ประกาศสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น

ฉบับที่ 7 / 2568

เรื่อง นโยบายการใช้ระบบเทคโนโลยีสารสนเทศ เพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน

(Acceptable Use Policy)

.....

สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น ได้เล็งเห็นว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022 เป็นมาตรฐานที่ได้รับการยอมรับอย่างแพร่หลายในระดับสากลและเหมาะสมต่อการนำมาประยุกต์ใช้ภายในหน่วยงาน จึงได้ดำเนินการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐานสากล ISO/IEC 27001:2022 ขึ้นอย่างเป็นทางการ

จากการพิจารณาการศึกษาบริบทของสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น พบว่ามีความต้องการและความมุ่งมั่นในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบ เพื่อเสริมสร้างความเชื่อมั่นแก่ผู้ใช้งานระบบสารสนเทศของมหาวิทยาลัยขอนแก่น ให้มีความมั่นคงปลอดภัย การดำเนินงานดังกล่าวยังมีเป้าหมายเพื่อให้สอดคล้องกับวิสัยทัศน์และพันธกิจของสำนักฯ รวมถึงเป็นไปตามข้อกำหนด ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด โดยสำนักฯ ได้นำมาตรฐาน ISO/IEC 27001:2022 มาใช้เป็นกรอบสำคัญในการกำหนดแนวทางและพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้มีประสิทธิภาพและยั่งยืน

อาศัยอำนาจตามความในมาตรา 40 แห่งพระราชบัญญัติมหาวิทยาลัยขอนแก่น พ.ศ. 2558 สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น จึงออกประกาศนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น เรื่อง นโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน”

ข้อ 2 ให้ประกาศมีผลบังคับใช้ถัดจากวันประกาศเป็นต้นไป

/ข้อ 3 นโยบาย...

ข้อ 3 นโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน ได้กำหนดขึ้น โดยมีวัตถุประสงค์เพื่ออำนวยความสะดวกในการติดต่อสื่อสารหรือการเผยแพร่แลกเปลี่ยนข้อมูลต่าง ๆ ภายในและภายนอกองค์กร ให้กับพนักงานในการปฏิบัติงานขององค์กร และบุคคลภายนอกที่ได้รับอนุญาตให้ใช้งาน เพื่อประโยชน์ขององค์กร ดังนั้น เพื่อให้การใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความปลอดภัย และถูกต้องตามกฎหมายต่าง ๆ ที่เกี่ยวข้อง รวมถึงเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง องค์กรจึงได้กำหนดนโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งานขึ้นไว้ภายใต้ขอบเขตการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ สำหรับการให้บริการด้านเทคโนโลยีสารสนเทศงานโครงสร้างพื้นฐานระบบดิจิทัล สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น

ข้อ 4 นโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน ประกอบด้วย

1) หมวดที่ 1 คำนิยามศัพท์
2) หมวดที่ 2 นโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน

ประกาศ ณ วันที่ สิงหาคม พ.ศ. 2568

(ผู้ช่วยศาสตราจารย์พิพัธน์ เรืองแสง)
ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล

เอกสารแนบท้ายประกาศ

นโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน

สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น

พ.ศ. 2568

หมวดที่ 1 คำนิยามศัพท์

1) **องค์กร** หมายความว่า สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น

2) **ผู้บังคับบัญชา** หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

3) **ผู้ดูแลระบบ** หมายความว่า พนักงานภายใต้ งานโครงสร้างพื้นฐานระบบดิจิทัล สำนักเทคโนโลยีดิจิทัล ซึ่งเป็นผู้ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ รวมถึงห้องคอมพิวเตอร์และอุปกรณ์เครือข่าย ซึ่งสามารถเข้าถึงโปรแกรม อุปกรณ์เครือข่ายคอมพิวเตอร์ และระบบสนับสนุนห้องคอมพิวเตอร์และอุปกรณ์เครือข่าย เพื่อการจัดการระบบเทคโนโลยีสารสนเทศขององค์กร

4) **บุคลากร** หมายความว่า ผู้ปฏิบัติงานในมหาวิทยาลัย ได้แก่ พนักงานมหาวิทยาลัย ข้าราชการ ลูกจ้างของส่วนราชการ พนักงานราชการ และลูกจ้างของมหาวิทยาลัยที่เกี่ยวข้องกับการให้บริการภายใต้ขอบเขตการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัล

5) **ผู้ใช้งาน** หมายความว่า บุคลากรของสำนักเทคโนโลยีดิจิทัล รวมถึงบุคลากรภายนอกที่ได้รับอนุญาตจากองค์กรให้ใช้งานระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ของสำนักเทคโนโลยีดิจิทัล

6) **บุคลากรภายนอก** หมายความว่า หน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิเข้าถึง และใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของสำนักเทคโนโลยีดิจิทัล ตามอำนาจหน้าที่ที่รับผิดชอบ

7) **ผู้ให้บริการภายนอก** หมายความว่า ผู้ให้บริการจากภายนอกซึ่งเป็นคู่สัญญากับองค์กร ได้แก่ กลุ่มผู้ให้บริการด้านฮาร์ดแวร์ ซอฟต์แวร์ ระบบคลาวด์ (Cloud) ระบบสาธารณูปโภค และบุคคลที่ปฏิบัติหน้าที่ตามสัญญาจ้างขององค์กรที่เกี่ยวข้องกับการให้บริการภายใต้ขอบเขตการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีดิจิทัล

8) **ทรัพย์สินสารสนเทศ** หมายความว่า

(1) ทรัพย์สินสารสนเทศประเภทระบบ ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบงาน

(2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ซึ่งได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วงคอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(3) ทรัพย์สินสารสนเทศประเภทข้อมูล ซึ่งได้แก่ ข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์

9) **ข้อมูลคอมพิวเตอร์** หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยการผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพ หรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

10) **ระบบคอมพิวเตอร์** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

11) **ระบบเทคโนโลยีสารสนเทศ** หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

12) **ระบบเครือข่ายคอมพิวเตอร์** หมายความว่า ระบบการเชื่อมโยงระหว่างคอมพิวเตอร์ตั้งแต่สองเครื่องขึ้นไป โดยใช้สื่อกลาง และสามารถสื่อสารแลกเปลี่ยนข้อมูลกันทางอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพ และสามารถใช้ทรัพยากรที่อยู่ในเครือข่ายร่วมกันได้

13) **ระบบอินเทอร์เน็ต** หมายความว่า ระบบเครือข่ายที่มีการเชื่อมโยงเครือข่ายมากมายทั่วโลกเข้าด้วยกัน และเป็นแหล่งข้อมูลขนาดใหญ่ ที่มีข้อมูลในทุก ๆ ด้าน ให้ผู้ที่สนใจเข้าไปศึกษาค้นคว้าได้อย่างสะดวกและรวดเร็ว

14) **อุปกรณ์คอมพิวเตอร์แบบพกพา** หมายความว่า เครื่องคอมพิวเตอร์พกพา (Laptop computer) สมาร์ทโฟน (Smartphone) แท็บเล็ตคอมพิวเตอร์ (Tablet computer) ที่องค์กรอนุญาตให้เชื่อมต่อและใช้งานสารสนเทศขององค์กรได้

15) **สื่อบันทึกข้อมูล** หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Hard disk, Flash drive, Thumb drive, CD, DVD และ External hard disk เป็นต้น

หมวดที่ 2 นโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน

ผู้ใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ขององค์กร มีหน้าที่และความรับผิดชอบที่จะต้องปฏิบัติตามนโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งานฉบับนี้โดยเคร่งครัด ดังนี้

- การเข้าใช้งานใด ๆ ในระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ขององค์กร ให้ถือว่าผู้ใช้งานแสดงเจตนายอมรับ และจะปฏิบัติตามนโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งาน รวมทั้งกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายที่เกี่ยวข้อง
- องค์กรไม่สนับสนุนและไม่ยินยอมให้ผู้ใช้งานกระทำการหรืองดเว้นกระทำการใด ๆ อันเป็นการขัดต่อบทบัญญัติแห่งกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายที่เกี่ยวข้อง โดยถือว่าเป็นการกระทำส่วนบุคคลของผู้ใช้งาน
- องค์กรจัดหาระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ เพื่อให้บริการที่เกี่ยวข้องกับกิจการขององค์กรเท่านั้น ไม่อนุญาตให้ใช้เพื่อการอื่นใดที่ไม่เกี่ยวข้องกับกิจการหรือประโยชน์ขององค์กร
- องค์กรสงวนสิทธิในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอื่นใดอันสมควร หากพบว่ามีการละเมิดนโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยสำหรับผู้ใช้งานฉบับนี้ รวมทั้งกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายที่เกี่ยวข้อง

นอกจากนี้ ผู้ใช้งานจะต้องยึดถือและปฏิบัติตามข้อกำหนดต่าง ๆ ในการใช้ระบบเทคโนโลยีสารสนเทศ ดังต่อไปนี้

ข้อ 1 การใช้งานทรัพย์สินสารสนเทศ

1) ผู้ใช้งานสามารถถือครองอุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์โน๊ตบุ๊ค (Notebook) หรือคอมพิวเตอร์ตั้งโต๊ะ (PC/All in one PC) เพื่อใช้งานในกิจการขององค์กร โดยให้ขึ้นอยู่กับดุลพินิจของผู้บริหารระดับฝ่าย
2) ผู้ใช้งานมีหน้าที่ต้องดูแลรักษาและรับผิดชอบต่อการชำชุดเสียหายหรือการสูญหายของทรัพย์สินสารสนเทศ และ/หรืออุปกรณ์เทคโนโลยีสารสนเทศที่องค์กรมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง
3) ผู้ใช้งานมีหน้าที่ต้องชดใช้ให้แก่องค์กร ซึ่งค่าเสียหายอันเกิดจากการชำรุดเสียหายหรือการสูญหายของทรัพย์สินสารสนเทศ และ/หรืออุปกรณ์เทคโนโลยีสารสนเทศที่องค์กรมอบไว้ให้ใช้งานตามมูลค่าทรัพย์สินหรือค่าเสียหายที่เกิดขึ้นตามจริง หากความเสียหายนั้นเกิดจากสาเหตุดังนี้
    3.1) เกิดจากความจงใจ หรือประมาทเลินเล่อของผู้ใช้งาน
    3.2) เกิดจากการใช้งานผิดวัตถุประสงค์ หรือใช้งานที่ไม่ใช่เพื่อกิจการขององค์กร
    3.3) เกิดจากอนุญาตให้ผู้อื่น ทั้งที่เป็นบุคลากรในองค์กร หรือไม่ได้เป็นบุคลากรในองค์กรนำไปใช้งาน ยกเว้นได้รับเอกสารยินยอมให้บุคคลอื่นที่ไม่ใช่ผู้ถือครองนำอุปกรณ์คอมพิวเตอร์ไปใช้งานและได้รับอนุมัติโดยผู้บริหารระดับฝ่าย
4) ผู้ใช้งานจะต้องใช้ทรัพย์สินสารสนเทศ และ/หรืออุปกรณ์เทคโนโลยีสารสนเทศที่องค์กรจัดเตรียมไว้ให้สำหรับการดำเนินกิจการขององค์กรเท่านั้น ห้ามมิให้ผู้ใช้งานนำไปใช้งานที่ไม่เกี่ยวข้องกับองค์กร หรือติดตั้งซอฟต์แวร์ หรืออุปกรณ์ฮาร์ดแวร์อื่นใดเพื่อใช้งานในกิจการอื่น ๆ โดยเด็ดขาดไม่ว่าจะก่อให้เกิดความเสียหายหรือไม่ก็ตาม
5) ผู้ใช้งานที่เป็นผู้ถือครองอุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์โน๊ตบุ๊ค (Notebook) หรือคอมพิวเตอร์ตั้งโต๊ะ (PC/All in one PC) สามารถใช้งานโปรแกรมคอมพิวเตอร์ที่ถูกลิขสิทธิ์ตามที่มหาวิทยาลัยกำหนดเพื่อติดตั้งในเครื่องเท่านั้น สามารถศึกษาได้จากตามเว็บไซต์ software.kku.ac.th หากตรวจพบการติดตั้งใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์ในอุปกรณ์คอมพิวเตอร์ดังกล่าว ถือว่าเป็นการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัยขององค์กร ถึงแม้ว่าการละเมิดนั้นจะเป็นไปเพื่อการปฏิบัติงานขององค์กรก็ตาม ผู้ใช้งานต้องรับผิดชอบผลของความเสียหายที่เกิดขึ้นทั้งหมดแต่เพียงผู้เดียว
6) ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ถือเป็นทรัพย์สินขององค์กร ผู้ถือครองต้องรับผิดชอบดูแลและห้ามไม่ให้ทำการคัดลอกหรือทำซ้ำข้อมูลดังกล่าวให้แก่ผู้อื่นหรือหน่วยงานภายนอก ยกเว้นได้รับเอกสารยินยอมและอนุมัติโดยผู้บริหารระดับฝ่าย

7) เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งให้ฝ่ายโครงสร้างพื้นฐาน สำนักเทคโนโลยีสารดิจิทัลทราบเพื่อดำเนินการแก้ไขโดยทันที

8) ผู้ใช้งาน/ผู้ถือครองเครื่องคอมพิวเตอร์ต้องกำหนดให้มีการล็อคหน้าจอโดยรหัสผ่าน เมื่อไม่มีการใช้งานเกินกว่า 15 นาที

9) ผู้ใช้งานมีหน้าที่ในการดูแลรักษาข้อมูลคอมพิวเตอร์ซึ่งจัดเก็บอยู่ภายในเครื่องคอมพิวเตอร์ โดยการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ เพื่อสามารถเรียกข้อมูลคอมพิวเตอร์กลับมาใช้งานเมื่อเกิดปัญหาข้อมูลสูญหายหรือเสียหาย

10) ผู้ใช้งานต้องไม่ทิ้งเอกสารสำคัญหรือสื่อบันทึกข้อมูลไว้ที่โต๊ะทำงานโดยไม่มีผู้ดูแลหรือไม่ได้ใช้งาน และต้องจัดหาสถานที่จัดเก็บอย่างปลอดภัย เช่น เก็บในตู้ที่มีอุปกรณ์ล็อค เป็นต้น

11) ผู้ใช้งานต้องไม่ทิ้งเอกสารสำคัญไว้ที่เครื่องถ่ายเอกสาร เครื่องปริ้นเตอร์ หรือเครื่องสแกนเนอร์ เมื่อสั่งพิมพ์หรือสำเนาเรียบร้อยแล้วต้องเก็บเอกสารทันที

12) เมื่อหมดความจำเป็นในการใช้งานข้อมูล ผู้ใช้งานต้องดำเนินการทำลายข้อมูลที่อยู่ในสื่อบันทึกข้อมูลทันที โดยผู้ใช้งานต้องทำการตรวจสอบประเภทของข้อมูลบนสื่อบันทึกข้อมูล และคัดแยกสื่อบันทึกข้อมูลออกตามหมวดหมู่หรือประเภทตามลำดับชั้นความลับ และเลือกวิธีการทำลายข้อมูลตามลำดับชั้นความลับที่องค์กรกำหนดไว้

13) ห้ามผู้ใช้งานบันทึกไฟล์ข้อมูล อาทิ เพลง ภาพ วิดีโอ ภาพยนต์ ที่ไม่ถูกลิขสิทธิ์ไว้ในเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์โน๊ตบุ๊ค (Notebook) หรือคอมพิวเตอร์ตั้งโต๊ะ (PC/All in one PC) ขององค์กร โดยหากฝ่ายโครงสร้างพื้นฐาน สำนักเทคโนโลยีสารดิจิทัล ตรวจพบจะดำเนินการแจ้งเตือนให้ลบทิ้งโดยทันที

14) ห้ามผู้ใช้งานนำเอกสารที่มีข้อมูลสำคัญกลับมาใช้ซ้ำ (Reuse)

15) ห้ามผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่ายคอมพิวเตอร์อื่นในขณะที่มีการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ขององค์กรในเวลาเดียวกัน เพื่อป้องกันการบุกรุกหรือภัยคุกคามจากภายนอกเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กร

16) ห้ามผู้ใช้งานนำอุปกรณ์เครือข่ายไร้สาย (Wireless) มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access Point, Wireless Router

17) ผู้ใช้งานต้องทำลายข้อมูลสำคัญซึ่งอยู่บนกระดาษหรือวัสดุชั่วคราว เช่น CD/DVD เป็นต้น เมื่อหมดความจำเป็นต้องใช้งาน โดยทำให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้และไม่สามารถนำกลับมาใช้ใหม่ได้

18) ผู้ใช้งานจะต้องคืนทรัพย์สินสารสนเทศ และ/หรือ อุปกรณ์เทคโนโลยีสารสนเทศให้แก่องค์กรในทันที ณ วันที่หมดความจำเป็นที่ต้องใช้งาน หรือวันที่เปลี่ยนแปลงหน้าที่การทำงาน หรือวันที่พ้นสภาพการเป็นลูกจ้างขององค์กร หรือเมื่อองค์กรมีคำสั่งให้ส่งคืนอุปกรณ์

ข้อ 2 การกำหนดรหัสผ่านและการใช้รหัสผ่าน

1) ผู้ใช้งานต้องกำหนดรหัสผ่านในการเข้าใช้งานระบบคอมพิวเตอร์ หรือแอพพลิเคชั่นขององค์กร ดังนี้

   1.1) ตัวอักขระมีความยาวไม่น้อยกว่า 8 ตัวอักขระ

   1.2) ตัวอักขระต้องมีการผสมกันระหว่างตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ เช่น % $ # * ! เป็นต้น เข้าด้วยกัน เพื่อลดโอกาสของความสำเร็จในการคาดเดารหัสผ่าน

   1.3) ผู้ใช้งานจะต้องไม่ใช้โครงสร้างรหัสผ่านหรือคุณลักษณะที่ง่ายต่อการเดา อาทิ

   - การใช้อักขระเรียงลำดับหรือกลุ่มเหมือนกัน เช่น abc1234 หรือ aabb4321 เป็นต้น
   - การใช้คำที่มีอยู่ในพจนานุกรม เช่น password หรือ hello เป็นต้น
   - การใช้คำที่เกี่ยวข้องกับองค์กร เช่น ชื่อองค์กร ชื่อหน่วยงาน รหัสพนักงาน เป็นต้น
   - การใช้ข้อมูลส่วนบุคคล เช่น ชื่อ เบอร์โทรศัพท์ วันเดือนปีเกิด เป็นต้น
   - การคัดลอกหรือผสมจากชื่อผู้ใช้ ข้อมูลส่วนบุคคล หรือประโยควลีใด ๆ ที่สามารถคาดเดาได้ง่าย

2) ผู้ใช้งานต้องบริหารจัดการการใช้งานรหัสผ่านสำหรับเข้าถึงระบบคอมพิวเตอร์ หรือแอพพลิเคชั่นขององค์กร ดังนี้

   2.1) เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีที่ทำการล็อคอินเข้าสู่เครื่องคอมพิวเตอร์หรือระบบงานครั้งแรก หรือหลังจากที่ผู้ดูแลระบบเปลี่ยนรหัสผ่านใหม่ให้ (Reset Password)

   2.2) ไม่ควรใช้รหัสผ่านที่เป็นรหัสผ่านตั้งต้น (Default Password)

   2.3) บังคับให้มีการใช้งานพิสูจน์ตัวตนแบบหลายขั้นตอนทุกบัญชีผู้ใช้งาน Multi-Factor Authentication (MFA)

   2.4) เปลี่ยนแปลงรหัสผ่านทุกครั้งเมื่อได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่าน เมื่อทราบหรือสงสัยว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือมีผู้อื่นล่วงรู้

   2.5) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

   2.6) ไม่ควรใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

   2.7) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

   2.8) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากการปฏิบัติงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

2.9) ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำทุกอย่างที่เกิดขึ้นหากการกระทำนั้นสามารถบ่งชี้ให้เห็นว่าเกิดจากบัญชีผู้ใช้งานนั้น และจะต้องไม่อนุญาตให้ผู้อื่นกระทำการใด ๆ โดยใช้บัญชีผู้ใช้งานของตน หรือกระทำการใด ๆ โดยใช้บัญชีผู้ใช้งานอื่นที่ไม่มีสิทธิ์

2.10) กรณีที่ผู้ใช้งานระบุรหัสผ่านเข้าระบบผิดเกิน 5 ครั้ง ระบบจะระงับสิทธิ์การเข้าใช้งานในทันที และจะทำการปลดล็อคเมื่อระยะเวลาผ่านไป 30 นาที โดยอัตโนมัติ หรือผู้ใช้งานสามารถติดต่อผู้ดูแลระบบเพื่อขอเปิดสิทธิการใช้งานตามกระบวนการที่องค์กรกำหนด

ข้อ 3 การเข้าถึงและการใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์

1) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ขององค์กรต้องกรอก “แบบฟอร์มขอสร้าง เปลี่ยนแปลง และยกเลิกสิทธิผู้ใช้งานระบบ” หรือร้องขอผ่านทางระบบอิเล็กทรอนิกส์ และขออนุมัติการใช้งานจากผู้มีอำนาจอนุมัติ เพื่อให้งานโครงสร้างพื้นฐานระบบดิจิทัล สำนักเทคโนโลยีดิจิทัล กำหนดสิทธิ์การเข้าถึง
2) <u>ห้าม</u> ผู้ใช้งานกระทำการใด ๆ ดังต่อไปนี้
   2.1) ล่วงรู้ข้อมูลบัญชีผู้ใช้และรหัสผ่านของผู้อื่น รวมถึงนำบัญชีผู้ใช้และรหัสผ่านของผู้อื่นไปใช้งาน
   2.2) อนุญาตให้ผู้อื่นใช้ร่วม เผยแพร่ แจกจ่าย หรือทำให้ล่วงรู้บัญชีผู้ใช้และรหัสผ่านของตน
3) ผู้ใช้งานต้องป้องกันและดูแลรักษาข้อมูลบัญชีผู้ใช้และรหัสผ่านของตน หากทราบว่าข้อมูลบัญชีผู้ใช้ และ/หรือรหัสผ่านถูกเปิดเผยต้องเปลี่ยนรหัสผ่านใหม่ทันที
4) ผู้ใช้งานจะต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ระบบคอมพิวเตอร์ขององค์กร และหากพบว่าการพิสูจน์ตัวตนนั้นไม่สามารถกระทำการได้สำเร็จ เช่น ลืมรหัสผ่าน รหัสผ่านโดนล็อค หรือเกิดจากปัญหาหรือข้อผิดพลาดใด ๆ ผู้ใช้งานจะต้องแจ้งงานโครงสร้างพื้นฐานระบบดิจิทัล สำนักเทคโนโลยีดิจิทัลโดยทันที
5) ผู้ใช้งานจะต้องทำการล็อคหน้าจอเครื่องคอมพิวเตอร์ด้วยรหัสผ่านทุกครั้งเมื่อไม่ได้ใช้งาน และต้องทำการพิสูจน์ตัวตนเมื่อกลับมาใช้งานเครื่องคอมพิวเตอร์
6) ผู้ใช้งานต้องออกจากระบบงานเมื่อสิ้นสุดหรือไม่มีความจำเป็นต้องใช้งาน
7) ผู้ใช้งานต้องปิดเครื่องคอมพิวเตอร์เมื่อการปฏิบัติงานประจำวันเสร็จสิ้น
8) ผู้ใช้งานต้องกำหนดรหัสผ่านและใช้รหัสผ่านตามข้อกำหนด ข้อ 2. การกำหนดรหัสผ่านและการใช้รหัสผ่าน
9) เมื่อพบว่าระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์มีความผิดปกติ หรือบกพร่อง หรือไม่เอื้ออำนวยต่อการปฏิบัติงาน ให้รายงานความบกพร่องหรือปัญหาที่เกิดขึ้นต่อผู้บังคับบัญชาหน่วยงาน และงานโครงสร้างพื้นฐานระบบดิจิทัล สำนักเทคโนโลยีดิจิทัล เพื่อดำเนินการแก้ไขโดยทันที

10) ผู้ใช้งานที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในองค์กรต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชาและและงานโครงสร้างพื้นฐานระบบดิจิทัล สำนักเทคโนโลยีดิจิทัล รวมถึงห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

11) ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำใด ๆ ในระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ขององค์กรที่เกิดขึ้นจากบัญชีชื่อผู้ใช้งาน และ/หรือรหัสผ่านของผู้ใช้งานนั้น ไม่ว่าการกระทำนั้น ๆ จะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ 4 การใช้งานจดหมายอิเล็กส์ทรอนิกส์ (E-mail), โปรแกรมการสนทนา (Chat) และการติดต่อสื่อสารทางอิเล็กส์ทรอนิกส์อื่น ๆ

สำนักเทคโนโลยีดิจิทัล ได้จัดสรรให้บุคลากรขององค์กรมีบัญชีจดหมายอิเล็กทรอนิกส์ส่วนบุคคล และโปรแกรมการสนทนาเฉพาะที่องค์กรกำหนดไว้เท่านั้น ได้แก่ Google Chat เพื่อใช้ในการปฏิบัติงานขององค์กร ดังนั้นบุคลากรต้องใช้จดหมายอิเล็กทรอนิกส์และโปรแกรมการสนทนาดังกล่าวอย่างระมัดระวังและปฏิบัติตามระเบียบ ดังต่อไปนี้

1) เมื่อผู้ใช้งานได้รับบัญชีผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ให้ผู้ใช้งานเข้าใช้งานจดหมายอิเล็กทรอนิกส์ โดยบัญชีผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ที่ได้รับและให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที เมื่อเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรก
2) ผู้ใช้งานต้องไม่ใช้บัญชีผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของผู้อื่น เพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของบัญชีผู้ใช้ และให้ถือว่าเจ้าของบัญชีผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์รายนั้น เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน
3) ผู้ใช้งานต้องตรวจสอบรายชื่อผู้รับจดหมายอิเล็กทรอนิกส์ให้ถูกต้องก่อนส่งทุกครั้ง เพื่อป้องกันการส่งผิดตัวผู้รับ
4) ผู้ใช้งานสามารถระบุรายละเอียดข้อความลงท้ายจดหมายอิเล็กทรอนิกส์ (E-mail Signature) โดยให้มีข้อมูลชื่อ ตำแหน่ง สังกัด ชื่อองค์กร หมายเลขโทรศัพท์ และชื่อบัญชีจดหมายอิเล็กทรอนิกส์ให้ชัดเจน
5) ไม่อนุญาตให้ใช้จดหมายอิเล็กทรอนิกส์ขององค์กร รวมถึงโปรแกรมการสนทนาในการปฏิบัติงาน ดังต่อไปนี้
    5.1) ส่งจดหมายขยะ (Spam Mail)
    5.2) ส่งจดหมายลูกโซ่ (Chain Letter)
    5.3) ส่งจดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

5.4) ใช้ข้อความที่ไม่สุภาพ หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม อันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์ ทั้งนี้ ให้รวมถึงการใช้ข้อความที่ไม่สุภาพและไม่เหมาะสมผ่านโปรแกรมการสนทนาและการติดต่อสื่อสารทางอิเล็กทรอนิกส์อื่น ๆ

5.5) รับหรือส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อความที่ผิดกฎหมาย น่ารังเกียจ ลามกอนาจาร มีเจตนามุ่งร้าย ข่มขู่ทำร้าย ละเมิด หลอกลวง หมิ่นประมาท ใส่ร้าย แสดงถึงความเกลียดชัง หรือสนับสนุนการกระทำซึ่งเป็นอาชญากรรม หรือสร้างความไม่สงบเรียบร้อย หรือกระทบต่อศิลธรรมอันดี หรือฝ่าฝืนนโยบายขององค์กร ซึ่งรวมถึงข้อมูลหรือสิ่งที่ถือว่าน่ารังเกียจ หรือก้าวร้าว ได้แก่ ข่าวสารหรือข้อความใดที่ส่อเจตนาไปในทางเหยียดสีผิว หรือดูถูกเชื้อชาติ ละเมิดเกี่ยวกับเรื่องของเพศ หรือวิพากษ์วิจารณ์สถานะทางเพศในทางเสื่อมเสีย กล่าวดูถูกทำให้ผู้อื่นเสียชื่อเสียง หรือการแสดงความคิดอย่างก้าวร้าวต่อบุคคลอื่นที่เกี่ยวข้องกับ อายุ เพศ ศาสนา หรือความเชื่อทางการเมือง ชาติกำเนิด หรือความไร้สมรรถภาพต่าง ๆ ทั้งนี้ ให้รวมถึงการรับหรือส่งข้อความดังกล่าวผ่านโปรแกรมการสนทนาและการติดต่อสื่อสารทางอิเล็กทรอนิกส์อื่น ๆ

5.6) ใช้จดหมายอิเล็กทรอนิกส์ขององค์กรโฆษณาหรือใช้ประโยชน์สำหรับตนเองและผู้อื่นซึ่งไม่เกี่ยวข้องกับการปฏิบัติงานขององค์กร

5.7) การส่งจดหมายอิเล็กทรอนิกส์ขององค์กรร่วมไปกับบัญชีจดหมายอิเล็กทรอนิกส์ภายนอกองค์กร

5.8) นำบัญชีจดหมายอิเล็กทรอนิกส์ (Email Account) ซึ่งเป็นขององค์กรไปเผยแพร่สู่บุคคลอื่น ไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในเว็บบอร์ด ในชุดคำถามหรือแบบสอบถามจากผู้ค้า เป็นต้น เว้นแต่การเผยแพร่นั้นเป็นไปเพื่อผลประโยชน์ขององค์กร หรือได้รับอนุญาตจากผู้มีอำนาจแล้วเท่านั้น

5.9) ส่งข้อความที่เป็นความเห็นส่วนบุคคลโดยอ้างว่าเป็นความเห็นขององค์กร หรือก่อให้เกิดความเสียหายต่อองค์กร

6) ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เพื่อเป็นการป้องกันในการเปิดไฟล์ที่สามารถประมวลผลได้ (Executable File) เช่น .bat, .exe, .com เป็นต้น

7) ผู้ใช้งานควรบริหารจัดการแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื่อที่ระบบจดหมายอิเล็กทรอนิกส์

8) ไม่อนุญาตให้ส่งข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานหรือการดำเนินงานขององค์กรผ่านระบบจดหมายอิเล็กทรอนิกส์หรือโปรแกรมการสนทนาอื่นใดที่องค์กรไม่ได้เป็นผู้จัดสรรให้ หรือที่

องค์กรไม่ได้กำหนดไว้ โดยจะอนุญาตให้ใช้โปรแกรม Google Chat เฉพาะการติดต่อสื่อสารหรือประสานงานเท่านั้น

9) ห้ามผู้ใช้งานกระทำการใด ๆ โดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบคอมพิวเตอร์ขององค์กร หรือระบบผู้อื่น

10) ข้อมูลในแฟ้มอิเล็กทรอนิกส์ (Attached File) ที่แนบกับข้อความที่จัดส่งทางจดหมายอิเล็กทรอนิกส์ขององค์กร จะจำกัดขนาดข้อมูลไม่เกิน 25 เมกะไบท์ ต่อการส่งจดหมายอิเล็กทรอนิกส์ 1 ฉบับ

11) หากผู้ใช้งานพบเห็นการใช้งานจดหมายอิเล็กทรอนิกส์ โปรแกรมการสนทนา หรือการติดต่อสื่อสารทางอิเล็กทรอนิกส์อื่น ๆ ที่อาจขัดต่อนโยบายฉบับนี้ หรือขัดต่อกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายที่เกี่ยวข้อง ให้ผู้ใช้งานแจ้งต่อผู้บังคับบัญชาโดยตรงของตน หรือแจ้งต่อผู้ดูแลเครือข่ายคอมพิวเตอร์ขององค์กรโดยเร็ว

ข้อ 5 การใช้งานอินเทอร์เน็ต

1) ผู้ใช้งานต้องตระหนักถึงความมั่นคงปลอดภัยของข้อมูลคอมพิวเตอร์ที่รับส่งผ่านอินเทอร์เน็ต

2) ผู้ใช้งานต้องไม่ดาวน์โหลด เปิด หรือใช้ชุดคำสั่ง โปรแกรมระบบงาน หรือข้อมูลบนเครือข่ายอินเทอร์เน็ตที่เป็นการละเมิดลิขสิทธิ์ หรือเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูลองค์กร

3) ไม่อนุญาตให้ผู้ใช้งานโพสต์ หรืออัพโหลด หรือดาวน์โหลดภาพ ข้อมูล หรือข้อความใด ๆ หรือใช้งานในลักษณะ หรือโดยมีวัตถุประสงค์ ดังต่อไปนี้

   3.1) ขัดต่อกฎหมายว่าด้วยกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายที่เกี่ยวข้อง

   3.2) ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน

   3.3) อาจมีไวรัส หรือชุดคำสั่งไม่พึงประสงค์ (Malicious Code)

   3.4) ไม่เกี่ยวข้องต่อการปฏิบัติงานขององค์กร หรือไม่ก่อให้เกิดประโยชน์กับกิจการขององค์กร

   3.5) อาจก่อให้เกิดความเสื่อมเสียแก่ชื่อเสียงและเกียรติคุณขององค์กร

   3.6) เป็นการแสดงความคิดเห็นส่วนบุคคลของผู้ใช้งานในลักษณะที่อาจก่อให้เกิดความแตกแยก ความขัดแย้ง ความวุ่นวาย ความสับสน หรือก่อให้เกิดการเข้าใจผิด หรือความเสียหายแก่องค์กร

   3.7) เป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือของบุคคลอื่นใด

   3.8) มีลักษณะอันลามกอนาจาร

4) ผู้ใช้งานต้องไม่ใช้บริการบนระบบอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน เช่น ไม่เปิดหรือใช้งานโปรแกรมออนไลน์

ทุกประเภทเพื่อความบันเทิง ไม่เปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit torrent) เป็นต้น

5) ห้ามผู้ใช้งานเข้าถึงเครือข่ายคอมพิวเตอร์ขององค์กรในขณะเดียวกันกับที่ผู้ใช้งานเชื่อมต่ออยู่กับเครือข่ายคอมพิวเตอร์อื่น ๆ เช่น การเชื่อมต่อแบบ Personal Hotspot

ข้อ 6 การปฏิบัติงานจากภายนอกสำนักงาน หรือการเข้าถึงเครือข่ายจากทางไกล (Remote Access)

1) ผู้ใช้งานที่ต้องการเข้าถึงเครือข่ายภายในองค์กรโดยใช้วิธีการเข้าถึงผ่านเครือข่ายจากภายนอกองค์กร (Remote Access) ต้องกรอกข้อมูลผ่าน “แบบฟอร์มขอสร้าง เปลี่ยนแปลง และยกเลิกสิทธิผู้ใช้งานระบบ” และขออนุมัติการใช้งานจากผู้มีอำนาจอนุมัติก่อนดำเนินการ
2) ก่อนเข้าใช้งานระบบคอมพิวเตอร์บนเครือข่ายคอมพิวเตอร์ขององค์กร โดยผ่านการเข้าถึงเครือข่ายจากทางไกลทุกครั้ง พนักงานต้องตรวจสอบให้แน่ใจว่าเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ที่เกี่ยวข้องทั้งหมดที่จะใช้เข้าถึงเครือข่ายจากทางไกลนั้นได้รับการอัพเดทโปรแกรมแก้ไขจุดอ่อน หรือช่องโหว่ (Vulnerability) ให้เป็นรุ่นล่าสุดแล้ว
3) เครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ที่เกี่ยวข้องทั้งหมดต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสรุ่นล่าสุด ณ ขณะที่ใช้งานแล้วเท่านั้น ที่จะได้รับอนุญาตจากองค์กรให้เข้าใช้งานระบบคอมพิวเตอร์บนเครือข่ายคอมพิวเตอร์ขององค์กร โดยผ่านการเข้าถึงเครือข่ายจากทางไกล
4) กรณีที่ผู้ใช้งานมีความจำเป็นต้องเบิกใช้อุปกรณ์คอมพิวเตอร์แบบพกพาซึ่งเป็นทรัพย์สินสารสนเทศส่วนกลางของหน่วยงาน ให้ผู้ใช้งานขออนุมัติเบิกใช้จากผู้บังคับบัญชาก่อนนำไปใช้งาน โดยเมื่อหมดความจำเป็นต้องใช้งานให้รีบนำส่งคืนหน่วยงานทันที
5) ผู้ใช้งานที่มีความจำเป็นต้องนำเครื่องคอมพิวเตอร์พกพาออกไปใช้งานนอกสถานที่ ผู้ใช้งานต้องใช้งานด้วยความระมัดระวัง ไม่ละทิ้งเครื่องคอมพิวเตอร์พกพาไว้ในที่สาธารณะโดยไม่มีผู้ดูแล และต้องไม่อนุญาตให้บุคคลอื่นเข้าใช้เครื่องคอมพิวเตอร์พกพา เพื่อป้องกันการเข้าถึงหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
6) ผู้ใช้งานต้องระวังการสูญหายของเครื่องคอมพิวเตอร์พกพา และการสูญหายของข้อมูลซึ่งจัดเก็บอยู่ภายในเครื่องคอมพิวเตอร์แบบพกพา
7) ผู้ใช้งานต้องระมัดระวังการจัดเก็บเครื่องคอมพิวเตอร์พกพาภายในรถยนต์ซึ่งจอดทิ้งไว้ โดยให้จัดเก็บไว้ในกระโปรงท้ายรถ เพื่อป้องกันไม่ให้เป็นจุดสนใจสำหรับบุคคลอื่น
8) ผู้ใช้งานที่ต้องเดินทางไปพร้อมกับเครื่องคอมพิวเตอร์พกพา ต้องไม่ฝากเครื่องคอมพิวเตอร์เหมือนการฝากกระเป๋าสัมภาระทั่วไป และให้เก็บเครื่องคอมพิวเตอร์พกพาไว้ในกระเป๋าซึ่งใช้สำหรับการจัดเก็บคอมพิวเตอร์โดยเฉพาะเพื่อป้องกันการกระแทก ฝุ่น หรือน้ำ ซึ่งอาจทำให้เกิดความเสียหายแก่เครื่องคอมพิวเตอร์ได้
9) ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์พกพาเข้ากับเครือข่ายสาธารณะที่ไม่รู้จัก

ข้อ 7 การบริหารจัดการระบบงานและข้อมูลข่าวสารสารสนเทศ

1) ผู้ใช้งานมีหน้าที่ในการป้องกันและดูแลรักษาชุดคำสั่ง โปรแกรมระบบงาน ทรัพย์สิน และข้อมูลขององค์กรดังนั้น หากเกิดการสูญหาย เสียหาย นำไปใช้ในทางที่มิชอบ เผยแพร่โดยไม่รับอนุญาต ไม่ว่าจะด้วยเจตนาหรือประมาทเลินเล่อของผู้ใช้งาน ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายนั้นทั้งสิ้น
2) ผู้ใช้งานมีหน้าที่ใช้งานชุดคำสั่ง โปรแกรมระบบงาน ทรัพย์สินและข้อมูลที่องค์กรจัดเตรียมไว้ให้สำหรับการดำเนินงานขององค์กรเท่านั้น
3) ชุดคำสั่ง โปรแกรมระบบงาน ทรัพย์สิน และข้อมูลที่ผู้ใช้งานพัฒนาหรือสร้างสรรค์ขึ้นสำหรับการดำเนินงานขององค์กรให้ถือว่าเป็นลิขสิทธิ์ และ/หรือทรัพย์สินทางปัญญาขององค์กรแต่เพียงผู้เดียวเท่านั้น
4) ห้ามผู้ใช้งานกระทำการ ดังต่อไปนี้
    4.1) ติดตั้ง ชุดคำสั่ง โปรแกรมระบบงาน หรือข้อมูลที่ไม่ได้รับอนุญาตจากองค์กร หรือไม่เกี่ยวข้องกับการดำเนินธุรกิจขององค์กร หรือเป็นการละเมิดลิขสิทธิ์ และ/หรือทรัพย์สินทางปัญญาของผู้อื่น
    4.2) ทำให้เสียหาย ทำลาย ถอดถอน เปลี่ยนแปลง แก้ไข เพิ่มเติม หรือทำสำเนา ไม่ว่าทั้งหมดหรือบางส่วนซึ่งชุดคำสั่ง โปรแกรมระบบงาน ทรัพย์สิน ข้อมูล ข้อความ เอกสาร หรือทรัพย์สินใด ๆ ขององค์กรหรือของผู้อื่นโดยมิชอบ เว้นแต่การกระทำดังกล่าวจะกระทำเพื่อการปฏิบัติงานและได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
    4.3) เข้าถึงโดยมิชอบซึ่งชุดคำสั่ง โปรแกรมระบบงาน ทรัพย์สิน ข้อมูล หรือระบบคอมพิวเตอร์ที่มีมาตรการการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน
    4.4) เผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินขององค์กร
5) <u>ห้าม</u>ผู้ใช้งานใช้ระบบคอมพิวเตอร์ขององค์กร กระทำการดังต่อไปนี้
    5.1) นำข้อมูลดังต่อไปนี้ เข้าสู่ระบบคอมพิวเตอร์ขององค์กร หรือระบบผู้อื่น
        - ข้อมูลปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่องค์กร หรือผู้อื่น
        - ข้อมูลอันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชนทั่วไป
        - ข้อมูลใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

- ข้อมูลใด ๆ ที่มีลักษณะน่ารังเกียจ ลามกอนาจาร มีเจตนามุ่งร้าย ข่มขู่ทำร้าย ละเมิด หลอกลวง หมิ่นประมาท ใส่ร้าย แสดงถึงความเกลียดชัง และข้อมูลนั้นประชาชนทั่วไปอาจเข้าถึงได้

5.2) เผยแพร่หรือส่งต่อซึ่งข้อมูลโดยรู้อยู่แล้วว่าเป็นข้อมูลตามที่ได้ระบุไว้ในข้อที่ 5.1 ข้างต้น

6) ห้ามนำข้อมูลที่ปรากฏเป็นภาพของผู้อื่นเข้าสู่ระบบคอมพิวเตอร์ขององค์กร หรือระบบของผู้อื่นที่ประชาชนทั่วไปอาจเข้าถึงได้ และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือได้รับความอับอาย เว้นแต่จะเป็นการนำข้อมูลเข้าสู่ระบบโดยสุจริต

7) กระทำการ และ/หรือละเว้นการกระทำใด ๆ อันถือว่าหรืออาจถือว่าเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมาย และ/หรือกฎระเบียบอื่นที่มีผลบังคับใช้ต่อองค์กร

ข้อ 8 การรักษาความลับข้อมูล

1) อนุญาตให้ผู้ใช้งานเผยแพร่ข้อมูลที่อยู่ในระดับชั้นความลับข้อมูลทั่วไป (Public) เท่านั้น

2) ผู้ใช้งานต้องปฏิบัติต่อข้อมูลในระดับชั้นความลับข้อมูลใช้ภายใน (Internal Use) ข้อมูลความลับ (Confidential) และข้อมูลความลับเฉพาะ (Strictly Confidential) ขององค์กร เช่น กลยุทธ์การดำเนินงาน ข้อมูลของบุคลากรภายในองค์กร ข้อมูลทางการเงิน ข้อมูลระบบที่ใช้ในการปฏิบัติงาน ข้อมูลลูกค้า เป็นต้น โดยถือว่าข้อมูลเหล่านี้เป็นความลับขององค์กร และต้องไม่เปิดเผยข้อมูลไม่ว่าทั้งหมดหรือแต่บางส่วนต่อบุคคลภายนอกหรือต่อสาธารณะชน โดยปราศจากการยินยอมเป็นลายลักษณ์อักษรจากผู้บริหารระดับฝ่ายของหน่วยงานเจ้าของข้อมูล เว้นแต่จำเป็นเพื่อการปรึกษาหารือเกี่ยวกับการปฏิบัติงานกับบุคลากรที่เกี่ยวข้องภายในองค์กร หรือผู้ได้รับมอบอำนาจขององค์กร หรือตามที่องค์กรได้อนุญาตเป็นลายลักษณ์อักษร

3) ผู้ใช้งานต้องเก็บรักษาข้อมูลที่เป็นความลับที่ได้รับมาไว้ในสถานที่ปลอดภัยที่บุคคลทั่วไปไม่สามารถเข้าถึงได้โดยง่ายและรักษาข้อมูลที่เป็นความลับที่ได้รับมาในลักษณะและระดับเดียวกันกับการรักษาข้อมูลที่เป็นความลับของตนเอง แต่ทั้งนี้จะต้องไม่น้อยกว่าระดับที่วิญญูชนพึงรักษาข้อมูลที่เป็นความลับของตนเอง

4) ผู้ใช้งานต้องไม่ทำสำเนา หรือทำซ้ำข้อมูลที่อยู่ในระดับชั้นความลับและลับที่สุด แม้เพียงส่วนหนึ่งส่วนใดหรือทั้งหมด เว้นแต่การทำซ้ำเพื่อการใช้ข้อมูลที่เป็นความลับในการปฏิบัติงานตามความจำเป็นและสมควรเท่านั้น

5) ผู้ใช้งานต้องไม่กระทำการเปลี่ยนแปลง เปิดเผย หรือทำลายข้อมูลในระบบคอมพิวเตอร์ขององค์กรโดยไม่ได้รับอนุญาต

6) ผู้ใช้งานต้องส่งคืนข้อมูลเมื่อสิ้นสุดสัญญาจ้าง หรือเมื่อได้รับการร้องขอจากองค์กร โดยต้องไม่ทำสำเนา หรือทำซ้ำข้อมูลที่เป็นความลับ ไม่ว่าจะเป็นเพียงส่วนหนึ่งส่วนใดหรือทั้งหมด เว้นแต่การทำซ้ำเพื่อการใช้ข้อมูลที่เป็นความลับในการปฏิบัติงานตามความจำเป็นและสมควรเท่านั้น และต้องส่งคืนวัสดุที่บันทึกข้อมูลอันเป็นความลับไม่ว่าจะอยู่ในรูปของเอกสารและวัสดุอื่น ๆ ทั้งต้นฉบับและสำเนาให้แก่องค์กรทั้งหมด หรือต้องทำลายข้อมูลอันเป็นความลับนั้นหากองค์กรมีความประสงค์ให้ทำลาย

ข้อ 9 การปฏิบัติตามกฎหมายและข้อบังคับ

1) ผู้ใช้งานต้องปฏิบัติตามนโยบาย ระเบียบปฏิบัติ กฎข้อบังคับต่าง ๆ ขององค์กร รวมถึงกฎหมายด้านเทคโนโลยีสารสนเทศใด ๆ ที่มีผลบังคับใช้กับองค์กร เพื่อลดความเสี่ยงที่อาจก่อให้เกิดความเสียหายและสนับสนุนให้การดำเนินงานขององค์กรดำเนินไปอย่างมีประสิทธิผล
2) กรณีที่พบว่าผู้ใช้งานกระทำผิดโดยการไม่ปฏิบัติตามนโยบาย ระเบียบปฏิบัติ กฎข้อบังคับต่าง ๆ ขององค์กร รวมถึงกฎหมายใด ๆ ที่มีผลบังคับใช้กับองค์กร ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานต้องได้รับการลงโทษทางวินัยตามที่องค์กรกำหนดไว้ ทั้งนี้หากการกระทำดังกล่าวมีข้อขัดแย้งต่อกฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ/หรือกฎหมายอื่นใดที่เกี่ยวข้อง อาจถูกดำเนินคดีทางแพ่งและทางอาญาตามที่กฎหมายกำหนด

ข้อ 10 การขอเข้าปฏิบัติงานในพื้นที่สำหรับหน่วยงานภายนอก

บุคลากรภายในองค์กร หรือเจ้าของโครงการต้องควบคุมดูแลให้หน่วยงานภายนอกที่ต้องการเข้ามาปฏิบัติงานในพื้นที่ต้องปฏิบัติตามนโยบาย ระเบียบปฏิบัติ ข้อตกลงในสัญญา กฎข้อบังคับต่าง ๆ ขององค์กร รวมถึงกฎหมายใด ๆ ที่มีผลบังคับใช้กับองค์กร ดังต่อไปนี้

1) แจ้งหน่วยงานภายนอกให้ปฏิบัติตามนโยบาย ระเบียบปฏิบัติ กฎข้อบังคับต่าง ๆ และกฎหมายด้านเทคโนโลยีสารสนเทศใด ๆ ที่มีผลบังคับใช้กับองค์กรเช่นเดียวกับบุคลากรในองค์กร และต้องควบคุมให้หน่วยงานผู้รับจ้างช่วงที่ผู้ให้บริการภายนอกเป็นผู้จัดจ้างถือปฏิบัติเช่นเดียวกัน
2) กรณีที่พบว่าหน่วยงานภายนอกกระทำผิดโดยการไม่ปฏิบัติตามนโยบาย ระเบียบปฏิบัติ ข้อตกลงในสัญญา กฎข้อบังคับต่าง ๆ ขององค์กร รวมถึงกฎหมายใด ๆ ที่มีผลบังคับใช้กับองค์กร ผู้พบเห็นต้องแจ้งให้ผู้บังคับบัญชาและงานโครงสร้างพื้นฐานระบบดิจิทัล สำนักเทคโนโลยีดิจิทัล รับทราบโดยเร็วที่สุด

ข้อ 11 ให้มีการทบทวนนโยบายการใช้ระบบเทคโนโลยีสารสนเทศเพื่อความมั่นคงปลอดภัย สำหรับผู้ใช้งานให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง

ข้อ 12 ประกาศนี้ให้ใช้บังคับกับพนักงานและบุคลากรที่เกี่ยวข้องภายในองค์กร ตั้งแต่วันถัดจากวันประกาศเป็นต้นไป