไม่มีระดับ VP ให้ระดับ MD เป็นผู้มีอำนาจอนุมัติ

19. การกำหนดผู้ดูแลรับผิดชอบทรัพย์สินอุปกรณ์สารสนเทศ

19.1 ทรัพย์สินหมวดอุปกรณ์สารสนเทศและซอฟแวร์ ทุกชิ้นของบริษัท ต้องได้รับการกำหนดตัวบุคคล หน่วยงาน หรือผู้รับผิดชอบดูแลทรัพย์สินอย่างชัดเจน เพื่อให้มั่นใจได้ว่าทรัพย์สินได้รับการดูแลและควบคุมการใช้งานอย่างเหมาะสม

19.2 ให้ Asset Owner มีหน้าที่รับผิดชอบดูแล ควบคุมการใช้งานทรัพย์สิน ดังนี้

19.2.1 กำหนดตัวบุคคล ผู้ครอบครองทรัพย์สิน พร้อมรูปภาพทรัพย์สินที่ติดฉลากรหัสทรัพย์สินอย่างชัดเจนในระบบงาน

19.2.2 ตรวจสอบความถูกต้อง สมบูรณ์ของทรัพย์สินที่ได้รับมาจากการซื้อ หรือรับโอน

19.2.3 ตรวจสอบสภาพการติดตั้ง การใช้งาน การบำรุงรักษา ซ่อมแซม จัดเก็บ เพื่อให้อยู่ในสภาพที่พร้อมใช้งานได้เป็นปกติ และมีความปลอดภัยตลอดเวลา

19.2.4 หากพบทรัพย์สินชำรุด ไม่คุ้มค่ากับค่าซ่อมแซม ให้สร้างคำขอตัดจำหน่ายกรณีชำรุด ในระบบ Asset Management System และนำทรัพย์สินที่ชำรุดส่งคืน IT Asset Controller

19.2.5 หากพบทรัพย์สินสูญหาย ให้สร้างคำขอตัดจำหน่ายกรณีสูญหาย ในระบบ Asset Management System ซึ่ง Asset Owner ต้องเป็นผู้รับผิดชอบค่าใช้จ่ายในทรัพย์สินนั้น

19.2.6 เมื่อ Asset Owner มีการโยกย้ายงาน หรือเปลี่ยน Cost Center ต้องประสานงานเพื่อทำการโอนย้ายทรัพย์สินของตนไปยังบุคคลอื่นให้ถูกต้อง

20. การใช้งานเครื่องคอมพิวเตอร์ตั้งโต๊ะ (PC Desktop Computer)

20.1 ผู้ใช้งานต้องปิดเครื่องคอมพิวเตอร์ ถอดปลั๊กไฟออกเมื่อเลิกใช้งาน และต้อง Log off หน้าจอคอมพิวเตอร์ทุกครั้ง เมื่อไม่ได้ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์นานเกิน 20 นาที

20.2 บริษัทขอสงวนสิทธิ์ที่จะควบคุมระบบคอมพิวเตอร์ให้เกิดความมั่นคงปลอดภัย โดยไม่อนุญาตให้ผู้ใช้งานแก้ไขเปลี่ยนแปลงค่าพารามิเตอร์ต่าง ๆ ของเครื่อง เช่น Computer Name, System Configuration, Program Configuration เป็นต้น

20.3 ผู้ใช้งานต้องศึกษาการใช้เครื่องคอมพิวเตอร์ตั้งโต๊ะที่ถูกต้อง และมีหน้าที่รับผิดชอบดูแลให้อยู่ในสภาพที่ใช้งานได้ดี ในกรณีที่อุปกรณ์คอมพิวเตอร์เสียหายจากการใช้งานที่ไม่ถูกต้อง ผู้ใช้งานต้องรับผิดชอบต่อทรัพย์สินดังกล่าว

20.4 อุปกรณ์คอมพิวเตอร์ของบริษัทต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใดๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้นๆ และพนักงานต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ บนเครื่องคอมพิวเตอร์ขององค์กรอย่างเด็ดขาด

21. การใช้งานเครื่องคอมพิวเตอร์พกพา (Notebook Computer)

21.1 เครื่องคอมพิวเตอร์พกพา เป็นทรัพย์สินของบริษัทที่อนุญาตให้พนักงานยืมไปใช้เพื่องานของบริษัทในสถานที่ต่างๆ จึงเกิดความเสี่ยงในเรื่องการรั่วไหลของข้อมูลสำคัญหรือเครื่องสูญหาย ดังนั้นพนักงานพึงตระหนักในหน้าที่ความรับผิดชอบ ปฏิบัติตามการใช้งานเครื่องคอมพิวเตอร์พกพาอย่างเคร่งครัด

21.2 ผู้ใช้งานต้องระวังรักษาเครื่องคอมพิวเตอร์พกพาให้ปลอดภัยจากโจรกรรม หากเกิดการ สูญหาย ผู้ใช้งานต้องรับผิดชอบต่อทรัพย์สินดังกล่าว

21.3 ไม่ควรใส่เครื่องคอมพิวเตอร์พกพาไปในกระเป๋าเดินทางที่เสียงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

21.4 การใช้เครื่องคอมพิวเตอร์พกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

21.5 ผู้ใช้งานควรมีการ Log off หน้าจอคอมพิวเตอร์ทุกครั้งเมื่อไม่ได้ใช้งานนานเกิน 20 นาที

21.6 ผู้ใช้งานต้องศึกษาการใช้เครื่องคอมพิวเตอร์พกพาอย่างถูกต้อง และมีหน้าที่รับผิดชอบดูแลให้อยู่ในสภาพที่ใช้งานได้ดี ในกรณีที่อุปกรณ์คอมพิวเตอร์เสียหายจากการใช้งานที่ไม่ถูกต้อง ผู้ใช้งานต้องรับผิดชอบต่อทรัพย์สินดังกล่าว

22. การใช้งานเครื่องพิมพ์

22.1 เมื่อผู้ใช้งานสั่งพิมพ์งานทุกครั้ง ให้ตระหนักถึงความจำเป็นในการพิมพ์งานสี และให้ตรวจสอบการตั้งค่าการพิมพ์ให้ถูกต้องก่อนการสั่งพิมพ์ทุกครั้ง

22.2 หากผู้ใช้งานกำลังใช้เครื่องพิมพ์อยู่นั้น เกิดปัญหากระดาษติดขัด หรือทำงานผิดปกติ ผู้ใช้งานต้องไม่ทิ้งอุปกรณ์นั้นไว้โดยลำพังจนกว่าจะลบ หรือกำจัดข้อมูลสำคัญออกจากเครื่องพิมพ์

22.3 ผู้ใช้งานต้องตรวจสอบกระดาษที่นำกลับมาใช้งานซ้ำให้ละเอียดว่า ไม่มีข้อมูลที่เป็นความลับติดอยู่กระดาษนั้น หากมีข้อมูลที่เป็นความลับให้ทำลายทิ้งทันที

23. การใช้ซอฟแวร์ของเครื่องคอมพิวเตอร์ (Software)

23.1 บริษัทอนุญาตให้ใช้ซอฟแวร์ ที่บริษัทมีลิขสิทธิ์หรือซอฟแวร์ที่ไม่ต้องเสียค่าใช้จ่าย (Freeware) ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้ง หรือใช้งานซอฟแวร์อื่นใดที่ละเมิดลิขสิทธิ์ หากมีการตรวจสอบพบความผิด บริษัทถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

23.2 ซอฟแวร์ที่บริษัทจัดเตรียมไว้ให้ผู้ใช้งานเป็นทรัพย์สินของบริษัท เป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

23.3 ห้ามไม่ให้ผู้ใช้งานทำการติดตั้ง หรือใช้งานซอฟแวร์อื่นใดนอกเหนือจากที่บริษัทกำหนด

24. การใช้งานอินเตอร์เน็ท (Internet)

24.1 บริษัทจัดหาบริการอินเตอร์เน็ทไว้เพื่ออำนวยความสะดวกแก่พนักงานในการทำวิจัย การค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก ลูกค้า คู่ค้า เพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของบริษัท

24.2 ผู้ใช้งานต้องใช้อินเตอร์เน็ทด้วยความระมัดระวัง ไม่ทำให้บริษัทและบุคคลที่เกี่ยวข้องกับบริษัทได้รับความเสียหาย เสื่อมเสียชื่อเสียง หรือการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเตอร์เน็ทในทางที่ผิด ถือเป็นความผิดทางวินัยและอาจถูกดำเนินคดีตามกฎหมาย

24.3 ผู้ใช้งานต้องไม่เข้าใช้อินเตอร์เน็ทในเว็บไซต์ที่มีความเสี่ยงต่อการติดไวรัส เช่น เว็บไซต์การพนัน ลามกอนาจาร และไม่ดาว์นโหลด (Download) ข้อมูลที่มีขนาดใหญ่ หรือโปรแกรมที่ไม่มีประโยชน์ต่อการทำงาน เช่น เกมส์ เพลง ภาพยนตร์ Hacking Tool, Cracking Tool, Exploit Tool, Peer to Peer Software

24.4 ห้ามผู้ใช้งานเผยแพร่ข้อมูล หรือกระทำการอื่นใดอันก่อให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ

24.5 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญ เช่น ข้อมูลลับทางการค้า สูตรการประดิษฐ์คิดค้นต่างๆ ข้อมูลความลับของหน่วยงาน ข้อมูลเกี่ยวกับผู้ร่วมทุนผ่านระบบอินเตอร์เน็ท นอกจากหน่วยงานที่บริษัทกำหนดให้เป็นผู้ให้ข้อมูลแก่สาธารณะชน ได้แก่ สำนักกรรมการผู้จัดการใหญ่ หน่วยงานสื่อสารองค์กร และหน่วยงานนักลงทุนสัมพันธ์

24.6 บริษัทขอสงวนสิทธิที่จะปิดการเข้าถึงอินทราเน็ท อินเตอร์เน็ท ของเว็บไซต์ที่ไม่เหมาะสม

24.7 การโพสต์ข้อความในเว็บบอร์ด (Web board) หรือเว็บบล็อก (Web Blog)

24.7.1 ให้ผู้ใช้งานตั้งคำถาม หรือแสดงความคิดเห็น แลกเปลี่ยนความรู้ ประสบการณ์ ในแง่มุมต่างๆ เชิงสร้างสรรค์

24.7.2 ห้ามมิให้ผู้ใช้งานตั้งคำถาม หรือแสดงความคิดเห็นที่เกี่ยวข้อง พาดพิง กระทบต่อสถาบันชาติ ศาสนา และพระมหากษัตริย์ ในทางที่เสื่อมเสีย

24.7.3 ห้ามมิให้ผู้ใช้งานตั้งคำถามหรือแสดงความคิดเห็น อันจะก่อให้เกิดความขัดแย้ง หรือโจมตี ปรักปรำ ให้บุคคล องค์กร สถาบัน หรือสังคมใด เสื่อมเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง ได้รับความอับอาย และได้รับความเดือดร้อน

24.7.4 ห้ามมิให้ผู้ใช้งานเผยแพร่ข้อความ เนื้อหา รูปภาพ เสียง คลิปวีดิโอ ในทางลามกอนาจาร ก้าวร้าว หยาบคาย หรือการเผยแพร่สิ่งที่ละเมิดลิขสิทธิ์

24.7.5 ผู้ใช้งานต้องไม่แอบอ้างชื่อบริษัท โพสต์ข้อความใดๆ ในเว็บบอร์ดสาธารณะ

24.8 การสื่อสารในเครือข่ายสังคมออนไลน์ (Social Network)

24.8.1 พนักงานต้องไม่ใช้ชื่อผู้ใช้ (User Name) / ชื่อบัญชีผู้ใช้อีเมล์ (e-mail Account) และรหัสผ่าน (Password) ซ้ำกับชื่อผู้ใช้ / ชื่อบัญชีผู้ใช้อีเมล์ และรหัสผ่านของบริษัท ในการลงทะเบียนใช้งานในเครือข่ายสังคมออนไลน์

24.8.2 พนักงานไม่ควรแสดงข้อมูลสำคัญส่วนตัว ที่สามารถเข้าถึงความเป็นตัวตนมากเกินไป เช่น วันเดือนปีเกิด ที่อยู่ที่บ้าน ที่ทำงาน ชื่อบุตรหลาน รูปภาพคนในครอบครัว กิจกรรมที่ทำเป็นประจำ

24.8.3 พนักงานควรตั้งค่าระดับการรักษาความปลอดภัยให้สูง เพื่อจำกัดสิทธิผู้ที่จะเข้าถึงข้อมูลส่วนตัว รูปส่วนตัว ข้อคิดเห็น ความสนใจ ได้เฉพาะกลุ่มเพื่อนที่รู้จักและไว้ใจได้เท่านั้น

24.8.4 พนักงานต้องไม่นำเรื่องเกี่ยวกับการทำงาน ข้อมูลสำคัญของบริษัท ความลับทางการค้า ข้อมูลทางการเงิน ไปเผยแพร่ไว้ใน Social Network อันจะทำให้เกิดความเสียหายแก่บริษัทและภาพลักษณ์ขององค์กร

24.8.5 พนักงานควรหลีกเลี่ยงการแสดงความคิดเห็นในประเด็นที่อ่อนไหว หรือส่งผลกระทบต่อสังคม อันอาจนำไปสู่ข้อพิพาทได้ เช่น เรื่องการเมือง ศาสนา เรื่องประเด็นทางกฎหมาย หรือเกี่ยวข้องกับคู่กรณีที่บริษัทกำลังดำเนินการฟ้องร้องอยู่

24.8.6 พนักงานต้องไม่ใช้เครือข่ายสังคมออนไลน์ในลักษณะที่หยาบคาย ก้าวร้าว กล่าวโทษให้ผู้อื่นเกิดความเสียหาย หรือละเมิดต่อสิทธิของผู้อื่น ขัดต่อศีลธรรมอันดี ขัดต่อรัฐธรรมนูญ หรือผิดต่อกฎหมาย

24.8.7 พนักงานควรตะหนักในการใช้ประโยชน์จากเครือข่ายสังคมออนไลน์อย่างสร้างสรรค์ถูกต้อง โดยการใช้เป็นเครื่องมือในการติดต่อสื่อสาร ประชาสัมพันธ์ แลกเปลี่ยนความรู้ เรียนรู้ และต่อยอดความคิดสร้างสรรค์ การชี้แจงข่าวสารที่เป็นจริง ไม่ใช้ในเรื่องส่วนตัวหรือเล่นเกมส์ในเวลาทำงาน

24.8.8 พนักงานจะต้องรับผิดชอบต่อข้อความ รูปภาพ เสียง คลิปวีดีโอ Link หรือสิ่งใดๆ ที่นำไปเผยแพร่ในเครือข่ายสังคมออนไลน์ทั้งหมด

24.8.9 บริษัทสงวนสิทธิ์ในการเฝ้าระวัง หรือจำกัดการใช้งานเครือข่ายสังคมออนไลน์ผ่านระบบเครือข่ายของบริษัท

25. การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

25.1 พนักงานผู้มีสิทธิใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท จะได้รับรายชื่อผู้ใช้งาน (e-mail account) เป็นของตนเอง

25.2 หน่วยงานใดที่มีความจำเป็นต้องให้บุคคลภายนอก ใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท ต้องถือปฏิบัติดังนี้

25.2.1 บุคคลภายนอกต้องปฏิบัติตามข้อตกลง ตามนโยบายการใช้งานจดหมายอิเล็กทรอนิกส์

25.2.2 หน่วยงานที่ดูแลบุคคลภายนอกต้องขอสิทธิในการใช้งานจดหมายอิเล็กทรอนิกส์ อย่างน้อยต้องระบุชื่อนิติบุคคล ชื่อ-นามสกุลของบุคคล เหตุผลความจำเป็น ระยะเวลาการใช้งาน เลขที่บัตรประจำตัวประชาชน

25.2.3 หน่วยงานที่ดูแลบุคคลภายนอก ต้องควบคุมการใช้งาน รับผิดชอบต่อความเสียหายที่เกิดขึ้น และแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีที่เลิกการปฏิบัติงานก่อนกำหนด

25.3 ผู้ดูแลระบบสามารถสร้างรายชื่อผู้ใช้งาน (e-mail Account) กลุ่มที่มีวัตถุประสงค์พิเศษ หรือเป็นรายชื่อผู้ใช้งานกลางของหน่วยงาน เช่น helpdesk@irpc.co.th, hrcommunication@irpc.co.th โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้เป็นเจ้าของ รับผิดชอบรายชื่อผู้ใช้งานนั้น

25.4 รายชื่อผู้ใช้งานทั้งหมด และ e-mail ทุกฉบับ (รวมถึง e-mail ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ของบริษัท ถือเป็นทรัพย์สินของบริษัท ดังนั้นห้ามใช้ e-mail account ของบริษัทประกาศข้อมูลใดๆ บนอินเตอร์เน็ท เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้อง หรือเป็นส่วนหนึ่งของการทำงานให้กับบริษัท และห้ามใช้ e-mail account ของบริษัทกระทำการใดๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย

25.5 ผู้ใช้งานต้องมีการส่งต่อข้อมูลข่าวสารทาง e-mail อย่างระมัดระวังเสมอ ไม่ส่งต่อข้อมูล หรือเปิดเผยข้อมูลความลับขององค์กรให้ผู้ที่ไม่เกี่ยวข้องทราบ

25.6 ผู้ใช้งานต้องมีความตระหนักต่อฟิชชิ่งเมล์ ระมัดระวัง e-mail ที่ส่งมาจากคนที่ไม่รู้จัก ไม่เปิดไฟล์แนบหรือคลิกลิงก์ใน e-mail ที่น่าสงสัย มีการตรวจทาน e-mail Account ก่อนส่งให้มั่นใจว่าไม่ส่งถึงผู้รับผิดคน มีการใส่รหัสผ่านในไฟล์ข้อมูลลับที่แนบก่อนส่ง

25.7 ผู้ใช้งานไม่ควรให้บุคคลอื่นทำการส่ง e-mail โดยใช้ e-mail Account ของตน ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม

25.8 ห้ามผู้ใช้งานส่ง e-mail ที่มีลักษณะเป็นจดหมายขยะ (Junk Mail) หรือโฆษณาสินค้าต่างๆ (Spam Mail) หรือจดหมายลูกโซ่ อันไม่พึงประสงค์ต่อผู้รับ หรือมีลักษณะเป็นการรบกวนการใช้งานของบุคคลอื่น หรือปลอม ปกปิดชื่อที่อยู่ e-mail ของตน ส่งไปยังผู้อื่น

25.9 ห้ามผู้ใช้งานเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ที่มีลักษณะลามกอนาจาร หรือเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา ไปยังผู้อื่น

25.10 ผู้ใช้งานต้องไม่ส่ง e-mail กระจายถึงพนักงานทุกคน (Group All) โดยไม่มีเหตุจำเป็น เว้นแต่จะกระทำโดยผู้มีหน้าที่โดยตรงต่อการปฏิบัติงาน หรือผู้ที่ได้รับมอบหมายให้ดำเนินการได้ และเนื้อหาที่ส่งนั้นต้องเกี่ยวข้องกับงานของบริษัทเท่านั้น

25.11 ผู้ใช้งานต้องจัดการเนื้อที่ตู้เก็บ Mailbox ของตนเองตามสิทธิที่ได้รับ โดยหมั่นลบ e-mail ที่ไม่จำเป็น และไม่เกี่ยวข้องกับการทำงานออกจากระบบ เพื่อรักษาพื้นที่เก็บ e-mail ที่มีขนาดจำกัดให้สามารถรับ-ส่ง e-mail ได้ตามปกติต่อไป

26. การใช้งานข้อความแชท (Instant Messaging)

26.1 ผู้ใช้งานต้องไม่ใช้ e-mail Account และรหัสผ่านซ้ำกับ e-mail Account และรหัสผ่าน ของบริษัท ในการลงทะเบียนใช้ในข้อความแชท (Instant Messaging)

26.2 ผู้ใช้งานต้องไม่สนทนาหรือส่งข้อมูลที่เป็นความลับผ่านข้อความแชท

26.3 ผู้ใช้งานต้องตระหนักในการใช้ข้อความแชท ให้เกิดประโยชน์ต่อการทำงาน เช่น การปรึกษางาน การประสานงานภายใน การฝากข้อความ ลดจำนวนการใช้โทรศัพท์ ลดจำนวน e-mail เป็นต้น และไม่ใช้สนทนาในเรื่องส่วนตัวอื่นๆ ที่ไม่เกี่ยวข้องกับการทำงาน อันอาจทำให้ประสิทธิภาพการทำงานลดลงได้

27. การเปลี่ยนมือ เคลื่อนย้าย อุปกรณ์

27.1 ผู้ใช้งานต้องทำการลบหรือทำลายข้อมูล และซอฟแวร์ลิขสิทธิ์ทั้งหมดในอุปกรณ์ทุกครั้งก่อนการเปลี่ยนมือ การเลิกใช้ เพื่อป้องกันการรั่วไหลของข้อมูล และซอฟแวร์ของบริษัท

27.2 หากมีการเปลี่ยนแปลงตำแหน่ง ชั้น ที่ตั้งอุปกรณ์สารสนเทศใดๆ ผู้ใช้งานหรือผู้รับผิดชอบในอุปกรณ์นั้น ต้องแจ้งมายังฝ่ายเทคโนโลยีสารสนเทศทันที เพื่อประโยชน์ในการควบคุมและบำรุงรักษาอุปกรณ์นั้น

27.3 หากมีการเปลี่ยนแปลงผู้ใช้งาน แม้ว่าจะเป็นในหน่วยงานเดิม หรือโยกย้ายหน้าที่การงานไปยังหน่วยงานใหม่ ผู้ใช้งานเดิมมีหน้าที่แจ้งคืน และผู้ใช้งานใหม่ต้องขออนุมัติใช้งานตามสิทธิการขอใช้อุปกรณ์สารสนเทศ

หมวดที่ 5
การรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ โดยมีมาตรการและการดำเนินการในการป้องกัน รับมือกับสถานการณ์ด้านภัยคุกคามที่จะส่งผลต่อการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์อินเทอร์เน็ตของบริษัท ลดความเสี่ยงจากภัยคุกคามทางด้านไซเบอร์ทั้งจากภายใน และภายนอกบริษัท ให้สามารถลดความเสียหายที่อาจเกิดขึ้น โดยให้ผู้บริหารด้านเทคโนโลยีสารสนเทศ ดำเนินการตามแนวทางปฏิบัติที่สำคัญดังนี้

28. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยต่อระบบเครือข่ายคอมพิวเตอร์ในทุกด้านในระดับสูงเพื่อป้องกันภัยคุกคามทางด้านไซเบอร์

29. จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมินรวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง

30. กำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของบริษัท รวมถึงมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

31. ลักษณะของภัยคุกคามทางด้านไซเบอร์ แบ่งออกเป็น 3 ระดับ ดังนี้

31.1 ระดับไม่ร้ายแรง หมายถึง ระดับที่ทำให้ระบบคอมพิวเตอร์ หรือโครงสร้างพื้นฐานสารสนเทศของบริษัทด้อยประสิทธิภาพลง

31.2 ระดับร้ายแรง หมายถึง ระดับที่มีผลทำให้ระบบคอมพิวเตอร์ หรือโครงสร้างพื้นฐานสารสนเทศของบริษัทไม่สามารถทำงานหรือให้บริการได้

31.3 ระดับวิกฤต หมายถึง ระดับที่ส่งผลกระทบรุนแรงทำให้ระบบคอมพิวเตอร์ หรือโครงสร้างพื้นฐานสารสนเทศของบริษัทล้มเหลวทั้งระบบ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้าง

32. เมื่อมีเหตุภัยคุกคามทางด้านไซเบอร์เกิดขึ้นต่อระบบสารสนเทศอย่างมีนัยสำคัญในระดับร้ายแรงหรือระดับวิกฤต ให้รายงานต่อคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Committee) และคณะกรรมการกำกับดูแลระบบเทคโนโลยีสารสนเทศ (IT Steering Committee) และต่อหน่วยงานควบคุมกำกับดูแลภายนอกตามที่กฎหมายกำหนด และดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของบริษัท รวมถึงพฤติการณ์แวดล้อม ประเมินผลกระทบดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางด้านไซเบอร์อย่างทันท่วงที

33. ให้ความร่วมมือและประสานงานกับหน่วยงานภายใน และภายนอกที่เกี่ยวข้อง ในการรวบรวมข้อมูลเฝ้าระวัง/ตรวจสอบระบบคอมพิวเตอร์เพื่อหาข้อบกพร่อง ตรวจสอบการเข้าถึงข้อมูลคอมพิวเตอร์ ทดสอบการทำงานของคอมพิวเตอร์ ยึดหรืออายัดคอมพิวเตอร์ แก้ไขภัยคุกคาม กำจัดชุดคำสั่งที่ไม่พึงประสงค์ เพื่อระงับภัยคุกคามทางด้านไซเบอร์ที่ดำเนินการอยู่

34. ส่งเสริมความรู้ สร้างความเข้าใจ ความตระหนักรู้ด้านการใช้งานบนอินเตอร์เน็ตให้มีความมั่นคงปลอดภัย ให้แก่พนักงานอย่างสม่ำเสมอ

หมวดที่ 6
การบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัย

เพื่อกำหนดบทบาทหน้าที่ความรับผิดชอบของพนักงาน และบุคคลภายนอกที่เกี่ยวข้อง ในการระวังสังเกตุ ร่วมกันดูแล จัดการสถานการณ์ที่ทำให้เชื่อได้ว่าเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศของบริษัท ไม่มีความมั่นคงปลอดภัย

35. การรายงานเหตุละเมิดและจุดอ่อนเกี่ยวกับความมั่นคงปลอดภัย

35.1 พนักงานและบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท มีหน้าที่รายงานเหตุล่วงละเมิดหรือจุดอ่อนด้านความมั่นคงปลอดภัยใดๆ ที่พบเห็น หรือต้องสงสัยว่าจะเกิดขึ้นกับบริษัท ต่อผู้บังคับบัญชา หรือแจ้งกับเจ้าหน้าที่ ICT Service Desk โทร. 6999 เพื่อให้สามารถแก้ไขปัญหาอย่างทันท่วงที

35.2 พนักงานและบุคคลภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร ที่เป็นผู้ใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท ที่พบเห็นเหตุละเมิดหรือจุดอ่อนด้านความปลอดภัย ต้องไม่กล่าวถึงเหตุที่ตนพบเห็นนั้นกับบุคคลอื่นใด ยกเว้น ผู้บังคับบัญชา ผู้บริหารด้านเทคโนโลยีสารสนเทศ และ ICT Service Desk

35.3 เหตุละเมิดและจุดอ่อนเกี่ยวกับความมั่นคงปลอดภัยที่ต้องรายงาน ได้แก่

35.3.1 ระบบงานหลัก SAP ขัดข้อง ไม่สามารถเข้าใช้งานได้

35.3.2 การพบไวรัส ฟิชชิ่งเมล์ การเรียกค่าไถ่ข้อมูล หรือโปรแกรมมุ่งร้ายต่างๆ

35.3.3 การใช้งานข้อมูล หรือระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่เหมาะสม

35.3.4 การเข้าถึงข้อมูล หรือระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

35.3.5 การตรวจพบความพยายามบุกรุกเข้าระบบ หรือเครื่องมือที่ใช้ในการบุกรุกเข้าระบบ

35.3.6 การโจรกรรมข้อมูลและทรัพย์สิน

35.3.7 การกระทำที่ผิดกฎหมายว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือระเบียบข้อบังคับของบริษัท

36. การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุละเมิด

36.1 บริษัทต้องทำการระบุตัวบุคคลที่มีหน้าที่รับผิดชอบต่อการรับมือเหตุละเมิดความมั่นคงปลอดภัยอย่างชัดเจน และมอบอำนาจแก่บุคคลเหล่านั้น เพื่อดำเนินการรับมือกับเหตุละเมิดนั้นๆ อย่างได้ผล และมีความเป็นระบบระเบียบที่ดี

36.2 บุคคลที่มีหน้าที่รับผิดชอบต่อการรับมือเหตุละเมิดความมั่นคงปลอดภัย ต้องดำเนินการตอบสนองต่อเหตุด้วยความรวดเร็ว มีสติรอบคอบ และต้องติดต่อประสานงานกับฝ่ายต่างๆ ที่เกี่ยวข้องอย่างเหมาะสม รวมถึงบันทึกข้อมูลและจัดทำเอกสารเกี่ยวกับเหตุละเมิดความมั่นคงปลอดภัยโดยละเอียด

36.3 ผู้ดูแลระบบต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย และพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

36.4 บริษัทจะให้ความคุ้มครองพนักงานทุกคน และบุคคลภายนอกที่ปฏิบัติงานอยู่ภายในองค์กรที่แจ้งเหตุเข้ามา ซึ่งเชื่อว่าเป็นเหตุละเมิดความมั่นคงปลอดภัย เป็นการกระทำที่ผิดกฎหมาย หรือเป็นอันตรายที่คุกคามความปลอดภัยของเพื่อนพนักงาน โดยให้ความคุ้มครองจากการถูกพักงาน การข่มขู่ หรือการถูกกีดกันจากเพื่อนร่วมงาน

36.5 หากมีความจำเป็นต้องรายงาน เหตุละเมิดความมั่นคงปลอดภัยต่อหน่วยงานภายนอก ตามที่กฎหมายกำหนด การรายงานนั้นต้องถูกดำเนินการโดยบุคคลที่ได้รับอนุญาต ซึ่งได้รับการแต่งตั้งจากกรรมการผู้จัดการใหญ่เท่านั้น

36.6 บริษัทต้องจัดทำสื่อเพื่อเสริมสร้างการตระหนักรู้ และความเข้าใจเกี่ยวกับเหตุละเมิดความมั่นคงปลอดภัย วิธีการรายงานเหตุ วิธีการรวบรวมข้อมูลที่เป็นประโยชน์ต่อการสืบสวน และการเก็บรักษาหลักฐานให้แก่พนักงาน

36.7 เครื่องคอมพิวเตอร์ของพนักงานที่พ้นสภาพการเป็นพนักงานบริษัท ต้องถูกแยกออกจากระบบเครือข่ายทั้งภายในและภายนอกโดยทันที และก่อนนำกลับมาใช้ใหม่ ต้องมีการสำรองข้อมูลจากฮาร์ดดิสก์ (Hard

disk) เสียก่อน แล้วจึงทำการฟอร์แมท (Format) เครื่องคอมพิวเตอร์นั้น เพื่อป้องกันการแพร่กระจายของซอฟแวร์มุ่งร้าย ไวรัส หนอนคอมพิวเตอร์ โทรจัน เป็นต้น และเพื่อกำจัดซอฟแวร์ที่ไม่ได้รับอนุญาตซึ่งอาจถูกติดตั้งไว้ในเครื่อง

37. การเก็บรวบรวมหลักฐาน

37.1 ฝ่ายกฎหมาย และฝ่ายเทคโนโลยีสารสนเทศ ต้องรวบรวมข้อมูล พยานเอกสาร พยานบุคคล และจัดเก็บหลักฐานตามกฎเกณฑ์ สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้น มีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่ง กฎหมายอาญา หรือกฎหมายที่เกี่ยวข้อง

หมวดที่ 7
การบริหารความต่อเนื่องทางธุรกิจ

เพื่อให้การบริหารความต่อเนื่องทางธุรกิจในกระบวนการสำคัญ สามารถรองรับเหตุการณ์ฉุกเฉินและเหตุภัยพิบัติที่อาจส่งผลทำให้เกิดความล้มเหลวต่อระบบเทคโนโลยีสารสนเทศ ให้ผู้บริหารด้านเทคโนโลยีสารสนเทศร่วมกับส่วนงานที่เกี่ยวข้อง ปฏิบัติดังต่อไปนี้

38. จัดให้มีการประเมินความเสี่ยงโดยพิจารณาจากกระบวนการดำเนินงาน การวิเคราะห์ผลกระทบทางธุรกิจเพื่อระบุเหตุการณ์ที่สามารถทำให้บริการด้านเทคโนโลยีสารสนเทศหยุดชะงักลงได้

39. จัดให้มีการทำแผนการบริหารความต่อเนื่องของธุรกิจ ซึ่งประกอบด้วยหัวข้อดังต่อไปนี้

39.1 ระบุกระบวนทางธุรกิจที่มีความสำคัญ การใช้งานทรัพยากรร่วมกัน หรือความต่อเนื่องกันของกระบวนการเหล่านั้น

39.2 ลำดับความสำคัญของกระบวนการที่ต้องกู้คืน

39.3 ระบุหน้าที่ความรับผิดชอบ และการเตรียมการสำหรับกรณีฉุกเฉิน ทั้งในส่วนของผู้บริหาร เจ้าหน้าที่ดูแลระบบ ผู้ใช้งาน พนักงานทั่วไป และหน่วยงานภายนอก

39.4 กำหนดกลยุทธ์ที่ใช้ในการกู้คืน และทรัพยากรที่ต้องการ เช่น สถานที่ปฏิบัติงานสำรอง ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายสำรอง ข้อมูลที่ได้สำรองไว้

39.5 ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายสำรองที่กำหนดในแผนการบริหารความต่อเนื่องทางธุรกิจ จะต้องมีการทดสอบความพร้อมใช้งาน และความเข้ากันได้กับระบบปฏิบัติงานจริง

39.6 กำหนดให้มีการทบทวนความสอดคล้องของแผนการบริหารความต่อเนื่องทางธุรกิจปรับปรุงให้ทันสมัยอยู่เสมอ

40. จัดให้มีการทดสอบด้านการบริหารความต่อเนื่องของธุรกิจ อย่างน้อยปีละ 1 ครั้ง โดยกำหนดวิธีทดสอบ เกณฑ์ที่ใช้ ก่อนดำเนินการจริง พร้อมทั้งติดตามข้อบกพร่อง ที่พบในระหว่างการทดสอบเพื่อให้มีการปรับปรุงประสิทธิภาพต่อไป

หมวดที่ 8
บทกำหนดโทษ

41. พนักงานและผู้ใช้งานผู้ใดก็ตามที่ละเมิดหลักการและกระทำความผิดตามระเบียบนี้ จะได้รับการพิจารณาลงโทษทางวินัยตามระเบียบบริษัท และ/หรือกฎหมายที่เกี่ยวข้องตามความเหมาะสมแล้วแต่กรณี

หมวดที่ 9
บทเฉพาะกาล

42. งานหรือการดำเนินใดที่อยู่ระหว่างดำเนินการและยังไม่แล้วเสร็จในวันที่ระเบียบ บริษัท ไออาร์พีซี จำกัด (มหาชน) และบริษัทในเครือ ว่าด้วย การบริหารงานเทคโนโลยีสารสนเทศ พ.ศ. 2562 ฉบับนี้ใช้บังคับ ให้ดำเนินการต่อไปจนกว่าจะดำเนินการแล้วเสร็จ หรือจนกว่าจะสามารถดำเนินการตามระเบียบฉบับนี้ได้

43. ให้บังคับใช้ระเบียบนี้กับบริษัทในเครือโดยอนุโลม

ประกาศและให้มีผลใช้บังคับ ณ วันที่ 13 พฤศจิกายน 2562

(นายนพดล ปิ่นสุภา)
กรรมการผู้จัดการใหญ่