บริษัท สบาย คอนเน็กซ์ เทค จำกัด (มหาชน)

นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท สบาย คอนเน็กซ์ เทค จำกัด (มหาชน) และบริษัทในเครือ

การควบคุมเอกสาร

ครั้งที่	วันที่	รายละเอียด	ผู้ดูแลเอกสาร	ผู้ตรวจทาน	ผู้อนุมัติ
1	มีนาคม 2556	เขียนขึ้นใหม่ทั้งฉบับ	รองกรรมการผู้จัดการสนับสนุนธุรกิจ		ประธานกรรมการบริหาร
2	12 มิถุนายน 2566	แก้ไขให้สอดคล้องกับมาตรฐานความปลอดภัยและนโยบายขององค์กร	รองประธานเจ้าหน้าที่บริหาร กลุ่มเทคโนโลยีสารสนเทศ		ประธานเจ้าหน้าที่บริหาร

หลักการและเหตุผล

บริษัท สบาย คอนเน็กซ์ เทค จำกัด (มหาชน) มีภารกิจในการประกอบธุรกิจการผลิตและจำหน่ายเครื่องกรองน้ำดื่ม ด้วยประสบการณ์อันยาวนานมากว่า 47 ปี จากรุ่นสู่รุ่น และจากปณิธานอันแน่วแน่ที่ “อยากให้พี่น้องคนไทย มีน้ำดื่มที่สะอาด” บริษัทฯ จึงมุ่งมั่นที่จะพัฒนาผลิตภัณฑ์ที่มีคุณภาพ และเป็นมาตรฐานสากล ด้วยการนำระบบเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานตลอดจนกระบวนการผลิต เพื่อให้มั่นใจว่าบุคลากรของบริษัทฯ และประชาชนคนไทยทุกคนจะต้องได้รับการบริการที่ดี มีคุณภาพ แต่โดยที่ระบบสารสนเทศ มีความสำคัญกับการรองรับการทำงานของบริษัทฯมากขึ้น เพื่อป้องกันความเสี่ยง รวมถึงการช่วยลดผลกระทบ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังการเกิดปัญหากับระบบเทคโนโลยีสารสนเทศของบริษัทฯ จึงเห็นควรจัดทำนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของ บริษัทฯ และบริษัทในเครือ ให้เป็นมาตรฐานสากล โดยอ้างอิงจากมาตรฐานสากล ISO/IEC 27001 เพื่อเป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของ บริษัทฯ และบริษัทในเครือ ต่อไป

วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ บริษัทฯ และบริษัทในเครือดำเนินการอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ มีความมั่นคงปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

โดยมีวัตถุประสงค์ ดังต่อไปนี้

1. จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่ายคอมพิวเตอร์ของ บริษัทฯ และบริษัทในเครือ

2. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐานสากล และมีการปรับปรุงอย่างต่อเนื่อง

3. นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

4. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

5. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปี

องค์ประกอบของนโยบาย

นิยาม

ส่วนที่ 1 นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy)

ส่วนที่ 2 นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ส่วนที่ 3 นโยบายความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

ส่วนที่ 4 นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

ส่วนที่ 5 นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ
(Firewall Policy, Access control Policy)

ส่วนที่ 6 นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก
(Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy)

ส่วนที่ 7 นโยบายการสำรองและกู้คืนข้อมูล

ส่วนที่ 8 นโยบายการใช้เครื่องคอมพิวเตอร์และอุปกรณ์พกพา (BYOD)

ส่วนที่ 9 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ 10 แนวปฏิบัติการประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ 11 การพัฒนาระบบงานคอมพิวเตอร์ (Development)

ส่วนที่ 12 การใช้บริการคลาวด์คอมพิวติ้ง (Cloud Computing)

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทฯนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ ซึ่งพนักงานของบริษัทฯและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

นิยาม

- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของบริษัทฯ
- **ผู้บริหาร** หมายถึง ผู้ที่แบ่งงานให้ผู้ใต้บังคับบัญชาตามความรู้ความสามารถ พร้อมให้คำแนะนำอย่างเหมาะสม เพื่อให้งานบรรลุผลอย่างมีคุณภาพ
- **ผู้ดูแลระบบ (System Administrators, Network Administrators)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
- **การพิสูจน์ตัวตน (Authentication)** หมายถึง ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง
- **ระบบสารสนเทศ (Information System)** หมายถึง ระบบของการจัดเก็บ ประมวลผลข้อมูล และการเชื่อมต่อเข้าระบบเครือข่ายโดยอาศัยบุคคลและเทคโนโลยีสารสนเทศในการดำเนินการ เพื่อให้ได้สารสนเทศที่เหมาะสมกับงานหรือภารกิจแต่ละอย่าง (ระบบ SBNEXT Application, ERP Wireless, Internet)
- **สินทรัพย์ (Asset)** หมายถึง ข้อมูล ระบบข้อมูล ทรัพย์สินด้านเทคโนโลยีสารสนเทศ ทรัพย์สินด้านระบบคอมพิวเตอร์และเครือข่าย โปรแกรมประยุกต์ (Application Software) และโปรแกรมระบบ (System Software) เป็นต้น รวมถึงสิ่งใดก็ตามที่มีคุณค่าสำหรับบริษัทฯ ซึ่งเป็นสิ่งที่จับต้องได้และจับต้องไม่ได้
- **ทรัพย์สินทางปัญญา (Intellectual Property)** หมายถึง ผลงานอันเกิดจากการประดิษฐ์คิดค้น หรือสร้างสรรค์ของมนุษย์ โดยรัฐให้ความคุ้มครองว่าเป็นสิทธิของผู้ประดิษฐ์ หรือผู้สร้างสรรค์ในการนำไปหาประโยชน์ได้อย่างเต็มที่

- **จดหมายอิเล็กทรอนิกส์ (E-mail)** หมายถึง วิธีการรับส่งข้อมูลระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงกัน โดยข้อมูลที่ได้จะเป็นทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง ในรูปแบบดิจิทอล (Digital) ซึ่งประกอบด้วยเนื้อหา ที่อยู่ของผู้ส่ง และที่อยู่ของผู้รับ (ซึ่งอาจมีมากกว่าหนึ่ง)
- **บัญชีชื่อผู้ใช้งาน (Username)** หมายถึง บัญชีของผู้ใช้งานที่ได้รับอนุญาต (Authorized user) ให้สามารถใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาทที่บริษัทฯกำหนด
- **ผู้ใช้งาน (User)** หมายถึง เจ้าหน้าที่ของบริษัทฯ ผู้มีสิทธิเข้าใช้ทรัพย์สิน ระบบสารสนเทศของบริษัทฯ
- **สิทธิ์ของผู้ใช้งาน (User right)** หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตดังกล่าวนั้น สำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
- **ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)** หมายถึง การรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
- **เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืน

นโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

- **ความลับ (Confidentiality)** หมายถึง การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับ และจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

- **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของบริษัทฯ ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

- **การรักษาความถูกต้องครบถ้วน (Integrity)** หมายถึงการรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ์ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

- **ความพร้อมใช้งาน (Availability)** หมายถึงการรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

- **ความถูกต้องแท้จริง (Authenticity)** หมายถึง การความสามารถในการพิสูจน์ฝ่าย (Authentication) และการสามารถในการพิสูจน์สิทธิ์ (Authorization) ของผู้ที่เกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ ทั้งภายในและภายนอก

- **การสามารถในการพิสูจน์สิทธิ์ (Authorization)** หมายถึงการตรวจสอบว่า บุคคล อุปกรณ์ไอที หรือแอพพลิเคชั่น นั้นๆ ได้รับอนุญาตให้ดำเนินการอย่างหนึ่งอย่างใดต่อระบบสารสนเทศหรือไม่

- **ความรับผิด (Accountability)** หมายถึง ความพร้อมที่จะให้ตรวจสอบ และ ความรับผิดชอบต่องานและข้อมูลของผู้ใช้งานและเจ้าของข้อมูล โดยมีผู้อื่นซึ่งได้รับมอบหมายจากผู้บังคับบัญชา เข้ามาตรวจสอบได้ตลอดเวลา
- **การปกป้องข้อมูล (Data Protection)** หมายถึงการป้องกันข้อมูลส่วนบุคคลต่อการประสงค์ร้ายของบุคคลที่สาม
- **นโยบายด้านความมั่นคงปลอดภัย (Security Policy)** หมายถึงนโยบายที่แสดงเป้าหมายที่จะต้องปกป้อง และขั้นตอนทั่วไปของกระบวนการรักษาความมั่นคงปลอดภัย ในบริบทของความต้องการอย่างเป็นทางการของบริษัทฯ
- **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- **เจ้าหน้าที่ของบริษัท** หมายถึง บุคลากรที่ปฏิบัติงาน หรืออยู่ในความดูแลของบริษัทฯ
- **เครือข่ายไร้สาย (Wireless)** หมายถึง เครือข่ายเฉพาะที่ ถ่ายโอนข้อมูลผ่านอากาศในย่านความถี่วิทยุที่อนุญาตให้ใช้ได้โดยไม่ต้องจดทะเบียนโดยปราศจากการใช้สายสัญญาณ
- **ระบบเครือข่ายไร้สาย (WLAN= Wireless Local Area Network)** หมายถึง ระบบการสื่อสารข้อมูลที่นำมาใช้ทดแทน หรือเพิ่มต่อกับระบบเครือข่ายใช้สายแบบดั้งเดิมโดยใช้การส่งคลื่นความถี่วิทยุในย่านวิทยุ RF และคลื่นอินฟราเรดในการรับและส่งข้อมูลระหว่างคอมพิวเตอร์แต่ละเครื่องผ่านทางอากาศ ทะลุกำแพง เพดาน หรือสิ่งก่อสร้างอื่นๆ โดยปราศจากความต้องการของการเดินสาย

- **VPN (Virtual Private Network)** หมายถึง เทคโนโลยีการเชื่อมต่อเครือข่ายนอกอาคาร (WAN - Wide Area Network) เป็นระบบเครือข่ายภายในบริษัทฯ ซึ่งเชื่อมเครือข่ายในแต่ละสาขาเข้าด้วยกัน โดยอาศัย Internet เป็นตัวกลาง มีระบบเข้ารหัสป้องกันการลักลอบใช้ข้อมูล
- **DMZ (Demilitarized Zone)** หมายถึง เป็นคำจำกัดความของโซนอีกประเภทหนึ่งที่ไม่ใช่ทั้ง Internal (เครือข่ายภายใน) และ External (เครือข่ายภายนอกหรือเครือข่ายอินเทอร์เน็ต) แต่หมายถึงเครือข่ายที่ต้องมีการสื่อสารกับทั้งเครือข่ายภายในและเครือข่ายภายนอก
- **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานที่ไม่ได้อยู่ภายใต้บริษัทฯ ที่บริษัทฯ อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
- **คอมพิวเตอร์พกพา** หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่สามารถประมวลผลได้ และสามารถเชื่อมต่อกับระบบเครือข่ายสื่อสารได้
- **กลุ่มเทคโนโลยีสารสนเทศ** หมายถึง กลุ่มเทคโนโลยีสารสนเทศของ บริษัท สบาย คอนเน็กซ์ เทค จำกัด (มหาชน)
- **เจ้าหน้าที่ BA** หมายถึง Business Analyst บุคลากรในหน่วยงานคอมพิวเตอร์ ทำ หน้าที่ในการวิเคราะห์ข้อมูลขององค์กรและการดำเนินธุรกิจทั้งข้อมูลจริง และ สมมุติฐาน แล้วนำข้อมูลที่ได้ไปสู่ระบบ หรือกระบวนการแก้ไขปัญหาต่อไป
- **เจ้าหน้าที่ SA** หมายถึง System Analyst บุคลากรในหน่วยงานคอมพิวเตอร์ ทำหน้าที่รับผิดชอบในการออกแบบ และสร้างระบบประมวลผลข้อมูลตั้งแต่การเตรียมข้อมูลกำหนดโครงสร้างข้อมูล วิธีการประมวลผลโดยออกแบบเป็นผังลำดับการทำงานจนกระทั่งได้ผลตามต้องการ
- **เจ้าหน้าที่ Application Support** หมายถึง บุคลากรในหน่วยงานคอมพิวเตอร์ ทำหน้าที่ทดสอบระบบที่ทาง Programmer ได้ดำเนินการพัฒนาหรือดำเนินการแก้ไขระบบฯ

- **ระบบ Software** หมายถึง ระบบสารสนเทศที่อยู่ในรูปแบบซอฟต์แวร์
- **บำรุงรักษาระบบ Software** หมายถึง การตรวจสอบระบบให้มีความสมบูรณ์พร้อมใช้งาน โดยตรวจหาข้อผิดพลาดที่จะทำให้ระบบเกิดปัญหา แล้วนำปัญหาที่ตรวจพบไปแก้ไขตามกระบวนการพัฒนาระบบสารสนเทศ ข้อ 3.
- **Process Owner** หมายถึง ผู้รับผิดชอบในกระบวนการ และผู้อนุมัติการทำงานของฝ่ายงานที่ขอใช้บริการฯ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท สบาย คอนเน็กซ์ เทค จำกัด (มหาชน) และบริษัทในเครือ

ส่วนที่ 1

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy)

วัตถุประสงค์

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ ของบริษัทฯ จัดทำขึ้นเพื่อเป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ และเพื่อยกระดับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ ให้เป็นมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังการเกิดปัญหากับระบบเทคโนโลยีสารสนทศของบริษัทฯ เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของบริษัทฯ

แนวปฏิบัติ

หมวด 1 ว่าด้วยการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

1.1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน และรหัสผ่านโดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน ยกเว้น ระบบ ERP ที่ใช้บัญชีร่วมกันโดยผู้ดูแลระบบ ต้องสอบทานสิทธิ์การใช้งานปีละ 2 ครั้ง และต้องลงลายลักษณ์อักษรผู้ใช้บัญชีร่วมกัน ทั้งนี้ผู้ใช้บัญชีร่วมกันต้องตระหนักถึงความรับผิดชอบร่วมกันที่ไม่สามารถปฏิเสธความรับผิด

1.2 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

1.3 ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรมากกว่า 8 ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข ตัวอักษร และตัวอักษรพิเศษ

1.4 ผู้ใช้งาน ระบบควบคุมส่วนกลาง ต้องเปลี่ยนรหัสผ่าน ทุกๆ 3 เดือนและรหัสต้องไม่ซ้ำเดิมก่อนหน้า 3 ครั้ง

1.5 ผู้ใช้งานระบบควบคุมส่วนกลาง ใส่รหัสผ่านผิดเกิน 3 ครั้ง จะล็อคการเข้าใช้งานเป็นระยะ 15 นาที

1.6 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน ทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของบริษัทฯ โดย

1.6.1 คอมพิวเตอร์พกพา ต้องทำการพิสูจน์ตัวตนผ่านระบบที่บริษัทฯจัดหาไว้ ก่อนการใช้งาน

1.6.2 คอมพิวเตอร์ทุกเครื่องที่เป็นทรัพย์สินของบริษัทฯ ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

1.6.3 การใช้งานอินเทอร์เน็ต ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูล ซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

1.6.4 เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตน ก่อนการใช้งานทุกครั้ง

1.7 หากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อค หรือเกิดจากความผิดพลาดใดๆ ที่เกิดขึ้นจากผู้ใช้ หรือจากระบบ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

หมวด 2 ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

2.1 ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่ายของบริษัทฯ และศูนย์ผู้ให้บริการคลาวด์คอมพิวติ้ง (Cloud Computing) ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

2.2 ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่ายของบริษัทฯ และศูนย์ผู้ให้บริการคลาวด์คอมพิวติ้ง (Cloud Computing) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

2.3 ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

2.4 ผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

2.5 ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

2.6 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทฯ มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

2.7 กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของบริษัทฯที่ได้รับมอบหมาย

2.8 ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

2.9 ทรัพย์สินและระบบสารสนเทศต่างๆ ที่บริษัทฯ จัดเตรียมไว้ให้ใช้งาน มีวัตถุประสงค์เพื่อการใช้งานของบริษัทฯเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่บริษัทฯไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อบริษัทฯ

2.10 ความเสียหายใดๆ ที่เกิดจากการละเมิดตามหมวด 2 ว่าด้วยการบริหารจัดการทรัพย์สิน ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด 3 ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

3.1 ผู้ใช้งานต้องตระหนัก และระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของบริษัทฯ หรือเป็นข้อมูลของบุคคลภายนอก

3.2 ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของบริษัทฯ ถือเป็นทรัพย์สินของบริษัทฯ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมาย

3.3 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัทฯ หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

3.4 ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

3.5 ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร บริษัทฯจะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่บริษัทฯ ต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับบริษัทฯ ซึ่งบริษัทฯ อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด 4 ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

4.1 ผู้ใช้งานที่มีสิทธิ์ใช้งานโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการดังนี้

4.1.1 แก้ไขโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือถอดรหัสผ่านของบุคคลอื่น

4.1.2 แก้ไขโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

4.1.3 แก้ไขโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ซอฟต์แวร์

4.1.4 นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

4.2 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit torrent) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมาย

4.3 ห้ามเปิดหรือใช้งาน (Run) โปรแกรม ออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างปฏิบัติงาน

4.4 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทฯ ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของบริษัทฯ

4.5 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทฯ เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของบริษัทฯ

4.6 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัทฯเพื่อประโยชน์ทางการค้า

4.7 ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัทฯ โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

4.8 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัทฯ ต้องหยุดชะงัก

4.9 ห้ามใช้ระบบสารสนเทศของบริษัทฯ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมาย

4.10 ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

4.11 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัทฯ โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมาย

หมวด 5 ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

5.1 บรรดากฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของบริษัทฯ ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด 6 ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

6.1 บริษัทฯได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัทฯอนุญาตให้ใช้งานหรือที่บริษัทฯมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และบริษัทฯห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่

ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัทฯถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

6.2 ซอฟต์แวร์ ที่บริษัทฯได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อไปใช้งานที่อื่น

หมวด 7 ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

7.1 คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ตามที่บริษัทฯได้ประกาศให้ใช้

7.2 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

7.3 ผู้ดูแลระบบต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการให้เป็นปัจจุบันอยู่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

7.4 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดี ตลอดเวลารวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

7.5 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

7.6 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นทรัพย์สินของบริษัทฯหรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมาย หากกระทำการผิดใดๆ ดังที่กล่าวไว้ จะมีบทลงโทษตามระเบียบของบริษัทฯ

7.7 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์มัลแวร์หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของบริษัทฯ หากกระทำการผิดใดๆ ดังที่กล่าวไว้จะมีบทลงโทษตามระเบียบของบริษัทฯ

หมวด 8 ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

8.1 ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

หมวด 9 ว่าด้วยการให้ความรู้และฝึกอบรมเรื่องที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

9.1 บริษัทให้ความสำคัญกับการฝึกอบรมและให้ความรู้ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศแก่พนักงานอย่างสม่ำเสมอ เพื่อให้พนักงานทุกคนที่ความพร้อมในการความร่วมมือด้านการรักษาความปลอดภัยสารสนเทศของบริษัท

9.2 ผู้ใช้งานทุกคนจำเป็นต้องเข้ารับการฝึกอบรมและจำเป็นต้องรับทราบนโยบายรักษาความปลอดภัยสารสนเทศของบริษัท โดยให้มีการลงนามไว้เป็นลายลักษณ์อักษรชัดเจน

ส่วนที่ 2

นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ของบริษัทฯ โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

แนวปฏิบัติ

1. ห้ามผู้ใช้งานนำอุปกรณ์เครือข่ายไร้สายมาติดตั้งเองในระบบเครือข่ายของบริษัทฯ โดยไม่ได้รับอนุญาต
2. การติดตั้งระบบเครือข่ายไร้สาย ผู้ดูแลระบบต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับชา และต้องกำหนดรหัสการเข้าใช้งาน
3. ห้ามผู้ใช้งานเปิดการใช้ ad-hoc หรือ peer-to-peer Network
4. ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด โดยการกำหนดจุดติดตั้ง ต้องตระหนักถึงความปลอดภัยของอุปกรณ์ และห้ามติดตั้งใกล้กับผนัง หรือ หน้าต่างที่ติดกับภายนอกบริษัท
5. ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ โดยกำหนดชื่อ SSID ต้องเป็นชื่อที่คาดเดาได้ยาก มาใช้งาน

6. ผู้ดูแลระบบต้องกำหนดค่า WPA (Wi-Fi Protected Access) หรือเทคโนโลยีที่ทันสมัย ณ ปัจจุบัน ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point)
7. ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) หรือชื่อผู้ใช้ รหัสผ่าน ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) หรือชื่อผู้ใช้ และรหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง
8. ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงาน ต่อผู้บังคับบัญชาทราบทันที
9. ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

ส่วนที่ 3

นโยบายความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ผ่านระบบเครือข่ายของบริษัทฯ ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบ เครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวปฏิบัติ

1. ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) และยื่นคำขอกับฝ่ายเทคโนโลยีสารสนเทศผ่านความเห็นชอบของผู้บังคับบัญชา โดยผู้ดูแลระบบต้องตั้งชื่อ (e-mail) ตามรูปแบบบริษัทกำหนด ให้ชื่อเต็มภาษาอังกฤษ + “.” +อักษรแรกของนามสกุล ในกรณีที่ชื่อที่ต้องการซ้ำจะเพิ่มอักษรที่ 2, ที่ 3 หรือเพิ่มไปจนกว่าจะไม่ซ้ำ
2. ผู้ดูแลระบบต้องกำหนดขนาดของ Mailbox ผู้ใช้งาน (e-mail) จะมีพื้นที่จัดเก็บข้อมูล Mailbox ดังต่อไปนี้

   2.1 ผู้ใช้ทั่วไป (ระดับพนักงาน) ขนาด -1-GB

   2.2 ผู้จัดการ หรือหัวหน้างาน ขนาด -3-GB

   2.3 ผู้อำนวยการฝ่ายขึ้นไป ขนาด -5-GB

   ในกรณีขอเพิ่มขนาด Mailbox ต้องผ่านการพิจารณาจากผู้อนุมัติตามโครงสร้างการบังคับบัญชาของหน่วยงานผู้ขอ

3. เมื่อผู้ใช้งาน (User) ได้รับรหัสผ่าน (Password) ในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของบริษัทฯแล้ว และเมื่อมีการเข้าสู่ระบบในครั้งแรกต้องปลี่ยนรหัสผ่าน (Password) โดยทันที
3. ห้ามบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์
4. ระบบจะทำการแจ้งเตือนให้ปลี่ยนรหัสผ่าน (Password) ทุก 3 เดือน
5. ข้อกำหนดในการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

   5.1 ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

   5.2 ห้ามใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของบริษัทฯ ไปใช้ในงานที่ไม่ใช้งานของบริษัทฯ

   5.3 ห้ามสร้าง หรือ ส่งข้อความ และแนบไฟล์ที่มีเนื้อหา ข้อความ รูปภาพที่สื่อไปในทางไม่เหมาะสมเช่น เรื่องทางเพศ เรื่องว่าร้ายผู้อื่น เป็นต้น หากผู้ใช้งาน (user) ได้รับอีเมล์ที่มีลักษณะดังกล่าว ต้องลบทิ้งทันที และห้ามส่งต่อไปโดยเด็ดขาด
6. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง
7. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)
8. การลงทะเบียนและเงื่อนไขในการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ให้เป็นไปตามแนวทางปฏิบัติการเข้าถึงระบบสารสนเทศของบริษัทฯ

ส่วนที่ 4

นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต อย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

แนวปฏิบัติ

1. ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายก่อน
2. ผู้ใช้งานต้องใช้ข้อความที่สุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้งานเครือข่ายเท่านั้น
3. ไม่ใช้ระบบอินเทอร์เน็ต ของบริษัทฯ เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับบริษัทฯ
4. ห้ามมิให้ผู้ใช้งานอินเทอร์เน็ตในระหว่างเวลาทำงานเพื่อการรับส่งข้อมูลหรือการใช้งานแฟ้มข้อมูลร่วมกัน (Shared File) หรือที่มิได้เกี่ยวข้องกับการทำงาน เช่น ข้อมูลหนัง ข้อมูลเพลง ข้อมูลเกมส์ เป็นต้น

5. ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น กล่าวคือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การเผยแพร่ข้อความใดๆ ที่ก่อนให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว บริษัทฯไม่มีส่วนรับผิดชอบความเสียหายดังกล่าว
6. ห้ามมิให้ผู้ใช้งานปฏิบัติการใดๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของบริษัทฯ
7. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทฯที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต
8. ระมัดระวังการดาวน์โหลด และการอัพเดท โปรแกรมใช้งานจากระบบอินเทอร์เน็ตและโปรแกรมต่างๆ โดยจะต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์
9. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของบริษัทฯ และไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัทฯ การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ
10. หลังจากเลิกใช้งานระบบต่างๆ ที่มีการเข้าสู่ระบบ ให้ทำการออกจากระบบทุกครั้งเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ส่วนที่ 5

นโยบายความมั่นคงปลอดภัยและการควบคุมการเข้าถึงระบบ

(Firewall Policy and Access control Policy)

วัตถุประสงค์

เพื่อควบคุมการสื่อสารระหว่างเครือข่ายภายในบริษัทฯกับเครือข่ายภายนอกบริษัทฯ และกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศ และการสื่อสารให้หยุดชะงัก โดยการกำหนด ตั้งค่าของไฟร์วอลล์ ของบริษัทฯ ให้มีประสิทธิภาพในการทำงาน และกำหนดให้กับอุปกรณ์ที่ต้องการเชื่อมโยงสื่อสารภายในบริษัทฯ รวมทั้งมีการทบทวนสิทธิ์ของผู้ใช้งานอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบไฟร์วอลล์ และการควบคุมการเข้าถึงระบบ

แนวปฏิบัติ

หมวด 1 ความปลอดภัยและการป้องกันไฟร์วอลล์

1. ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการระบบรักษาความปลอดภัยไฟร์วอลล์ทั้งหมด
2. ผู้ดูแลระบบต้องกำหนดนโยบาย การใช้งานไฟร์วอลล์
3. ผู้ดูแลระบบต้องกำหนดค่า (Configuration) หรือกำหนดนโยบาย เพื่อกลั่นกรองข้อมูลให้มีความปลอดภัยต่อระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ ป้องกันการบุกรุก ไวรัสรวมทั้ง Malicious code ต่าง ๆ มิให้เข้าถึงหรือสร้างความเสียหาย แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์
4. ผู้ดูแลระบบต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลง

ค่าพารามิเตอร์ (Parameter) ในลักษณะผิดปกติ ต้องดำเนินการแก้ไข และรายงานผู้บังคับบัญชาโดยทันที

5. ผู้ดูแลระบบต้องเปิดใช้งานไฟร์วอลล์ตลอดเวลา
6. ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ (Parameter) การกำหนดค่าใช้บริการ และการเชื่อมต่อ ที่ได้รับอนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง
7. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
8. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บ ข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน
9. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการ
10. ผู้ดูแลระบบ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

    10.1 ผู้ขอใช้งาน หรือผู้ที่ได้รับมอบหมายต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บังคับบัญชา โดยระบุข้อมูลดังนี้

        1. หมายเลข Port ที่ต้องการเปิด
        2. หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร
        3. วัตถุประสงค์ หรือ Application ที่ต้องการใช้งานผ่าน Port นั้น ๆ
        4. วันที่เริ่มใช้ และวันที่สิ้นสุดการใช้

10.2 ในการขอใช้งานหากพบว่าขัดต่อนโยบาย ประกาศ ระเบียบ ของบริษัทฯ หรือกฎหมาย หรืออาจเกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ ผู้บังคับบัญชาไม่อนุญาตให้ใช้งาน

10.3 ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานขัดต่อนโยบาย ประกาศ ระเบียบ ของบริษัทฯหรือกฎหมายหรืออาจเกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ ผู้บังคับบัญชาจะมอบหมายผู้ดูแลระบบยกเลิกการให้บริการทันที

11. ผู้ดูแลระบบมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

11.1 ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ทันที และแจ้งผู้บังคับบัญชาต้นสังกัดให้รับทราบต่อไป

หมวด 2 การควบคุมการเข้าถึงระบบสารสนเทศ

2.1 บริษัทฯ กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบสารสนเทศของบริษัทฯ เพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของบริษัทฯ จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บังคับบัญชา หรือผู้ที่ได้รับมอบหมาย

2.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

2.3 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของบริษัทฯ และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

2.4 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

หมวด 3 การบริหารจัดการการเข้าถึงระบบสารสนเทศ

3.1 การบริหารจัดการการเข้าถึงของผู้ใช้

3.1.1 การลงทะเบียนเจ้าหน้าที่ใหม่ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในบริษัทฯ เป็นต้น

3.1.2 กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบ เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอและผู้ใช้งานต้องรับทราบสิทธิ์เป็นลายลักษณ์อักษร

3.1.3 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน และรหัสผ่านของเจ้าหน้าที่

1. ผู้ดูแลระบบที่รับผิดชอบระบบนั้นๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ

2. การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน กรณีระบบจดหมายอิเล็กทรอนิกส์ ระบบอินทราเน็ต ระบบงานสารสนเทศหลัก ระบบฐานข้อมูลหลัก ต้องปฏิบัติตาม “แนวทางปฏิบัติการเข้าถึงระบบสารสนเทศของบริษัทฯ”
3. ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา
    3.1 ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ
    3.2 ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
    3.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
    3.4 ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น จำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

3.2 การบริหารจัดการการเข้าถึงระบบเครือข่าย

3.2.1 การเข้าสู่ระบบเครือข่ายภายในของบริษัทฯ โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายสื่อสารก่อนที่จะสามารถใช้งานได้ในทุกกรณี

3.2.2 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

3.2.3 ผู้ดูแลระบบต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

3.2.4 ระบบเครือข่ายทั้งหมดของบริษัทฯที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกบริษัทฯ ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ ไฟร์วอลล์ หรือ ฮาร์ดแวร์ อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

3.2.5 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของบริษัทฯในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

3.2.6 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

หมวดที่ 4 การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

4.1 ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ อย่างชัดเจน เพื่อความปลอดภัย

และสามารถใช้งานได้อย่างต่อเนื่อง โดยไม่เกิดการหยุดชะงักในการดำเนินงาน รวมถึงอุปกรณ์ที่ใช้งานร่วมทุกๆ ระบบภายในของบริษัท

4.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานเป็นลายลักษณ์อักษรโดยทันที เช่น บริการตรวจสอบช่องโหว่ความปลอดภัยของระบบ (VA Scan)

4.3 ต้องเปิดใช้บริการ เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

4.4 ต้องได้รับการติดตั้งปรับปรุงระบบซอฟท์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ อย่างสม่ำเสมอ โดยการดำเนินการต้องเป็นผู้ที่รับผิดชอบทดสอบบนระบบทดสอบ (UAT) และบันทึกการติดตั้ง หรือ เปลี่ยนแปลงค่าต่างๆ ต้องแจ้งผู้ที่เกี่ยวข้องทราบ เพื่อป้องกันผลกระทบที่อาจเกิดกับระบบนั้นๆ และปฏิบัติเช่นเดียวกับระบบหลัก (PROD) เช่น Web Server , Windows Server เป็นต้น

4.5 ต้องได้รับการติดตั้งและมีการทดสอบระบบป้องกันไวรัส เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งาน

4.6 ต้องได้รับการติดตั้งระบบสำรองข้อมูล (Backup) โดยมีการกำหนดช่วงเวลาที่ชัดเจน เพื่อป้องกันเหตุการณ์ต่างๆ อันอาจก่อให้เกิดความสูญเสียข้อมูลที่มีความสำคัญ และมีการทดสอบการย้อนคืนข้อมูล (Restore) โดยการทดสอบจะต้องมีผู้ใช้งาน (User) ร่วมทดสอบและลงลายลักษณ์อักษรปีละ 2 ครั้ง

4.7 ระบบคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อภายในระบบเครือข่ายของบริษัทฯ ต้องได้รับการ Join Domain ให้อยู่ภายใต้กลุ่ม Domain

หมายเหตุ กรณีมีข้อยกเว้นให้ระบุรายละเอียดคุณลักษณะระบบคอมพิวเตอร์แม่ข่ายที่ไม่ Join Domain เช่น

3.7.1 ระบบคอมพิวเตอร์แม่ข่ายที่ติดตั้งใน DMZ เพื่อป้องกันการโจมตีจากภายนอก

3.7.2 ระบบคอมพิวเตอร์แม่ข่าย Standalone ที่ไม่สามารถปรับปรุงระบบปฏิบัติการ (OS) ได้เพราะข้อจำกัดด้าน Software ต้องจัดทำบันทึกภายในเสนออนุมัติจากผู้มีอำนาจของฝ่ายเทคโนโลยีสารสนเทศ

3.7.3 การตั้งชื่อระบบคอมพิวเตอร์แม่ข่าย ต้องดำเนินการตั้งให้สอดคล้องตามมาตรฐานของบริษัทฯ

4.8 ต้องทำการกำหนดค่าตามเอกสาร Configuration Standard ที่กำหนด และห้ามติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์ หรือก่อให้เกิดช่องโหว่ ในด้านความปลอดภัยลงในระบบคอมพิวเตอร์แม่ข่ายของบริษัทฯ

4.9 กรณีที่มีการเข้าสู่ระบบคอมพิวเตอร์แม่ข่าย หากไม่ใช้งานแล้ว ให้ทำการ Log Off ออกจากระบบทันที

หมวดที่ 5 การบริหารจัดการการบันทึกและตรวจสอบ

5.1 ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่นบันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90วัน โดยต้องสอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

5.2 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่ 6 การควบคุมการเข้าใช้งานระบบจากภายนอก

6.1 การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของบริษัทฯ การควบคุมบุคคลที่เข้าสู่ระบบของบริษัทฯจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน โดยต้องได้รับการอนุมัติให้ใช้จากผู้มีอำนาจ ผู้อนุมัติตามโครงสร้างการบังคับบัญชาของหน่วยงาน ผ่านระบบ VPN Software ตามที่บริษัทกำหนดเท่านั้น และเป็นความรับผิดชอบของผู้ที่ได้รับสิทธิเข้าใช้ระบบ ที่ต้องปฏิบัติตามนโยบายอย่างเคร่งครัด และไม่ให้บุคคลอื่นเข้ามาใช้ระบบในนามของตนเอง

6.2 วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

6.3 ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับบริษัทฯอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

6.4 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ต ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

6.5 เครื่องคอมพิวเตอร์ของผู้ใช้งาน (User) ต้องติดตั้งโปรแกรมป้องกันไวรัส ตามที่บริษัทกำหนด

หมวดที่ 7 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

7.1 ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบของบริษัทฯ สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

1) การแสดงตัวตน คือขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้

2) การพิสูจน์ยืนยันตัวตน คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง โดยผ่าน การยืนยันตัวตนผ่านระบบ Login Active Directory (AD) หรือ การยืนยันตัวตนผ่านระบบ Single Sign-On (SSO) หรือ Multifactor Authentication (MFA) ยกเว้นบางระบบที่กำลังดำเนินการพัฒนาจะเป็นไปตามบทเฉพาะกาล

ส่วนที่ 6

นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

(Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

วัตถุประสงค์

เพื่อป้องกันการบุกรุก โจมตีจากภายนอกบริษัทฯ โดยมีการตรวจสอบการใช้งานบนระบบเครือข่ายภายในบริษัทฯ รวมไปถึงพฤติกรรมต่างๆ ที่เกิดขึ้นบนเครือข่ายสื่อสารของบริษัทฯ และจะต้องมีการบันทึกเป็นลายลักษณ์อักษร สามารถตรวจสอบย้อนหลังได้

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ (IPS) เหตุการณ์ผิดปกติและการแจ้งเตือนต่างๆ ที่อุปกรณ์ตรวจพบจะถูกทำการวิเคราะห์และหาสาเหตุของการบุกรุกในระบบเทคโนโลยีสารสนเทศของบริษัทฯ เพื่อเป็นเครื่องมือสำหรับการสืบสวนหาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด ป้องกันก่อนที่จะเกิดการโจมตี
2. ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามที่บุกรุกหรือโจมตีบริษัทฯ เป็นเครื่องมือในการวัด ประสิทธิภาพในการป้องกันภัยและระบบรักษาความปลอดภัยอื่น ๆ เช่น ไฟร์วอลล์ เป็นต้น เพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตรายที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก รวมทั้งไวรัสประเภทต่างๆ
3. ผู้ดูแลระบบต้องมีการบริหารจัดการเหตุการณ์บุกรุกระบบ (Incident Management) เป็นการตอบสนองต่อเหตุการณ์บุกรุกทางเครือข่าย สามารถวิเคราะห์ลักษณะการบุกรุกทางเครือข่าย และทำให้สามารถแก้ไขสถานการณ์ได้อย่างถูกต้อง ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการบุกรุก โดยต้องจัดลำดับความสำคัญของการบุกรุกจาก

ผลกระทบที่เกิดขึ้นกับบริษัทฯและจัดหาวิธีปฏิบัติที่ถูกต้องให้กับบริษัทฯเพื่อป้องกันเหตุการณ์เกิดซ้ำ

4. การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง
5. ผู้ดูแลระบบต้องทำการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอต้องประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงานระบบรักษาความปลอดภัย และการทำงานของระบบงานที่เกี่ยวข้อง
6. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IPS
7. โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IPS จะต้องมีการบันทึกผลการตรวจสอบ
8. มีการตรวจสอบและ Update Patch/Signature ของ IPS เป็นประจำ
9. ผู้ดูแลระบบต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรมและบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายอย่างสม่ำเสมอ
    9.1 พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ผู้ดูแลระบบต้องรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ
10. IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ
11. พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ ผู้ดูแลระบบต้องรายงานให้ผู้บังคับบัญชาทราบ ภายใน 1 ชั่วโมงที่ตรวจพบ

12. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน หรือตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือตามที่กฎหมายกำหนด
13. การบริหารจัดการการบุกรุกเครือข่ายต้องมีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน
14. ผู้ดูแลระบบมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า
15. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของบริษัทฯ การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศจะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของบริษัทฯ จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ 7

นโยบายการสำรองและกู้คืนข้อมูล

วัตถุประสงค์

เพื่อป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลและระบบสารสนเทศของบริษัทฯ หากระบบสารสนเทศไม่สามารถใช้งานได้ หรือข้อมูลที่อยู่ในฐานข้อมูลหลักเกิดความเสียหาย

แนวปฏิบัติ

1. ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และเป็นไปตามนโยบายการสำรองและกู้คืนข้อมูลของบริษัทฯ
2. ผู้ดูแลระบบ หรือผู้รับผิดชอบต้องมีการจัดทำแผนในการรองรับสถานการณ์ฉุกเฉินหากเกิดปัญหาไม่สามารถใช้งานข้อมูลที่ทำการสำรอง และมีวิธีการกู้คืนข้อมูล
3. มีขั้นตอนการปฏิบัติการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบฐานข้อมูลและข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ
4. ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขเป็นลายลักษณ์อักษร
5. ผู้ดูแลระบบต้องมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้
6. ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมาย
7. ให้ผู้ดูแลระบบกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล เช่น Backup VM Server (Snapshot) หรือ Network Attached

Storage (NAS) โดยความถี่ในการสำรองตามขึ้นอยู่กับความสำคัญของระบบปฏิบัติการ (operating system) , ข้อมูลที่สำคัญทางธุรกิจ (Critical business information) หรือโปรแกรมระบบงาน (application system)

9. ต้องมีขั้นตอน หรือวิธีปฏิบัติในการสำรองข้อมูล เพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยอย่างน้อยควรมีรายละเอียดดังนี้

   9.1 ประเภทข้อมูลที่ทำการสำรอง และความถี่ในการสำรอง

   9.2 ประเภทสื่อบันทึก (Media)

   9.3 จำนวนที่ต้องสำรอง (Copy)

   9.4 ขั้นตอน และวิธีการสำรองโดยละเอียด

   9.5 สถานที่ และวิธีการเก็บรักษาสื่อบันทึก

10. มีการทบทวนคู่มือการปฏิบัติงานอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับสถานการณ์ปัจจุบัน

11. ต้อทดสอบการสำรองข้อมูลอย่างน้อย ปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมถึงระบบต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วน และใช้งานได้จริง

12. จัดทำขั้นตอน หรือวิธีปฏิบัติในการทดสอบการสำรองข้อมูลจากสื่อบันทึกข้อมูลมาใช้งาน กรณีมีการทดสอบควรให้ผู้เกี่ยวข้องเข้ามาร่วมทำการทดสอบข้อมูลให้ครบถ้วน และลงลายลักษณ์อักษร

13. ต้องจัดเก็บสื่อบันทึกข้อมูลไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออก เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง ในกรณีที่ต้องจัดเก็บสื่อบันทึกข้อมูลเป็นระยะเวลานาน ควรต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น การ Software Backup

14. การขอใช้งานสื่อบันทึกข้อมูลควรได้รับการอนุมัติจากผู้มีอำนาจตามโครงสร้าง และมีการจัดทำทะเบียนคุมการรับ และส่งมอบข้อมูล โดยควรมีรายละเอียดเกี่ยวกับผู้รับ-ผู้ส่งให้ชัดเจน

15. นโยบายที่เกี่ยวข้องกับการสำรองและกู้คืนข้อมูล ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนการปฏิบัติอย่างเคร่งครัด

ส่วนที่ 8

นโยบายการใช้เครื่องคอมพิวเตอร์และอุปกรณ์พกพา (BYOD)

วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกบริษัทฯ หรือการนำเครื่องส่วนตัวเพื่อปฏิบัติงานภายในบริษัท เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ของบริษัทฯ ให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยง ในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

แนวปฏิบัติ

หมวดที่ 1 การใช้เครื่องคอมพิวเตอร์แบบพกพาของบริษัทฯ

1. **การใช้งานทั่วไป**

1.1 เครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาที่บริษัทฯอนุญาตให้ใช้งาน เป็นทรัพย์สินของบริษัทฯดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานของบริษัทฯ

1.2 โปรแกรมที่ได้ถูกติดตั้งบนเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาต้องเป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

1.3 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาเพื่อตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่รับมอบหมายเท่านั้น

1.4 ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

2. **ความปลอดภัยทางด้านกายภาพ**

2.1 ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล๊อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2.2 ผู้ใช้ ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

3. **การควบคุมการเข้าถึงระบบปฏิบัติการ**

3.1 ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่าน ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

3.2 ผู้ใช้ควรกำหนดรหัสผ่านให้มีความปลอดภัย ตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

3.3 ผู้ใช้ต้องทำการบันทึกออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

4. **การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)**

4.1 ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

4.2 หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์มัลแวร์ (Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

หมวดที่ 2 การใช้เครื่องคอมพิวเตอร์แบบพกพาของส่วนบุคคล (BYOD)

1. **การใช้งานทั่วไป**

1.1 เครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาส่วนบุคคลจะต้องได้รับอนุญาตโดยผู้มีอำนาจตามโครงสร้างบริษัทฯของแต่ละหน่วยงาน และต้องลงทะเบียนยืนยันตัวตนการใช้งานคอมพิวเตอร์และอุปกรณ์แบบพกพา

1.2 โปรแกรมที่ได้ถูกติดตั้งบนเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาต้องเป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย และผู้ครอบครองต้องเป็นผู้รับผิดชอบหากถูกตรวจสอบลิขสิทธิ์

2. **ความปลอดภัยทางด้านกายภาพ**

2.1 ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล๊อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2.2 ผู้ใช้ ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

3. **การควบคุมการเข้าถึงระบบปฏิบัติการ**

3.1 ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่าน ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

3.2 ผู้ใช้ควรกำหนดรหัสผ่านให้มีความปลอดภัย ตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

3.3 ผู้ใช้ต้องทำการบันทึกออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

4. **การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)**

4.1 เครื่องคอมพิวเตอร์ และอุปกรณ์พกพาส่วนบุคคล ต้องติดตั้งระบบการป้องกันไวรัส ให้พร้อมใช้งานอยู่เสมอ

4.2 หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์มัลแวร์ (Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

ส่วนที่ 9

การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องเครื่องคอมพิวเตอร์และห้องเครือข่ายสื่อสารข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ

แนวปฏิบัติ

1. แบ่งแยกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ และสถานที่ติดตั้งเครื่องคอมพิวเตอร์ แม่ข่ายและอุปกรณ์เครือข่ายสื่อสารข้อมูลให้ชัดเจนและเป็นลายลักษณ์อักษร
2. กำหนดสิทธิให้กับเจ้าหน้าที่ให้มีสิทธิสามารถเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย
3. กำหนดผู้รับผิดชอบในการบันทึกการเข้า-ออก และจัดทำรายงานการเข้า-ออกพื้นที่เสนอผู้บังคับบัญชา
4. บุคคลภายนอกที่เข้ามาติดต่อ หรือ บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้อง ต้องได้รับอนุญาตจากเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศในการ เข้า-ออก ห้องเครื่องคอมพิวเตอร์และห้องเครือข่ายสื่อสารข้อมูล
5. ทบทวนข้อกำหนดในการเข้าใช้งานพื้นที่ห้องเครื่องคอมพิวเตอร์และห้องเครือข่ายสื่อสารข้อมูล อย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 10

แนวปฏิบัติการประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

แนวปฏิบัติ

1. บริษัทฯจะต้องจัดทำแผนบริหารความเสี่ยง เพื่อใช้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ โดยผู้ตรวจสอบภายใน หรือผู้ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง ให้เป็นไปตามแนวปฏิบัติการประเมินความเสี่ยงด้านสารสนเทศที่กำหนด
2. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานเพื่อการประเมินความเสี่ยงนั้นๆ
3. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น
4. ติดตามการดำเนินการตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทฯ ที่ได้กำหนดไว้
5. ทบทวนและปรับปรุงแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทฯในด้านต่างๆ อย่างน้อยปีละ 1 ครั้ง ให้สอดคล้องกับสถานการณ์

ส่วนที่ 11

การพัฒนาระบบงานคอมพิวเตอร์ (Development)

วัตถุประสงค์

เพื่อการปรับปรุงกระบวนการทำงานพัฒนาระบบสารสนเทศ ให้มีประสิทธิภาพและรองรับการใช้งานในอนาคต โดยอยู่ในความรับผิดชอบของฝ่ายเทคโนโลยีสารสนเทศ จึงขอให้พนักงานผู้ที่เกี่ยวข้องทุกฝ่าย ทำความเข้าใจและปฏิบัติตามระเบียบ

แนวปฏิบัติ

1. **ประเภทของการพัฒนาระบบฯ มี 2 วิธี ดังนี้**
    - 1.1 การพัฒนาระบบฯ โดยพนักงานบริษัทฯ (In-House)
        - 1.1.1 ผู้จัดการโครงการ – มีหน้าที่ควบคุมโครงการให้เป็นไปตามแผน และวางแผนกลยุทธ์ในการพัฒนาระบบฯ
        - 1.1.2 หัวหน้าโครงการ – มีหน้าที่ควบคุมการดำเนินงานให้สอดคล้องตามแผนงานเพื่อให้บรรลุวัตถุประสงค์
        - 1.1.3 ผู้ที่รับผิดชอบพัฒนาระบบ–มีหน้าที่ดำเนินการพัฒนาระบบฯ ตามเอกสาร QP-IT-ITD01
2. การพัฒนาระบบฯ โดยการว่าจ้างบุคคลภายนอก (Outsource)
    - 2.1 ผู้จัดการโครงการ – มีหน้าที่ควบคุมโครงการให้เป็นไปตามแผน และวางแผนกลยุทธ์ในการพัฒนาระบบฯ
    - 2.2 หัวหน้าโครงการ – มีหน้าที่ควบคุมการดำเนินงานให้สอดคล้องตามแผนงานเพื่อให้บรรลุวัตถุประสงค์
    - 2.3 ผู้รับจ้างจากภายนอก (Outsource) – มีหน้าที่พัฒนาระบบฯ ตามสัญญาข้อตกลง

2.4 ผู้ที่รับผิดชอบพัฒนาระบบฯ – มีหน้าที่ประสานงาน และดำเนินการตามมาตรฐานการปฏิบัติงาน SOP เลขที่ QP-IT-ITD01

3. การควบคุมการพัฒนาระบบด้านความปลอดภัย ต้องออกแบบ หรือพัฒนาระบบโดยยึดนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ อาทิเช่น

3.1 มาตรฐานความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ เช่น API Login With Password Policy , การเข้ารหัสข้อมูล, การประมวลผลข้อมูล PDPA, การจัดเก็บและสำรองฐานข้อมูล (Database)

3.2 ต้องคำนึงถึงการประเมินความเสี่ยง หรือผลกระทบ กรณีที่มีการเปลี่ยนแปลงตลอดจนควบคุมการทำงาน

3.3 การป้องกันการตรวจจับการบุกรุก การโจมตี รวมถึงการป้องกันข้อมูลตาม PDPA และการจัดทำประวัติการสืบค้นข้อมูล

3.4 การรับมือภัยคุกคามที่เกิดขึ้นกับระบบ

3.5 มีระบบ Backup ข้อมูล

4. กระบวนการการพัฒนาระบบสารสนเทศจะดำเนินตามกระบวนการที่เรียกว่า System Development life cycle (SDLC) นำมาประยุกต์ใช้งานแบบ Agile โดยระบุขั้นตอนการพัฒนาระบบฯ ดังนี้

4.1 การพัฒนาระบบฯ โดยพนักงานบริษัทฯ (In-House)

4.1.1 ผู้ขอใช้บริการ แจ้งขอใช้บริการพัฒนาระบบฯ ผ่านระบบ https://k2.portal.sabuyconnext.com/ ผ่านทางโปรแกรมขอใช้บริการเทคโนโลยีสารสนเทศแล้วเลือกประเภทขอใช้บริการ 4. FM-IT-03 แจ้งความต้องการใช้งาน

4.1.2 PM จะกำหนดให้ BA จะไปเก็บ Requirement ความต้องการของโครงการ นำมาวิเคราะห์ความเป็นไปได้ของโครงการ

4.1.2.1 กรณีประเมินโครงการไม่ผ่าน จะแจ้งผู้ขอใช้บริการเพื่อยกเลิกโครงการ และทำการยกเลิกในระบบ

4.1.2.2 กรณีประเมินโครงการผ่านทาง BA จัดทำเอกสารโครงการพร้อมจัดทำ (Proposal) โดยกำหนดระยะเวลาดำเนินการโครงการ ผู้รับผิดชอบโครงการ และนำเข้าประชุมกลุ่มเทคโนโลยีสารสนเทศ เพื่อขออนุมัติพิจารณาโครงการ

4.1.2.3 ทางที่ประชุมกลุ่มเทคโนโลยีสารสนเทศ จะพิจารณาตามความสำคัญ, ความเร่งด่วน ของโครงการ

4.1.2.4 กรณีเมื่อไม่ผ่านพิจารณาโครงการ ทางกล่มเทคโนโลยีสารสนเทศจะดำเนินการแจ้งผู้ขอใช้บริการเพื่อยกเลิกโครงการ และทำการยกเลิกในระบบฯ

4.1.2.5 กรณีผ่านพิจารณาโครงการจะแจ้งผู้ขอใช้บริการ

4.1.3 เมื่อผ่านพิจารณาโครงการทางกลุ่มเทศโนโลยีสารสนเทศจะให้ทาง BA รวบรวมความต้องการของโครงการพร้อมจัดทำ System Requirement Specification (SRS) เพื่อเป็นขอกำหนดในการพัฒนาระบบสารสนเทศ

4.1.4 SA วิเคราะห์และออกแบบระบบให้ทางผู้ใช้งานลงนามยอมรับ และส่งต่อให้ Programmer เพื่อพัฒนาระบบ

4.1.5 Programmer พัฒนาระบบและทดสอบระบบเบื้องต้น

4.1.6 SA/ Application Support หรือ Tester จัดทำขั้นตอนการทดสอบระบบ และทำการสรุปผลการทดสอบ จากนั้นให้ผู้ขอใช้บริการร่วมทดสอบ

ระบบบนเครื่อง UAT หากมีการแก้ไข Programmer ต้องแก้ไขตามขอบเขตของ (SRS)

4.1.7 BA/SA/Application จัดทำคู่มือใช้งานระบบ และฝึกสอนการใช้งานระบบให้แก้ผู้ขอใช้บริการ

4.1.8 ผู้ขอใช้บริการ/ ผู้ใช้งานระดับผู้จัดการฝ่ายขึ้นไป / ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศลงนามรับทราบปิดโครงการ

4.2 การพัฒนาระบบฯ โดยพนักงานบริษัทฯ (Outsource)

4.2.1 ผู้ขอใช้บริการ แจ้งขอใช้บริการพัฒนาระบบฯ ผ่านระบบ https://k2.portal.sabuyconnext.com/ ผ่านทางโปรแกรมขอใช้บริการเทคโนโลยีสารสนเทศแล้วเลือกประเภทขอใช้บริการ 4. FM-IT-03 แจ้งความต้องการใช้งาน

4.2.2 PM จะกำหนดให้ BA จะไปเก็บ Requirement ความต้องการของโครงการนำมาวิเคราะห์ความเป็นไปได้ของโครงการ

4.2.2.1 กรณีประเมินโครงการไม่ผ่าน จะแจ้งผู้ขอใช้บริการเพื่อยกเลิกโครงการ และทำการยกเลิกในระบบ

4.2.2.2 กรณีประเมินโครงการผ่านทาง BA จัดทำเอกสารโครงการพร้อมจัดทำ (Proposal) โดยกำหนดระยะเวลาดำเนินการโครงการ ผู้รับผิดชอบโครงการ และนำเข้าประชุมกลุ่มเทคโนโลยีสารสนเทศ เพื่อขออนุมัติพิจารณาโครงการ

4.2.2.3 ทางที่ประชุมกลุ่มเทคโนโลยีสารสนเทศ จะพิจารณาตามความสำคัญ, ความเร่งด่วน ของโครงการ

4.2.2.4 กรณีเมื่อไม่ผ่านพิจารณาโครงการ ทางกลุ่มเทคโนโลยีสารสนเทศจะดำเนินการแจ้งผู้ขอใช้บริการเพื่อยกเลิกโครงการและทำการยกเลิกในระบบฯ

4.2.2.5 กรณีผ่านพิจารณาโครงการทางฝ่ายเทคโนโลยีสารสนเทศจะจัดทำ Scope และ Requirement ของโครงการเพื่อให้แผนกจัดซื้อหา Vendor ให้ทางฝ่ายเทคโนโลยีสารสนเทศและผู้ใช้บริการเพื่อพิจารณาเปรียบเทียบ Outsource ดำเนินเรื่องอนุมัติจ้างผ่านแผนกจัดซื้อ

4.2.3 เมื่อได้บริษัท Outsource ทางกลุ่มเทศโนโลยีสารสนเทศกับ Outsource ร่วมกันรวบรวมความต้องการของโครงการพร้อมจัดทำ System Requirement Specification (SRS) เพื่อเป็นขอกำหนดในการพัฒนาระบบสารสนเทศ

4.2.4 กลุ่มเทคโนโลยีสารสนเทศ ติดตามงาน Outsource ให้เป็นไปตามแผนงานของโครงการ

4.2.5 กลุ่มเทคโนโลยีสารสนเทศและผู้ขอใช้บริการ ทดสอบระบบ/รายงานตาม Test Scenario กรณี Test ไม่ผ่านแจ้งให้ทาง Outsource ดำเนินการแก้ไข กรณี Test ผ่านให้ผู้ขอใช้บริการลงนามในเอกสาร UAT

4.2.6 กลุ่มเทคโนโลยีสารสนเทศแจ้ง Outsource เพื่อจัดทำคู่มือการทำงาน คู่มือการดูแลระบบ และฝึกอบรมสอนการใช้งานระบบกับผู้ขอใช้บริการ

4.2.7 ผู้ขอใช้บริการ/ ผู้ใช้งานระดับผู้จัดการฝ่ายขึ้นไป / ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศลงนามรับทราบปิดโครงการ

ส่วนที่ 12

การใช้บริการคลาวด์คอมพิวติ้ง (Cloud Computing)

วัตถุประสงค์

เพื่อกำหนดหลักเกณฑ์และมาตรฐานการใช้งานระบบ Cloud Computing Service ในการให้บริการข้อมูล และระบบงานต่าง ๆ ให้มีความปลอดภัย และสามารถใช้งานได้อย่างต่อเนื่อง โดยไม่เกิดการหยุดชะงักในการดำเนินงาน โดยครอบคลุมถึงการใช้งานครื่องเซิร์ฟเวอร์บน Public Cloud และ Private Cloud ที่เกี่ยวข้องกับข้อมูล หรือระบบต่าง ๆของบริษัท

แนวปฏิบัติ

1. **การใช้บริการแบบสาธารณะผ่านอินเทอร์เน็ต (Public Cloud)**
   - 1.1 บริษัทเลือกใช้ผู้ให้บริการจากผู้ดำเนินธุรกิจที่ให้บริการ Public Cloud ที่มีความน่าเชื่อถือโดยเฉพาะ และมีมาตรฐานหรือมีการรับประกันการรักษาความปลอดภัยของข้อมูลอย่างชัดเจน โดยผู้ให้บริการต้องมี มาตรฐานรองรับ ISO/IEC 27001 และ ISO/IEC 20000-1
   - 1.2 การนำระบบงานหรือข้อมูลขององค์กรไปเก็บไว้ใน Public Cloud จะต้องผ่านการพิจารณาร่วมกันระหว่างหน่วยงานเจ้าของข้อมูลและฝ่ายเทคโนโลยีสารสนเทศ และจะต้องได้รับอนุมัติจากผู้มีอำนาจให้ดำเนินการ
   - 1.3 กรณีที่มีความจำเป็นต้องเชื่อมต่อระบบงาน ที่มีการเชื่อมต่อระบบ Cloud กับระบบงานที่มีอยู่ในเครือข่ายบริษัท จะต้องผ่านการพิจารณาร่วมกันระหว่างหน่วยงานเจ้าของข้อมูลและฝ่ายเทคโนโลยีสารสนเทศ
   - 1.4 การใช้บริการเครื่องเซิร์ฟเวอร์ที่อยู่ใน Public Cloud ให้เป็นไปตามนโยบายเรื่องการใช้งานเครื่องเซิร์ฟเวอร์

2. **ระบบการประมวลผลหรือการจัดเก็บข้อมูลของผู้ใช้งานที่ถูกจัดเก็บบนเครื่องเซิร์ฟเวอร์แบบส่วนตัว (Private Cloud)**

2.1 สำหรับการใช้บริการเครื่องเซิร์ฟเวอร์ที่อยู่ใน Private Cloud ให้เป็นไปตามนโยบายเรื่องการใช้งานเครื่องเซิร์ฟเวอร์

บทเฉพาะกาล

สำหรับระบบงานเทคโนโลยีสารสนเทศที่ใช้งานอยู่ในปัจจุบันที่ยังไม่รองรับตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีการปรับปรุงในฉบับนี้ ให้ทำการแก้ไขปรับปรุงให้เป็นไปตามมาตรฐาน ภายใน 365 วัน โดยระหว่างที่ดำเนินการแก้ไขปรับปรุง ให้มีการควบคุมทดแทนในระดับที่ยอมรับได้ และอนุมัติโดยประธานเจ้าหน้าที่บริหาร สำหรับระบบที่ขึ้นหลังประกาศฉบับนี้ ให้ปฏิบัติตามข้อกำหนดมาตรฐาน

ประกาศใช้ ณ วันที่ 12 มิถุนายน 2566

นาย วรานนท์ คงปฏิมากร
ประธานเจ้าหน้าที่บริหาร