นโยบายเทคโนโลยีสารสนเทศ
บริษัท อุบล ไบโอ เอทานอล จำกัด (มหาชน) และบริษัทย่อย

เพื่อให้การใช้งานเครื่องคอมพิวเตอร์และเครือข่ายในกลุ่มบริษัทอุบลไบโอเอทานอล เป็นไปอย่างมีระเบียบและเกิดประโยชน์สูงสุดแก่หน่วยงาน และไม่ให้เกิดการกระทำความผิดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ 1. นโยบายนี้เรียกว่า "**นโยบายเทคโนโลยีสารสนเทศ**" ว่าด้วยการใช้เครื่องคอมพิวเตอร์และเครือข่ายเพื่อความมั่นคงของระบบเทคโนโลยีสารสนเทศ ของบริษัท อุบล ไบโอ เอทานอล จำกัด (มหาชน) และบริษัทย่อย

ข้อ 2. นโยบายนี้ให้ใช้บังคับตั้งแต่ วันที่ 24 กุมภาพันธ์ 2569 เป็นต้นไป

หมวด 1
บทนิยาม

ข้อ 3. ในนโยบายเทคโนโลยีสารสนเทศนี้

"หน่วยงาน" หมายความว่า บริษัท อุบล ไบโอ เอทานอล จำกัด (มหาชน) และบริษัทย่อยของบริษัท อุบล ไบโอ เอทานอล จำกัด (มหาชน)

"เครื่องคอมพิวเตอร์และเครือข่าย" หมายความว่า เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ต่อพ่วง และอุปกรณ์เครือข่ายที่เชื่อมโยงคอมพิวเตอร์ต่างๆ ภายในหน่วยงาน ให้สามารถนำมาใช้งานร่วมกันได้ และให้หมายความถึงโปรแกรมและข้อมูลต่างๆ ที่มิได้จัดให้เป็นสื่อสาธารณะ ตลอดจนช่องสัญญาณเครือข่ายอินเทอร์เน็ต(Internet) และอินทราเน็ต (Intranet) ภายในหน่วยงาน

"เครื่องคอมพิวเตอร์ลูกข่าย" หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา หรืออุปกรณ์อื่นใดที่สามารถเชื่อมโยงเครือข่ายของหน่วยงาน

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

"ผู้ใช้บริการ" หมายความว่า ผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และเครือข่ายภายในหน่วยงาน

"หัวหน้าผู้ดูแลระบบ" หมายความว่า หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้บริหารให้มีหน้าที่ในการประสานงานเกี่ยวกับการดูแลรักษาระบบคอมพิวเตอร์และเครือข่ายในหน่วยงาน

"ผู้ดูแลระบบ" หมายความว่า เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้บริหารเทคโนโลยีสารสนเทศให้มีหน้าที่รับผิดชอบดูแล หรือจัดการระบบคอมพิวเตอร์และเครือข่าย

"โปรแกรมประสงค์ร้าย" หมายความว่า โปรแกรมคอมพิวเตอร์และ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหาย ไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์ เช่น Virus Computer หรือ Spyware หรือ Worm หรือ Trojan เป็นต้น

หมวด 2
บททั่วไป

ข้อ 4. ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำหนดบัญชีผู้ใช้บริการ (User Account) ให้กับผู้ใช้บริการ

ข้อ 5. ห้ามผู้ใดเข้าใช้งานเครื่องคอมพิวเตอร์และเครือข่ายโดยมิได้รับอนุญาตจากหัวหน้าผู้ดูแลระบบหรือผู้ดูแลระบบ

ข้อ 6. เพื่อให้นโยบายเทคโนโลยีสารสนเทศเป็นปัจจุบันเหมาะสมกับหลักปฏิบัติและการเปลี่ยนแปลง รวมถึงสอดคล้องกฎเกณฑ์ที่เกี่ยวข้องอยู่เสมอ จึงกำหนดให้มีการทบทวนนโยบายเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงใดๆ ตามความเหมาะสม

หมวด 3
นโยบายการใช้เครื่องคอมพิวเตอร์และเครือข่าย

ข้อ 7. ผู้ใช้บริการ หัวหน้าผู้ดูแลระบบ และผู้ดูแลระบบมีหน้าที่ที่ต้องปฏิบัติตามนโยบายของหน่วยงานดังต่อไปนี้

(1) ใช้เครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงานอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่หน่วยงาน

(2) ดูแลรักษาเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงานเพื่อให้สามารถใช้งานได้อย่างคุ้มค่า

(3) จะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงานในการกระทำที่ถือว่าเป็นความผิดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นๆ อันก่อให้เกิดความเสียหายแก่บุคคลทั่วไป หน่วยงาน หรือหน่วยงานภายนอก

หมวด 4
ข้อปฏิบัติของผู้ใช้บริการในการใช้งานเครื่องคอมพิวเตอร์และเครือข่าย

ข้อ 8. ผู้ใช้บริการจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และเครือข่ายโดยมีวัตถุประสงค์ดังต่อไปนี้

(1) เป็นการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหาย หรือเดือดร้อนรำคาญแก่บุคคลอื่น

(2) เป็นการกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน

(3) เพื่อการแสวงหากำไรเชิงพาณิชย์

(4) เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติหน้าที่ให้แก่หน่วยงาน ไม่ว่าจะเป็นข้อมูลของหน่วยงาน หรือบุคคลภายนอกก็ตาม

(5) เพื่อกระทำการอันมีลักษณะเป็นการละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญาของหน่วยงาน หรือบุคคลอื่น

(6) เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่น โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ หรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

(7) เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่หน่วยงาน เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังผู้ใช้บริการหรือบุคคลอื่น เป็นต้น

(8) เพื่อการขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของหน่วยงาน หรือของผู้ใช้บริการอื่นของหน่วยงาน หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของหน่วยงาน ไม่สามารถใช้งานได้ตามปกติ

(9) เพื่อแสดงความคิดเห็นส่วนบุคคล ในเรื่องที่เกี่ยวข้องกับการดำเนินงานของหน่วยงานไปยังที่อยู่เว็บ (web site) ใดๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจคลาดเคลื่อนไปจากความจริง

(10) เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ของหน่วยงาน หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่หน่วยงาน

ข้อ 9. ผู้ใช้บริการที่เป็นเจ้าของบัญชีผู้ใช้บริการ (User Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (User Account) ของเครื่องคอมพิวเตอร์และเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

ข้อ 10. ผู้ใช้บริการจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (User Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจก ให้แก่ผู้อื่น โดยมิได้รับอนุญาตจากหัวหน้าผู้ดูแลระบบ

ข้อ 11. ผู้ใช้บริการจะต้องเข้าระบบ (Login) โดยใช้บัญชีผู้ใช้บริการ (User Account) ของตนเอง และทำการออกจากระบบ (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

ข้อ 12. การตั้ง การใช้งานและการเก็บรักษารหัสผ่าน (Password) ให้เป็นไปในแนวทาง ดังนี้

(1) รหัสผ่านจะต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ ตัวอักขระพิเศษ

(2) ห้ามใช้รหัสผ่านเป็นชื่อ หรือชื่อสกุลของผู้ใช้บริการ ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนเองหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์

(3) ไม่อนุญาตให้เปลี่ยนรหัสผ่าน (Password) ซ้ำครั้งก่อน จนกว่าจะเปลี่ยนรหัสผ่าน (Password) 5 ครั้ง

(4) การเข้าระบบครั้งแรกผู้ใช้บริการต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

(5) ถ้าใส่รหัสผ่าน (Password) ผิดติดต่อกัน 5 ครั้ง ระบบจะทำการระงับบัญชีผู้ใช้บริการชั่วคราว โดยผู้ใช้บริการต้องติดต่อผู้ดูแลระบบเพื่อทำการปลดล็อค

(6) ให้ทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงานทุก 90 วัน

(7) ไม่ควรใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้งาน

(8) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ซึ่งง่ายต่อการสังเกตเห็นของบุคคลอื่น

(9) จะต้องเก็บรักษารหัสผ่านสำหรับการใช้งานเครื่องคอมพิวเตอร์และเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบรหัสผ่านดังกล่าว

ข้อ 13. ไม่ทำการนำเข้า เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ใดๆ อันเป็นเท็จ รวมถึงข้อมูล คอมพิวเตอร์ที่มีลักษณะลามก และข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นซึ่งเกิดจากการสร้างขึ้น ตัด ต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือด้วยวิธีการอื่นใด

ข้อ 14. เพื่อความปลอดภัยในการใช้เครื่องคอมพิวเตอร์และเครือข่ายโดยส่วนรวม ผู้ใช้บริการจะต้องปฏิบัติดังต่อไปนี้

(1) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์

(2) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ของหน่วยงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงานได้

(3) ปิดเครื่องคอมพิวเตอร์ของหน่วยงานที่ตนเองครอบครองใช้งาน เมื่อใช้งานประจำเสร็จสิ้นหรือเมื่อไม่มีการใช้งาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ต้องใช้งานตลอด 24 ชั่วโมง

(4) ตรวจสอบข้อมูลที่ได้รับจากภายนอกหรือภายในหน่วยงานทุกครั้ง ด้วยโปรแกรมคอมพิวเตอร์สำหรับตรวจสอบและกำจัดโปรแกรมประสงค์ร้ายที่หน่วยงานจัดให้ ก่อนปฏิบัติงานเสมอ และหากตรวจพบโปรแกรมประสงค์ร้ายฝังตัวอยู่ในข้อมูลส่วนใด จะต้องรีบดำเนินการทำลายโปรแกรมประสงค์ร้ายหรือข้อมูลนั้นโดยเร็วที่สุด

(5) ไม่ใช้บริการอินเทอร์เน็ต (Internet) ที่มีการครอบครองช่องสัญญาณ (Bandwidth) จำนวนมากหรือเป็นเวลานาน ในระหว่างเวลาทำงาน เช่น ดาวน์โหลดไฟล์ขนาดใหญ่โดยไม่จำเป็น เกมออนไลน์ สนทนาออนไลน์ เปิดวิทยุหรือดูคลิปวีดีโอผ่านอินเทอร์เน็ต เป็นต้น

(6) ไม่เปิดจดหมายอิเล็กทรอนิกส์ที่มีเอกสารแนบเป็นไฟล์ที่ไม่รู้จักหรือเป็นไฟล์ที่มีนามสกุลที่สามารถประมวลผลได้เองได้ไม่ว่าจะส่งมาจากบุคคลที่รู้จักหรือไม่ก็ตามเช่น .exe .com .bat .vbs .scr .hta เป็นต้น

(7) ลบข้อมูลคอมพิวเตอร์ที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ของหน่วยงานเพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

(8) ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ก่อนได้รับอนุญาตจากหัวหน้าผู้ดูแลระบบหรือผู้ดูแลระบบ

(9) คืนทรัพย์สินอันเกี่ยวข้องกับการใช้งานเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงาน เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว ฯลฯ ให้แก่หน่วยงานนับแต่วันพ้นสภาพการเป็นผู้ใช้บริการ

หมวด 5
การเชื่อมต่อและใช้งานเครื่องคอมพิวเตอร์และเครือข่าย

ข้อ 15. ผู้ใดจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจาก หัวหน้าผู้ดูแลระบบ/หรือผู้ได้รับอนุมัติและต้องปฏิบัติตามระเบียบนี้อย่างเคร่งครัด

ข้อ 16. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์ค้นหาเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับเครือข่ายหลัก เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

หมวด 6
ข้อปฏิบัติของผู้ดูแลระบบ

ข้อ 17. ผู้ดูแลระบบมีหน้าที่ ดังต่อไปนี้

(1) ติดตั้งเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงาน ระบบการเข้ารหัสข้อมูลอัตโนมัติ ระบบป้องกันและตรวจจับการบุกรุก ระบบป้องกันและกำจัดโปรแกรมประสงค์ร้าย รวมทั้งอุปกรณ์และระบบอื่นใดที่จำเป็นต่อการใช้เครื่องคอมพิวเตอร์และเครือข่าย เพื่อให้สามารถใช้งานได้อย่างมั่นคง

(2) ตรวจสอบดูแลการใช้งานเครื่องคอมพิวเตอร์และเครือข่าย ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และเครือข่าย ให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้บริการที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้บริการผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบพิจารณาระงับการใช้เครือข่ายคอมพิวเตอร์ของผู้ใช้บริการดังกล่าวทันที โดยมีการควบคุมการอนุญาตใช้เครื่องคอมพิวเตอร์และเครือข่าย

(3) ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และเครือข่ายที่เกี่ยวกับความมั่นคง ให้มีความมั่นคงในการใช้งานและทันสมัยอยู่เสมอ

(4) ตรวจสอบความมั่นคงในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ ทุก 4 เดือน

(5) เปลี่ยนรหัสผ่านสำหรับการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และเครือข่ายคอมพิวเตอร์ ทุก 90 วัน หรือเมื่อมีความจำเป็นเพื่อความมั่นคงในการใช้งาน

(6) สำรองข้อมูลที่มีความสำคัญแบบสมบูรณ์ อย่างน้อยเดือนละ 1 ครั้ง และทดสอบการกู้กลับข้อมูลทุก 6 หรือ 12 เดือน

(7) เก็บข้อมูลที่บันทึกการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และเครือข่ายคอมพิวเตอร์ (Log File) ย้อนหลังไม่น้อยกว่า 90 วัน ไว้ในหน่วยความจำเครื่องคอมพิวเตอร์อย่างน้อย 1 เครื่อง ซึ่งแยกต่างหากจากเครื่องคอมพิวเตอร์แม่ข่าย และจัดให้มีการสอบทานบันทึกการเข้าใช้ระบบ (Access log) ทุก 90 วัน

(8) ดูแลรักษาและตรวจสอบช่องทางการสื่อสาร (Communication port) ของเครือข่ายคอมพิวเตอร์อยู่เสมอ และปิดช่องทางการสื่อสาร (Communication port) ของเครือข่ายคอมพิวเตอร์ที่ไม่มีความจำเป็นต้องใช้งานในทันที

(9) ดูแลรักษา และปรับปรุงบัญชีผู้ใช้งานบริการอินเตอร์เน็ต/บัญชีจดหมายอิเล็กทรอนิกส์ (E-mail) การใช้งาน Internet/Network, Microsoft 365 (Email, OneDrive, SharePoint) SAP, VPN หรืออื่น ๆ ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

บัญชีผู้ใช้บริการมีการกำหนดดังต่อไปนี้

(9.1) การกำหนดบัญชีผู้ใช้บริการรายใหม่ (พนักงานเข้าใหม่), E-mail , Internet/Network, Microsoft 365 (Email, OneDrive, SharePoint) SAP, VPN อ้างอิงคู่มือปฏิบัติงาน "การขอใช้งานระบบภายในบริษัท"

(9.2) การขอใช้บริการ และกำหนดการใช้งาน Internet WIFI Visitor โดยการใช้งานต้องกรอกแบบฟอร์มขอใช้งานพนักงานต้อนรับของบริษัท อ้างอิงคู่มือปฏิบัติงาน "การขอใช้งาน Internet บริษัทของบุคลลภายนอก" และเอกสารการขอใช้จะมีกฎระเบียบการปฏิบัติแนบมากับแบบฟอร์มขอใช้งานเพื่อทำความเข้าใจในการใช้งานว่าโดยกฎระเบียบการใช้บริการ Internet ผ่านเครือข่ายไร้สายของกลุ่มบริษัทอุบลไบโอเอทานอล

(9.3) การกำหนดบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) เจ้าหน้าที่เทคโนโลยีสารสนเทศ จะเป็นผู้ลงทะเบียนผู้ใช้บริการให้ การกำหนด E-mail ผู้ใช้บริการ จะตั้งจากชื่อและตามด้วยตัวอักษรตัวแรกของนามสกุลเสมอ ถ้าหากชื่อซ้ำกันคนต่อไปจะตามด้วยตัวอักษรที่2 หรือ ลำดับถัดไป

(9.4) กรณีลาออกโดยจัดทำใบลาออก เมื่อผู้บริหารหน่วยงานอนุมัติลาออก พนักงานจะต้องส่งบันทึกตรวจสอบทรัพย์สิน และยกเลิกสิทธิ์การทำงานในระบบ โดยส่งให้ฝ่ายเทคโนโลยีสารสนเทศ ตรวจสอบการถือครองเครื่องคอมพิวเตอร์และยกเลิกสิทธิ์การใช้งานในระบบ E-mail, Internet/Network, Microsoft 365 (Email, OneDrive,

SharePoint), SAP, VPN และอื่นๆ (ถ้ามี) อ้างอิงคู่มือปฏิบัติงาน "การยกเลิกใช้งานระบบสารสนเทศ"

(9.5) กรณีผู้ที่ลาออกจากการเป็นพนักงาน ฝ่ายทรัพยากรบุคคลต้องส่งรายชื่อให้ผู้จัดการส่วนเทคโนโลยีสารสนเทศหลังจากวันพ้นสภาพของพนักงาน เพื่อยกเลิกการใช้ E-mail , Internet/Network, Microsoft 365 (Email, OneDrive, SharePoint), SAP, VPN กลุ่มบริษัทอุบลไบโอเอทานอล อ้างอิงคู่มือปฏิบัติงาน "การยกเลิกใช้งานระบบสารสนเทศ" โดยฝ่ายเทคโนโลยีสารสนเทศจะทำการตรวจสอบทรัพย์สิน และยกเลิกสิทธิ์การทำงานในระบบ และเปลี่ยนรหัสผ่านใหม่แล้วแจ้งไปยังหัวหน้างานของพนักงานที่พ้นสภาพ และจะมีการใช้งานไปจนกว่าจะได้รับเอกสารการยินยอมจากหัวหน้างานเพื่อทำการลบ E-mail นั้น โดยหัวหน้าฝ่ายต้องดำเนินการภายใน 30 วัน กรณีลาออกโดยมิได้ผ่านขั้นตอนการลาออกปกติ

(10) การบำรุงรักษาเครื่องคอมพิวเตอร์เครือข่าย และ Share drive ของหน่วยงาน

(11) เสนอรายงานการให้บริการและการใช้งานระบบคอมพิวเตอร์ รวมทั้งความเห็นและข้อสังเกตต่อผู้บังคับบัญชาที่เหนือขึ้นไป เพื่อทราบหรือเพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารระบบคอมพิวเตอร์

(12) การใช้ระบบการสื่อสารข้อมูลของเครือข่ายคอมพิวเตอร์แบบไร้สาย ผู้ดูแลระบบต้องดำเนินการดังต่อไปนี้

(12.1) ใช้เทคโนโลยีการรักษาความมั่นคงของระบบการสื่อสารข้อมูลของเครือข่ายคอมพิวเตอร์แบบไร้สายที่ต้องมีการเข้ารหัสข้อมูลในการสื่อสารระหว่างเครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ในการส่งและรับสัญญาณของเครือข่ายคอมพิวเตอร์แบบไร้สาย ซึ่งมีมาตรฐานของเทคโนโลยีไม่ต่ำกว่า WPA (Wi-Fi Protected Access)

(12.2) ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ในการส่งและรับสัญญาณของเครือข่ายคอมพิวเตอร์แบบไร้สาย ซึ่งมีกลไกการตรวจสอบพิสูจน์ตัวตนของผู้ใช้บริการ (User Authentication) ที่มีความมั่นคง เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าใช้งานเครือข่ายคอมพิวเตอร์ไร้สายได้

(12.3) ติดตั้งและใช้งานระบบตรวจจับผู้บุกรุก (Intrusion Detection System) เช่น Firewall ประเภทต่างๆ เป็นต้น

(12.4) ติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

(13) บริการจัดการการเปลี่ยนแปลงระบบงาน จะต้องมีการประเมินผลกระทบจากการเปลี่ยนแปลง มีการขออนุมัติจากผู้มีอำนาจ และดำเนินการเปลี่ยนแปลงอย่างรอบคอบรัดกุมตลอดจนมีการทบทวนผลการดำเนินการเปลี่ยนแปลง

(14) การแก้ไขปัญหาหรือเหตุการณ์ไม่ปกติด้านเทคโนโลยีสารสนเทศ กำหนดให้มีการบันทึกข้อมูลการแจ้งปัญหา วิธีแก้ไขปัญหา รวมถึงการแบ่งประเภทและระดับความสำคัญของ

ปัญหา สถานะของปัญหา ระยะเวลาเป้าหมายในการแก้ปัญหา ระยะเวลาที่ใช้แก้ปัญหา เพื่อนำมาใช้ประโยชน์ในการวิเคราะห์ปรับปรุงประสิทธิภาพในการแก้ไขปัญหาด้านเทคโนโลยีสารสนเทศ และมีการกำหนดเกณฑ์การวัดผลการแก้ไขปัญหา เพื่อให้สามารถนำมาใช้ในการบริหารจัดการ การวัดผลการให้บริการด้านการแก้ไขปัญหาของฝ่ายเทคโนโลยีสารสนเทศ

ข้อ 18. หัวหน้าผู้ดูแลระบบและผู้ดูแลระบบ จะต้องปฏิบัติดังต่อไปนี้

(1) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

(2) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

หมวด 7
นโยบายความมั่นคงปลอดภัยของระบบสารสนเทศ ว่าด้วยการสำรอง/กู้คืนข้อมูล

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรฐานในการสำรองข้อมูล/กู้คืนข้อมูลระบบสารสนเทศ และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีที่มีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลา 24 ชั่วโมง

แนวทางปฏิบัติในการสำรองข้อมูล/กู้คืนข้อมูล

(1) มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบของแต่ละระบบ

(2) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่ทำสำรองและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

(3) มีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน

(4) มีการซ้อมแผนฉุกเฉินอย่างน้อย ปีละ 1 ครั้ง

หมวด 8
การบริหารจัดการช่องโหว่ทางเทคนิค

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องควบคุมให้ระบบสารสนเทศของบริษัทฯ ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) จัดให้มีการทดสอบการเจาะระบบ (Penetration Test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายสาธารณะ (Untrusted Network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (Risk and Business Impact Analysis) ดังนี้

(1.1) กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ

(1.2) กรณีที่เป็นระบบงานที่มีความสำคัญอื่น ๆ ต้องทดสอบอย่างน้อยทุก 3 ปี

(2) จัดให้มีการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) กับระบบงานที่มีความสำคัญอย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานที่เกี่ยวข้องเพื่อให้รับทราบและหาแนวทางการแก้ไขและป้องกัน

(3) จัดให้มีการทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (Cyber Security Drill)

(4) จัดให้มีการบริหารจัดการเหตุการณ์ความมั่นคงไซเบอร์ (Cyber Security Incident Management)

หมวด 9
การบริหารจัดการการเข้าถึงของผู้ใช้งาน

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

(1) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(2) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(3) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(4) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

หมวด 10
กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัทฯ อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทฯรับทราบและปฏิบัติตาม

หมวด 11
ทรัพย์สินสูญหาย เสียหาย หรือชำรุด

ทรัพย์สิน หมายถึง เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง หรืออุปกรณ์ทางด้านเทคโนโลยีของบริษัทที่พนักงานนำไปใช้/ผู้รับผิดชอบ หากทรัพย์สินสูญหาย หรือได้รับความเสียหาย ชำรุด โดยประมาท ผู้นำไปใช้/ผู้ที่รับผิดชอบชดใช้ค่าใช้จ่ายเองทั้งหมด กระบวนการดังต่อไปนี้

(1) พนักงานที่สูญหาย/เสียหายหรือชำรุด ต้องแจ้งหัวหน้าสายงานในทันที พร้อมทำบันทึกเหตุการณ์แจ้งแผนกเทคโนโลยีสารสนเทศ หากเกิดเพิกเฉยจะได้รับใบเตือน

(2) พนักงานต้องส่งอุปกรณ์ที่ชำรุดให้แผนกเทคโนโลยีสารสนเทศ เพื่อทำการตรวจเช็ค

(3) แผนกเทคโนโลยีสารสนเทศดำเนินการส่งอุปกรณ์ที่ชำรุดให้กับทางร้านซ่อมภายนอกประเมินราคาซ่อม

(4) ส่งใบแจ้งค่าใช้จ่ายให้แผนกทรัพยากรบุคคลเพื่อแจ้งผู้ที่ทำทรัพย์สินสูญหาย/เสียหายหรือชำรุดเพื่อรับทราบการหักเงินพร้อมทำหนังสือแจ้งเตือน/แผนกทรัพยากรบุคคลหักเงินผู้ที่ทำทรัพย์สินตามราคาซ่อม

หมวด 12
การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศมีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลด ความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ (Integrity risk) โดยมีเนื้อหา ครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้น ซึ่งได้แก่ การร้องขอจนถึงการนำระบบงานที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

แนวทางปฏิบัติ

- ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็น ลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน

- ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและ ขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง
- ในกรณีมีบุคคลหรือหน่วยงานภายนอกบริษัทเข้ามาออกแบบหรือพัฒนาหรือเปลี่ยนแปลงหรือบำรุงรักษาระบบสารสนเทศ และมีความเกี่ยวข้องกับข้อมูลส่วนบุคคล จะต้องมีการลงนามในสัญญาประมวลผลข้อมูลส่วนบุคคล (Personal data processing agreement) ระหว่างบริษัทฯ และหน่วยงานหรือบุคคลภายนอก ซึ่งกำหนดให้หน่วยงานหรือบุคคลภายนอกต้องทำการเฉพาะตามคำสั่งของบริษัทฯ และมีหน้าที่รักษาความปลอดภัยของข้อมูลส่วนบุคคลด้วย
- ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม
- การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร โดยอาจเป็นการดำเนินการทางอิเล็กทรอนิกส์ (Electronic Transaction) เช่น อีเมล เป็นต้น และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หรือผู้รับผิดชอบระบบสารสนเทศ เป็นต้น
- ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง
- ควรสอบทานกฎหมายที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎหมาย

การปฏิบัติงานพัฒนาระบบงาน

- ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น รวมทั้งการแบ่งส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ การแบ่งส่วนดังกล่าวอาจกระทำโดยแยกใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้
- ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้อง ควรมีส่วนร่วมในกระบวนการออกแบบหรือพัฒนาหรือแก้ไขเปลี่ยนแปลงหรือบำรุงรักษาเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ
- ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง
- การทดสอบระบบ ผู้ที่ร้องขอและงานระบบเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ ทดลอง ตรวจสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับ การพัฒนาหรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

หมวด 13
การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้มีวิธีการที่สอดคล้องกันและมีประสิทธิภาพสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึงการแจ้งสถานการณ์ความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การแจ้งรายงานจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งการแจ้งเหตุการณ์หรือภัยคุกคามอันอาจส่งผลกระทบต่อข้อมูลส่วนบุคคลในระบบสารสนเทศของกลุ่มธุรกิจบริษัทฯ

แนวทางปฏิบัติ

- ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทฯ
- ต้องกำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน
- หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องแจ้งเหตุการณ์ดังกล่าวต่อส่วนเทคโนโลยีสารสนเทศ
- กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใชงานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว
- ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณา ถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อที่จะได้เรียนรู้และเตรียมการป้องกัน
- ต้องมีการประเมินความเสี่ยง ตรวจสอบ และแจ้งเหตุการณ์ภัยคุกคามหรือความเสี่ยงอันอาจส่งผลกระทบต่อข้อมูลส่วนบุคคลที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทฯ ตามลำดับขั้นและจัดทำรายงานผลกระทบ รวมทั้งแจ้งรายงานตามเงื่อนไขของกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

หมวด 14
การควบคุมการเข้าถึงข้อมูล การโอนย้ายข้อมูล

วัตถุประสงค์

เพื่อควบคุม มิให้บุคคลใด เข้าถึง ใช้ เปิดเผย หรือแก้ไขเปลี่ยนแปลง ข้อมูลหรือการทำงานของระบบสารสนเทศโดยไม่มีสิทธิหรือไม่มีอำนาจหรือเกินขอบอำนาจหน้าที่

แนวทางปฏิบัติ

(1) การบริหารจัดการข้อมูล

SR

- ต้องมีการจัดลำดับชั้นความลับของข้อมูลและข้อมูลสารสนเทศ โดยต้องมีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนดวิธีบริหารจัดการกับข้อมูลแต่ละประเภท กำหนดประเภทและลำดับของข้อมูลส่วนบุคคลโดยจัดอยู่ในประเภท "ข้อมูลสำคัญ" รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการยกเลิกหรือการนำกลับมาใช้ใหม่

- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL(Secure Socket Layer) การใช้ VPN (Virtual Private Network) เป็นต้น

- ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลและข้อมูลสำคัญที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

- ควรมีมาตรการรักษาความปลอดภัยข้อมูลและข้อมูลสำคัญ ซึ่งรวมถึงข้อมูลส่วนบุคคล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัทฯ เช่น ส่งซ่อม โดยมาตรการรักษาความปลอดภัยดังกล่าวรวมถึงการทำลายหรือทำให้ข้อมูลส่วนบุคคลที่เก็บอยู่ในสื่อบันทึกอยู่ในรูปแบบที่ไม่สามารถระบุตัวตนบุคคลได้

การควบคุมการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Privilege)

- ต้องควบคุมการเข้าถึงข้อมูล ข้อมูลสำคัญ ข้อมูลส่วนบุคคล และอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิพนักงานหรือบุคคลใดให้เป็นผู้ใช้งานที่มีหน้าที่รับผิดชอบและมีสิทธิเข้าถึงข้อมูลสำคัญและข้อมูลส่วนบุคคล รวมทั้งดำเนินการเพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

- ต้องกำหนดสิทธิ์การใช้ข้อมูล ข้อมูลสำคัญ ข้อมูลส่วนบุคคล และระบบสารสนเทศ เช่น สิทธิ์การใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิ์การใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็น ลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

- ในกรณีมีความจำเป็นต้องใช้ ผู้ใช้งาน หรือ User ที่มีสิทธิ์พิเศษ ต้องมีการควบคุมการ ใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิ์พิเศษมีความรัดกุมเพียงพอหรือไม่นั้น บริษัทฯ จะใช้ปัจจัยประกอบการพิจารณาในภาพรวมดังต่อไปนี้

  - ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่
  - ควรควบคุมการใช้งานของผู้ใช้งานที่มีสิทธิ์พิเศษอย่างเข้มงวด เช่น จำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

- ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็น ในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ควรเปลี่ยนรหัสผ่านทุก 6 เดือน เป็นต้น
- ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องหรืออุปกรณ์คอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิ์และหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น
- ผู้ใช้งานหรือผู้ปฏิบัติงานที่ได้รับสิทธิเข้าถึงระบบสารสนเทศและระบบเครือข่ายของ บริษัทฯ ไม่สามารถอนุญาตหรือให้สิทธิบุคคลอื่น เว้นแต่มีเหตุจำเป็นและเป็นระยะเวลาชั่วคราว โดยต้องมีการขออนุมัติจากผู้บังคับบัญชาหรือผู้มีอำนาจของบริษัทฯ ก่อน ภายใต้เงื่อนไขขั้นตอนหรือวิธีปฏิบัติที่บริษัทฯ กำหนด รวมทั้งต้อง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อ พ้นระยะเวลาดังกล่าว
- ในกรณีผู้ใช้งานหรือผู้ปฏิบัติงานได้รับอนุญาตในการให้สิทธิผู้ใช้งานหรือผู้ปฏิบัติงานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลในความรับผิดชอบของตนในกรณีจำเป็นดังกล่าวข้างต้น เช่น การ Share Files ผู้ใช้งานจะต้องให้สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิ์ดังกล่าวทันทีเมื่อสิ้นสุดเหตุความจำเป็นตาม ที่ได้รับอนุญาต รวมทั้งต้องบันทึกหลักฐานการให้สิทธิ์ดังกล่าวเพื่อการตรวจสอบด้วย
- ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือเข้าถึงหรือแก้ไขเปลี่ยนแปลง

หมวด 15
บทลงโทษ

กรณี ผู้ใช้บริการฝ่าฝืนนโยบายอันทำให้บริษัทได้รับความเสียหาย

(1) ดำเนินการตามกฎระเบียบของบริษัท/ตามกฎหมายที่เกี่ยวข้อง

(2) กรณีไม่ร้ายแรง ผู้ให้บริการส่งเรื่องฝ่ายบุคคล และผู้บังคับบัญชาทำหนังสือแจ้งเตือน

(3) ผิดร้ายแรง ไล่ออก งดให้ผลประโยชน์ ตามสิทธิ์พนักงาน ทุกประเภท

พิจารณาทบทวนและประกาศ ณ วันที่ 24 กุมภาพันธ์ 2569

(นายพลากร สุวรรณรัฐ)
ประธานคณะกรรมการ
บริษัท อุบล ไบโอ เอทานอล จำกัด (มหาชน)