noble

บริษัท โนเบิล ดีเวลลอปเมนท์ จำกัด (มหาชน)

นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ
(Information Security Policy)

สารบัญ

นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ

บริษัท โนเบิล ดีเวลลอปเมนท์ จำกัด (มหาชน) ต่อไปนี้เรียกว่า "บริษัทฯ" มีความมุ่งมั่นที่จะให้ระบบเทคโนโลยีสารสนเทศ ที่เป็นปัจจัยสำคัญในการดำเนินธุรกิจ มีความทันสมัย มีมาตรฐาน และมีความมั่นคงปลอดภัย อีกทั้งมุ่งส่งเสริมพัฒนา ความรู้และขีดความสามารถของพนักงานในด้านเทคโนโลยีสารสนเทศให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ และมีการใช้งานเป็นไปตามกฎหมาย จึงได้มีการจัดทำนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อเป็นหลักปฏิบัติในการดำเนินงานของผู้บริหาร และพนักงานทุกคน

คำนิยาม

คำนิยามที่ใช้ภายใต้เอกสารฉบับนี้

"**บริษัท**" หมายถึง บริษัท โนเบิล ดีเวลลอปเมนท์ จำกัด (มหาชน) และ บริษัท คอนติเนนตัล ซิตี้ จำกัด

"**ผู้ใช้งาน**" หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งกำหนดไว้ดังนี้

- **ผู้บริหาร** หมายถึง ผู้อำนวยการ/เทียบเท่าผู้อำนวยการเทคโนโลยีสารสนเทศ
- **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
- **พนักงาน** หมายถึง พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำ บุคคลใดที่ได้รับมอบหมายหน้าที่จากบริษัทฯ หรือพนักงานของบริษัทฯ

"**ข้อมูล**" หมายถึง ข้อความ ข่าวสาร เอกสาร เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ที่อยู่ในรูปของตัวเลข ภาษา ภาพ สัญลักษณ์ต่างๆ ที่ยังไม่ผ่านการประมวลผล ทั้งที่อยู่ในรูปอิเล็กทรอนิกส์ หรือที่อยู่ในรูปสื่อสิ่งพิมพ์และให้ความหมายรวมถึงข้อมูลคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์ตามกฎหมาย ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"**ข้อมูลอิเล็กทรอนิกส์**"

หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ เป็นต้น

"**สารสนเทศ**"

หมายถึง ข้อมูลต่าง ๆ ที่ได้ผ่านการเปลี่ยนแปลง การประมวลผล หรือวิเคราะห์ ผลสรุปด้วยวิธีการต่าง ๆ ให้สื่อความหมาย ตรงตามวัตถุประสงค์ที่ต้องการ หรือให้อยู่ในรูปแบบที่สามารถนำไปใช้ประโยชน์ในการใช้งานได้ เพื่อให้เกิดความรู้ ทำให้เกิดความคิด ความเข้าใจ วิเคราะห์ผล การตัดสินใจ และการวางแผนการบริหารงาน

"**หน่วยงานภายนอก**"

หมายถึง บุคคลที่สาม ผู้ค้า หุ้นส่วนการค้า ผู้ให้บริการ/จำหน่ายระบบ (Vendor) และผู้มีสัญญาทำงานให้บริษัท โนเบิล ดีเวลลอปเมนท์ จำกัด (มหาชน) และบริษัท คอนติเนนตัล ซิตี้ จำกัด ได้รับอนุญาตให้มีสิทธิเข้าถึงและใช้งานระบบสารสนเทศ ของบริษัท โนเบิล ดีเวลลอปเมนท์ จำกัด (มหาชน) และบริษัท คอนติเนนตัล ซิตี้ จำกัด ตามอำนาจหน้าที่ที่รับผิดชอบ

"**ระบบสารสนเทศ**"

หมายถึง ข้อมูลของบริษัท โนเบิล ดีเวลลอปเมนท์ จำกัด (มหาชน) และบริษัท คอนติเนนตัล ซิตี้ จำกัด ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และระบบเครือข่ายมาสร้างสารสนเทศ และสามารถนำสารสนเทศมาใช้ในการบริหารการวางแผน การพัฒนา การควบคุม และสนับสนุนการดำเนินงาน

"**ระบบเครือข่าย**"

หมายถึง กลุ่มของคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่ถูกนำมาเชื่อมต่อกันเพื่อให้ผู้ใช้งานในเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และใช้อุปกรณ์ต่าง ๆ ในเครือข่ายร่วมกันได้

"**มาตรฐาน**"

หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

"**เจ้าของข้อมูล**"

หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาหรือตามตำแหน่งหน้าที่ ให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

"**ทรัพย์สิน**"

หมายถึง

1. อุปกรณ์เทคโนโลยีสารสนเทศ และอุปกรณ์อื่นใดที่ใช้งานร่วมกับอุปกรณ์เทคโนโลยีสารสนเทศที่เกี่ยวข้องทุกประเภท
2. ชุดคำสั่ง โปรแกรมระบบงานสารสนเทศ และโปรแกรมอื่นใดที่ใช้งานร่วมกับโปรแกรม ระบบงานสารสนเทศ
3. ข้อมูลสารสนเทศ และ/หรือ ทรัพย์สินทางปัญญาใดๆ

"**อุปกรณ์คอมพิวเตอร์**"

หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"**อุปกรณ์พกพา**"

หมายถึง เครื่องคอมพิวเตอร์พกพา (Laptop) สมาร์ทโฟน (Smartphone) แท็บเล็ตคอมพิวเตอร์ (Tablet) ที่บริษัทอนุญาตให้เชื่อมต่อและใช้งานสารสนเทศของบริษัทได้

"**ซอฟต์แวร์**"

หมายถึง คำสั่ง ชุดของคำสั่งหรือรูปแบบที่เขียนขึ้น พัฒนาขึ้น หรือได้มาไม่ว่าด้วยวิธีการอื่นใดเพื่อใช้เก็บรวบรวมข้อมูล จัดการกับข้อมูล และ/หรือประมวลผลข้อมูลด้วยวิธีการทางอิเล็กทรอนิกส์ หรือสิ่งอื่นใดที่นำไปใช้กับเครื่องคอมพิวเตอร์เพื่อให้เครื่องคอมพิวเตอร์ทำงานหรือเพื่อให้ได้รับผลอย่างหนึ่งอย่างใด ทั้งนี้ไม่ว่าจะเป็นภาษาคอมพิวเตอร์ลักษณะใด

"**จดหมายอิเล็กทรอนิกส์**"

หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

"**รหัสผ่าน**"

หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"**ชุดคำสั่งไม่พึงประสงค์**"

หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

"**สื่อบันทึกข้อมูล**"

หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Hard drive หรือ Flash drive หรือ Handy drive หรือ Thumb drive หรือ External hard drive เป็นต้น

"**เหตุการณ์ด้านความมั่นคงปลอดภัย**"

หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"**สถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ**"

หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของบริษัทถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"**Social Network**"

หมายถึง เครือข่ายสังคมออนไลน์ หรือเป็นการบริการที่เชื่อมโยงบุคคลหลายบุคคลเข้าไว้ด้วยกันผ่านอินเทอร์เน็ต ตัวอย่างของ Social Network ได้แก่ Facebook Twitter Blogger เป็นต้น

หน้าที่ความรับผิดชอบ

กลุ่มงานเทคโนโลยีสารสนเทศ

(1) กำหนดนโยบาย แผนงาน มาตรการ วิธีการ และการตรวจสอบเกี่ยวกับการใช้งานและการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

(2) ประเมินและจัดการความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยให้คำนึงถึงประโยชน์และประสิทธิภาพต่อบริษัทฯ เป็นสำคัญและนำส่งข้อมูลพร้อมกับหลักการปฏิบัติให้หน่วยงานต่างๆ

(3) ติดตามความเคลื่อนไหวเกี่ยวกับภัยคุกคามทางคอมพิวเตอร์ทั้งภายในและภายนอกบริษัท

(4) มีหน้าที่ในการจัดการเหตุฉุกเฉินด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ (Security Incident)

(5) ระบบงานหรือข้อมูลที่มีผลกระทบต่อการดำเนินธุรกิจของบริษัทฯ กลุ่มงานเทคโนโลยีสารสนเทศ เป็นผู้พิจารณากำหนดพื้นที่ส่วนกลางและสิทธิในการเข้าถึง สำรองและเก็บรักษา (Backup) ข้อมูล และผู้ใช้สามารถเข้าใช้งานระบบและเข้าถึงข้อมูลได้ต่อเมื่อได้รับการอนุมัติจากหน่วยงานเจ้าของข้อมูล

เจ้าของข้อมูล และเจ้าของระบบงาน

เป็นผู้อนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

การโยกย้ายเจ้าหน้าที่ข้ามส่วนงาน / การลาออกของเจ้าหน้าที่

กรณีมีการโยกย้ายเจ้าหน้าที่ข้ามส่วนงาน หรือลาออก หรือพ้นหน้าที่รับผิดชอบในการใช้ระบบคอมพิวเตอร์ใดๆ หน่วยงานของเจ้าหน้าที่ดังกล่าวต้องแจ้งมายัง กลุ่มงานเทคโนโลยีสารสนเทศเพื่อให้ยกเลิกสิทธิเข้าถึงระบบคอมพิวเตอร์นั้นหรือเปลี่ยนรหัสผ่านใหม่ในกรณีที่ยังคงต้องการใช้บัญชีรายชื่อนั้นอยู่ โดยระบุวันที่พ้นหน้าที่และแจ้งล่วงหน้าก่อนที่จะมีผลบังคับหรือทันทีตามใบขอโยกย้ายพนักงาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดทำขึ้นเพื่อเป็นการกำหนดหลักเกณฑ์และวิธีการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับแนวนโยบายที่ได้กำหนดไว้ในหมวด 13 ดังต่อไปนี้

แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ (Information security policies)

(1) บริษัทฯ ต้องจัดทำเอกสารแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) อย่างเป็นลายลักษณ์อักษร และต้องได้รับอนุมัติจากคณะกรรมการบริษัท พร้อมทั้งเผยแพร่นโยบายฯ ให้ผู้ใช้งานรับทราบ

(2) บริษัทฯ ต้องทบทวนแนวนโยบาย และรายงานผลการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) อย่างน้อยปีละ 1 ครั้ง

แนวปฏิบัติด้านโครงสร้างความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ (Organization of information security)

(1) บริษัทฯ ต้องกำหนดบทบาทหน้าที่และความรับผิดชอบสำหรับผู้ใช้งานที่เกี่ยวข้องกับกระบวนการในการรักษาความมั่นคงปลอดภัย

(2) บริษัทฯ ต้องแยกหน้าที่ความรับผิดของแต่ละหน่วยงานออกจากกัน เพื่อลดโอกาสที่จะเกิดเหตุการณ์การแก้ไขโดยไม่ได้ตั้งใจ หรือที่เกิดจากการที่ผู้ไม่มีสิทธิหรือการใช้งานทรัพย์สินของบริษัทฯ ที่ผิดวัตถุประสงค์

(3) บริษัทฯ ต้องจัดทำรายชื่อสายงานการสั่งการหรือสายงานการอนุมัติการทำงานที่เหมาะสม และเผยแพร่ให้ผู้ที่เกี่ยวข้องรับทราบ

(4) บริษัทฯ ต้องจัดทำ ปรับปรุง บำรุงรักษารายชื่อผู้เชี่ยวชาญความมั่นคงปลอดภัยให้เป็นปัจจุบัน

(5) บริษัทฯ ต้องระบุรายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการที่เกี่ยวข้องกับระบบสารสนเทศ

แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบุคลากร (Human resource security)

(1) ฝ่ายบริหารทรัพยากรบุคคลต้องตรวจสอบและกลั่นกรองประวัติการศึกษา ประสบการณ์ รวมทั้งประวัติการทำงานของพนักงานก่อนรับเข้ามาทำงาน

(2) ฝ่ายบริหารทรัพยากรบุคคลต้องตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นผู้บริหาร พนักงานและลูกจ้าง โดยจะต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบสารสนเทศของหน่วยงานใดมาก่อน

(3) บริษัทฯ ต้องมีเงื่อนไข ข้อตกลงในการปฏิบัติงาน รวมทั้งข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศต่อผู้ใช้งาน พร้อมทั้งให้ลงนามในข้อตกลงดังกล่าว

(4) บริษัทฯ ต้องกำหนดกิจกรรมเพื่อสนับสนุน และส่งเสริมสร้างจิตสำนึกให้แก่ผู้ใช้งาน เพื่อสร้างความตระหนักด้านระบบความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

(5) บริษัทฯ ต้องจัดให้ความรู้ ฝึกอบรมหรือพัฒนาความรู้ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ดูแลระบบ

(6) เมื่อสิ้นสุดการจ้างหรือเปลี่ยนลักษณะการจ้างงาน ผู้ใช้งานจะต้องคืนทรัพย์สินทางด้านสารสนเทศอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของบริษัทฯ

แนวปฏิบัติด้านการบริหารจัดการทรัพย์สิน (Asset management)

(1) บริษัทฯ ต้องจัดทำบัญชีรายการทรัพย์สินสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศ พร้อมทั้งระบุผู้รับผิดชอบรายการทรัพย์สินและต้องดำเนินการทบทวนให้เป็นปัจจุบันอยู่เสมอ

(2) บริษัทฯ ต้องจัดประเภทของข้อมูล ระดับชั้นความลับของข้อมูล สิทธิการเข้าถึง ระยะเวลาการจัดเก็บข้อมูล เวลาที่ได้เข้าถึงข้อมูล ช่องทางการเข้าถึงข้อมูล สถานที่จัดเก็บข้อมูล

(3) บริษัทฯ ต้องทำสัญลักษณ์ หรือป้ายชื่อ บนสื่อที่จัดเก็บข้อมูล เพื่อช่วยในการควบคุม กำกับดูแลข้อมูลและสารสนเทศ ทำให้ง่ายและสะดวกต่อการดำเนินงาน หรือสามารถนำออกไปเผยแพร่ต่อได้

(4) ในกรณีที่ผู้ใช้งานจำเป็นต้องนำสื่อบันทึกข้อมูลออกจากบริษัทฯ จะต้องลงทะเบียนยืมคืน และดูแลรักษาเพื่อป้องกันความเสียหาย ซึ่งเกิดระหว่างการส่งสื่อบันทึกเหล่านั้นออกภายนอกบริษัทฯ และการเข้าถึงจากผู้ไม่มีสิทธิ

(5) บริษัทฯ ต้องมีวิธีการทำลายสื่อบันทึกข้อมูลที่เหมาะสมและชัดเจน ในกรณีที่ทำลายสื่อบันทึกข้อมูล โดยผู้ให้บริการภายนอก ต้องมีการทำสัญญาข้อตกลงเรื่องการรักษาความลับของบริษัทฯ

(6) หากผู้ใช้งานนำเครื่องคอมพิวเตอร์แบบพกพาจากภายนอกเข้ามาใช้งาน และก่อให้เกิดความเสียหายกับระบบสารสนเทศ ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งนี้ และแจ้งต่อกลุ่มงานเทคโนโลยีสารสนเทศเพื่อดำเนินการควบคุมแก้ไข

แนวปฏิบัติด้านการควบคุมการเข้าถึง (Access control)

(1) กลุ่มงานเทคโนโลยีสารสนเทศต้องจัดกำหนดกระบวนการควบคุมการเข้าถึงรวมทั้งได้รับการพิจารณาทบทวนให้เป็นปัจจุบันอยู่เสมอ

(2) กลุ่มงานเทคโนโลยีสารสนเทศต้องกำหนดกระบวนการสำหรับลงทะเบียน ปรับปรุงและยกเลิกสิทธิผู้ใช้งาน ซึ่งกระบวนการดังกล่าวจะต้องมีการจัดเก็บเป็นหลักฐานเพื่อการตรวจสอบหากมีปัญหาเกิดขึ้น

(3) ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบสารสนเทศตามการใช้งาน ดังนี้

3.1) ระดับสิทธิสูงสุดของระบบ (Root / High Privileged User)

3.2) ระดับผู้ดูแลระบบ (Administrator)

3.3) ระดับผู้ใช้งาน (User)

(4) เจ้าของระบบสารสนเทศต้องทบทวนสิทธิการใช้งานอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

(5) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงระบบสารสนเทศได้

(6) การให้สิทธิพิเศษกับผู้ใช้งานมากกว่าการใช้งานตามปกติต้องได้รับอนุญาตจากเจ้าของระบบสารสนเทศนั้น ๆ เป็นลายลักษณ์อักษรและกำหนดระยะเวลาในการใช้งาน และเมื่อพ้นกำหนดระยะเวลาดังกล่าวแล้วให้ระงับสิทธิการใช้งานโดยทันที

(7) เจ้าของระบบต้องปรับปรุงสิทธิการเข้าถึงสิทธิของผู้ใช้งาน เมื่อมีพนักงาน ลาออก พ้นจากตำแหน่งเดิม หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบ

(8) เจ้าของระบบจะต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (Username account) และรหัสผ่าน (Password) ที่รับผิดชอบระบบสารสนเทศนั้น ๆ จะต้องกำหนดสิทธิการเข้าถึงระบบให้กับผู้ใช้งานแยกตามหน้าที่ความรับผิดชอบ

(9) ผู้ใช้งานจะต้องถูกกำหนดให้ปฏิบัติตามวิธีการใช้งานรหัสผ่านของบริษัทฯ (ยกเว้นระบบที่มีข้อจำกัด) ดังนี้

9.1) ผู้ใช้งานต้องกำหนดให้รหัสผ่านมีไม่น้อยกว่า 8 ตัวอักษร

9.2) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุก 180 วัน

9.3) การกำหนดรหัสผ่านต้องประกอบด้วยตัวอักขระทั้งตัวพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และสัญลักษณ์พิเศษรวมกันหรือประกอบด้วยสามอย่างข้างต้นเป็นอย่างน้อย

9.4) ผู้ใช้งานต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อ นามสกุล และไม่ควรกำหนดรหัสผ่านจากชื่อบุคคลใกล้ชิดหรือจากคำศัพท์ในพจนานุกรม

9.5) ผู้ใช้งานต้องไม่ใช้งานโปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ

9.6) ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่านให้ผู้อื่นรับทราบหรือจดบันทึกรหัสผ่านไว้ในสถานที่ที่บุคคลอื่นสามารถเข้าถึงได้โดยง่าย

9.7) ผู้ใช้งานไม่ควรอนุญาตให้ผู้ใช้งานอื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์

9.8) ผู้ใช้งานต้องใส่ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์ และควรทำการเปลี่ยนรหัสผ่านตามวิธีการใช้งานรหัสผ่านของบริษัทฯ

(10) บริษัทฯ ต้องควบคุมการเข้าถึงระบบสารสนเทศด้วยการพิสูจน์ตัวตน (Username และ Password)

(11) กลุ่มงานเทคโนโลยีสารสนเทศต้องควบคุมและจำกัดการใช้งานโปรแกรมเฉพาะผู้ที่ได้รับสิทธิเท่านั้น

(12) ผู้ดูแลระบบต้องควบคุมการเข้าถึงซอร์สโค้ด

(13) สำหรับการเข้าถึงระบบเครือข่ายของพนักงานต้องมีการควบคุมและจำกัดการใช้งานตามหน้าที่ความรับผิดชอบ

แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

(1) พื้นที่ศูนย์คอมพิวเตอร์ ต้องจัดสรรพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า – ออกของบริษัทฯ เพื่อป้องกันการเข้าถึงสารสนเทศ

(2) พื้นที่ศูนย์คอมพิวเตอร์ ต้องกำหนดให้การเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่น ๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย

(3) พื้นที่ศูนย์คอมพิวเตอร์ ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์ โดยผู้ให้บริการภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินของบริษัทฯ

(4) พื้นที่ศูนย์คอมพิวเตอร์ต้องมีระบบป้องกันภัยต่าง ๆ ที่อาจจะเกิดกับอุปกรณ์ไว้อย่างเหมาะสม ได้แก่ ติดตั้งอุปกรณ์ดับเพลิง กล้องวงจรปิด ระบบปรับอากาศ ระบบสำรองกระแสไฟฟ้า

(5) การเข้า – ออกศูนย์คอมพิวเตอร์ต้องได้รับอนุญาตจากผู้ดูแลระบบของบริษัทฯ

(6) กลุ่มงานเทคโนโลยีสารสนเทศต้องกำหนดสิทธิของผู้ใช้งานในการเข้า – ออกศูนย์คอมพิวเตอร์ โดยกำหนดให้เฉพาะผู้ใช้งานที่เกี่ยวข้องเท่านั้นที่จะสามารถเข้า - ออกศูนย์คอมพิวเตอร์ เช่น ผู้ดูแลระบบ เป็นต้น

(7) ผู้ใช้งานที่ต้องการเข้าศูนย์คอมพิวเตอร์จะต้องปฏิบัติตามข้อปฏิบัติในการใช้บริการศูนย์คอมพิวเตอร์ของบริษัทฯ บริษัทฯ ต้องควบคุมการเข้า – ออก ของบุคคลภายนอกและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกระหว่างปฏิบัติงานภายในบริษัทฯ

แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศด้านการดำเนินการ (Operations security)

(1) กลุ่มงานเทคโนโลยีสารสนเทศต้องมีการวางแผนความต้องการใช้งานทรัพยากรสารสนเทศเพิ่มในอนาคต เพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน

(2) ผู้ดูแลระบบต้องตั้งเวลาของเครื่องคอมพิวเตอร์ในบริษัทฯ ไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการข้อมูลเวลา โดยการตั้งเวลาของเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ โดยการตั้งเวลาด้วย Network Time Protocol (NTP) ไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการข้อมูลเวลา

(3) ในกรณีที่มีการเปลี่ยนแปลงของอุปกรณ์ ระบบสารสนเทศและระบบเครือข่าย ผู้ดูแลระบบหรือผู้พัฒนาระบบต้องดำเนินการตามการบริหารจัดการการเปลี่ยนแปลง

(4) หากผู้ดูแลระบบหรือผู้ให้บริการภายนอกต้องการใช้เครื่องมือต่างๆ (tools) เพื่อการตรวจสอบระบบเครือข่ายหรือการติดตั้งอุปกรณ์เครือข่ายต้องได้รับการอนุมัติจากผู้บริหารบริษัทฯและดำเนินการติดตั้งโดยเจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศที่ได้รับมอบหมายเท่านั้น

(5) กลุ่มงานเทคโนโลยีสารสนเทศต้องแยกระบบสำหรับการพัฒนารวมทั้งการทดสอบ และระบบให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริง โดยไม่ได้รับอนุญาต

(6) ผู้ใช้งานมีหน้าที่ดูแลให้มีการติดตั้งซอฟต์แวร์ป้องกันมัลแวร์และไวรัสที่เครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบ และมีการอัปเดตให้เป็นปัจจุบันอยู่เสมอ

(7) หากผู้ใช้งานสงสัยว่าเครื่องคอมพิวเตอร์ถูกจู่โจมด้วยโปรแกรมไม่ประสงค์ดี ไม่อนุญาตให้ผู้ใช้งานเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายของบริษัทฯ เพื่อป้องการไม่ให้ชุดคำสั่งไม่พึงประสงค์แพร่กระจายในระบบเครือข่ายของบริษัทฯ และควรแจ้งให้กลุ่มงานเทคโนโลยีสารสนเทศทราบเพื่อดำเนินการต่อไป

(8) กลุ่มงานเทคโนโลยีสารสนเทศต้องดำเนินการทบทวนการปรับปรุงเวอร์ชันระบบปฏิบัติการและซอฟต์แวร์บนเครื่องคอมพิวเตอร์แม่ข่ายให้เป็นปัจจุบัน

(9) การติดตั้งและเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบ

(10) ให้กลุ่มงานเทคโนโลยีสารสนเทศกำหนดให้มีการบันทึกการใช้งาน (Log) ของระบบสารสนเทศ เพื่อประโยชน์ในการตรวจสอบการใช้งานระบบสารสนเทศ

(11) บริษัทฯ ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของบริษัทฯ ให้เป็นไปตามพระราชบัญญัติว่าด้วยกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พ.ศ. ๒๕๖๐ รวมถึงฉบับที่มีการปรับปรุง

(12) บริษัทฯ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึง และการแก้ไขเปลี่ยนแปลงสิทธิของระบบ สำหรับผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

แนวปฏิบัติด้านความมั่นคงปลอดภัยทางด้านการสื่อสาร (Communications security)

(1) กลุ่มงานเทคโนโลยีสารสนเทศต้องจัดระบบเครือข่ายให้เป็นสัดส่วนชัดเจน เช่น พื้นที่ส่วนระบบเครือข่าย (Network zone) พื้นที่ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server zone) เพื่อความสะดวกในการปฏิบัติงาน และควบคุมการเข้าถึงอุปกรณ์ต่าง ๆ ได้

(2) กลุ่มงานเทคโนโลยีสารสนเทศจะต้องติดตั้งหรือดูแลการติดตั้งการเชื่อมต่อระบบแม่ข่าย

(3) ระบบเครือข่ายที่เชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกบริษัทฯ ต้องผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall) หรือโปรแกรมที่ใช้ในการกรองข้อมูล (Packet Filtering)

(4) กลุ่มงานเทคโนโลยีสารสนเทศต้องจัดทำแผนผังระบบเครือข่าย (Network diagram) ซึ่งมีรายละเอียดของเครือข่ายภายใน เครือข่ายภายนอกและอุปกรณ์เครือข่ายต่างๆ พร้อมทั้งจัดระดับชั้นความลับและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(5) ผู้ดูแลระบบเครือข่ายต้องตรวจสอบสิทธิการเข้าถึงระบบเครือข่ายของผู้ใช้งานอย่างสม่ำเสมอ

(6) ผู้ดูแลระบบต้องกำหนดคุณสมบัติด้านความมั่นคงปลอดภัยและระดับการให้บริการ สำหรับบริการเครือข่ายที่บริษัทฯ ใช้บริการ

(7) กลุ่มงานเทคโนโลยีสารสนเทศต้องกำหนดข้อตกลงความพร้อมใช้ (SLA) ของระบบเครือข่ายและต้องมีการทบทวนทุก 1 ปี

(8) ไม่อนุญาตให้ผู้ใช้งานเปิดเผยข้อมูลหมายเลขประจำเครื่องคอมพิวเตอร์ (IP Address) แผนผังระบบเครือข่าย (Network diagram) การตั้งค่าอุปกรณ์ (Configuration) หรือข้อมูลที่เกี่ยวข้องกับเชื่อมต่อเครือข่ายและระบบสารสนเทศให้ผู้ที่ไม่มีสิทธิหรือบุคคลภายนอกรับทราบ

(9) ผู้ดูแลระบบต้องจัดเตรียมระบบสำหรับการแลกเปลี่ยนสารสนเทศระหว่างบริษัทฯ กับบุคคลหรือหน่วยงานภายนอก โดยมีมาตรการการรักษาความมั่นคงปลอดภัย

(10) ผู้ใช้งานต้องไม่เชื่อมต่ออินเทอร์เน็ตผ่านสมาร์ทโฟน ในกรณีที่มีการเชื่อมต่อกับระบบเครือข่ายของบริษัทฯ อยู่แล้ว

(11) ไม่อนุญาตให้ผู้ใช้งาน กระจายหรือส่งสัญญาณระบบเครือข่ายไร้สายให้กับบุคคลอื่นในกรณีเชื่อมต่อระบบเครือข่ายของบริษัทฯ

(12) สำหรับการใช้บริการด้านเครือข่ายจากผู้ให้บริการภายนอกในข้อตกลงควรกำหนดคุณสมบัติผู้ให้บริการภายนอก เช่น ต้องมีความรู้ความสามารถในการบริหารจัดการเครือข่าย หรือมีใบรับรองต่าง ๆเป็นต้น

(13) สำหรับการใช้บริการด้านเครือข่ายจากผู้ให้บริการภายนอกในข้อตกลงควรกำหนดคุณสมบัติด้านความมั่นคงปลอดภัยสำหรับการสร้างความมั่นคงปลอดภัยในการให้บริการเครือข่าย ได้แก่ การพิสูจน์ตัวตน การเข้ารหัสข้อมูล การเชื่อมต่อทางเครือข่าย

(14) สำหรับการใช้บริการด้านเครือข่ายจากผู้ให้บริการภายนอกในข้อตกลงควรกำหนดให้บริษัทฯ สามารถดำเนินการตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอกได้

แนวปฏิบัติด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition , development and maintenance)

(1) การพัฒนาระบบ การจัดหา การบำรุงรักษา ต้องได้รับอนุญาตจากผู้มีอำนาจก่อนดำเนินการ

(2) บริษัทฯ ต้องกำหนดกฎสำหรับการพัฒนาซอฟต์แวร์และนโยบายการพัฒนาระบบให้มีความปลอดภัย (Secure development policy) และนำมาใช้งานสำหรับการพัฒนาภายในบริษัทฯ

(3) การพัฒนาระบบต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบดังต่อไปนี้

3.1) การให้สิทธิ์ต่ำที่สุด (Least Privileges)

3.2) การให้สิทธิ์เฉพาะที่จำเป็นในการปฏิบัติงาน (Need to know)

3.3) การออกแบบระบบให้สามารถป้องกันได้หลายๆ ชั้น (Defense in-Depth)

3.4) การออกแบบในลักษณะเปิด (Open Design)

3.5) หลักการวิศวกรรมด้านความมั่นคงปลอดภัย (Security Engineering Principles)

(4) การพัฒนาระบบจะต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยดังต่อไปนี้

4.1) การรักษาความลับของข้อมูลสารสนเทศ (Confidentiality)

4.2) การรักษาความถูกต้องสมบูรณ์ของข้อมูลสารสนเทศ (Integrity)

4.3) ความพร้อมใช้ของข้อมูลสารสนเทศ (Availability)

4.4) การระบุตัวตนผู้ใช้งาน (Identification)

4.5) การพิสูจน์ตัวตนผู้ใช้งาน (Authentication)

4.6) การกำหนดสิทธิ์ (Authorization)

4.7) มีการจัดเก็บ Audit Logging

4.8) มาตรฐานรักษาความมั่นคงปลอดภัยที่ต้องปฏิบัติตาม เช่น OWASP Top 10, SANS Top 20 เป็นต้น

4.9) ความต่อเนื่องของการให้บริการระบบสารสนเทศ (Continuity)

(5) ผู้พัฒนาระบบมีสิทธิที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการดังนี้

5.1) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยของระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

5.2) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

5.3) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่น ในลักษณะเช่นเดียวกับหนอนหรือมัลแวร์

5.4) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

5.5) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพ ที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย ไม่ว่าจากช่องทางการสื่อสารใด ๆ ก็ตาม

(6) ในกรณีพัฒนาซอฟต์แวร์ต้องปฏิบัติตามมาตรฐานการพัฒนาเว็บแอปพลิเคชัน

(7) การเปลี่ยนแปลงต่อระบบภายในวงจรการพัฒนา เช่น กระบวนการ SDLC จะได้รับการควบคุม โดยอาศัยกระบวนการควบคุมการเปลี่ยนแปลงที่เป็นทางการ

(8) เมื่อต้องการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวข้องกับแอปพลิเคชันจะต้องได้รับการทดสอบก่อนการใช้งานจริง เพื่อให้มั่นใจว่าไม่มีผลกระทบต่อการดำเนินการของบริษัทฯ หรือต่อความมั่นคงปลอดภัยสารสนเทศ

(9) ในกรณีที่มีการแก้ไขเปลี่ยนแปลงชุดซอฟต์แวร์แพ็คเกจจะต้องถูกป้องกันจำกัดการเปลี่ยนแปลงที่จำเป็นและการเปลี่ยนแปลงทั้งหมดจะต้องถูกควบคุมอย่างเข้มงวด

(10) บริษัทฯ จะต้องกำหนดและป้องกันความมั่นคงปลอดภัยสภาพแวดล้อม เพื่อการพัฒนาให้เหมาะสม

(11) การจ้างบุคคลภายนอกมาพัฒนาซอฟต์แวร์จะต้องได้รับการตรวจสอบและดูแลเฝ้าระวัง โดยเจ้าของระบบและกลุ่มงานเทคโนโลยีสารสนเทศ

(12) การพัฒนาระบบจะต้องดำเนินการทดสอบฟังก์ชันความมั่นคงปลอดภัยในระหว่างการพัฒนาระบบ

(13) ต้องมีการทดสอบและเกณฑ์การตรวจรับสำหรับระบบสารสนเทศใหม่ และหากมีการปรับปรุงควรได้รับการปรับเวอร์ชันอย่างเหมาะสม

(14) ต้องมีการควบคุมข้อมูลที่ใช้ในการทดสอบ ไม่ควรนำข้อมูลจากระบบงานจริงมาใช้ทดสอบ ควรดำเนินการสร้างข้อมูลจำลองขึ้นมา หรือหากมีความจำเป็นที่ต้องนำข้อมูลจากระบบงานจริงมาใช้ ควรจะทำเครื่องหมายหรือแทนที่ข้อมูล เพื่อไม่ให้สามารถอ้างถึงข้อมูลจริงได้

แนวปฏิบัติด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

(1) เจ้าของระบบมีอำนาจหน้าที่และความรับผิดชอบในการอนุมัติการเข้าถึงระบบสารสนเทศ โดยบุคคลภายนอกจะต้องทำหนังสือขออนุญาตเข้าถึงระบบสารสนเทศเป็นลายลักษณ์อักษร และต้องมีรายละเอียดประกอบอย่างน้อย ดังนี้

1.1) เหตุผลในการเข้าถึงระบบสารสนเทศ

1.2) ระยะเวลาในการเข้าถึงระบบสารสนเทศ

1.3) คำยินยอมจากเจ้าของระบบที่รับผิดชอบในการนำบุคคลภายนอกเข้ามาปฏิบัติงานภายในบริษัท

(2) บริษัทคู่สัญญาที่ปฏิบัติงานให้กับบริษัทฯ ไม่ว่าจะปฏิบัติงานในบริษัทฯ หรือนอกบริษัทฯ จะต้องลงนามในสัญญาจ้าง โดยจะต้องจัดทำสัญญาจ้างให้เสร็จสิ้นก่อนการกำหนดสิทธิให้บุคคลภายนอกนั้นเข้าถึงระบบสารสนเทศ

(3) บริษัทคู่สัญญาที่พัฒนาระบบสารสนเทศจะต้องลงนามในสัญญาให้เก็บรักษาข้อมูลไว้เป็นความลับและสรุปรายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการภายนอก

(4) บริษัทฯ จะต้องควบคุมให้บุคคลภายนอกรักษาความมั่นคงปลอดภัย ทั้งทางด้านการรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาให้ระบบพร้อมให้บริการอยู่เสมอ (Availability) อย่างเคร่งครัด

(5) บริษัทฯ ต้องควบคุมและเฝ้าระวังการปฏิบัติงานของผู้ให้บริการภายนอกให้เป็นไปตามขอบเขตที่ได้กำหนดไว้

(6) ในกรณีที่มีการเปลี่ยนแปลงเงื่อนไขการให้บริการ การเปลี่ยนแปลงรูปแบบหรือเทคโนโลยีของการให้บริการ ผู้ที่เกี่ยวข้องจะต้องทบทวนการแก้ไขเปลี่ยนแปลงสัญญาร่วมกับผู้ให้บริการภายนอก

(7) ผู้ให้บริการภายนอกมีหน้าที่ต้องแจ้งให้กับเจ้าของระบบทราบทันทีที่พบว่ามีการคุกคามที่มีผลต่อความมั่นคงปลอดภัย และเจ้าของระบบต้องแจ้งให้กลุ่มงานเทคโนโลยีสารสนเทศและผู้ดูแลระบบทราบ

แนวปฏิบัติด้านการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสนเทศ (Information security incident management)

(1) บริษัทฯ ต้องกำหนดหน้าที่และกระบวนการปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อให้มั่นใจว่าการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยจะดำเนินการได้อย่างรวดเร็วเป็นระบบและมีประสิทธิผล

(2) บริษัทฯ ต้องจัดหาช่องทางสำหรับรายงานเหตุการณ์ความมั่นคงปลอดภัยที่เหมาะสม และรวดเร็วเท่าที่เป็นไปได้

(3) ผู้ดูแลระบบต้องทำการวิเคราะห์และแก้ไขสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

แนวปฏิบัติด้านประเด็นด้านการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

(1) บริษัทฯ ต้องจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผน อย่างน้อยปีละ 1 ครั้ง

(2) บริษัทฯ จะต้องจัดเตรียมอุปกรณ์ประมวลผลสารสนเทศสำรองและศูนย์คอมพิวเตอร์สำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

(3) ผู้ใช้งานต้องสำรองข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานได้อย่างเพียงพอเพื่อนำมาดำเนินงานต่อไปได้ ในกรณีฉุกเฉินที่เกิดขึ้น

แนวปฏิบัติด้านการปฏิบัติตามข้อกำหนด (Compliance)

(1) บริษัทฯ ต้องทบทวนแนวทางในการบริหารจัดการความปลอดภัยสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญเกิดขึ้น

(2) ผู้ใช้งานต้องระมัดระวังไม่ใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ และบริษัทฯ จะไม่รับผิดชอบต่อความผิดที่เกิดจากการใช้ซอฟต์แวร์ที่ไม่ลิขสิทธิ์ของผู้ใช้งาน

(3) บริษัทฯ ต้องจัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

(4) บริษัทฯ ต้องมีการจัดทำแนวทางในการตรวจประเมิน และดำเนินการตรวจประเมินด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งการตรวจประเมินโดยผู้ตรวจสอบภายใน (Internal auditor) หรือผู้ตรวจสอบอิสระจากภายนอก (External auditor)

ระเบียบปฏิบัติการใช้ระบบสารสนเทศสำหรับผู้ใช้งาน

ผู้ใช้งานระบบสารสนเทศของบริษัทฯมีหน้าที่ และความรับผิดชอบที่จะต้องปฏิบัติตามนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ และระเบียบปฏิบัติฉบับนี้โดยเคร่งครัด ดังนี้

การใช้งานทรัพย์สินสารสนเทศ

(1) ผู้ใช้งานสามารถถือครองอุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์โน๊ตบุ๊ค (Notebook) หรือคอมพิวเตอร์ตั้งโต๊ะ (PC / All in one PC) เพื่อใช้งานในกิจการของบริษัทฯ

(2) ผู้ใช้งานมีหน้าที่ต้องดูแลรักษาและรับผิดชอบต่อการชำชุดเสียหายหรือการสูญหายของทรัพย์สินสารสนเทศ และ/หรือ อุปกรณ์เทคโนโลยีสารสนเทศที่บริษัทฯ มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

(3) ผู้ใช้งานมีหน้าที่ต้องชดใช้ให้แก่บริษัทฯ ซึ่งค่าเสียหายอันเกิดจากการชำรุดเสียหายหรือการสูญหายของทรัพย์สินสารสนเทศ และ/หรือ อุปกรณ์เทคโนโลยีสารสนเทศที่บริษัทฯมอบไว้ให้ใช้งาน ตามมูลค่าทรัพย์สินหรือค่าเสียหายที่เกิดขึ้นตามจริง หากความเสียหายนั้นเกิดจากสาเหตุดังนี้

3.1) เกิดจากความจงใจ หรือ ประมาทเลินเล่อของผู้ใช้งาน

3.2) เกิดจากการใช้งานผิดวัตถุประสงค์ หรือ ใช้งานที่ไม่ใช่เพื่อกิจการของบริษัทฯ

3.3) เกิดจากอนุญาตให้ผู้อื่น ทั้งที่เป็นบุคลากรในบริษัทฯ หรือไม่ได้เป็นบุคลากรในบริษัทฯนำไปใช้งาน ยกเว้นได้รับเอกสารยินยอมให้บุคคลอื่นที่ไม่ใช่ผู้ถือครอง นำอุปกรณ์คอมพิวเตอร์ไปใช้งานและได้รับอนุมัติโดยผู้บริหารระดับกลุ่มงาน

(4) ผู้ใช้งานจะต้องใช้ทรัพย์สินสารสนเทศ และ/หรือ อุปกรณ์เทคโนโลยีสารสนเทศที่บริษัทฯจัดเตรียมไว้ให้สำหรับการดำเนินกิจการของบริษัทฯเท่านั้น ห้ามมิให้ผู้ใช้งานนำไปใช้งานที่ไม่เกี่ยวข้องกับบริษัทฯ หรือติดตั้งซอฟต์แวร์ หรืออุปกรณ์ฮาร์ดแวร์อื่นใดเพื่อใช้งานในกิจการอื่นๆ โดยเด็ดขาดไม่ว่าจะก่อให้เกิดความเสียหายหรือไม่ก็ตาม

(5) ผู้ใช้งานที่เป็นผู้ถือครองอุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์โน๊ตบุ๊ค (Notebook) หรือคอมพิวเตอร์ตั้งโต๊ะ (PC / All in one PC) สามารถใช้งานโปรแกรมคอมพิวเตอร์ตามที่กลุ่มงานเทคโนโลยีสารสนเทศติดตั้งในเครื่องให้เท่านั้น ไม่อนุญาตให้ติดตั้งโปรแกรมคอมพิวเตอร์อื่นใดเพิ่มเติม หากตรวจพบการละเมิดลิขสิทธิ์ที่ติดตั้งใช้งานในอุปกรณ์คอมพิวเตอร์ดังกล่าว ถือว่าเป็นการละเมิดนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ ถึงแม้ว่าการละเมิดนั้นจะเป็นไปเพื่อการปฏิบัติงานของบริษัทฯ ก็ตาม ผู้ใช้งานต้องรับผิดชอบผลของความเสียหายที่เกิดขึ้นทั้งหมดแต่เพียงผู้เดียว

(6) กรณีที่ผู้ใช้งานต้องการติดตั้งโปรแกรมอื่นใดเพื่อใช้ในการปฏิบัติงานซึ่งนอกเหนือจากที่กลุ่มงานเทคโนโลยีสารสนเทศจัดสรรให้ในเบื้องต้น ผู้ใช้งานต้องแจ้งความประสงค์ขอติดตั้งโปรแกรมดังกล่าวมาที่กลุ่มงานเทคโนโลยีสารสนเทศ ทั้งนี้หากกลุ่มงานเทคโนโลยีสารสนเทศพิจารณาโปรแกรมดังกล่าวแล้วพบว่าโปรแกรมดังกล่าวอาจส่งผลกระทบให้เกิดความเสียหายต่อระบบสารสนเทศของบริษัทฯ กลุ่มงานเทคโนโลยีสารสนเทศจะดำเนินการยกเลิกคำขอทันที

(7) โปรแกรมที่กลุ่มงานเทคโนโลยีสารสนเทศได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการปฏิบัติงานห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่นๆ ยกเว้นได้รับการอนุญาตจากผู้บริหารระดับกลุ่มงาน หรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์ซอฟต์แวร์นั้น

(8) ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ถือเป็นข้อมูลลับและเป็นทรัพย์สินของบริษัทฯ ต้องจัดเก็บข้อมูล ในพื้นที่ที่จัดเตรียมไว้ให้เท่านั้น ห้ามไม่ให้ทำการคัดลอกหรือทำซ้ำข้อมูลดังกล่าว ให้แก่ผู้อื่นหรือหน่วยงานภายนอก ยกเว้นได้รับเอกสารยินยอมและอนุมัติโดยผู้บริหารระดับกลุ่มงาน

(9) ผู้ใช้งาน ต้องไม่ทิ้งเอกสารสำคัญหรือสื่อบันทึกข้อมูลไว้ที่โต๊ะทำงานโดยไม่มีผู้ดูแล หรือไม่ได้ใช้งาน และต้องจัดหาสถานที่จัดเก็บอย่างปลอดภัย เช่น เก็บในตู้ที่มีอุปกรณ์ล็อค เป็นต้น

(10) ผู้ใช้งาน ต้องไม่ทิ้งเอกสารสำคัญไว้ที่เครื่องถ่ายเอกสาร เครื่องปริ้นเตอร์ หรือเครื่องสแกนเนอร์ เมื่อสั่งพิมพ์หรือสำเนาเรียบร้อยแล้วต้องเก็บเอกสารทันที

(11) เมื่อหมดความจำเป็นในการใช้งานข้อมูล ผู้ใช้งานต้องดำเนินการทำลายข้อมูลที่อยู่ในสื่อบันทึกข้อมูลทันที โดยผู้ใช้งานต้องทำการตรวจสอบประเภทของข้อมูลบนสื่อบันทึกข้อมูล และคัดแยกสื่อบันทึกข้อมูลออกตามหมวดหมู่หรือประเภทตามลำดับชั้นความลับ และเลือกวิธีการทำลายข้อมูลตามลำดับชั้นความลับที่บริษัทฯกำหนดไว้

(12) ห้ามผู้ใช้งานบันทึกไฟล์ข้อมูล อาทิ เพลง ภาพ วีดีโอ ภาพยนต์ ที่ไม่ถูกลิขสิทธิ์ไว้ในเครื่องคอมพิวเตอร์อุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์โน๊ตบุ๊ค (Notebook) หรือคอมพิวเตอร์ตั้งโต๊ะ (PC / All in one PC) ของบริษัทฯ โดยหากกลุ่มงานเทคโนโลยีสารสนเทศตรวจพบจะดำเนินการลบทิ้งโดยทันที

(13) ห้ามผู้ใช้งานนำเอกสารที่มีข้อมูลสำคัญกลับมาใช้ซ้ำ (Reuse)

13.1) ห้ามผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่ายอื่นในขณะที่มีการเชื่อมต่อระบบเครือข่ายของบริษัทฯในเวลาเดียวกันเพื่อป้องกันการบุกรุกหรือภัยคุกคามจากภายนอกเข้าสู่ระบบเครือข่ายของบริษัทฯ

13.2) ห้ามผู้ใช้งานนำอุปกรณ์เครือข่ายไร้สาย (Wireless) มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB Client หรือ Wireless Card โดยไม่ได้รับอนุญาตจากกลุ่มงานเทคโนโลยีสารสนเทศ

13.3) ผู้ใช้งานต้องทำลายข้อมูลสำคัญซึ่งอยู่บนกระดาษหรือวัสดุชั่วคราว เช่น CD/DVD เป็นต้น เมื่อหมดความจำเป็นต้องใช้งาน โดยทำให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้และไม่สามารถนำกลับไปใช้ได้

13.4) ผู้ใช้งานจะต้องคืนทรัพย์สินสารสนเทศ และ/หรือ อุปกรณ์เทคโนโลยีสารสนเทศให้แก่บริษัทฯในทันที ณ วันที่หมดความจำเป็นที่ต้องใช้งาน หรือวันที่เปลี่ยนแปลงหน้าที่การทำงาน หรือวันที่พ้นสภาพการเป็นลูกจ้างของบริษัทฯ หรือเมื่อบริษัทฯมีคำสั่งให้คืน

การเข้าถึงและการใช้งานระบบสารสนเทศ

(1) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศและระบบงานของบริษัทฯ จะต้องขออนุมัติการใช้งานจากผู้มีอำนาจอนุมัติ เพื่อให้กลุ่มงานเทคโนโลยีสารสนเทศกำหนดสิทธิ์การเข้าถึง

(2) ห้าม ผู้ใช้งานกระทำการใดๆ ดังต่อไปนี้

2.1) ล่วงรู้ข้อมูลบัญชีผู้ใช้และรหัสผ่านของผู้อื่น รวมถึงนำบัญชีผู้ใช้และรหัสผ่านของผู้อื่นไปใช้งาน

2.2) อนุญาตให้ผู้อื่น ใช้ร่วม เผยแพร่ แจกจ่าย หรือทำให้ล่วงรู้บัญชีผู้ใช้และรหัสผ่านของตน

(3) ผู้ใช้งานต้องป้องกันและดูแลรักษาข้อมูลบัญชีผู้ใช้ และรหัสผ่านของตน หากทราบว่าข้อมูลบัญชีผู้ใช้ และ/หรือ รหัสผ่านถูกเปิดเผยต้องเปลี่ยนรหัสผ่านใหม่ทันที

(4) ผู้ใช้งานจะต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ระบบสารสนเทศหรือระบบงานของบริษัทฯ และหากพบว่าการพิสูจน์ตัวตนนั้นไม่สามารถกระทำการได้สำเร็จ เช่น ลืมรหัสผ่าน รหัสผ่านโดนล็อค หรือเกิดจากปัญหาหรือข้อผิดพลาดใดๆ ผู้ใช้งานจะต้องแจ้งกลุ่มงานเทคโนโลยีสารสนเทศโดยทันที

(5) ผู้ใช้งาน จะต้องทำการล็อคหน้าจอเครื่องคอมพิวเตอร์ด้วยรหัสผ่านทุกครั้งเมื่อไม่ได้ใช้งาน และต้องทำการพิสูจน์ตัวตนเมื่อกลับมาใช้งานเครื่องคอมพิวเตอร์

(6) ผู้ใช้งานต้องออกจากระบบงานเมื่อสิ้นสุดหรือไม่มีความจำเป็นต้องใช้งาน

(7) ห้ามมิให้พนักงานเปิดเพลงที่ไม่มีใบอนุญาตและเพลงที่ทางบริษัทไม่ได้เป็นผู้จัดส่งให้เข้าในระบบกระจายเสียงของบริษัท ทั้งนี้รวมถึงการเปิดเพลงจากแผ่นเสียงที่มีลิขสิทธิ์ถูกต้อง หรือจากเครือข่ายสาธารณะ เช่น วิทยุ YouTube เป็นต้น เนื่องจากการกระทำดังกล่าวถือเป็นการละเมิดลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ ในเรื่องของการเผยแพร่ผลงานต่อสาธารณชนโดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

(8) เมื่อพบว่าระบบสารสนเทศ หรือระบบงานมีความผิดปกติ หรือบกพร่อง หรือไม่เอื้ออำนวยต่อการปฏิบัติงาน ให้รายงานความบกพร่องหรือปัญหาที่เกิดขึ้นต่อผู้บังคับบัญชาหน่วยงานและแจ้งกลุ่มงานเทคโนโลยีสารสนเทศเพื่อดำเนินการแก้ไขโดยทันที

(9) ผู้ใช้งานที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใดๆ ในบริษัทฯ ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชาและกลุ่มงานเทคโนโลยีสารสนเทศ รวมถึงห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

(10) ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำใดๆ ในระบบสารสนเทศของบริษัทฯ ที่เกิดขึ้นจากบัญชีชื่อผู้ใช้งาน และ/หรือรหัสผ่านของผู้ใช้งานนั้น ไม่ว่าการกระทำนั้นๆ จะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

กลุ่มงานเทคโนโลยีสารสนเทศ ได้จัดสรรให้บุคลากรของบริษัทฯ มีบัญชีจดหมายอิเล็กทรอนิกส์ส่วนบุคคลเพื่อใช้ในการปฏิบัติงานของบริษัทฯ ดังนั้นบุคลากรต้องใช้จดหมายอิเล็กทรอนิกส์อย่างระมัดระวัง และปฏิบัติตามระเบียบดังต่อไปนี้

(1) เมื่อผู้ใช้งานได้รับบัญชีผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ให้ผู้ใช้งานเข้าใช้งานจดหมายอิเล็กทรอนิกส์โดยรหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ที่ได้รับ และให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันทีเมื่อเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรก

(2) ผู้ใช้งานต้องไม่ใช้บัญชีผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของบัญชีผู้ใช้และให้ถือว่าเจ้าของบัญชีผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์รายนั้นเป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

(3) ผู้ใช้งานต้องตรวจสอบรายชื่อผู้รับจดหมายอิเล็กทรอนิกส์ให้ถูกต้องก่อนส่งทุกครั้ง เพื่อป้องกันการส่งผิดตัวผู้รับ

(4) ผู้ใช้งานสามารถระบุรายละเอียดข้อความลงท้ายจดหมายอิเล็กทรอนิกส์ (E-mail Signature) โดยให้มีข้อมูล ชื่อ ตำแหน่ง สังกัด ชื่อบริษัทฯ หมายเลขโทรศัพท์ และชื่อบัญชีจดหมายอิเล็กทรอนิกส์ให้ชัดเจน

(5) ไม่อนุญาตให้ใช้จดหมายอิเล็กทรอนิกส์ของบริษัทฯในการปฏิบัติงานดังต่อไปนี้

5.1) ส่งจดหมายขยะ (Spam Mail)

5.2) ส่งจดหมายลูกโซ่ (Chain Letter)

5.3) ส่งจดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

5.4) ใช้ข้อความที่ไม่สุภาพ หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม อันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์

5.5) รับหรือส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อความที่ผิดกฎหมาย น่ารังเกียจ ลามกอนาจารมีเจตนามุ่งร้าย ข่มขู่ทำร้าย ละเมิด หลอกลวง หมิ่นประมาท ใส่ร้าย แสดงถึงความเกลียดชัง หรือสนับสนุนการกระทำซึ่งเป็นอาชญากรรมหรือสร้างความไม่สงบเรียบร้อย หรือกระทบต่อศีลธรรมอันดี หรือฝ่าฝืนนโยบายของบริษัท

5.6) ใช้จดหมายอิเล็กทรอนิกส์ของบริษัทฯโฆษณาหรือใช้ประโยชน์สำหรับตนเองและผู้อื่นซึ่งไม่เกี่ยวข้องกับการปฏิบัติงานของบริษัทฯ

5.7) การส่งจดหมายอิเล็กทรอนิกส์ของบริษัทฯร่วมไปกับบัญชีจดหมายอิเล็กทรอนิกส์ภายนอกบริษัทฯ

5.8) นำบัญชีจดหมายอิเล็กทรอนิกส์ (Email Account) ซึ่งเป็นของบริษัทฯไปเผยแพร่สู่บุคคลอื่น ไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในเว็บบอร์ด ในชุดคำถามหรือแบบสอบถามจากผู้ค้า เป็นต้น เว้นแต่การเผยแพร่นั้นเป็นไปเพื่อผลประโยชน์ของบริษัทฯ หรือได้รับอนุญาตจากผู้มีอำนาจแล้วเท่านั้น

5.9) ส่งข้อความที่เป็นความเห็นส่วนบุคคลโดยอ้างว่าเป็นความเห็นของบริษัทฯหรือก่อให้เกิดความเสียหายต่อบริษัทฯ

(6) ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เพื่อเป็นการป้องกันในการเปิดไฟล์ที่สามารถประมวลผลได้

(7) ผู้ใช้งานควรบริหารจัดการแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

(8) ไม่อนุญาตให้ผู้ใช้งานใช้อีเมลภายนอกระบบเครือข่ายของบริษัทฯ เช่น Hotmail, Gmail เป็นต้น ในการรับส่งข้อมูลสำคัญของบริษัทฯ เพื่อป้องกันข้อมูลความลับของบริษัทฯ รั่วไหล

(9) ห้ามผู้ใช้งานกระทำการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบ สารสนเทศของบริษัทฯหรือระบบผู้อื่น

การใช้งานอินเตอร์เน็ต

(1) ผู้ใช้งานต้องตระหนักถึงความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านอินเตอร์เน็ต

(2) ผู้ใช้งานต้องไม่ดาวน์โหลด เปิด หรือใช้ ชุดคำสั่ง โปรแกรมระบบงาน หรือข้อมูล บนเครือข่ายอินเตอร์เน็ต ที่เป็นการละเมิดลิขสิทธิ์ หรือเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูลบริษัทฯ

(3) ไม่อนุญาตให้ผู้ใช้งานดาวโหลดไฟล์ข้อมูล หรือรูปภาพใดๆ ที่

3.1) เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พ.ศ. ๒๕๖๐ รวมถึงฉบับที่มีการปรับปรุง

3.2) เข้าข่ายผิดต่อพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ รวมถึงฉบับที่มีการปรับปรุง

3.3) มีไวรัส หรือชุดคำสั่งไม่พึงประสงค์ (Malicious Code)

3.4) ไม่เกี่ยวข้องต่อการปฏิบัติงานของบริษัทฯ

(4) ผู้ใช้งาน ต้องไม่ใช้บริการบนระบบอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน เช่น ไม่เปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง ไม่เปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit torrent) เป็นต้น

(5) พนักงานทุกคนต้องตระหนักถึงความมั่นคงปลอดภัย ในการใช้งาน Social Network เช่น การเปิดเผยข้อมูลความลับของบริษัทฯ ซึ่งมีผลกระทบทางลบต่อภาพลักษณ์บริษัทฯ เป็นต้น

การปฏิบัติงานจากภายนอกสำนักงาน

(1) ผู้ใช้งานที่ต้องการเข้าถึงเครือข่ายภายในบริษัทฯ โดยใช้วิธีการเข้าถึงผ่านเครือข่ายจากภายนอกบริษัทฯ (Remote Login) ต้องขออนุมัติการใช้งานจากผู้มีอำนาจอนุมัติก่อนดำเนินการ

(2) กรณีที่ผู้ใช้งานมีความจำเป็นต้องเบิกใช้อุปกรณ์สื่อสารประเภทพกพาซึ่งเป็นทรัพย์สินสารสนเทศส่วนกลาง ของหน่วยงาน ให้ผู้ใช้งานขออนุมัติเบิกใช้จากผู้บังคับบัญชาและกลุ่มงานเทคโนโลยีสารสนเทศก่อนนำไปใช้งาน โดยเมื่อหมดความจำเป็นต้องใช้งานให้รีบนำส่งคืนหน่วยงานทันที

(3) ผู้ใช้งานที่มีความจำเป็นต้องนำเครื่องคอมพิวเตอร์พกพาออกไปใช้งานนอกสถานที่ ผู้ใช้งานต้องใช้งานด้วยความระมัดระวัง ไม่ละทิ้งเครื่องคอมพิวเตอร์พกพาไว้ในที่สาธารณะโดยไม่มีผู้ดูแลและต้องไม่อนุญาตให้บุคคลอื่นเข้าใช้เครื่องคอมพิวเตอร์พกพา เพื่อป้องกันการเข้าถึงหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

(4) ผู้ใช้งานต้องระวังการสูญหายของเครื่องคอมพิวเตอร์พกพา และการสูญหายของข้อมูลซึ่งจัดเก็บอยู่ภายในเครื่องคอมพิวเตอร์แบบพกพา

(5) ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์พกพาเข้ากับเครือข่ายสาธารณะ(Public Wi-Fi) ที่ไม่รู้จัก

(6) ในกรณีที่ผู้ใช้งานต้องปฏิบัติงานจากภายนอกบริษัทฯ จะต้องเชื่อมต่อเข้าระบบของบริษัทฯ โดยใช้ช่องทางที่กลุ่มงานเทคโนโลยีสารสนเทศจัดเตรียมให้เท่านั้น

การบริหารจัดการระบบงานและข้อมูลข่าวสารสารสนเทศ

(1) ผู้ใช้งานมีหน้าที่ในการป้องกันและดูแลรักษาชุดคำสั่ง โปรแกรมระบบงาน ทรัพย์สิน และข้อมูลของบริษัทฯ ดังนั้น หากเกิดการสูญหาย เสียหาย นำไปใช้ในทางที่มิชอบ เผยแพร่โดยไม่รับอนุญาต ไม่ว่าจะด้วยเจตนาหรือประมาทเลินเล่อของผู้ใช้งาน ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายนั้นทั้งสิ้น

(2) ผู้ใช้งานมีหน้าที่ใช้งานชุดคำสั่ง โปรแกรมระบบงาน ทรัพย์สินและข้อมูลที่บริษัท จัดเตรียมไว้ให้สำหรับการดำเนินธุรกิจของบริษัทฯ เท่านั้น

(3) ชุดคำสั่ง โปรแกรมระบบงาน ทรัพย์สิน และข้อมูล ที่ผู้ใช้งานพัฒนาหรือสร้างสรรค์ขึ้นสำหรับการดำเนินธุรกิจของบริษัทฯ ให้ถือว่าเป็นลิขสิทธิ์และ/หรือ ทรัพย์สินทางปัญญาของบริษัทฯแต่เพียงผู้เดียวเท่านั้น

(4) ห้ามผู้ใช้งานใช้ระบบสารสนเทศของบริษัทฯ กระทำการดังต่อไปนี้

4.1) นำข้อมูลดังต่อไปนี้ เข้าสู่ระบบสารสนเทศของบริษัทฯ หรือ ระบบผู้อื่น

- ข้อมูลปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่บริษัทฯ ผู้อื่นหรือลูกค้า
- ข้อมูลอันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชนทั่วไป
- ข้อมูลใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
- ข้อมูลใดๆ ที่มีลักษณะน่ารังเกียจ ลามกอนาจาร มีเจตนามุ่งร้าย ข่มขู่ทำร้าย ละเมิด หลอกลวง หมิ่นประมาท ใส่ร้าย แสดงถึงความเกลียดชัง และข้อมูลนั้นประชาชนทั่วไปอาจเข้าถึงได้

4.2) เผยแพร่หรือส่งต่อซึ่งข้อมูลโดยรู้อยู่แล้วว่าเป็นข้อมูลตามที่ได้ระบุไว้ในข้อที่ 4.1)

(5) ห้ามนำข้อมูลที่ปรากฏเป็นภาพของผู้อื่นเข้าสู่ระบบสารสนเทศของบริษัทฯ หรือระบบของผู้อื่น ที่ประชาชนทั่วไปอาจเข้าถึงได้ และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือได้รับความอับอาย เว้นแต่จะเป็นการนำข้อมูลเข้าสู่ระบบโดยสุจริต

(6) กระทำการ และ/หรือ ละเว้นการกระทำใดใด อันถือว่าหรืออาจถือว่าเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมาย และ/หรือ กฎระเบียบอื่นที่ผลบังคับใช้ต่อบริษัทฯ

การปฏิบัติตามกฎหมายและข้อบังคับ

(1) ผู้ใช้งาน ต้องปฏิบัติตามนโยบาย ระเบียบปฏิบัติ กฎข้อบังคับต่างๆ ของบริษัทฯ รวมถึงกฎหมายด้านเทคโนโลยีสารสนเทศใดๆ ที่มีผลบังคับใช้กับบริษัทฯ เพื่อลดความเสี่ยงที่อาจก่อให้เกิดความเสียหายและสนับสนุนให้การดำเนินงานของบริษัทฯ ดำเนินไปอย่างมีประสิทธิผล

(2) กรณีที่พบว่าผู้ใช้งานกระทำผิดโดยการไม่ปฏิบัติตามนโยบาย ระเบียบปฏิบัติ กฎข้อบังคับต่างๆ ของบริษัทฯ รวมถึงกฎหมายใดๆ ที่มีผลบังคับใช้กับบริษัทฯ ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานต้องได้รับการลงโทษทางวินัยตามที่บริษัทฯกำหนดไว้ ทั้งนี้หากการกระทำดังกล่าวมีข้อขัดแย้งต่อกฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ/หรือ พระราชบัญญัติลิขสิทธิ์ และ/หรือ กฎหมายอื่นใดที่เกี่ยวข้อง อาจถูกดำเนินคดีทางแพ่งและทางอาญาตามกฎหมายกำหนด

ประกาศ ณ วันที่ 22 กุมภาพันธ์ 2566

(นายธงชัย บุศราพันธ์)
ประธานเจ้าหน้าที่บริหารร่วม
บริษัท โนเบิล ดีเวลลอปเมนท์ จำกัด (มหาชน)