ข้อกำหนด บริษัท โกลบอลกรีนเคมิคอล จำกัด (มหาชน)
ว่าด้วย นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
(Information Technology Security Policy)
พ.ศ. 2565

เพื่อให้ระบบสารสนเทศของ บริษัท โกลบอลกรีนเคมิคอล จำกัด (มหาชน) และบริษัทในเครือ มีความมั่นคงปลอดภัย ดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพ สอดคล้องตามหลักมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) หรือกรอบการดำเนินงานที่เป็นมาตรฐานสากล และกำหนดแนวปฏิบัติเพื่อสร้างความตระหนัก รวมถึงกำหนดวิธีการป้องกันภัยคุกคาม จากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจนการปฏิบัติให้เกิดความสอดคล้องกับกฎหมายตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้อง กรรมการผู้จัดการจึงออกข้อกำหนดไว้ดังนี้

ข้อ 1 ข้อกำหนดนี้เรียกว่า "ข้อกำหนด บริษัท โกลบอลกรีนเคมิคอล จำกัด (มหาชน) ว่าด้วย นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Information Technology Security Policy) พ.ศ. 2565"

ข้อ 2 ข้อกำหนดนี้ใช้บังคับตั้งแต่ วันที่ 1 ตุลาคม พ.ศ. 2565 เป็นต้นไป

ข้อ 3 ให้ยกเลิก ข้อกำหนด บริษัท โกลบอลกรีนเคมิคอล จำกัด (มหาชน) ว่าด้วย นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Information Technology Security Policy) พ.ศ. 2563

หมวดที่ 1
บททั่วไป

ข้อ 4 ในข้อกำหนดนี้

4.1 "บริษัท" หมายถึง บริษัท โกลบอลกรีนเคมิคอล จำกัด (มหาชน)

4.2 "บริษัทในเครือ" หมายถึง บริษัทหรือนิติบุคคลที่บริษัทถือหุ้นไม่ว่าทางตรงหรือทางอ้อม

4.3 "ผู้ใช้งาน" หมายถึง ผู้ใช้งานระบบสารสนเทศที่ได้รับอนุญาตให้สามารถเข้าถึงหรือใช้งานระบบสารสนเทศและเครือข่ายของบริษัท

4.4 “ผู้บริหาร” หมายถึง ผู้บริหาร บริษัท โกลบอลกรีนเคมิคอล จำกัด (มหาชน) ตั้งแต่ระดับผู้จัดการฝ่าย และรักษาการผู้จัดการฝ่ายขึ้นไป

4.5 “พนักงาน” หมายถึง พนักงานบริษัทและพนักงานบริษัทในเครือ ซึ่งได้รับมอบหมายให้ปฏิบัติงาน

4.6 “ผู้ปฏิบัติงานตามสัญญาจ้าง” หมายถึง นิติบุคคลหรือตัวแทนนิติบุคคลตามสัญญาที่ปฏิบัติงานให้กับบริษัท โดยมีการว่าจ้างตามระเบียบของบริษัท ซึ่งมีระยะเวลาปฏิบัติงานตามช่วงเวลาที่ระบุในสัญญาจ้าง

4.7 “นักศึกษาฝึกงาน” หมายถึง นักศึกษาจากมหาวิทยาลัยหรือสถาบันการศึกษาที่ได้รับอนุญาตให้เข้าฝึกงานกับบริษัทและบริษัทในเครือ ซึ่งมีระยะเวลาฝึกงานตามช่วงเวลาที่กำหนดไว้ในบันทึกข้อตกลงระหว่างบริษัทหรือบริษัทในเครือ และสถาบันการศึกษานั้น ๆ

4.8 “ผู้ดูแลระบบ” หมายถึง ผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการควบคุมดูแลระบบสารสนเทศ หรือระบบเครือข่ายของบริษัท

4.9 “พนักงาน ServiceDesk” หมายถึง พนักงานหน่วยงานที่มีหน้าที่ให้คำปรึกษาหรือตอบรับปัญหาของผู้ใช้งานในการใช้งานระบบสารสนเทศ

4.10 “หน่วยงานเทคโนโลยีสารสนเทศ” หมายถึง หน่วยงานที่รับผิดชอบ กำกับ ดูแล และบริหารจัดการระบบสารสนเทศของบริษัท

4.11 “หน่วยงานที่รับผิดชอบ” หมายถึง หน่วยงานของบริษัทที่ได้รับมอบหมายจากผู้บริหารให้ปฏิบัติงานตามที่ได้รับมอบหมาย

4.12 “หน่วยงานเจ้าของข้อมูลหรือหน่วยงานเจ้าของระบบงาน” หมายถึง ผู้ที่ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

4.13 “หน่วยงานภายนอก” หมายถึง องค์กรหรือหน่วยงานภายนอกที่บริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของบริษัท โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับข้อมูลของบริษัท ตามสัญญาการรักษาความลับ

4.14 “ผู้ให้บริการคลาวด์ภายนอก” หมายถึง หน่วยงานภายนอกที่ให้บริการในรูปแบบของระบบคลาวด์

4.15 “เครื่องคอมพิวเตอร์” หมายถึง อุปกรณ์ประมวลผลข้อมูลคอมพิวเตอร์ ที่ทำงานผ่านระบบปฏิบัติการ (Operating System) ซึ่งประกอบด้วย หน่วยประมวลผล จอภาพ และคีย์บอร์ด

4.16 “อุปกรณ์แบบพกพา (Mobile Device)” หมายถึง อุปกรณ์ที่เคลื่อนย้ายได้ง่าย มีการประมวลผลผ่านระบบปฏิบัติการ (Operating System) สามารถรับข้อมูลนำเข้า (Input) แสดงผลผ่านหน้าจอและเข้าถึงเครือข่ายได้ เช่น Smart phone, Tablet, Netbook, Notebook เป็นต้น

4.17 “อุปกรณ์แบบพกพาส่วนบุคคล” หมายถึง อุปกรณ์แบบพกพาส่วนตัวของผู้ใช้งานที่นำมาเชื่อมต่อระบบสารสนเทศของบริษัท

4.18 “อุปกรณ์เครือข่าย” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ที่ใช้เชื่อมต่อกับเครื่องคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ เพื่อให้สามารถแลกเปลี่ยนข้อมูลคอมพิวเตอร์และสารสนเทศระหว่างกันได้

4.19 “ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้ความหมายรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

4.20 “ระบบสารสนเทศ” หมายถึง ระบบงาน เครื่องคอมพิวเตอร์เครือข่าย เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์ต่าง ๆ ที่มีไว้เพื่อให้บริการสารสนเทศของบริษัท

4.21 “สารสนเทศ (Information)” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

4.22 “ข้อมูลสารสนเทศ” หมายถึง ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่เกี่ยวข้องกับงานในกิจการของบริษัทและบริษัทในเครือ ซึ่งครอบคลุมทั้งรูปแบบอิเล็กทรอนิกส์และสื่อสิ่งพิมพ์

4.23 “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

4.24 “Data at Rest” หมายถึง ข้อมูลที่ถูกจัดเก็บอยู่ในสื่อบันทึกข้อมูลต่าง ๆ ของบริษัท เช่น Share Drive, Files Server, Database หรือในเครื่องคอมพิวเตอร์ของผู้ใช้งาน

4.25 “เครือข่ายคอมพิวเตอร์” หมายถึง การเชื่อมต่อเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายผ่านระบบสื่อสารเพื่อแลกเปลี่ยนสารสนเทศ ภายในเครือข่ายร่วมกัน (Shared Resource)

4.26 “เครือข่ายสังคมออนไลน์ (Social Network)” หมายถึง ระบบงานที่ทำให้มีการสื่อสารทั้งการรับรู้ข่าวสารและการแบ่งปันข้อมูลกับคนจำนวนมากผ่านช่องทางอินเทอร์เน็ต โดยการใช้งานเทคโนโลยีประเภทสื่อสังคม (Social Media)

4.27 “สินทรัพย์” หมายถึง ข้อมูลคอมพิวเตอร์ ระบบสารสนเทศ และทรัพย์สินด้านสารสนเทศของบริษัท เช่น เครื่องคอมพิวเตอร์ อุปกรณ์แบบพกพาของบริษัท อุปกรณ์เครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ของบริษัท เป็นต้น

4.28 “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ที่อาจนำไปสู่ความเสียหายหรือการสูญเสียของบริษัททุกกรณี ต่อบุคลากร สินทรัพย์ หรือก่อให้เกิดความไม่มั่นคง รวมทั้งเกิดการรั่วไหลของสารสนเทศ

4.29 “มาตรฐาน (Standard)” หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

4.30 “วิธีการปฏิบัติ (Procedure)” หมายถึง รายละเอียดที่บอกขั้นตอนที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ให้กำหนดไว้ตามวัตถุประสงค์

4.31 “ระบบบริหารความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ” หมายถึง การบริหารจัดการระบบสารสนเทศ เพื่อสร้างความมั่นคงปลอดภัย ซึ่งพิจารณาจากความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินสารสนเทศของบริษัท โดยกำหนดมาตรการและดำเนินการตามแผนการลดความเสี่ยงที่จัดทำขึ้น รวมถึงทบทวนและปรับปรุงความเสี่ยง และกระบวนการต่าง ๆ อย่างสม่ำเสมอ

4.32 “ระบบคอมพิวเตอร์ (Computer System)” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

4.33 “ระบบเครือข่าย (Network System)” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบสารสนเทศต่าง ๆ ของบริษัทได้ เช่น ระบบ LAN, ระบบ Intranet, ระบบ Internet เป็นต้น

4.34 “ระบบ LAN และ ระบบ Internet” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลสารสนเทศภายในหน่วยงาน

4.35 “ระบบอินเทอร์เน็ต (Internet)” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ข องบริษัทเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

4.36 “ระบบคลาวด์” หมายถึง ระบบสารสนเทศที่ให้บริการในรูปแบบการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์ เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน

4.37 “พื้นที่ใช้งานระบบสารสนเทศ (Information Technology System Workspace)” หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบสารสนเทศ

4.38 “จดหมายอิเล็กทรอนิกส์ (E-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP, POP3 และ IMAP เป็นต้น

4.39 "รหัสผ่าน (Password)" หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล และเพื่อควบคุมการเข้าถึงข้อมูล และระบบสารสนเทศของบริษัท

4.40 "ชุดคำสั่งไม่พึงประสงค์" หมายถึง ชุดคำสั่งที่มีผลทำให้เครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

4.41 "คอมพิวเตอร์แม่ข่าย (Server)" หมายถึง เครื่องคอมพิวเตอร์ตัวหลักในเครือข่าย ที่จะทำหน้าที่ควบคุมคอมพิวเตอร์อื่น ๆ ในเครือข่ายนั้นทั้งหมด โดยเป็นทั้งที่เก็บโปรแกรมและข้อมูลที่คอมพิวเตอร์ในเครือข่ายจะเรียกใช้ได้

4.42 "สื่อบันทึกข้อมูลที่ถอดแยกได้ (Removable Media)" หมายถึง อุปกรณ์การจัดเก็บใด ๆ ที่สามารถถอดออกจากเครื่องคอมพิวเตอร์ได้ โดยที่เครื่องคอมพิวเตอร์ยังคงปฏิบัติการอยู่ได้ เช่น Hard drives, Thumb drives, การ์ดความจำ (Memory cards), USB flash drives เป็นต้น

4.43 "ฟิชชิ่ง (Phishing)" หมายถึง ภัยคุกคามทางไซเบอร์รูปแบบหนึ่ง โดยมักจะมาในรูปแบบของการปลอมแปลงจดหมายอิเล็กทรอนิกส์ หรือเว็บไซต์ที่สร้างขึ้นเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางด้านการเงิน หรือข้อมูลส่วนตัวต่าง ๆ เช่น หมายเลขบัตรเครดิต หมายเลขประจำตัวผู้ใช้ (User Name) รหัสผ่าน (Password) หรือ หมายเลขบัตรประจำตัวประชาชน เป็นต้น

4.44 "ภัยคุกคามทางไซเบอร์" หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

4.45 "การ Jailbreak หรือ Root" หมายถึง การดัดแปลงระบบปฏิบัติการของอุปกรณ์แบบพกพาส่วนบุคคล เพื่อให้สามารถติดตั้งซอฟท์แวร์ ที่ไม่ผ่านการตรวจสอบจากเจ้าของระบบปฏิบัติการ

4.46 "แอปพลิเคชัน" หมายถึง ชุดคำสั่งที่เขียนขึ้นเพื่อให้เครื่องคอมพิวเตอร์ทำงานตามวัตถุประสงค์เฉพาะอย่าง

4.47 "แพทช์ (Patch)" หมายถึง โปรแกรมหรือซอฟต์แวร์ที่ผู้ผลิตออกมาเพื่อทำการแก้ไขข้อผิดพลาดหรือช่องโหว่ของซอฟต์แวร์ ระบบปฏิบัติการ หรืออื่น ๆ เพื่อให้มีความเสถียรและลดช่องโหว่จากการถูกโจมตีจากผู้ไม่ประสงค์ดี

4.48 "Key Management" หมายถึง การบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสข้อมูล (Encryption) และการถอดรหัสข้อมูล (Decryption) ซึ่งเป็นวิธีการในการทำให้ข้อมูลเป็นความลับ และไม่สามารถอ่านได้โดยบุคคลอื่นที่ไม่เกี่ยวข้อง

หมวดที่ 2
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

ข้อ 5 กำหนดนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ให้เป็นไปตามมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) วิธีการปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

5.1 ทำให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของบริษัทและบริษัทในเครือ ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

5.2 กำหนดขอบเขตของการบริหารความมั่นคงปลอดภัยของระบบสารสนเทศ โดยอ้างอิงมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

5.3 เผยแพร่นโยบายให้พนักงานทุกระดับในบริษัทและบริษัทในเครือ ได้รับทราบและพนักงานต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

5.4 กำหนดมาตรฐาน แนวทาง และวิธีการปฏิบัติ ให้ผู้บริหาร ผู้ดูแลระบบ พนักงาน ผู้ปฏิบัติงานตามสัญญาจ้าง นักศึกษาฝึกงาน และหน่วยงานภายนอกที่ปฏิบัติงานให้กับบริษัทรับทราบถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศของบริษัทและบริษัทในเครือ และต้องปฏิบัติตามอย่างเคร่งครัด

ข้อ 6 นโยบายนี้ประกอบด้วย

ส่วนที่ 1 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
ส่วนที่ 2 การควบคุมการเข้าถึงระบบสารสนเทศและการสื่อสาร
ส่วนที่ 3 การใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์แบบพกพา
ส่วนที่ 4 การใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์
ส่วนที่ 5 การใช้งานจดหมายอิเล็กทรอนิกส์
ส่วนที่ 6 การสำรองข้อมูลและการเตรียมพร้อมกรณีฉุกเฉิน
ส่วนที่ 7 การจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้
ส่วนที่ 8 การสร้างความตระหนักรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ
ส่วนที่ 9 การรักษาความมั่นคงปลอดภัยด้านไซเบอร์
ส่วนที่ 10 การรักษาความมั่นคงปลอดภัยระบบคลาวด์
ส่วนที่ 11 การพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย
ส่วนที่ 12 การรักษาความปลอดภัยข้อมูล
ส่วนที่ 13 การใช้งานอุปกรณ์แบบพกพาส่วนบุคคล

องค์ประกอบในแต่ละส่วนที่กล่าวมาข้างต้น จะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติของการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท

ส่วนที่ 1
การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกัน และรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ รวมถึงเพื่อกำหนดมาตรการควบคุมป้องกันและรักษาความมั่นคงปลอดภัยของพื้นที่ใช้งานที่มีการเก็บ ใช้ และประมวลผลข้อมูลส่วนบุคคล โดยพิจารณามาตรการต่าง ๆ ตามความสำคัญของระบบสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ

2. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

2.1 กำหนดให้สถานที่ตั้งของระบบสารสนเทศเป็นพื้นที่ควบคุมการเข้าออก และอนุญาตให้เฉพาะผู้ที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

2.2 จำแนกและกำหนดพื้นที่ใช้งานระบบสารสนเทศอย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

2.3 กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน

2.4 กำหนดสิทธิ์ให้กับผู้ดูแลระบบให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศเพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

2.4.1 จัดทำทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่ เพื่อใช้งานระบบสารสนเทศ

2.4.2 บันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสารหรือข้อมูลบันทึกการเข้าออกพื้นที่

2.4.3 ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่อย่างน้อยปีละ 1 ครั้ง

2.5 หน่วยงานเทคโนโลยีสารสนเทศสงวนสิทธิ์ที่จะระงับการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศหากพบว่ามีการละเมิดความมั่นคงปลอดภัยสารสนเทศ หรือพบภัยคุกคามที่อาจจะส่งผลกระทบให้บริษัทได้รับความเสียหาย

ส่วนที่ 2
การควบคุมการเข้าถึงระบบสารสนเทศและการสื่อสาร
(Access Control Security)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศของบริษัทโดยบุคคลที่ไม่ได้รับอนุญาต และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกโดยใช้โปรแกรมชุดคำสั่งไม่พึงประสงค์ ซึ่งจะสร้างความเสียหายแก่ระบบสารสนเทศ หรือทำให้การทำงานของระบบสารสนเทศหยุดชะงักรวมถึงสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของบริษัทได้อย่างถูกต้อง

2. การควบคุมการเข้าถึงระบบสารสนเทศ

2.1 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติ กำหนด และแก้ไขสิทธิ์ในการเข้าถึงระบบสารสนเทศให้แก่ผู้ใช้งาน และจะต้องมีการทำเป็นเอกสารการกำหนดสิทธิ์ในการเข้าสู่ระบบ และต้องจัดเก็บเอกสารดังกล่าวไว้เป็นหลักฐานด้วย

2.2 หน่วยงานเจ้าของข้อมูลหรือหน่วยงานเจ้าของระบบงานต้องอนุญาตให้ผู้ใช้งานเข้าสู่ระบบสารสนเทศหรือให้สิทธิ์เฉพาะส่วนที่จำเป็นต้องรู้ตามหน้าที่ที่ต้องปฏิบัติงานเท่านั้น เพื่อป้องกันการให้สิทธิ์ในการใช้งานเกินความจำเป็น อันจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่

2.3 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศตามหลักการให้สิทธิ์น้อยที่สุดเพื่อให้สามารถปฏิบัติหน้าที่ตามที่กำหนดเท่านั้น

2.4 ต้องกำหนดให้มีการแบ่งแยกหน้าที่ระหว่างผู้ดูแลระบบที่เข้าถึงฐานข้อมูล (Database) และระบบปฏิบัติการ (Operating system) อย่างเหมาะสม เพื่อไม่ให้ผู้ดูแลระบบสามารถปฏิบัติงานในกระบวนการบริหารจัดการระบบสารสนเทศได้ตั้งแต่ต้นจนจบกระบวนการ

2.5 ผู้ดูแลระบบต้องกำหนดวิธีการตัดการเชื่อมต่อระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานนาน (Session Time-out) ตามที่กำหนดไว้ในวิธีการปฏิบัติ "P-(G-HC-IT)-002 มาตรฐานการให้บริการระบบสารสนเทศ"

2.6 การพิสูจน์ตัวตนสองขั้นตอน (Two Factors Authentication)

2.6.1 ผู้ดูแลระบบต้องจัดให้มีการพิสูจน์ตัวตนสองขั้นตอน สำหรับการเข้าใช้งานระบบสารสนเทศที่สำคัญ

2.6.2 ผู้ใช้งานต้องนำอุปกรณ์แบบพกพาส่วนบุคคลมาลงทะเบียนเพื่อใช้งานการพิสูจน์ตัวตนสองขั้นตอนตามที่บริษัทได้จัดไว้ให้

2.6.3 การใช้งานอุปกรณ์การพิสูจน์ตัวตนสองขั้นตอนต้องได้รับการอนุมัติจากหน่วยงานเทคโนโลยีสารสนเทศ

2.6.4 ในกรณีที่อุปกรณ์สื่อสารพกพา หรือ Token สูญหาย หรือสงสัยว่ารหัสถูกปลอมแปลง ผู้ใช้งานต้องแจ้งให้หน่วยงานเทคโนโลยีสารสนเทศรับทราบโดยทันที

3. การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

3.1 การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีวิธีการปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งมีวิธีการปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออก หรือเมื่อเปลี่ยนตำแหน่งงานภายในบริษัท เป็นต้น

3.2 บริษัทไม่อนุญาตให้มีการใช้บัญชีรายชื่อผู้ใช้งานร่วมกัน (Shared User Account)

3.3 กรณีที่มีความจำเป็นต้องให้สิทธิ์พิเศษ หรือสิทธิ์สูงสุดกับผู้ใช้งาน ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษ หรือสิทธิ์สูงสุดนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

3.3.1 ต้องได้รับความเห็นชอบ และอนุมัติจากผู้จัดการฝ่ายหน่วยงานเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้จัดการฝ่ายหน่วยงานเทคโนโลยีสารสนเทศ และผู้ดูแลระบบงานนั้น ๆ

3.3.2 ต้องมีการควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

3.3.3 ต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3.3.4 ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน

3.4 การใช้รหัสผ่าน (Password)

3.4.1 ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก ต้องเปลี่ยนรหัสผ่านใหม่ทันที เพื่อให้เป็นความลับเฉพาะตัว ในกรณีที่รหัสผ่านถูกเปิดเผย หรือสงสัยว่ามีบุคคลอื่นทราบรหัสผ่านส่วนบุคคลของตน ผู้ใช้งานจะต้องทำการเปลี่ยนรหัสผ่านใหม่ทันที

3.4.2 แนวทางการบริหารจัดการรหัสผ่านให้เป็นไปตามวิธีการปฏิบัติ “P-(G-HC-IT)-002 มาตรฐานการให้บริการระบบสารสนเทศ” และต้องปฏิบัติตามอย่างเคร่งครัด

4. การบริหารจัดการการเข้าถึงระบบเครือข่าย

4.1 ต้องกำหนดผู้ที่รับผิดชอบในการดูแลระบบเครือข่าย (Communication Network) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของระบบ (System Configuration) อย่างชัดเจน

4.2 ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้งานและกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกทำได้อย่างเป็นระบบ

4.3 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

4.4 กำหนดผู้ดูแลระบบที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไข หรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

4.5 ระบบเครือข่ายทั้งหมดของบริษัทที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกบริษัท ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

4.6 ต้องติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของบริษัทในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

4.7 การเข้าสู่ระบบเครือข่ายภายในบริษัท โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

4.8 IP address ของระบบเครือข่ายภายในของบริษัท จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของระบบสารสนเทศได้โดยง่าย

4.9 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

4.10 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

4.11 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

5. การบริหารจัดการคอมพิวเตอร์แม่ข่าย

5.1 ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลคอมพิวเตอร์แม่ข่าย (Server) การกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

5.2 มีขั้นตอนหรือวิธีการปฏิบัติในการตรวจสอบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

5.3 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น SSH, SFTP เป็นต้น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

5.4 ทำการปรับปรุง (Update) ระบบซอฟท์แวร์ให้เป็นปัจจุบัน เพื่อปิดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

5.5 มีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความมั่นคงปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

5.6 การติดตั้ง และการเชื่อมต่อคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

5.7 ต้องกำหนดให้พิจารณาติดตั้งแพทช์ (Patch) อย่างเหมาะสมกับอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย ตามคำแนะนำของผู้ผลิต โดยการติดตั้งต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management) ตามวิธีการปฏิบัติ "P-(G-HC-IT)-006: การบริหารจัดการระบบสารสนเทศ"

6. การควบคุมการเข้าใช้งานระบบสารสนเทศจากภายนอก

6.1 การเข้าสู่ระบบสารสนเทศจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ของบริษัทหรือบริษัทในเครือ ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของบริษัท การควบคุมผู้ใช้งานที่เข้าสู่ระบบสารสนเทศของบริษัทจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบจากภายใน

6.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศได้จากระยะไกลต้องได้รับการอนุมัติจากผู้จัดการฝ่ายหน่วยงานทรัพยากรมนุษย์และงานสนับสนุนองค์กรหรือผู้ที่ได้รับมอบหมายจากผู้จัดการฝ่ายหน่วยงานทรัพยากรมนุษย์และงานสนับสนุนองค์กรก่อน และต้องมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

6.3 ผู้ใช้งานต้องไม่นำ User Account ของการเข้าสู่ระบบสารสนเทศจากระยะไกลไปให้บุคคลอื่นใช้งาน และต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

6.4 บริษัทสงวนสิทธิ์ที่จะระงับการเข้าใช้งานระบบสารสนเทศจากระยะไกล หากมีเหตุสงสัยว่าคอมพิวเตอร์นั้นไม่ปลอดภัยต่อระบบเครือข่าย

6.5 เมื่อผู้ใช้งานจะเข้าใช้งานระบบสารสนเทศจากระยะไกลต้องมีการพิสูจน์ตัวตนตามวิธีการที่บริษัทได้จัดไว้ให้

7. การบริหารจัดการการบันทึกและตรวจสอบ

7.1 กำหนดให้มีการจัดเก็บบันทึกเหตุการณ์ (Log) การทำงานของคอมพิวเตอร์แม่ข่าย (System Log) เครือข่าย (Network Log) ระบบงาน (Application Log) และระบบป้องกันการบุกรุก (Security Log) ซึ่งหมายความรวมถึงระบบที่มีการเก็บหรือประมวลผลข้อมูลส่วนบุคคลด้วย โดยกำหนดให้มีการจัดเก็บ Log แบบ Online เป็นระยะเวลา 3 เดือน และ Offline เป็นระยะเวลา 9 เดือน เพื่อประโยชน์ในการใช้ตรวจสอบ

7.2 ต้องจัดเก็บข้อมูลบันทึกเหตุการณ์ที่เกิดจากบัญชีรายชื่อผู้ใช้งานทุกระดับ (Privileged User และ Non Privileged User)

7.3 ผู้ดูแลระบบต้องตรวจสอบบันทึกการใช้งานของผู้ใช้งานอย่างสม่ำเสมอ

7.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

7.5 ต้องจัดเก็บข้อมูลบันทึกเหตุการณ์ในการเข้าถึง Event Logging Storage

7.6 กำหนดให้มีกระบวนการติดตาม และตรวจสอบข้อมูลบันทึกเหตุการณ์ (Event Logging) และจัดทำระบบแจ้งเตือนกรณีมีเหตุการณ์เกิดขึ้น

8. การขออนุญาตให้ผู้ปฏิบัติงานชั่วคราวเข้าใช้ระบบสารสนเทศ

8.1 หน่วยงานที่มีความจำเป็นต้องขออนุมัติให้ผู้ปฏิบัติงานชั่วคราวเข้าใช้ระบบสารสนเทศต้องดำเนินการตามวิธีการปฏิบัติ "P-(G-HC-IT)-001 กระบวนการดำเนินงานการขอใช้บริการสารสนเทศ" และ "P-(G-HC-IT)-005 กระบวนการให้สิทธิ์และทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศ"

8.2 หัวหน้าหน่วยงานต้องควบคุมการใช้งานระบบสารสนเทศของผู้ปฏิบัติงานชั่วคราวให้เป็นไปตามนโยบายนี้ และจะต้องแจ้งผู้ดูแลระบบทันทีที่ผู้ปฏิบัติงานชั่วคราวดังกล่าวหมดความจำเป็นหรือเมื่อเลิกการปฏิบัติงานก่อนกำหนด

ส่วนที่ 3
การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพา
(Use of Computer and Mobile Device)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพา ผู้ใช้งานต้องทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อให้ข้อมูลและอุปกรณ์ของบริษัทมีความมั่นคงปลอดภัย มีความพร้อมใช้งานอยู่เสมอ รวมทั้งการบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยงในการใช้งานให้ได้ประสิทธิภาพสูงสุด

2. การใช้งานทั่วไป

2.1 ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิมพร้อมใช้งานอยู่เสมอ และต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์

2.2 เครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาที่บริษัทอนุญาตให้ผู้ใช้งานเป็นทรัพย์สินของบริษัท ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพ เพื่อการทำงานของบริษัทเท่านั้น และต้องเก็บรักษาไว้ในที่ปลอดภัย เพื่อป้องกันการสูญหาย รวมทั้งต้องไม่นำอุปกรณ์ดังกล่าวให้ผู้อื่นใช้งาน

2.3 ผู้ใช้งานต้องไม่ใช้เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ และทรัพยากรอื่น ๆ ของบริษัท เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว เผยแพร่ข้อมูลที่ไม่เหมาะสม หรือกระทำการใด ๆ ที่ขัดต่อกฎหมาย ศีลธรรม ต่อต้านชาติ ศาสนา พระมหากษัตริย์ หรือเป็นภัยต่อความมั่นคงและต่อสังคม

2.4 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่บริษัทได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.5 ห้ามผู้ใช้งานนำซอฟต์แวร์ที่ไม่ได้รับอนุญาตมาใช้งานกับเครื่องคอมพิวเตอร์หรืออุปกรณ์แบบพกพาของบริษัท และหากเกิดการฟ้องร้องจากผู้เสียหายแล้ว ผู้ใช้งานต้องรับผิดชอบความเสียหายที่เกิดขึ้นทั้งหมด

2.6 ห้ามผู้ใช้งานใช้อุปกรณ์คอมพิวเตอร์เพื่อทำการผลิต ครอบครอง หรือจำหน่ายคอมพิวเตอร์ซอฟต์แวร์ที่ไม่เหมาะสม หรือผิดกฎหมาย

2.7 ผู้ใช้งานต้องรับผิดชอบในข้อความ รูปภาพ เสียง หรือ แฟ้มข้อมูลที่ส่งออกจากเครื่องคอมพิวเตอร์ของผู้ใช้งานนั้นทั้งหมด

2.8 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) จะต้องกำหนดโดยผู้ดูแลระบบของบริษัทเท่านั้น

2.9 การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ เพื่อตรวจซ่อมจะต้องดำเนินการโดยหน่วยงานเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายเท่านั้น

2.10 ผู้ใช้งานควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

2.11 ผู้ใช้งานควรจัดเก็บข้อมูลสำคัญของบริษัท ตามที่บริษัทได้จัดเตรียมไว้ให้ เช่น ระบบ SharePoint หรือ OneDrive หรือสื่อบันทึกข้อมูลที่ถอดแยกได้ที่บริษัทจัดหาให้ เป็นต้น

2.12 ผู้ใช้งานต้องไม่บันทึกข้อมูลต่าง ๆ ไว้ที่ Drive C และหน้า Desktop

2.13 ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของบริษัท

2.14 ผู้ใช้งานต้องรายงานเหตุการณ์ผิดปกติที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือสารสนเทศให้ผู้ดูแลระบบทราบ

2.15 บริษัทขอสงวนสิทธิ์ที่จะเข้าตรวจสอบเครื่องคอมพิวเตอร์ หากมีเหตุต้องสงสัยว่าผู้ใช้งานกระทำการสิ่งใดที่อาจส่งผลกระทบในทางเสียหายต่อบริษัท

2.16 ผู้ใช้งานต้องรายงานการสูญหาย หรือถูกขโมยของอุปกรณ์แบบพกพามายังหน่วยงานเทคโนโลยีสารสนเทศ นับแต่ทราบเหตุการณ์สูญหายหรือถูกขโมยนั้น

3. การควบคุมการเข้าถึงระบบปฏิบัติการ

3.1 ผู้ใช้งานควรกำหนดรหัสผ่านให้สอดคล้องตามที่ระบุไว้ในวิธีการปฏิบัติ "P-(G-HC-IT)-002 มาตรฐานการให้บริการระบบสารสนเทศ"

3.2 ผู้ใช้งานต้องทำการล็อคหน้าจอทันทีเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่านอีกครั้ง

3.3 ผู้ใช้งานต้องทำการ Log Off ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอ

4. การป้องกันจากไวรัสคอมพิวเตอร์ และโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

4.1 ผู้ดูแลระบบต้อง Update โปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ และเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

4.2 ผู้ดูแลระบบมีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

4.3 ผู้ดูแลระบบหรือผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกข้อมูลที่ถอดแยกได้ทุกครั้งก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

4.4 ผู้ใช้งานต้องไม่ปรับแต่ง หรือยกเลิกการทำงานของโปรแกรมป้องกันไวรัสที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่ผู้ดูแลระบบจัดหาให้

4.5 ผู้ใช้งานที่นำเครื่องคอมพิวเตอร์ไปใช้งานภายนอกเครือข่าย เมื่อจะนำกลับมาใช้ในเครือข่ายให้ทำการตรวจสอบไวรัสด้วยตนเอง ตามที่ผู้ดูแลระบบจัดเตรียมให้ทุกครั้ง

4.6 ผู้ใช้งานต้องไม่ดาวน์โหลดข้อมูลหรือซอฟต์แวร์จากเว็บไซต์ที่ไม่เหมาะสม

4.7 ผู้ใช้งานมีหน้าที่ต้องแจ้งผู้ดูแลระบบโดยทันทีและห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับเครือข่าย หากสงสัยหรือตรวจพบว่าเครื่องคอมพิวเตอร์ติดไวรัส หรือชุดคำสั่งไม่พึงประสงค์ เพื่อป้องกันการแพร่กระจายไปยังเครื่องคอมพิวเตอร์อื่น

4.8 ผู้ใช้งานต้องไม่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์แบบพกพาที่ไม่ใช่ของบริษัทมาทำการเชื่อมต่อเครือข่าย เว้นแต่จะได้รับการอนุมัติ

4.9 ผู้ใช้งานควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

4.10 บริษัทสงวนสิทธิ์ที่จะระงับไม่ให้คอมพิวเตอร์ที่ติดไวรัส หรือสงสัยว่าอาจนำพาไวรัสเชื่อมต่อเข้าสู่เครือข่ายภายในบริษัท

ส่วนที่ 4
การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์
(Use of the Internet and Online Social Networking)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ และแนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์อย่างปลอดภัย และป้องกันไม่ให้เป็นการละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของบริษัทถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. การใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์

2.1 ผู้ใช้งานต้องไม่ใช้อินเทอร์เน็ตของบริษัท เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

2.2 ผู้ใช้งานต้องไม่ใช้อินเทอร์เน็ตของบริษัท ในการนำเข้า เผยแพร่ หรือส่งต่อข้อมูลคอมพิวเตอร์ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก

2.3 ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ แต่งเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ซึ่งจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

2.4 ผู้ใช้งานต้องไม่ใช้เครือข่ายสังคมออนไลน์ที่ก่อให้เกิดความเสียหายต่อบริษัท ละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม แสวงหาผลประโยชน์หรืออนุญาตให้บุคคลอื่นแสวงหาประโยชน์ในเชิงธุรกิจ ที่เป็นการหาประโยชน์ส่วนตัว

2.5 ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัท หรือทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

2.6 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

2.7 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัท ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

2.8 ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัท

2.9 ผู้ใช้งานต้องไม่สนทนาหรือส่งข้อมูลที่เป็นความลับผ่านเครือข่ายสังคมออนไลน์

2.10 ผู้ใช้งานต้องไม่ใช้บัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ของบริษัทในการลงทะเบียนใช้งานเครือข่ายสังคมออนไลน์

2.11 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย และต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

2.12 ผู้ใช้งานต้องไม่ใช้อินเทอร์เน็ตของบริษัท เพื่อการดาวน์โหลดเพลง เกมส์ โปรแกรม Hacking Tools หรือโปรแกรมใด ๆ ที่อาจทำให้การจราจรข้อมูลติดขัด

2.13 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ส่วนที่ 5
การใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่อาจเกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ์ หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบนั้นอย่างเคร่งครัด ซึ่งจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. การใช้งานในการส่งจดหมายอิเล็กทรอนิกส์

2.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งาน และหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งการทบทวนสิทธิ์การเข้าใช้งานอย่างต่อเนื่องสม่ำเสมอ

2.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีผู้ใช้งานรายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของบริษัท

2.3 ผู้ใช้งานควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อบริษัท หรือละเมิดสิทธิ์ สร้างความรำคาญต่อบุคคลอื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัท

2.4 ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่น เพื่ออ่าน รับ ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมหรือมอบหมาย (Delegate) จากเจ้าของ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

2.5 ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อการทำงานของบริษัทเท่านั้น

2.6 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องทำการ Logoff ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

2.7 ผู้ใช้งานที่ใช้จดหมายอิเล็กทรอนิกส์ผ่านเว็บไซต์ (Web Access) ต้องทำการ Sign out ออกจากระบบทุกครั้งหลังการใช้งาน และต้องไม่บันทึกชื่อบัญชีผู้ใช้งานและรหัสผ่านบนเครื่องคอมพิวเตอร์

2.8 ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟโดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

2.9 ผู้ใช้งานต้องไม่เปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์จากผู้ส่งที่ไม่รู้จักและไม่เกี่ยวข้องกับธุรกิจ หรือส่งต่อจดหมายดังกล่าว เว้นแต่ได้รับการตรวจสอบไวรัส

2.10 ผู้ใช้งานพึงใช้ข้อความที่สุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์

2.11 ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพ หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมอันอาจทำให้เสียชื่อเสียงของบริษัท ทำให้เกิดความแตกแยกระหว่างบริษัทผ่านทางจดหมายอิเล็กทรอนิกส์

2.12 ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

2.13 ผู้ใช้งานต้องไม่ส่งข้อความ รูปภาพ เสียง หรือแฟ้มข้อมูล กระจายถึงกลุ่มผู้ใช้งานทุกคน (All Group Mail) ยกเว้นผู้บริหารระดับฝ่ายขึ้นไป หรือเทียบเท่า ผู้แทนจากหน่วยงานต่าง ๆ ที่ได้รับการอนุมัติจากผู้รับผิดชอบ โดยเนื้อหาที่ส่งนั้นต้องเกี่ยวข้องกับงานของบริษัท

ส่วนที่ 6
การสำรองข้อมูลและการเตรียมพร้อมกรณีฉุกเฉิน
(Backup and IT Continuity Plan)

1. วัตถุประสงค์

เพื่อเป็นแนวทางการสำรองข้อมูลและระบบสารสนเทศของบริษัท รวมทั้งการทดสอบเพื่อเตรียมความพร้อมการกู้คืนระบบสารสนเทศกรณีเกิดเหตุฉุกเฉิน และเพื่อให้ข้อมูลและระบบสารสนเทศมีความพร้อมใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ ในเวลาที่ต้องการ

2. การสำรองข้อมูลและระบบสารสนเทศ

2.1 ผู้ดูแลระบบต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงระบบปฏิบัติการ ฐานข้อมูลโปรแกรมประยุกต์ และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน และสามารถพร้อมใช้งานได้อย่างต่อเนื่อง

2.2 ผู้ดูแลระบบต้องจัดทำวิธีการปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางในการปฏิบัติงาน

2.3 ผู้ดูแลระบบต้องจัดเก็บข้อมูลสำรองไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่ศูนย์ข้อมูลหลักได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีการควบคุมการเข้าออกและการป้องกันความเสียหายทางกายภาพด้วย

2.4 ผู้ดูแลระบบต้องจัดทำขั้นตอนการทำลายข้อมูลสำคัญ และสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่าง ๆ ตามระดับชั้นข้อมูลของบริษัท

3. การเตรียมความพร้อมการกู้คืนระบบกรณีเกิดเหตุฉุกเฉิน

3.1 ต้องจัดทำแผนการกู้คืนระบบสารสนเทศเพื่อรองรับความต่อเนื่องทางธุรกิจของบริษัท

3.2 ต้องปรับปรุงแผนการกู้คืนระบบสารสนเทศให้เป็นปัจจุบันอยู่เสมอ และมีการสื่อความแผนดังกล่าวให้บุคคลที่เกี่ยวข้องได้รับทราบ

3.3 ต้องมีการซ้อมแผนการกู้คืนระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติและต้องมีการบันทึกผลการทดสอบไว้ด้วย

3.4 ผู้ใช้งานต้องให้ความร่วมมือกับบริษัทในการซ้อมแผนการกู้คืนระบบสารสนเทศ หรือแผนการอื่นที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ส่วนที่ 7
การจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้
(Removable Media Handling)

1. วัตถุประสงค์

เพื่อกำหนดเป็นแนวปฏิบัติในการป้องกันการเปิดเผย การดัดแปลง การถอดออก หรือทำลายระบบสารสนเทศที่จัดเก็บบนสื่อบันทึกข้อมูลที่ถอดแยกได้ โดยไม่ได้รับอนุญาต หรือรั่วไหลโดยไม่ได้ตั้งใจ รวมถึงเพื่อลดความเสี่ยงของการแพร่กระจายของโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware) หรือเป็นช่องทางการโจมตีจากผู้ไม่ประสงค์ดี

2. การใช้งานทั่วไป

2.1 ผู้ใช้งานต้องใช้งานสื่อบันทึกข้อมูลที่ถอดแยกได้ที่บริษัทจัดหาให้ ซึ่งมีคุณสมบัติการเข้ารหัสข้อมูลได้ และได้รับการลงทะเบียนจากบริษัทเท่านั้น และไม่เชื่อมต่อสื่อบันทึกข้อมูลที่ถอดแยกได้ของบริษัทกับเครื่องคอมพิวเตอร์ที่ไม่ได้ลงทะเบียนกับบริษัท หรือไม่ได้รับการตรวจสอบความปลอดภัยจากหน่วยงานเทคโนโลยีสารสนเทศ

2.2 ผู้ใช้งานมีหน้าที่รับผิดชอบสื่อบันทึกข้อมูลที่ถอดแยกได้ของบริษัทให้มีความปลอดภัยและพร้อมใช้งานอยู่เสมอ

2.3 เมื่อไม่ต้องการใช้งานแล้ว ผู้ใช้งานจะต้องดำเนินการลบข้อมูล และส่งคืนสื่อบันทึกข้อมูลที่ถอดแยกได้มาที่หน่วยงานเทคโนโลยีสารสนเทศ

2.4 ต้องมีการลงทะเบียนสื่อบันทึกข้อมูลที่ถอดแยกได้ เพื่อให้สามารถติดตามและลดโอกาสการรั่วไหลของข้อมูล

3. การกำจัดสื่อบันทึกข้อมูลที่ถอดแยกได้

สำหรับสื่อบันทึกข้อมูลที่ถอดแยกได้ที่ไม่ได้ใช้งานแล้ว หน่วยงานเทคโนโลยีสารสนเทศจะต้องดำเนินการทำลายข้อมูลในสื่อบันทึกข้อมูลที่ถอดแยกได้

4. การรายงานการสูญหาย

ผู้ใช้งานต้องรายงานการสูญหายของสื่อบันทึกข้อมูลที่ถอดแยกได้มาที่หน่วยงานเทคโนโลยีสารสนเทศทันที

ส่วนที่ 8
การสร้างความตระหนักรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ
(Security Awareness and Training)

1. วัตถุประสงค์

เพื่อกำหนดเป็นแนวปฏิบัติในการสร้างความตระหนักรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศให้แก่ผู้ใช้งานได้อย่างมีประสิทธิภาพ และมีการนำไปปฏิบัติอย่างจริงจัง ผู้ใช้งานจะต้องปฏิบัติตามอย่างเคร่งครัด เพื่อลดความเสี่ยงที่จะเป็นช่องโหว่ให้ผู้ไม่ประสงค์ดีใช้ในการโจมตี และเกิดภัยคุกคามทางไซเบอร์

2. การสร้างความตระหนักรู้และการฝึกอบรม

2.1 หน่วยงานที่รับผิดชอบจัดทำ และทบทวนแผนกลยุทธ์การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศให้แก่ผู้ใช้งานในบริษัท

2.2 หน่วยงานที่รับผิดชอบต้องดำเนินการพัฒนา และปรับปรุงหลักสูตรการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศให้เหมาะสมกับสถานการณ์ปัจจุบัน

2.3 หน่วยงานที่รับผิดชอบต้องดำเนินการจัดอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ และสื่อความข้อกำหนดฉบับนี้ให้แก่ผู้ใช้งานรับทราบ พร้อมทั้งกำหนดเกณฑ์การวัดประสิทธิผลอย่างสม่ำเสมอ

2.4 หน่วยงานที่รับผิดชอบต้องรายงานประสิทธิผลการดำเนินงานการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศให้แก่ผู้บริหารรับทราบ

2.5 ผู้ใช้งานต้องเข้ารับการอบรมและทดสอบการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ

2.6 ในกรณีที่ผู้ใช้งานไม่ผ่านการทดสอบการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศตามเกณฑ์ที่กำหนด หน่วยงานที่รับผิดชอบจะรายงานผลการทดสอบให้หน่วยงานต้นสังกัดรับทราบ และสงวนสิทธิ์ที่จะระงับการใช้งานระบบสารสนเทศชั่วคราว จนกว่าจะผ่านการทดสอบตามเกณฑ์ที่กำหนด

2.7 หน่วยงานที่รับผิดชอบต้องจัดให้มีการฝึกอบรมเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA Awareness Training) แก่พนักงานทุกคนของบริษัท เพื่อให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวกับข้อมูลส่วนบุคคล และเพื่อให้แน่ใจว่าพนักงานของบริษัทจะปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงนโยบายและกระบวนการปฏิบัติงานอันเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของบริษัท ทั้งนี้ หน่วยงานที่รับผิดชอบต้องจัดฝึกอบรมดังกล่าวให้แก่พนักงานใหม่ก่อนที่จะเริ่มทำงาน และจัดฝึกอบรมให้แก่พนักงานทุกคนเป็นประจำทุกปี โดยบริษัทต้องมีการจัดเก็บบันทึกเอกสารในการจัดฝึกอบรมไว้เป็นหลักฐานด้วย

ส่วนที่ 9
การรักษาความมั่นคงปลอดภัยทางไซเบอร์
(Cyber Security)

1. วัตถุประสงค์

เพื่อเป็นแนวปฏิบัติสำหรับการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ให้มีประสิทธิผล มีการจัดการความเสี่ยงอย่างมีประสิทธิภาพ และจัดให้มีการป้องกันภัยคุกคามทางไซเบอร์ที่อาจจะสร้างความเสียหายแก่ระบบสารสนเทศ และส่งผลกระทบต่อการดำเนินงานทางธุรกิจของบริษัทได้อย่างต่อเนื่อง

2. การบริหารจัดการความมั่นคงปลอดภัยด้านไซเบอร์

2.1 หน่วยงานที่รับผิดชอบต้องรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ให้แก่ผู้บริหารรับทราบอย่างสม่ำเสมอ

2.2 ต้องกำหนดมาตรการควบคุม และบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์เพื่อลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์

2.3 ต้องมีการป้องกัน เฝ้าระวัง ตรวจจับการบุกรุก และตอบสนองต่อภัยคุกคามทางไซเบอร์ พร้อมทั้งรายงานผลตรวจสอบให้แก่ผู้บริหารรับทราบอย่างสม่ำเสมอ

2.4 ต้องจัดให้มีการตรวจประเมินช่องโหว่ (Vulnerability Assessment) ระบบสารสนเทศอย่างน้อยปีละ 2 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบสารสนเทศอย่างมีนัยสำคัญ

2.5 ต้องจัดให้มีการทดสอบเจาะระบบ (Penetration Test) สำหรับระบบสารสนเทศที่มีความเสี่ยงจากภัยคุกคามทางไซเบอร์อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบสารสนเทศอย่างมีนัยสำคัญ

2.6 หน่วยงานที่รับผิดชอบต้องจัดทำแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงจัดให้มีการซ้อมแผนอย่างน้อยปีละ 1 ครั้ง และประเมินประสิทธิผลเพื่อนำไปใช้ปรับปรุงแผนการซ้อมในครั้งถัดไป

2.7 ทุกหน่วยงานที่เกี่ยวข้องกับการซ้อมแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ต้องให้ความร่วมมือ สนับสนุนและผลักดันให้เกิดการปฏิบัติอย่างจริงจัง

ส่วนที่ 10
การรักษาความมั่นคงปลอดภัยระบบคลาวด์
(Cloud Security)

1. วัตถุประสงค์

เพื่อเป็นแนวปฏิบัติสำหรับการใช้บริการคลาวด์ ทั้งจากภายในบริษัท และผู้ให้บริการภายนอกให้มีความมั่นคงปลอดภัย ไม่ส่งผลกระทบต่อระบบสารสนเทศของบริษัท

2. การใช้บริการคลาวด์ภายนอก

2.1 หน่วยงานที่รับผิดชอบต้องมีการจัดทำวิธีการปฏิบัติในการบริหารจัดการผู้ให้บริการคลาวด์ภายนอกให้เป็นไปตามหลักการทางด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

2.2 ในการใช้บริการระบบคลาวด์ภายนอก หน่วยงานที่รับผิดชอบต้องเลือกผู้ให้บริการที่ได้รับการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยด้านคลาวด์เช่น Cloud Security Alliance, ISO/IEC 27017 เป็นต้น

2.3 หน่วยงานที่รับผิดชอบต้องจัดให้มีการประเมิน และคัดเลือกผู้ให้บริการคลาวด์ภายนอก

2.4 หน่วยงานที่รับผิดชอบต้องมีสัญญาข้อตกลงการให้บริการ (Service Level Agreement) โดยครอบคลุมด้านความมั่นคงปลอดภัยสารสนเทศและข้อมูลส่วนบุคคล

2.5 หน่วยงานที่รับผิดชอบต้องมีการเฝ้าระวังและทบทวนการทำงานของระบบคลาวด์อย่างสม่ำเสมอ

2.6 หน่วยงานที่รับผิดชอบต้องทำการประเมินการให้บริการผู้ให้บริการคลาวด์ภายนอกอย่างน้อยปีละ 1 ครั้ง

2.7 หน่วยงานที่รับผิดชอบต้องมีการรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident) ที่ส่งผลกระทบต่อการดำเนินธุรกิจให้แก่ผู้บริหารรับทราบ

2.8 หน่วยงานที่รับผิดชอบต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของระบบคลาวด์อย่างสม่ำเสมอ

2.9 ระบบสารสนเทศที่ติดตั้งบนระบบคลาวด์ต้องมีการเข้ารหัสข้อมูลในการรับและส่งข้อมูลผ่านเครือข่ายสาธารณะอย่างเหมาะสม

2.10 กรณีที่มีการย้ายไปใช้บริการผู้ให้บริการคลาวด์ภายนอกรายอื่น ต้องจัดให้มีการคัดลอกหรือโอนถ่ายข้อมูล (Data Portability) ระหว่างระบบคลาวด์ไปสู่ระบบใด ๆ ด้วยวิธีการที่มีความปลอดภัย

2.11 การยกเลิกการใช้บริการระบบคลาวด์ภายนอก หน่วยงานที่รับผิดชอบต้องแจ้งให้ผู้ให้บริการคลาวด์ภายนอกดำเนินการทำลาย หรือลบข้อมูลของบริษัทที่อยู่ในระบบคลาวด์

ส่วนที่ 11
การพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย
(Secure System Development Life Cycle)

1. วัตถุประสงค์

เพื่อให้การพัฒนาระบบสารสนเทศของบริษัทสอดคล้องกับความต้องการของผู้ใช้งาน และมีแนวทางการพัฒนาที่สอดคล้องกับหลักองค์ประกอบด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากลซึ่งเป็นที่ยอมรับ

2. การออกแบบและพัฒนาระบบสารสนเทศ

2.1 หน่วยงานที่รับผิดชอบต้องดำเนินการพัฒนาหรือปรับปรุงระบบสารสนเทศให้สอดคล้องตามมาตรฐานสากล

2.2 หน่วยงานที่รับผิดชอบต้องจัดให้มีวิธีการปฏิบัติการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย โดยต้องครอบคลุมด้านความมั่นคงปลอดภัยสารสนเทศ และข้อมูลส่วนบุคคล

2.3 ผู้ดูแลระบบต้องแยกระบบสารสนเทศที่ให้บริการจริง (Production Environment) ออกจากระบบสารสนเทศสำหรับการทดสอบ (Test Environment) และการพัฒนา (Development Environment)

2.4 ในกรณีการพัฒนาระบบสารสนเทศที่มีการส่งข้อมูลผ่านเครือข่ายสาธารณะ หน่วยงานที่รับผิดชอบต้องมีการประเมินความเสี่ยงการรับส่งและถ่ายโอนข้อมูล รวมทั้งวางมาตรการควบคุมการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม

2.5 หน่วยงานที่รับผิดชอบต้องจัดให้มีการจัดทำคู่มือการปฏิบัติงาน เอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่พัฒนา รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

3. การป้องกันชุดข้อมูลทดสอบ และการทดสอบระบบสารสนเทศก่อนให้บริการ

3.1 ผู้ที่เกี่ยวข้องในการพัฒนาระบบสารสนเทศต้องเข้าร่วมการทดสอบ เพื่อให้มั่นใจว่าระบบสารสนเทศที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ ตรงกับความต้องการและมีความมั่นคงปลอดภัย

3.2 ผู้พัฒนาระบบต้องป้องกันข้อมูลหรือสารสนเทศที่จะนำมาใช้ในการทดสอบระบบสารสนเทศ และควบคุมการนำข้อมูลหรือสารสนเทศมาใช้งานให้มีความมั่นคงปลอดภัยเพื่อป้องกันข้อมูลรั่วไหล

3.3 หน่วยงานที่รับผิดชอบต้องจัดให้มีการทดสอบความมั่นคงปลอดภัยระบบสารสนเทศก่อนให้บริการจริง

4. การควบคุมการเข้าถึงสภาพแวดล้อมการพัฒนาระบบและซอร์สโค้ด

4.1 ในกรณีที่มีการจัดจ้างหน่วยงานภายนอกพัฒนาระบบสารสนเทศ หน่วยงานที่รับผิดชอบต้องกำหนดให้เข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนา (Develop Environment) เท่านั้น

4.2 ผู้ดูแลระบบต้องจัดเตรียมพื้นที่สำหรับการจัดเก็บซอร์สโค้ด และต้องกำหนดสิทธิ์การเข้าถึงให้กับผู้ที่ได้รับอนุญาตเท่านั้น

4.3 ผู้ดูแลระบบต้องจัดให้มีการจัดเก็บข้อมูล Log ในการเข้าถึงและเปลี่ยนแปลงซอร์สโค้ด

ส่วนที่ 12
การรักษาความปลอดภัยข้อมูล
(Data Security)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมสำหรับการบริหารจัดการความมั่นคงปลอดภัยข้อมูลในระบบสารสนเทศให้สอดคล้องตามหลักองค์ประกอบด้านความมั่นคงปลอดภัยสารสนเทศที่ประกอบด้วยความลับ ความถูกต้อง ความพร้อมใช้ และลดความเสี่ยงที่อาจจะก่อให้เกิดความเสียหายต่อการดำเนินธุรกิจของบริษัท

2. การบริหารจัดการเข้าถึงข้อมูล

2.1 ผู้ใช้งานต้องระบุประเภทชั้นความลับของข้อมูลและดำเนินการเข้ารหัสข้อมูลให้มีความเหมาะสมเพื่อป้องกันข้อมูลเปิดเผยหรือรั่วไหล เช่น การใช้ 7-Zip Password เป็นต้น

2.2 ข้อมูลที่อยู่บนระบบงาน และสื่อบันทึกข้อมูล (Data at Rest) ต้องได้รับการออกแบบ และดำเนินการให้มั่นใจว่าข้อมูลถูกเก็บอย่างปลอดภัย มีการกำหนดสิทธิ์ในการเข้าใช้งานอย่างเหมาะสม และต้องได้รับการเข้ารหัสข้อมูลตามมาตรฐานซึ่งเป็นที่ยอมรับของอุตสาหกรรม เช่น การใช้ Advance Encryption Standard 256 (AES256) เป็นต้น

2.3 ผู้ดูแลระบบต้องจัดทำ Encryption Data Matrix โดยระบุถึงชนิดของข้อมูล แหล่งที่จัดเก็บ มาตรการในการควบคุมและการป้องกันข้อมูล และระยะเวลาในการจัดเก็บข้อมูล

2.4 ผู้ดูแลระบบต้องจัดทำรายละเอียด Key Management โดยระบุถึงกระบวนการในการสร้างคีย์ (Key Generation Process) ระยะเวลาในการจัดเก็บคีย์ (Key Retention Period) และกระบวนการในการควบคุมและป้องกันคีย์ (Key Protection Procedure) เพื่อรองรับการเข้ารหัสข้อมูล

2.5 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลโดยผู้ที่มีสิทธิ์และได้รับอนุญาตจากหน่วยงานเจ้าของข้อมูลเท่านั้น

2.6 ระบบสารสนเทศ และฐานข้อมูลต้องมีการปรับตั้งค่าโดยการยกบัญชีรายชื่อแยกจากกันและกำหนดสิทธิ์ให้เหมาะสมกับฟังก์ชันงาน

2.7 ผู้ดูแลระบบต้องจัดให้มีการป้องกันข้อมูลสูญหาย (Data Loss Prevention) เพื่อป้องกันการแบ่งปันข้อมูลบริษัทที่ไม่ได้รับอนุญาต

2.8 หน่วยงานเจ้าของข้อมูลต้องแจ้งให้ผู้ดูแลระบบจัดเก็บข้อมูล และสารสนเทศของบริษัทให้สอดคล้องตามที่กฎหมายกำหนด

2.9 ผู้ดูแลระบบต้องจัดให้มีวิธีการปฏิบัติการเฝ้าระวังและดูแลรักษาการจัดเก็บข้อมูล Log การเข้าถึงข้อมูล และระบบสารสนเทศของบริษัท

3. การแลกเปลี่ยนข้อมูล

3.1 ในกรณีที่ต้องมีการแลกเปลี่ยนข้อมูลบริษัทกับหน่วยงานภายนอกต้องได้รับอนุมัติจากผู้บริหาร และหน่วยงานที่รับผิดชอบต้องดำเนินการประเมินความเสี่ยง กำหนดมาตรการควบคุม พร้อมทั้งจัดให้มีวิธีการแลกเปลี่ยนข้อมูลที่มีความมั่นคงปลอดภัย

3.2 การรับและส่งข้อมูลที่มีความเสี่ยงหรือข้อมูลที่มีความลับผ่านเครือข่ายสาธารณะ ต้องใช้เทคโนโลยีที่มีความปลอดภัย เช่น SSL เป็น Protocol TLS Version 1.2 หรือ Version ที่สูงกว่า และมีการใช้มาตรฐานการเข้ารหัสข้อมูลขั้นสูง ที่เป็นที่ยอมรับของอุตสาหกรรม เช่น Advance Encryption Standard 256 (AES 256) เป็นต้น

3.3 ผู้ใช้งานต้องไม่แบ่งปัน จัดเก็บ และส่งข้อมูลบริษัทผ่านแพลตฟอร์มสาธารณะให้แก่บุคคลที่ไม่ได้รับอนุญาต

3.4 ผู้ใช้งานสามารถแบ่งปัน จัดเก็บ และส่งข้อมูลผ่านแพลตฟอร์มที่บริษัทอนุญาตให้ใช้งานได้เท่านั้น เช่น Microsoft Teams, SharePoint, OneDrive เป็นต้น

4. การสำรองและทำลายข้อมูล

4.1 ผู้ดูแลระบบต้องจัดให้มีวิธีการปฏิบัติการสำรองและการกู้คืนข้อมูลที่จัดเก็บในเครื่องคอมพิวเตอร์แม่ข่าย พร้อมทั้งดำเนินการสำรองข้อมูลอย่างสม่ำเสมอ

4.2 ผู้ดูแลระบบต้องจัดให้มีวิธีการปฏิบัติการทำลายข้อมูลและสื่อบันทึกข้อมูลที่มีประสิทธิผลเพื่อป้องกันข้อมูลบริษัทรั่วไหล

4.3 ผู้ดูแลระบบต้องจัดให้มีการบันทึกหลักฐานการทำลายข้อมูลและสื่อบันทึกข้อมูลเพื่อเก็บไว้เป็นหลักฐานในการตรวจสอบ

5. การควบคุมดูแลหน่วยงานภายนอก

สำหรับการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ต้องดำเนินการโดยหรือดำเนินการร่วมกับหน่วยงานภายนอก บริษัทต้องจัดให้มีการประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล ตามที่ระบุในคู่มือการประเมินคู่ค้าด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Third Party Assessment - Data Privacy Protection)

ส่วนที่ 13
การใช้งานอุปกรณ์แบบพกพาส่วนบุคคล
(Bring Your Own Device Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการในการนำอุปกรณ์แบบพกพาส่วนบุคคลมาใช้งาน หรือเชื่อมต่อกับระบบสารสนเทศของบริษัทและบริษัทในเครือ ให้เป็นไปอย่างราบรื่น มีความมั่นคงปลอดภัย ตลอดจนไม่ส่งผลกระทบต่อการทำงานของระบบสารสนเทศและข้อมูลของบริษัท

2. การร้องขอเข้าใช้งานระบบสารสนเทศ

2.1 การเข้าถึงระบบสารสนเทศหรือข้อมูลสารสนเทศของบริษัท ผู้ใช้งานต้องนำอุปกรณ์แบบพกพาส่วนบุคคลมาลงทะเบียน และติดตั้งระบบบริหารจัดการอุปกรณ์แบบพกพาส่วนบุคคล (Enterprise Mobile Management : EMM)

2.2 หน่วยงานเทคโนโลยีสารสนเทศต้องดำเนินการทบทวน มาตรฐานระบบปฏิบัติการอุปกรณ์แบบพกพาส่วนบุคคลที่กำหนดไว้ในวิธีการปฏิบัติ "P-(G-HC-IT)-002 มาตรฐานการให้บริการระบบสารสนเทศ" อย่างน้อยปีละ 1 ครั้ง

2.3 ผู้ใช้งานต้องทำการปรับปรุงระบบปฏิบัติการ (Update) ของอุปกรณ์แบบพกพาส่วนบุคคลให้สอดคล้องกับมาตรฐานที่ทางบริษัทกำหนดไว้ในวิธีการปฏิบัติ "P-(G-HC-IT)-002 มาตรฐานการให้บริการระบบสารสนเทศ"

2.4 ในกรณีที่มีการเก็บข้อมูลลับของบริษัทในอุปกรณ์แบบพกพาส่วนบุคคล ผู้ใช้งานต้องดำเนินการตามการกำหนดชั้นความลับ และการรักษาความปลอดภัยเกี่ยวกับเอกสารของบริษัท และต้องมีการเข้ารหัสเพื่อป้องกันข้อมูลรั่วไหล

3. การรับผิดชอบต่ออุปกรณ์แบบพกพาส่วนบุคคลที่มีข้อมูลสารสนเทศของบริษัท

3.1 กรณีเกิดการสูญหายหรือถูกขโมย

3.1.1 ผู้ใช้งานต้องรายงานการสูญหาย หรือถูกขโมยของอุปกรณ์สื่อสารพกพาส่วนบุคคลมายังหน่วยงานเทคโนโลยีสารสนเทศ นับแต่ทราบเหตุการณ์สูญหายหรือถูกขโมยนั้น เพื่อทำการลบข้อมูลสารสนเทศของบริษัท ก่อนที่จะแจ้งไปยังเครือข่ายผู้ให้บริการโทรศัพท์

3.1.2 บริษัทมีสิทธิ์ลบข้อมูลสารสนเทศของบริษัท ในอุปกรณ์แบบพกพาส่วนบุคคลเมื่อเกิดการสูญหาย หรือถูกขโมย

3.1.3 กรณียกเลิกหรือเปลี่ยนอุปกรณ์แบบพกพาส่วนบุคคล ผู้ใช้งานต้องรายงานการยกเลิกหรือเปลี่ยนอุปกรณ์แบบพกพาส่วนบุคคลมายังหน่วยงานเทคโนโลยีสารสนเทศล่วงหน้า

3.2 ผู้ใช้งานสามารถดาวน์โหลดและติดตั้งแอปพลิเคชันจากแอปพลิเคชันสโตร์มาตรฐาน เช่น Apple Store และ Play Store

3.3 ผู้ใช้งานมีหน้าที่รับผิดชอบในการสำรองข้อมูลส่วนบุคคลทั้งหมด บริษัทไม่รับรองความเสียหายจากการลบข้อมูล และแอปพลิเคชันบนอุปกรณ์แบบพกพาส่วนบุคคล หากเห็นว่ามีความจำเป็นต้องดำเนินการ เพื่อปกป้องข้อมูลสารสนเทศของบริษัท ถึงแม้ว่าข้อมูลจะถูกลบโดยไม่ได้เจตนาก็ตาม

3.4 การบริหารจัดการฟังก์ชันการทำงานของอุปกรณ์แบบพกพาส่วนบุคคล

3.4.1 ผู้ใช้งานต้องลบ หรือแจ้งให้หน่วยงานเทคโนโลยีสารสนเทศ ทำการลบข้อมูลสารสนเทศของบริษัท ออกจากอุปกรณ์แบบพกพาส่วนบุคคลเครื่องเดิมก่อนที่จะส่งมอบให้แก่ผู้อื่นไม่ว่าด้วยวิธีใดๆ

3.4.2 บริษัทไม่อนุญาตให้เครื่องที่มีการ Jailbreak หรือ Root หรือดัดแปลงแก้ไขระบบรักษาความปลอดภัยของอุปกรณ์แบบพกพาส่วนบุคคลเข้าใช้งาน

3.4.3 ผู้ใช้งานต้องระมัดระวังการนำอุปกรณ์แบบพกพาส่วนบุคคลให้บุคคลอื่นใช้งานและผู้ใช้งานต้องรับผิดชอบในการกระทำที่ใช้งานผ่านชื่อของผู้ใช้งาน และต้องไม่แจ้งรหัสผ่าน ตลอดจนข้อมูลส่วนบุคคลอื่น ๆ ของผู้ใช้งานให้บุคคลอื่นทราบ

3.5 การรักษาความปลอดภัยของอุปกรณ์แบบพกพาส่วนบุคคลและข้อมูลสารสนเทศ

3.5.1 ผู้ใช้งานต้องระมัดระวังการนำอุปกรณ์แบบพกพาส่วนบุคคลให้บุคคลอื่นใช้งานและผู้ใช้งานต้องรับผิดชอบในการกระทำที่ใช้งานผ่านชื่อของผู้ใช้งาน และต้องไม่แจ้งรหัสผ่าน ตลอดจนข้อมูลส่วนบุคคลอื่น ๆ ของผู้ใช้งานให้บุคคลอื่นทราบ

3.5.2 ผู้ใช้งานต้องปรับปรุงให้อุปกรณ์แบบพกพาส่วนบุคคลเป็นไปตามมาตรฐานของบริษัทตลอดเวลา ตามที่กำหนดไว้ใน Procedure "P-(G-HC-IT)-002 มาตรฐานการให้บริการระบบสารสนเทศ"

3.5.3 ผู้ใช้งานต้องมีการตั้งรหัสผ่านหรือวิธีการพิสูจน์ตัวตนก่อนเข้าใช้งานอุปกรณ์แบบพกพาส่วนบุคคล

3.5.4 ผู้ใช้งานต้องมีการตั้งค่าให้มีการพักหน้าจอ (Display Auto Lock (iOS), Screen Timeout (Android)) โดยอัตโนมัติ เมื่อไม่ได้มีการใช้งานเกินกว่า 5 นาที

3.5.5 ผู้ใช้งานต้องไม่วางอุปกรณ์แบบพกพาส่วนบุคคลไว้ให้มองเห็นได้ง่าย แม้จะเป็นระยะเวลาไม่นาน และต้องไม่ทิ้งอุปกรณ์สื่อสารไว้ในยานพาหนะตลอดคืน

3.5.6 ในขณะที่ใช้งานอุปกรณ์แบบพกพาส่วนบุคคล เพื่อแสดงผลข้อมูลที่เป็นความลับของบริษัทและบริษัทในเครือในพื้นที่สาธารณะ เช่น บนรถไฟ เครื่องบิน หรือร้านกาแฟ ผู้ใช้งานต้องวางอุปกรณ์ให้ผู้อื่นไม่สามารถมองเห็นหน้าจอได้ เพื่อปกป้องข้อมูลสารสนเทศของบริษัทและบริษัทในเครือ หรือปรับแสงหน้าจอให้อ่อน ๆ หรือใช้แผ่นกรองแสงชนิดพิเศษ เพื่อลดหรือป้องกันการมองเห็นหน้าจอในบางมุมมองได้

4. การช่วยเหลือทางเทคนิคและเงื่อนไขในการให้ความช่วยเหลือ

4.1 พนักงาน Service Desk จะให้ความช่วยเหลือทางเทคนิคสำหรับอุปกรณ์แบบพกพาส่วนบุคคลที่ได้รับอนุญาตให้เชื่อมต่อกับระบบเครือข่ายของบริษัท ระบบสารสนเทศ หรือแอปพลิเคชันที่ใช้ในการทำงาน และเรื่องที่เกี่ยวกับการปฏิบัติงานให้กับบริษัทเท่านั้น

4.2 พนักงาน Service Desk จะไม่ให้การช่วยเหลือในเรื่องของการให้อุปกรณ์ทดแทน การอัพเกรดอุปกรณ์ การใช้งานอุปกรณ์แบบพกพาส่วนบุคคล หรือการใช้งานแอปพลิเคชันอื่น ๆ ที่ไม่เกี่ยวข้องกับการปฏิบัติงานให้กับบริษัทฯ

4.3 พนักงาน Service Desk จะให้การช่วยเหลือเฉพาะเรื่องแอปพลิเคชันของบริษัท และการนำข้อมูลสารสนเทศของบริษัทใส่ลงในอุปกรณ์แบบพกพาส่วนบุคคลเท่านั้น สำหรับปัญหาอื่นใดนอกเหนือจากที่กล่าวมา จะต้องสอบถามไปทางผู้ให้บริการเครือข่าย หรือร้านค้าปลีกที่จำหน่ายอุปกรณ์โดยตรง

5. การเข้าถึงข้อมูลส่วนบุคคล

บริษัทจะไม่เข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานจากอุปกรณ์แบบพกพาส่วนบุคคลของผู้ใช้งาน และนำไปเปิดเผยแก่บุคคลที่สาม เว้นแต่จะได้รับอนุญาตจากผู้ใช้งานเป็นลายลักษณ์อักษร ยกเว้นในกรณีที่บริษัทได้รับการร้องขอเป็นลายลักษณ์อักษรจากหน่วยงานราชการที่เกี่ยวข้อง

6. การสิ้นสุดการจ้างงาน

6.1 เมื่อผู้ใช้งานสิ้นสุดการจ้างงาน บริษัทจะทำการลบข้อมูลสารสนเทศของบริษัทและบริษัทในเครือบนอุปกรณ์แบบพกพาส่วนบุคคลทั้งหมด

6.2 ผู้ใช้งานที่สิ้นสุดการจ้างงานไปแล้วจะไม่มีสิทธิในการกู้คืนข้อมูลสารสนเทศของบริษัทและบริษัทในเครือ และแอปพลิเคชันต่าง ๆ ที่เกิดขึ้นระหว่างการทำงานให้กับบริษัท ความพยายามในการกู้คืนข้อมูลใด ๆ ของบริษัท ถือเป็นความผิดของผู้ใช้งาน

หมวดที่ 3
เรื่องการตรวจสอบและการปฏิบัติตามนโยบาย

ข้อ 7 ให้มีการตรวจสอบการปฏิบัติงานตามนโยบายและรายงานผลตามวิธีการของการตรวจสอบภายในตามหลักมาตรฐานระบบบริหารความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

ข้อ 8 ให้หน่วยงานเทคโนโลยีสารสนเทศทำหน้าที่เสนอทบทวน หรือปรับปรุงนโยบายและข้อปฏิบัติของนโยบายนี้เป็นประจำทุกปี โดยรายงานผลการตรวจสอบภายในที่เสนอมา ถือเป็นส่วนหนึ่งของสิ่งที่ต้องนำมาทบทวนด้วย

ข้อ 9 ผู้ใช้งานที่ฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายนี้ รวมถึงหลักเกณฑ์ แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ซึ่งออกตามความในนโยบายนี้ ให้ถือว่าเป็นความผิดทางวินัย และต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นกับบริษัทและบุคคลอื่น

ทั้งนี้ มีผลตั้งแต่วันที่ 1 ตุลาคม พ.ศ. 2565 เป็นต้นไป

ประกาศ ณ วันที่ 12 ตุลาคม พ.ศ. 2565

(นายไพโรจน์ สมุทรธนานนท์)
กรรมการผู้จัดการ