นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. ความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับองค์กรและภาคธุรกิจ ซึ่งองค์กรใดที่มีระบบการจัดการข้อมูล และระบบสารสนเทศที่ดีถือเป็นข้อได้เปรียบในการดำเนินธุรกิจยิ่งขึ้น ทั้งนี้ระบบสารสนเทศยังสามารถสร้างความสะดวกในการสื่อสาร การเข้าถึงข้อมูลได้อย่างรวดเร็ว ช่วยให้ข้อมูลมีความถูกต้อง ลดต้นทุน แม้ว่าระบบเทคโนโลยีสารสนเทศจะมีประโยชน์แต่ในขณะเดียวกันเทคโนโลยีกลับมีความเสี่ยงสูง เช่น การถูกคุกคามทางด้านข้อมูลหรือระบบ ส่งผลกระทบทำให้เกิดการรั่วไหลของข้อมูลสำคัญ (Data Breach) ข้อมูลเกิดความเสียหาย และระบบขัดข้องไม่สามารถให้บริการได้

ดังนั้น บริษัท ไลท์อัพ ดีไซน์ จำกัด จึงจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร เพื่อเป็นแนวทางปฏิบัติให้เกิดความน่าเชื่อถือ และความมั่นคงปลอดภัยกับระบบสารสนเทศที่ใช้ในการทำงาน

2. หลักการบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์กรมีความมั่นคงปลอดภัย มีแนวปฏิบัติที่ดี สามารถทำให้การดำเนินงานขององค์กรมีความต่อเนื่อง มีการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศที่ไม่ถูกต้อง และมีการป้องกันภัยถูกคุกคามที่ส่งผลต่อระบบสารสนเทศ โดยมีการมอบหมายให้แผนกเทคโนโลยีสารสนเทศ เป็นหน่วยงานที่กำกับดูแลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

3. วัตถุประสงค์

1) เพื่อความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กร
2) เพื่อให้มีนโยบาย และแนวปฏิบัติสำหรับควบคุมการใช้งานสารสนเทศที่เป็นลายลักษณ์อักษรที่ถูกอนุมัติจากผู้บริหาร
3) เพื่อเป็นนโยบายสำหรับเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กร รวมถึงบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กรได้รับทราบและเป็นแนวทางในการปฏิบัติตามเพื่อความปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กร
4) เป็นนโยบายเพื่อเผยแพร่ให้ผู้ใช้งานทราบถึงประโยชน์ และภัยคุกคาม รวมถึงสร้างความตระหนักในการใช้งานสารสนเทศอย่างปลอดภัย
5) เพื่อจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีมาตรฐาน โดยอ้างอิงมาตรฐาน เช่น ISO/IEC 27001 มาประยุกต์ใช้
6) เพื่อทบทวน และปรับปรุงนโยบาย และแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

4. ขอบเขตนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1) ส่งเสริม และสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
2) กำหนดแนวทางปฏิบัติ แนวทางแก้ไข หรือบทลงโทษ ในด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
3) เผยแพร่ความรู้ความเข้าใจ และสร้างความตระหนักให้บุคลากรคำนึงถึงความปลอดภัยในการใช้งานระบบสารสนเทศขององค์กร
4) บริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ
5) ทำการติดตาม ตรวจสอบการดำเนินงาน ปรับปรุงนโยบาย และแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

5. บทลงโทษในการกระทำผิด

บริษัท ไลท์อัพ ดีไซน์ จำกัด ได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนั้นเพื่อควบคุมไม่ให้มีผู้ใดกระทำความผิด หรือทำให้องค์กร ลูกค้าขององค์กร หรือแม้แต่เพื่อนร่วมงานในองค์กรได้รับความเดือดร้อน องค์กรจึงมีบทลงโทษเพื่อป้องกันเหตุการณ์ดังกล่าวผ่านคณะกรรมการเพื่อพิจารณาการกระทำผิด โดยมีกระบวนการดังนี้

1) กรณีเป็นบุคคลภายในองค์กร
   - จัดให้มีคณะกรรมการพิจารณาการกระทำผิดเพื่อตรวจสอบข้อเท็จจริง และลงโทษ
   - ระดับการลงโทษ
     - ตักเตือน
     - ชดใช้ตามความเสียหายหรือเสียค่าปรับ
     - พักงาน
     - เชิญออก
2) กรณีเป็นบุคคลภายนอกองค์กร
   - จัดให้มีคณะกรรมการพิจารณาการกระทำผิดเพื่อตรวจสอบข้อเท็จจริง และลงโทษ
   - ระดับการลงโทษ
     - ชดใช้ตามความเสียหายหรือเสียค่าปรับ
     - ดำเนินคดีตามกฎหมาย

6. การทบทวนนโยบาย

บริษัท ไลท์อัพ ดีไซน์ จำกัด กำหนดให้มีการทบทวนนโยบาย และวางแผนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พร้อมทั้งติดตามแผนการดำเนินงาน เป็นประจำทุกปี

7. องค์ประกอบของนโยบาย และแนวทางปฏิบัติ

1) คำนิยามศัพท์ที่เกี่ยวข้อง
2) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical Security Policy)
3) นโยบายการรักษาความมั่นคงปลอดภัยของการเข้าถึงระบบ และการพิสูจน์ตัวตน (Password Authentication & Authorization Policy)
4) นโยบายการรักษาความมั่นคงปลอดภัยของการทำงานจากระยะไกล (Remote Access Policy)
5) นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)
6) นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)
7) นโยบายการรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (IDS/IPS Policy)
8) นโยบายการรักษาความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup/Restore Policy)
9) นโยบายการรักษาความมั่นคงปลอดภัยของการเชื่อมต่ออินเทอร์เน็ต (Internet Security Policy)
10) นโยบายการรักษาความมั่นคงปลอดภัยของการเชื่อมต่อเครือข่ายไร้สาย (Wireless Policy)
11) นโยบายการรักษาความมั่นคงปลอดภัยของการใช้จดหมายอิเล็กทรอนิกส์ (E-mail Policy)
12) นโยบายการบริหารจัดการทรัพยากรคอมพิวเตอร์ (Asset Management Policy)
13) นโยบายการบริหารจัดการโปรแกรมคอมพิวเตอร์ (Software Management Policy)
14) นโยบายการบริหารจัดการทรัพยากรผู้ใช้งาน (Resource Policy)
15) นโยบายการบริหารจัดการผู้ให้บริการองค์กรภายนอกในการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ (Outsource & Information System Change Policy)
16) นโยบายการรักษาความมั่นคงปลอดภัยของการใช้สื่อบันทึก และการโอนย้ายข้อมูล (Media Data Store & Transfer Policy)
17) นโยบายการรักษาความมั่นคงปลอดภัยของการบริหารจัดการข้อมูล (Data Management Policy)
18) การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Cyber Security Awareness)

1) **คำนิยามศัพท์ที่เกี่ยวข้อง**

องค์กร หมายถึง บริษัท ไลท์อัพ ดีไซน์ จำกัด

พนักงาน หมายถึง บุคคลที่องค์กรว่าจ้างให้ปฏิบัติงานตามหน้าที่

ผู้ใช้งาน หมายถึง พนักงานภายในองค์กร ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และเครือข่ายขององค์กร

เจ้าหน้าที่ หมายถึง พนักงานหรือบุคคลที่แผนกเทคโนโลยีสารสนเทศได้มอบหมายเป็นผู้ดำเนินการ

ผู้ดูแลระบบ (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์ และระบบเครือข่าย

ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) หมายถึง สถานที่รวบรวมอุปกรณ์เครื่องแม่ข่าย และอุปกรณ์เครือข่ายสำหรับให้บริการด้านสารสนเทศหรือเครือข่ายภายในองค์กร เป็นพื้นที่ควบคุมการเข้าถึงจากผู้ที่ไม่เกี่ยวข้อง หรือไม่ได้รับอนุญาต

ระบบสารสนเทศ หมายถึง เครื่องมือที่ใช้ในการจัดเก็บ ประมวลผล เผยแพร่ข้อมูลสารสนเทศ

ข้อมูล หมายถึง ข้อความ ตัวเลข รูปภาพ ฯลฯ ที่ถูกรวบรวม และจัดเก็บในระบบคอมพิวเตอร์

สารสนเทศ หมายถึง ข้อมูลที่มีถูกประมวลผลเพื่อนำไปใช้ประโยชน์ในด้านต่างๆ

ระบบเครือข่ายคอมพิวเตอร์ หมายถึง การเชื่อมต่อสื่อสารระหว่างคอมพิวเตอร์ และอุปกรณ์ สำหรับการรับ - ส่งข้อมูล

อินเทอร์เน็ต (Internet) หมายถึง การเชื่อมต่อสื่อสารผ่านระบบเครือข่ายกับองค์กรภายนอก

ระบบคอมพิวเตอร์ หมายถึง ระบบการทำงานที่ประกอบไปด้วย เครื่องคอมพิวเตอร์, หน้าจอคอมพิวเตอร์, แป้นพิมพ์ และเมาส์

โปรแกรมประสงค์ร้าย (Malware) หมายถึง โปรแกรมที่มีเจตนาเพื่อมุ่งประสงค์ร้ายต่อระบบคอมพิวเตอร์ในรูปแบบต่างๆ ซึ่งเป็นภัยต่อความมั่นคงปลอดภัยขององค์กร เช่น Adware, Spyware, Virus, Spam, Worm, Trojan, Backdoors, Ransomware ฯลฯ

บัญชีผู้ใช้งาน (Account) หมายถึง ข้อมูลที่ใช้ในการเข้าสู่ระบบ ประกอบไปด้วย Username และ Password

ชื่อผู้ใช้งาน (Username) หมายถึง ที่ใช้ระบุตัวตนผู้ใช้งาน

รหัสผ่าน (Password) หมายถึง ข้อมูลที่ใช้ในการยืนยันตัวผู้ใช้งาน

ไฟร์วอลล์ (Firewall) หมายถึง ซอฟต์แวร์หรือฮาร์ดแวร์สำหรับตรวจสอบ และคัดกรองความปลอดภัยของข้อมูลเพื่อป้องกันภัยคุกคามในระบบเครือข่าย

ซอฟต์แวร์ (Software) หมายถึง โปรแกรมที่ใช้ในการควบคุมคำสั่งคอมพิวเตอร์

พนักงานชั่วคราว (Outsource) หมายถึง ผู้ให้บริการภายนอกที่เข้ามาบำรุงรักษา ปรับปรุง หรือพัฒนาระบบในองค์กร

2) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical Security Policy)

(1) วัตถุประสงค์

การรักษาความมั่นคงปลอดภัยทางกายภาพเป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับพื้นที่จัดเก็บเครื่องแม่ข่าย, อุปกรณ์จัดการด้านเครือข่ายต่างๆ และเป็นพื้นที่จัดเก็บข้อมูลสารสนเทศที่สำคัญขององค์กร ซึ่งถือเป็นพื้นที่ควบคุม จึงจำเป็นต้องมีการควบคุมการเข้าถึงของบุคคลทั้งภายใน และภายนอกองค์กรอย่างรัดกุม ดังนั้นควรมีแนวทางปฏิบัติที่เข้มงวดเพื่อป้องกันการคุกคามซึ่งอาจก่อให้เกิดความเสียหายแก่องค์กรได้

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมีการมอบหมายให้แผนกเทคโนโลยีสารสนเทศ เป็นหน่วยงานทำหน้าที่บริหารการรักษาความมั่นคงปลอดภัยทางกายภาพ

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดำเนินการดูแลการเข้า - ออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) และจัดทำรายงานเพื่อนำเสนอทุก 1 เดือน

(2.3) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดำเนินการตรวจสอบด้านกายภาพของห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) และจัดทำรายงานนำเสนอทุก 1 เดือน

(2.4) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดำเนินการบำรุงรักษาห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) และอุปกรณ์ภายในห้อง

(3) แนวทางปฏิบัติ

(3.1) การควบคุมการเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room)

(3.1.1) มีการจัดทำรายชื่อผู้ใช้งานในห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) ที่สามารถเข้าทำการปฏิบัติงานตามภาระที่ได้รับมอบหมาย

(3.1.2) กรณีผู้ที่ไม่มีรายชื่อเป็นผู้ใช้งานห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) ต้องทำการขออนุญาตหัวหน้าแผนกเทคโนโลยีสารสนเทศ โดยจัดทำแบบฟอร์มการขออนุญาตเข้า - ออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room)

(3.1.3) ผู้เข้าห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) ต้องทำการลงบันทึกการเข้า - ออก ในบัญชีบันทึกการเข้า - ออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room)

(3.1.4) สำหรับผู้ที่ขออนุญาตเข้าห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) ต้องมีเจ้าหน้าที่ของห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) คอยดูแลอยู่ด้วยทุกครั้ง

(3.1.5) กำหนดให้มีการควบคุมการเข้า - ออก เช่น ระบบ Access Control สำหรับผู้ใช้งานในห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room)

(3.2) การบริหารจัดการด้านกายภาพ

(3.2.1) กำหนดให้มีระบบสำรองไฟฟ้าในกรณีที่เกิดไฟฟ้าขัดข้อง เช่น การใช้ UPS, เครื่องปั่นไฟ ตามความเหมาะสม

(3.2.2) กำหนดให้มีระบบแจ้งเตือนกรณีเกิดเหตุเพลิงไหม้ไปยังผู้รับผิดชอบหรือผู้เกี่ยวข้อง

(3.2.3) กำหนดให้มีระบบดับเพลิง เช่น ถังดับเพลิงหรือระบบดับเพลิงอัตโนมัติ ตามความเหมาะสม

(3.2.4) กำหนดให้มีระบบตรวจวัดอุณหภูมิ และความชื้นค่าปัจจุบัน ทั้งนี้ระบบยังสามารถแจ้งเตือนไปยังผู้รับผิดชอบหรือผู้เกี่ยวข้องได้โดยตรงเมื่อพบว่ามีค่าอุณหภูมิ และความชื้นอยู่ในเกณฑ์ที่ผิดปกติ

(3.3) การบำรุงรักษา

(3.3.1) กำหนดให้มีเจ้าหน้าที่ทำการสำรวจด้านกายภาพ และจัดทำรายงานเสนอหัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบ

(3.3.2) กำหนดมาตรการสำรองในกรณีที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) ไม่สามารถใช้งานได้ โดยให้ทำการติดตั้ง และเปิดใช้งานจากพื้นที่สำรองเป็นการชั่วคราว

(3.4) การบริหารจัดการ

(3.4.1) เจ้าหน้าที่จัดเก็บ และรวบรวมแบบฟอร์มการขออนุญาตเข้า - ออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) และจัดทำบันทึกการเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) เสนอให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกเดือน

(3.4.2) เจ้าหน้าที่คอยตรวจสอบระบบความปลอดภัยทางกายภาพทุกวัน และจัดทำรายการตรวจสอบห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) เสนอให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกเดือน โดยประกอบไปด้วยข้อมูลในการสำรวจ เช่น

- ค่าอุณหภูมิ และความชื้น
- การทำงานของระบบเครื่องปรับอากาศ
- การทำงานของระบบเครื่องสำรองไฟ (UPS)
- มีถังดับเพลิงที่พร้อมใช้งาน
- มีระบบควบคุมการเข้า - ออก (Access Control System)

(3.4.3) กรณีการสำรวจพบสิ่งผิดปกติ ให้เจ้าหน้าที่แจ้งหัวหน้าแผนกเทคโนโลยีสารสนเทศ เพื่อร่วมกันหาวิธี และดำเนินการแก้ไข

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มขอเข้าออกห้อง Server ทะเบียนการเข้าออกออกห้อง Server	หมายเลขเอกสาร : ITG-31-65-00
(4.2) ทะเบียนการเข้าออกออกห้อง Server	หมายเลขเอกสาร : ITG-31-65-01
(4.3) รายชื่อผู้ใช้งานในห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room)	หมายเลขเอกสาร : ITG-22-65-00

(4.4) รายงานการตรวจสอบห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) หมายเลขเอกสาร : ITG-28-65-00

3) นโยบายการรักษาความมั่นคงปลอดภัยของการเข้าถึง และพิสูจน์ตัวตนของระบบ (Password Authentication & Authorization Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการจัดการรหัสผ่าน และสิทธิเข้าใช้งานระบบสารสนเทศ, ระบบคอมพิวเตอร์, ระบบเครือข่ายคอมพิวเตอร์ขององค์กร สำหรับควบคุมการเข้าถึงข้อมูล และการใช้งานของพนักงานให้เป็นไปตามสิทธิภายใต้ตำแหน่งหรือภารกิจที่ได้รับมอบหมาย เพื่อป้องกันการบุกรุกผ่านระบบเครือข่ายหรือจากโปรแกรมประสงค์ร้ายที่อาจสร้างความเสียหายแก่ข้อมูล การทำงานของระบบสารสนเทศ หรือระบบเครือข่ายขององค์กร ทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศ และระบบเครือข่ายขององค์กรได้อย่างถูกต้อง หากไม่มีแนวทางปฏิบัติที่ดีอาจเกิดการละเมิดการเข้าถึงระบบ ทำให้เกิดความเสียหายได้

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กร มีการมอบหมายให้แผนกเทคโนโลยีสารสนเทศทำหน้าที่บริหารจัดการนโยบายการรักษาความมั่นคงปลอดภัยของการเข้าถึง และพิสูจน์ตัวตนของระบบ

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายเจ้าหน้าที่ในแผนกให้เป็นผู้ดำเนินการจัดการบัญชีผู้ใช้งาน และกำหนดสิทธิ

(2.3) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายเจ้าหน้าที่ในแผนกให้เป็นผู้ดำเนินการตรวจสอบสิทธิการใช้งาน การเข้าใช้งาน และจัดทำรายงานนำเสนอ

(3) แนวทางปฏิบัติ

(3.1) การขอรหัสผ่าน ยกเลิกรหัสผ่าน เปลี่ยนแปลงสิทธิ

(3.1.1) กำหนดขั้นตอนขออนุมัติดังนี้

- ขั้นตอนที่ 1 ผู้ใช้งานกรอกแบบฟอร์มขอหรือยกเลิกสิทธิเข้าถึงระบบสารสนเทศ ให้หัวหน้าแผนกต้นสังกัดพิจารณาอนุมัติ
- ขั้นตอนที่ 2 ส่งแบบฟอร์มให้หัวหน้าแผนกบุคคลพิจารณาอนุมัติ
- ขั้นตอนที่ 3 ส่งแบบฟอร์มเจ้าหน้าที่รับเรื่อง และจัดส่งให้หัวหน้าแผนกเทคโนโลยีสารสนเทศพิจารณาอนุมัติ
- ขั้นตอนที่ 4 เจ้าหน้าที่ ดำเนินการตามการร้องขอ

(3.1.2) กรณีที่มีพนักงานลาออกให้หัวหน้าแผนกบุคคลแจ้งเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศให้ดำเนินการยกเลิกสิทธิการใช้งานได้ทันที

(3.2) การกำหนดรหัสผ่าน

(3.2.1) ในการกำหนดรหัสผ่าน ประเภทระบบที่เป็นชนิดข้อความ ควรปฏิบัติดังนี้ดังนี้

- ต้องมีความยาวที่ไม่น้อยกว่า 8 ตัวอักษร เว้นแต่ระบบกำหนดจะกำหนดไม่ให้เกิน
- ในการกำหนดรหัสผ่านไม่ควรตั้งเป็นคำที่คาดเดาง่าย
- มีการผสมระหว่างตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่ และตัวอักษรภาษาอังกฤษตัวพิมพ์เล็ก
- มีการผสมตัวเลข และอักขระพิเศษ

(3.2.2) ในการกำหนดรหัสผ่านประเภทระบบที่เป็นตัวเลขอย่างเดียว ควรกำหนดให้เป็นเลขที่คาดเดายาก ไม่เป็นตัวเลขที่เรียงกัน ไม่เป็นตัวเลขเดียวกันทั้งหมด และไม่มีความเกี่ยวข้องกับข้อมูลส่วนตัว

(3.3) การใช้รหัสผ่าน

(3.3.1) ผู้ใช้งานห้ามเปิดเผย Password ให้ผู้อื่นทราบ

(3.3.2) ห้ามผู้ใช้งานใช้ Account ของผู้อื่น

(3.3.3) กรณีที่ผู้ใช้งานไม่สามารถจำรหัสผ่านได้ สามารถจดบันทึกรหัสผ่าน และบันทึกนั้นต้องมีการจัดเก็บเป็นอย่างดี ผู้อื่นไม่สามารถเข้าถึงได้โดยง่าย

(3.3.4) กำหนดให้มีการเปลี่ยนรหัสผ่าน อย่างน้อยทุก 3 เดือน และไม่ใช้รหัสผ่านที่เคยใช้งานแล้ว

(3.3.5) ระบบที่ใช้รหัสผ่านร่วมกันหลายคน เช่น รหัสผ่านสำหรับผู้ดูแลระบบ ทั้งนี้หากมีการบุคลากรที่ใช้พาสเวิดร่วมกันลาออก ต้องเปลี่ยนรหัสผ่านใหม่ทันทีที่ได้รับข้อมูลจากแผนกทรัพยากรบุคคล

(3.4) การบริหารจัดการ

(3.4.1) เจ้าหน้าที่จัดเก็บ และรวบรวมแบบฟอร์มขอหรือยกเลิกสิทธิการเข้าถึงระบบสารสนเทศ และจัดทำรายงานสรุปการขอหรือยกเลิกสิทธิการเข้าถึงระบบสารสนเทศ เสนอให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกเดือน

(3.4.2) เจ้าหน้าที่ตรวจสอบประวัติการเข้าใช้งานระบบสารสนเทศเป็นประจำทุกเดือน และรายงานให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบ

(3.4.3) เจ้าหน้าที่ตรวจสอบสิทธิที่มีการใช้งานในระบบให้เป็นปัจจุบัน และรายงานให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุก 3 เดือน หรือทุกการเปลี่ยนแปลงสิทธิ

(3.4.4) เจ้าหน้าที่สามารถดำเนินการเพิ่ม แก้ไข ลบ เปลี่ยนแปลงสิทธิ หรือทำการ Reset รหัสผ่านที่ได้รับการอนุมัติ

(3.4.5) เมื่อเจ้าหน้าที่ได้รับแจ้งว่ามีผู้ใช้งานลาออก ให้ระงับบัญชีผู้ใช้งาน (Account) ทันทีที่ได้รับเอกสารยืนยันการลาออกจากแผนกทรัพยากรบุคคล

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มขอหรือยกเลิกสิทธิการเข้าถึงระบบสารสนเทศ	หมายเลขเอกสาร : ITG-12-65-00
(4.2) รายงานการขอหรือยกเลิกสิทธิเข้าถึงระบบสารสนเทศ	หมายเลขเอกสาร : ITG-12-65-01
(4.3) รายงานการตรวจสอบสิทธิที่มีการใช้งานในระบบให้เป็นปัจจุบัน	หมายเลขเอกสาร : ITG-12-65-03
(4.4) ทะเบียนการกำหนดสิทธิเข้าถึงระบบสารสนเทศ	หมายเลขเอกสาร : ITG-23-65-00

4) นโยบายการรักษาความมั่นคงปลอดภัยของการทำงานจากระยะไกล (Remote Access Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของการทำงานจากระยะไกล เพื่อให้ระบบสารสนเทศ และระบบขององค์กรมีความมั่นคงปลอดภัย มีการควบคุมการใช้งาน และสามารถระบุตัวตนผู้ใช้งานจากระยะไกลได้ รวมถึงตรวจสอบการเข้าถึงข้อมูลของผู้ใช้งานจากทางไกล จึงต้องมีแนวทางปฏิบัติที่เข้มงวดเพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ และเข้าถึงส่วนงานใด หากไม่มีแนวทางปฏิบัติที่ดีอาจส่งผลให้องค์กรถูกบุคคลภายนอกใช้เป็นช่องทางเข้าถึงข้อมูลความลับ ทำให้ข้อมูลหรือระบบสารสนเทศขององค์กรเสียหาย

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมีการมอบหมายให้แผนกเทคโนโลยีสารสนเทศทำหน้าที่บริหารจัดการเรื่องรักษาความมั่นคงปลอดภัยของการทำงานจากระยะไกล (Remote Access)

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดำเนินการจัดการบัญชีผู้ใช้งาน และกำหนดช่องทางสำหรับการเข้าถึงจากระยะไกล (Remote Access)

(2.3) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดำเนินการจัดทำรายงานการขอเข้าถึงจากระยะไกล (Remote Access)

(3) แนวทางปฏิบัติ

(3.1) การกำหนดสิทธิเพื่อขอเข้าถึงระบบจากระยะไกล

(3.1.1) หัวหน้าแผนกเทคโนโลยีสารสนเทศ และผู้ที่ได้รับมอบหมาย จัดทำรายชื่อผู้มีสิทธิเข้าถึงจากระยะไกลเพื่อให้เจ้าหน้าที่สามารถทำงานหรือแก้ไขปัญหาจากระยะไกลได้ทันทีในกรณีที่ระบบภายในองค์กรเกิดขัดข้อง

(3.2) การขอสิทธิเพื่อขอเข้าถึงระบบจากระยะไกล

(3.2.1) กรณีพนักงานทั่วไปที่ต้องการขอสิทธิการเข้าถึงระยะไกล ให้ดำเนินการดังนี้

- ทำการขออนุญาตจากหัวหน้าแผนกที่ตนเองสังกัด
- หัวหน้าแผนกเทคโนโลยีสารสนเทศพิจารณาอนุมัติ

- เจ้าหน้าที่กำหนดช่องทาง และวิธีการเข้าถึงตามช่วงวัน และเวลาที่ได้ขออนุญาตไว้

(3.2.2) กรณีเป็นหน่วยงานภายนอกมีความประสงค์เข้าถึงจากระยะไกลเพื่อปรับปรุงระบบหรือดำเนินการตามสัญญาการให้บริการ ให้ดำเนินการดังนี้

- ทำการขออนุญาตหัวหน้าแผนกเทคโนโลยีสารสนเทศพิจารณาอนุมัติ
- เจ้าหน้าที่กำหนดช่องทาง และวิธีการเข้าถึงตามช่วงวัน และเวลาที่ได้ขออนุญาตไว้

(3.3) การบริหารจัดการ

(3.3.1) เจ้าหน้าที่กำหนดช่องทาง และวิธีการเข้าถึงให้กับผู้ที่ได้รับอนุญาต

(3.3.2) เจ้าหน้าที่จัดทำบัญชีรายชื่อการขอสิทธิเข้าถึงจากระยะไกล และทำรายงานสรุปให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกเดือน

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มขอเข้าถึงจากระยะไกล (Remote Access) หมายเลขเอกสาร : ITG-13-65-00

(4.2) รายงานบันทึกการขอเข้าถึงจากระยะไกล หมายเลขเอกสาร : ITG-13-65-01

5) นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ให้ผู้ใช้งานและผู้ควบคุมดูแลได้รับทราบถึงหน้าที่ และความรับผิดชอบ เป็นการป้องกันทรัพยากรและข้อมูลขององค์กรตามหลักการรักษาความมั่นคงปลอดภัย ประกอบไปด้วย ความลับ ความถูกต้อง และความพร้อมใช้งาน หากไม่มีแนวทางปฏิบัติที่ดีอาจส่งผลให้การเข้าถึงระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายเป็นไปด้วยความยากลำบาก ระบบอาจขัดข้องจากการใช้งานที่ผิดวิธี

(2) การกำหนดหน้าที่และความรับผิดชอบ

(2.1) องค์กรมีการมอบหมายให้แผนกเทคโนโลยีสารสนเทศทำหน้าที่บริหารจัดการนโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดูแลการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(3) แนวทางปฏิบัติ

(3.1) การใช้งานเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย

(3.1.1) กำหนดให้มีการแบ่งเครือข่ายตามกลุ่มการใช้งาน เพื่อให้สามารถควบคุม และป้องกันการบุกรุกเครือข่ายจากภายนอก

(3.1.2) กำหนดให้เจ้าหน้าที่สามารถเข้าไปตรวจสอบหรือการปรับแต่งอุปกรณ์ให้มีความเหมาะสมกับการใช้งาน

(3.1.3) กำหนดให้มีการจัดทำแผนผังการเชื่อมต่อเครือข่าย (Network Diagram) เพื่อการบริหารจัดการได้สะดวก

(3.1.4) ห้ามพนักงานทั่วไปทำการเคลื่อนย้ายอุปกรณ์เครือข่าย, ติดตั้งอุปกรณ์เกี่ยวกับเครือข่าย, ปรับแต่งอุปกรณ์เครือข่ายส่วนกลาง โดยไม่ได้รับอนุญาต

(3.1.5) กำหนดให้มีการใช้งานเครื่องมือตรวจจับเพื่อป้องกันการบุกรุกจากโปรแกรมประสงค์ร้าย

(3.1.6) กำหนดให้เจ้าหน้าที่เป็นผู้ทำการบำรุงรักษาระบบ ในการตรวจสอบประสิทธิภาพ การปรับปรุง และการเฝ้าระวังจากภัยคุกคาม

(3.1.7) กำหนดให้การเชื่อมต่อเครือข่ายภายนอก (อินเทอร์เน็ต) มีช่องทางสำรอง กรณีที่ช่องทางการสื่อสารหลักขัดข้อง

(3.2) การบริหารจัดการ IP Address

(3.2.1) กำหนดให้มีการใช้ IP Address V.4 หรือ V.6 ตามความเหมาะสมของการใช้งาน

(3.2.2) กำหนดให้มีการใช้งาน Public IP หรือ Private IP ตามความเหมาะสมของการใช้งาน

(3.2.3) กำหนดให้เจ้าหน้าที่เป็นผู้กำหนดหมายเลข IP Address ในการติดตั้งบนเครื่องผู้ใช้งาน

(3.2.4) กำหนดให้การใช้ IP Address แบบระบุ IP ต้องมีการบันทึกว่ามีการนำไปใช้งานกับอุปกรณ์ใด

(3.3) การเชื่อมต่อเครือข่ายแบบใช้สายสัญญาณ

(3.3.1) เมื่อผู้ใช้งานได้รับเครื่องคอมพิวเตอร์ หรือมีการย้ายตำแหน่งเครื่องคอมพิวเตอร์ เจ้าหน้าที่จะเป็นผู้ดำเนินการเดินสายสัญญาณจากจุดให้บริการมายังเครื่องคอมพิวเตอร์ของผู้ใช้งาน

(3.3.2) ไม่อนุญาตให้ผู้ใช้งานสลับสายสัญญาณเอง เว้นแต่จะได้รับอนุญาตหรือได้รับคำแนะนำจากเจ้าหน้าที่

(3.3.3) ไม่อนุญาตให้ผู้ใช้งานนำอุปกรณ์ทางด้านเครือข่าย เช่น Switch, Router, Access Point หรืออุปกรณ์อื่น ๆ ที่สามารถเชื่อมต่อเครือข่าย มาเชื่อมต่อเอง เว้นแต่จะได้รับอนุญาตหรือได้รับคำแนะนำจากเจ้าหน้าที่

(3.4) การเชื่อมต่อเครือข่ายแบบไร้สายสัญญาณ

(3.4.1) กรณีเป็นเครื่องคอมพิวเตอร์ขององค์กร ให้กำหนดค่าการเชื่อมต่อตามที่องค์กร กำหนดหรือให้เจ้าหน้าที่เป็นผู้ติดตั้งให้

(3.4.2) กรณีเป็นเครื่องคอมพิวเตอร์ภายนอกองค์กร ให้ทำการลงทะเบียนการใช้งานกับเจ้าหน้าที่ และกำหนดค่าการเชื่อมต่อตามที่องค์กร กำหนดหรือให้เจ้าหน้าที่ติดตั้งให้

(3.4.3) กรณีเป็นเครื่องคอมพิวเตอร์ของบุคคลภายนอก ให้ทำการลงทะเบียนการใช้งานกับเจ้าหน้าที่ และกำหนดค่าการเชื่อมต่อตามที่องค์กรกำหนดหรือให้เจ้าหน้าที่เป็นผู้ติดตั้งให้

(3.5) การเข้าถึงระบบสารสนเทศ เครื่องแม่ข่าย อุปกรณ์เครือข่าย

(3.5.1) ในการเข้าถึงระบบสารสนเทศ ระบบเครื่องแม่ข่าย ระบบเครือข่าย ภายในหน่วยงาน ต้องผ่านการ Login ด้วย Username และ Password

(3.5.2) กำหนดให้มีการบันทึกประวัติการ Login เข้าใช้งานของระบบ

(3.6) การบริหารจัดการ

(3.6.1) เจ้าหน้าที่จัดเก็บ และรวบรวมแบบฟอร์มการขอเชื่อมต่อเครือข่าย และจัดทำสรุปรายงานการขอเชื่อมต่อเครือข่ายให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบ เป็นประจำทุกเดือน

(3.6.2) เจ้าหน้าที่สำรวจการใช้หมายเลข IP Address และโครงสร้างการเชื่อมต่อ (Network Diagram) และจัดทำสรุปรายงานให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุก 6 เดือน หรือทุกครั้งที่มีการเปลี่ยนแปลง

(3.6.3) เจ้าหน้าที่รวบรวมประวัติการ Login เข้าสู่ระบบ และจัดทำสรุปรายงานให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกเดือน

(3.6.4) เจ้าหน้าที่ทำการตรวจสอบการทำงานของเครื่องแม่ข่าย และสรุปรายงานผลการตรวจสอบให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกเดือน

(3.6.5) เจ้าหน้าที่ทำการสำรวจอุปกรณ์เครือข่ายทั้งแบบใช้สายเชื่อมต่อ และแบบไร้สาย เป็นประจำทุก 3 เดือน

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มการขอเชื่อมต่อเครือข่าย	หมายเลขเอกสาร : ITG-14-65-00
(4.2) รายงานบันทึกการขออนุญาตเชื่อมต่อเครือข่าย	หมายเลขเอกสาร : ITG-14-65-01
(4.3) รายงานประวัติการ Login เข้าสู่ระบบสารสนเทศ	หมายเลขเอกสาร : ITG-30-65-00
(4.4) รายงานตรวจสอบการทำงานของเครื่องแม่ข่าย และอุปกรณ์เครือข่าย	หมายเลขเอกสาร : ITG-29-65-00
(4.5) บัญชีรายการบันทึกการใช้หมายเลข IP Address แบบกำหนดหมายเลข IP	หมายเลขเอกสาร : ITG-24-65-00
(4.6) บัญชีรายชื่อเครื่อง Server และรายชื่อระบบสารสนเทศ	หมายเลขเอกสาร : ITG-25-65-00
(4.7) แผนภาพการเชื่อมต่อเครือข่าย (Network Diagram) ที่เป็นปัจจุบัน	

6) นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ ให้มีการตั้งค่าการปกป้องสำหรับการเข้าถึงระบบสารสนเทศขององค์กรจากภายนอกอย่างเหมาะสม รวมถึงมีการตรวจสอบการกำหนดกฎระเบียบให้เป็นปัจจุบัน อย่างสม่ำเสมอ เพื่อให้มั่นใจว่าไฟร์วอลล์ยังมีประสิทธิภาพ หากไม่มีแนวทางปฏิบัติที่ดีอาจส่งผลให้มีการบุกรุกการเข้าถึงข้อมูลที่สำคัญขององค์กรได้

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมอบหมายให้แผนกเทคโนโลยีสารสนเทศบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายเจ้าหน้าที่ในแผนกให้เป็นผู้จัดการ และตรวจสอบกฎระเบียบของไฟร์วอลล์

(3) แนวทางปฏิบัติ

(3.1) การจัดการกฎระเบียบของไฟร์วอลล์

(3.1.1) การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

(3.1.2) กำหนดค่าบริการบนอินเทอร์เน็ตขาออก ที่ไม่ปลอดภัยเป็น การปฏิเสธ (Deny)

(3.1.3) กำหนดค่าบริการขาเข้าที่มีความจำเป็นในการใช้งาน เป็นอนุญาต (Permit)

(3.1.4) การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์สามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น

(3.1.5) การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ต้องเข้าด้วยช่องทางที่ผู้ดูแลระบบกำหนดเท่านั้น

(3.1.6) กำหนดให้อุปกรณ์ไฟร์วอลล์ต้องมีการ Login เพื่อเข้าไปจัดการ

(3.1.7) กรณีเปลี่ยนแปลงกฎระเบียบของไฟร์วอลล์จะต้องมีการลงบันทึก และต้องสำรองข้อมูล (Back Up) กฎระเบียบไว้ทุกครั้งหลังการเปลี่ยนแปลงข้อมูล

(3.1.8) การขอเปิดให้ข้อมูลผ่านเข้า - ออกได้ (การขอ Permit) ต้องทำการขออนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ โดยมีการกำหนดข้อมูล ดังต่อไปนี้

- ผู้ขออนุญาตเข้าใช้งาน
- หมายเลข Port ที่ต้องการขอให้เปิด
- หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร
- แอปพลิเคชันที่ต้องการใช้งาน และหมายเลขช่องทาง (Port)
- วัตถุประสงค์ของการใช้งาน
- ระยะเวลาในการใช้งาน

(3.2) การตรวจสอบกฎระเบียบของไฟร์วอลล์

(3.2.1) กำหนดให้เจ้าหน้าที่เข้าไปตรวจสอบกฎระเบียบของไฟร์วอลล์ ให้เป็นปัจจุบัน(Update) เป็นประจำทุก 6 เดือน

(3.2.2) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้า - ออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลไม่น้อยกว่า 90 วัน

(3.3) การบริหารจัดการ

(3.3.1) เจ้าหน้าที่ จัดทำรายงานการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

- กำหนดให้เจ้าหน้าที่จัดทำรายงานสรุปข้อมูลจราจรทางคอมพิวเตอร์ที่เข้า - ออกอุปกรณ์ไฟร์วอลล์ ให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกเดือน
- กำหนดให้เจ้าหน้าที่จัดทำรายงานบันทึกการเปลี่ยนแปลงกฎระเบียบของไฟร์วอลล์ ทุกครั้งที่ดำเนินการ
- กำหนดให้เจ้าหน้าที่จัดทำสรุปรายงานการการเข้าถึงไฟร์วอลล์ เป็นประจำทุกเดือน

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มขอเปิดช่องทางให้ข้อมูลผ่านเข้า – ออกไฟร์วอลล์ หมายเลขเอกสาร : ITG-15-65-00

(4.2) รายงานประวัติข้อมูลจราจรทางคอมพิวเตอร์

(4.3) รายงานสรุปผลการตรวจสอบกฎระเบียบไฟร์วอลล์

(4.4) รายงานบันทึกการเปลี่ยนแปลงกฎระเบียบของไฟร์วอลล์

7) **นโยบายการรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก** (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก โดยใช้เครื่องมือ IDS/IPS ในการตรวจสอบความปลอดภัยของระบบเครือข่ายทั้งภายใน และภายนอกองค์กรซึ่งอาจทำงานร่วมกับไฟร์วอลล์ ในการตรวจจับการบุกรุกและจัดการกับเหตุการณ์ที่น่าสงสัยหรือไม่เป็นไปตามข้อกำหนด หากไม่มีแนวทางปฏิบัติที่ดีอาจทำให้การตรวจจับไม่มีประสิทธิภาพส่งผลก่อให้เกิดความเสียหายแก่องค์กรได้

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมอบหมายให้แผนกเทคโนโลยีสารสนเทศ บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยในการตรวจจับการบุกรุก

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยในการตรวจจับการบุกรุก

(3) ขั้นตอนการปฏิบัติ

(3.1) การตรวจจับการบุกรุก

(3.1.1) เจ้าหน้าที่ผู้ดูแลระบบเครือข่ายตรวจสอบบันทึกกิจกรรมที่มีลักษณะเป็นการบุกรุกเข้าสู่ระบบคอมพิวเตอร์หรือเครือข่าย

(3.1.2) การเข้าถึงอินเทอร์เน็ตบนเครือข่ายจะต้องเชื่อมต่อผ่านอุปกรณ์ และซอฟต์แวร์ที่สามารถตรวจจับการบุกรุกเพื่อลดความเสี่ยงในการบุกรุกเข้าสู่ระบบคอมพิวเตอร์หรือเครือข่าย

(3.1.3) ทำการ Update Patch หรือ Signature ของ IDS/IPS เป็นประจำ

(3.1.4) หากตรวจสอบพบพฤติกรรมการใช้งาน และกิจกรรมที่น่าสงสัยซึ่งก่อให้เกิดความเสี่ยงต่อการถูกบุกรุก ต้องรายงานให้หัวหน้าแผนกเทคโนโลยีสารสนเทศทราบทันที

(3.1.5) กำหนดรูปแบบการตอบสนอง และวิธีการแก้ไขปัญหาต่อเหตุการณ์ที่อาจก่อให้เกิดความเสี่ยงในการบุกรุก

(3.1.6) กำหนดให้ยุติการเชื่อมต่อเครือข่าย และระงับการใช้งานเครื่องคอมพิวเตอร์ที่ต้องสงสัยทันที

(3.1.7) เจ้าหน้าที่ทำรายงานสรุปข้อมูลการตรวจจับการบุกรุกเพื่อนำเสนอให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกเดือน

(3.1.8) มีการจัดเก็บข้อมูลการบุกรุกไม่น้อยกว่า 90 วัน

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) รายงานการตรวจพบการบุกรุกเข้าสู่ระบบคอมพิวเตอร์ และเครือข่าย

8) นโยบายการรักษาความมั่นคงปลอดภัยของการสำรองข้อมูล และการกู้คืน (Backup/Restore Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของการสำรองข้อมูล และการกู้คืน เป็นสิ่งที่สำคัญในการรักษาความปลอดภัยของระบบสารสนเทศขององค์กรเพื่อให้ข้อมูลสำคัญขององค์กรไม่สูญหาย และสามารถกู้คืนได้อย่างรวดเร็วในกรณีเกิดเหตุการณ์ฉุกเฉิน หากไม่มีแนวทางปฏิบัติที่ดีอาจมีผลต่อการดำเนินธุรกิจขององค์กร

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมอบหมายให้แผนกเทคโนโลยีสารสนเทศ บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยของการสำรองข้อมูลและการกู้คืน

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดูแลการสำรองข้อมูล การทดสอบกู้คืนข้อมูล (Restore Test)

(3) แนวทางปฏิบัติ

(3.1) การสำรองข้อมูลสำหรับระบบสารสนเทศ

(3.1.1) กำหนดให้มีการสำรองข้อมูล (Backup) เป็นประจำทุกวัน

(3.1.2) กำหนดวิธีการสำรองข้อมูลอย่างเหมาะสมตามระบบสารสนเทศ

(3.1.3) มีการตรวจสอบการผลการสำรองข้อมูลว่ามีความผิดพลาดหรือไม่

(3.1.4) เจ้าหน้าที่ทำรายงานสรุปผลการสำรองข้อมูลของแต่ละวัน และนำเสนอให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกเดือน

(3.2) การทดสอบการกู้คืน (Restore Test) สำหรับระบบสารสนเทศ

(3.2.1) กำหนดให้มีการทดสอบการกู้คืนข้อมูลเป็นประจำทุก 3 เดือนเพื่อตรวจสอบว่าแผนการกู้คืนข้อมูลที่มีอยู่สามารถทำงานได้ตามที่กำหนดไว้หรือไม่

(3.2.2) เจ้าหน้าที่ทำรายงานสรุปผลการทดสอบการกู้คืนข้อมูล และนำเสนอหัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบประจำทุก 3 เดือน

(3.3) การกู้คืนเมื่อระบบเกิดความเสียหายสำหรับระบบสารสนเทศ

(3.3.1) เมื่อได้รับทราบว่าระบบเกิดปัญหาในการกู้ข้อมูล ให้เจ้าหน้าที่ดำเนินการเลือกวิธีการกู้คืนข้อมูลให้เหมาะสมกับประเภทของความเสียหาย และการสำรองข้อมูล

(3.3.2) เจ้าหน้าที่จะต้องเรียกใช้ข้อมูลที่มีการสำรอง (Backup) ล่าสุด ซึ่งเป็นข้อมูลที่เข้าถึงได้เพื่อทำการกู้คืนข้อมูล

(3.3.3) เจ้าหน้าที่ต้องตรวจสอบว่าข้อมูลที่กู้คืนมานั้นถูกต้อง และสมบูรณ์หรือไม่ รวมถึงตรวจสอบส่วนที่ขาดหายไปกรณีการกู้ไม่สมบูรณ์

(3.3.4) รายงานผลการกู้คืนข้อมูลให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบ ประจำทุกครั้งที่เกิดเหตุการณ์

(3.4) การสำรองข้อมูล และการกู้คืนสำหรับเครื่องคอมพิวเตอร์ผู้ใช้งาน

(3.4.1) ผู้ใช้งานทำการสำรองข้อมูลโดยการสำเนา (Copy) ข้อมูลไปยังอุปกรณ์อื่น

(3.4.2) เก็บข้อมูลสำรองให้อยู่ในที่ปลอดภัย เพื่อป้องกันการสูญหาย และการเข้าถึงจากบุคคลไม่หวังดี

(3.4.3) สำหรับข้อมูลที่มีความสำคัญต่อผู้ใช้ ควรทำการสำรองข้อมูลอย่างสม่ำเสมอ

(3.4.4) กรณีกู้คืนข้อมูลได้สำเร็จให้คัดลอกข้อมูลจากที่สำรองกลับมายังเครื่องที่ใช้งาน

(3.5) การสำรองข้อมูล และการกู้คืนสำหรับเครื่องการตั้งค่าของอุปกรณ์ (ค่า Config)

(3.5.1) เจ้าหน้าที่ทำการสำรองข้อมูลค่า Config จัดเก็บไว้ในอุปกรณ์ที่ใช้สำรองข้อมูล

(3.5.2) เจ้าหน้าที่ทำรายงานบันทึกประวัติการสำรองข้อมูล

(3.5.3) จัดเก็บอุปกรณ์ที่ใช้สำรองข้อมูลให้อยู่ในที่ปลอดภัย

(3.5.4) ทำการคืนค่า Config ลงบนอุปกรณ์เดิมหรืออุปกรณ์ทดแทนที่เป็นชนิดเดียวกัน

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แผนการสำรองข้อมูล และทดสอบการกู้คืนข้อมูล หมายเลขเอกสาร : ITG-21-65-00

(4.2) รายงานสรุปผลการการสำรองข้อมูล

(4.3) รายงานการตรวจสอบการสำรองข้อมูลข้อมูล หมายเลขเอกสาร : ITG-02-65-00

(4.4) รายงานสรุปผลการทดสอบการกู้คืนข้อมูล หมายเลขเอกสาร : ITG-08-65-00

(4.5) รายงานสรุปผลการกู้คืนข้อมูลเมื่อเกิดเหตุการณ์

9) นโยบายการรักษาความมั่นคงปลอดภัยของการเชื่อมต่ออินเทอร์เน็ต (Internet Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต เพื่อป้องกันความเสี่ยงจากการโจมตีทางไซเบอร์ ส่งเสริมให้ผู้ใช้งานตระหนักถึงความสำคัญของการใช้งานออนไลน์อย่างปลอดภัย หลีกเลี่ยงการใช้งานที่อาจก่อให้เกิดความเสียหายต่อความมั่นคงขององค์กร และผู้ใช้งานอินเทอร์เน็ต รวมถึงการกระทำที่อาจสร้างปัญหาให้กับระบบสารสนเทศในองค์กร

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมอบหมายให้แผนกเทคโนโลยีสารสนเทศ บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดูแลการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต

(3) แนวทางปฏิบัติ

(3.1) การใช้งานอินเทอร์เน็ต

(3.1.1) ให้ผู้ใช้งานมีการยืนยันตัวตนก่อนที่จะมีสิทธิในการเข้าถึงเครือข่ายอินเทอร์เน็ต หรือวิธีการอื่นใดที่สามารถระบุได้ว่าใครกำลังเข้าถึงเครือข่ายอินเทอร์เน็ต ตาม พรบ. คอมพิวเตอร์

(3.1.2) ไม่อนุญาตให้ใช้ระบบอินเทอร์เน็ตขององค์กรแสวงหาประโยชน์ส่วนตัว

(3.1.3) ไม่อนุญาตให้เข้าสู่เว็บไซต์หรือบริการบนเครือข่ายอินเทอร์เน็ตที่ไม่เหมาะสมโดยเจตนา

(3.1.4) กำหนดให้ผู้ใช้งานเข้าใจถึงความสำคัญของการใช้งานออนไลน์อย่างสุภาพ และในขอบเขตของกฎหมาย

(3.1.5) ไม่อนุญาตให้เปิดเผยข้อมูลสำคัญที่เป็นความลับขององค์กรผ่านระบบอินเทอร์เน็ต

(3.1.6) ผู้ใช้งานต้องใช้ความระมัดระวังในการดาวน์โหลด อัพโหลดข้อมูล อาจส่งผลต่อระบบสารสนเทศหรือระบบเครือข่ายในองค์กร

(3.1.7) กำหนดให้ผู้ใช้งานควรทำการลงชื่อออก (Sign out) ทุกครั้ง หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จสิ้นแล้ว เพื่อป้องกันการเข้าถึงแทนที่หรือการนำข้อมูลที่ไม่เหมาะสมออกจากระบบ และเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ใช้งาน

(3.1.8) เจ้าหน้าที่ควรให้คำแนะนำการใช้งานอินเทอร์เน็ตอย่างปลอดภัยแก่ผู้ใช้งาน

(3.1.9) เจ้าหน้าจัดทำบัญชีรายการเครื่องคอมพิวเตอร์ที่สามารถเชื่อมต่ออินเทอร์เน็ต และรายงานให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบทุกครั้งที่มีการเปลี่ยนแปลงใดๆในรายการดังกล่าว

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) รายงานประวัติข้อมูลจราจรทางคอมพิวเตอร์

10) นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการจัดการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย เพื่อเป็นมาตรฐานข้อกำหนดสำหรับการรักษาความปลอดภัยในการใช้งานเครือข่ายไร้สาย (Wi-Fi) ภายในองค์กร ทั้งนี้เจ้าหน้าที่ดูแลระบบสามารถตรวจสอบ และระบุตัวตนของผู้ใช้งานเครื่องคอมพิวเตอร์ได้ โดยผู้ใช้งานจะต้องลงทะเบียนเครื่องคอมพิวเตอร์เพื่อให้เจ้าหน้าที่ดูแลเครือข่ายอนุญาตให้เชื่อมต่อกับระบบ หากไม่มีแนวทางปฏิบัติที่ดีอาจทำให้ผู้ใช้งานที่ไม่ได้รับอนุญาตลักลอบใช้งานเครือข่ายไร้สายซึ่งอาจทำให้เข้าถึงข้อมูลที่สำคัญขององค์กรได้

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมอบหมายให้แผนกเทคโนโลยีสารสนเทศ บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดูแลการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

(2.3) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ทำการลงทะเบียนขอใช้เครือข่ายไร้สาย

(3) แนวทางปฏิบัติ

(3.1) การใช้งานเครือข่ายไร้สาย

(3.1.1) ไม่อนุญาตให้พนักงานนำอุปกรณ์ Wireless ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card มาติดตั้งหรือเปิดใช้งานร่วมกับเครือข่ายขององค์กรโดยไม่ได้รับอนุญาตจากเจ้าหน้าที่ขององค์กร

(3.1.2) ไม่อนุญาตให้พนักงาน เปิดการใช้งานแบบ Ad-hoc หรือ Peer-to-Peer Network ร่วมกับเครือข่ายขององค์กรโดยไม่ได้รับอนุญาตจากเจ้าหน้าที่ขององค์กร

(3.1.3) กำหนดให้ใช้วิธีการเชื่อมต่อที่มีความปลอดภัย เช่น WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ตามรูปแบบที่มีความเหมาะสม

(3.1.4) หากต้องการใช้งานเครือข่ายไร้สายอื่น ๆ ให้ติดต่อขออนุญาตจากเจ้าหน้าที่

(3.2) การบริหารจัดการ

(3.2.1) เจ้าหน้าที่ทำการจัดเก็บ และรวบรวมแบบฟอร์มการขอเชื่อมต่อเครือข่าย และจัดทำบัญชีรายการผู้ขอเชื่อมต่อเครือข่าย นำส่งให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกเดือน

(3.2.2) เจ้าหน้าที่จัดทำรายการตรวจสอบเครือข่ายไร้สายเพื่อส่งรายงานให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุก 3 เดือน

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มการขอเชื่อมต่อเครือข่าย หมายเลขเอกสาร : ITG-14-65-00

(4.2) รายงานบันทึกการขออนุญาตเชื่อมต่อเครือข่าย หมายเลขเอกสาร : ITG-14-65-01

(4.3) รายงานตรวจสอบการทำงานของเครื่องแม่ข่าย และอุปกรณ์เครือข่าย หมายเลขเอกสาร : ITG-29-65-00

11) นโยบายการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ เพื่อให้ผู้ใช้งานเข้าใจกฎเกณฑ์ของการใช้เครื่องมือเพื่อการสื่อสารอย่างปลอดภัยในองค์กร โดยไม่ละเมิดสิทธิหรือกระทำการใดๆ ที่อาจส่งผลต่อองค์กรหากไม่มีแนวทางปฏิบัติที่ดีอาจส่งผลให้มีผู้ไม่หวังดีทำการเจาะระบบ (Hack) เข้าถึงข้อมูลส่วนตัวผู้ใช้งาน และข้อมูลองค์กร

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมอบหมายให้แผนกเทคโนโลยีสารสนเทศ บริหารจัดการด้านการรักษาความมั่นคงปลอดภัย ของจดหมายอิเล็กทรอนิกส์

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดูแลการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์

(3) แนวทางปฏิบัติ

(3.1) การใช้บริการจดหมายอิเล็กทรอนิกส์

(3.1.1) การใช้บริการจดหมายอิเล็กทรอนิกส์เกี่ยวกับงานขององค์กรจะต้องใช้บัญชี (E-mail Account) ที่องค์กรกำหนด ซึ่งผู้ใช้งานสามารถเข้าถึงบริการจดหมายอิเล็กทรอนิกส์ได้ผ่านคอมพิวเตอร์หรือสมาร์ทโฟน

(3.1.2) ไม่อนุญาตให้ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่อการอ่าน และรับ - ส่งข้อความ

(3.1.3) ไม่อนุญาตให้นำข้อความในจดหมายของผู้อื่นไปใช้งานหรือเผยแพร่โดยไม่ได้รับอนุญาตจากเจ้าของบัญชี

(3.1.4) ไม่อนุญาตให้มีการปลอมแปลงข้อมูลของเจ้าของบัญชี

(3.1.5) ควรใช้ภาษาที่สุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสีหรือส่อไปในทางผิดกฎหมาย

(3.1.6) ไม่อนุญาตให้นำบัญชีผู้ใช้งาน (E-mail Account) ขององค์กรไปใช้สมัครบริการเพื่อการใช้งานส่วนตัว

(3.2) การขอบัญชีจดหมายอิเล็กทรอนิกส์ (E-mail Account)

(3.2.1) เจ้าหน้าที่ทำการสร้างบัญชีจดหมายอิเล็กทรอนิกส์ (E-mail Account) หลังจากได้รับข้อมูลคำขอจากผู้ใช้งาน

(3.2.2) เจ้าหน้าที่จัดทำรายการบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-mail Account) ของผู้ใช้งานในองค์กร เพื่อส่งให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบ ประจำทุกครั้งที่ดำเนินการ

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) รายการบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ หมายเลขเอกสาร : ITG-26-65-00

12) นโยบายการบริหารจัดการทรัพยากรคอมพิวเตอร์ (Asset Management Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการบริหารจัดการทรัพยากรคอมพิวเตอร์ ซึ่งประกอบไปด้วยเครื่องคอมพิวเตอร์, อุปกรณ์ต่อพ่วงคอมพิวเตอร์, อุปกรณ์เครื่องแม่ข่าย และอุปกรณ์ระบบเครือข่าย ให้อยู่ในสภาพพร้อมใช้งานอย่างมีประสิทธิภาพ เป็นการจัดการต้นทุนด้านเทคโนโลยีให้มีความคุ้มค่า ลดการสูญหายของอุปกรณ์ต่างๆ หากไม่มีแนวทางปฏิบัติที่ดีจะทำให้องค์กรไม่สามารถติดตามได้ว่าอุปกรณ์อยู่ที่ใคร ผู้ใดรับผิดชอบ และอาจทำให้ต้องมีการจัดซื้อมาซ้ำซ้อนเกินความจำเป็นส่งผลให้สิ้นเปลืองงบประมาณขององค์กร

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมอบหมายให้แผนกเทคโนโลยีสารสนเทศ บริหารจัดการทรัพยากรคอมพิวเตอร์

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดูแล และจัดการทรัพยากรคอมพิวเตอร์

(3) แนวทางปฏิบัติ

(3.1) การแจ้งซ่อมอุปกรณ์

(3.1.1) ผู้ใช้งานทำการแจ้งปัญหาไปยังเจ้าหน้าที่ผู้รับผิดชอบ

(3.1.2) เจ้าหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้นหากไม่สามารถดำเนินการแก้ไขได้ ให้ทำการจัดส่งอุปกรณ์ไปยังผู้ให้บริการรับซ่อมภายนอก

(3.1.3) หากกรณีที่แก้ไขปัญหาหรือซ่อมอุปกรณ์ไม่ได้ให้ทำการจัดซื้อของใหม่ทดแทน

(3.1.4) เจ้าหน้าที่ทำการจัดหาเครื่องคอมพิวเตอร์หรืออุปกรณ์สำรองให้แก่ผู้ใช้งานระหว่างรอซ่อม

(3.1.5) เมื่อดำเนินการแก้ไขหรือซ่อมเรียบร้อยให้นำเครื่องที่ได้รับการซ่อมเสร็จแล้วส่งคืนให้ผู้ใช้งาน และนำเครื่องสำรองส่งคืนแผนกเทคโนโลยีสารสนเทศ

(3.2) การยืม - คืนอุปกรณ์

(3.2.1) ผู้ใช้งานทำการขอยืมอุปกรณ์จากเจ้าหน้าที่ผู้รับผิดชอบ โดยต้องระบุระยะเวลายืม - คืนให้ชัดเจน

(3.2.2) เจ้าหน้าที่ต้องทำการตรวจสอบอุปกรณ์ก่อนให้ยืม

(3.2.3) ผู้ใช้งานต้องคืนอุปกรณ์ที่ยืมในเวลาที่กำหนด โดยตรวจสอบความสมบูรณ์ และประสิทธิภาพของอุปกรณ์ก่อนคืนให้แผนกหรือผู้รับผิดชอบ

(3.2.4) เจ้าหน้าที่ต้องทำการตรวจสอบอุปกรณ์ก่อนรับคืน

(3.3) การเบิกวัสดุอุปกรณ์

(3.3.1) ผู้ใช้งานทำการขอเบิกวัสดุอุปกรณ์กับเจ้าหน้าที่ผู้รับผิดชอบ

(3.3.2) เจ้าหน้าที่ทำการตรวจสอบจำนวนวัสดุอุปกรณ์ที่เบิกให้ตรงกับจำนวนที่ระบุไว้ในใบเบิก

(3.3.3) เจ้าหน้าที่ทำการตรวจสอบวัสดุอุปกรณ์ให้พร้อมใช้งาน

(3.4) การบำรุงรักษา และการสอบทาน

(3.4.1) เจ้าหน้าที่ทำการสำรวจอุปกรณ์เครื่องคอมพิวเตอร์, เครื่องพิมพ์ (Printer), กล้อง CCTV ในองค์กรว่ายังมีการใช้งานหรือไม่ และอยู่ในความดูแลของใคร จากนั้นทำสรุปรายงานแจ้งให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุก 6 เดือน

(3.4.2) หากพบว่าอุปกรณ์ชำรุดให้ตรวจสอบว่ายังอยู่ในประกันหรือเงื่อนไขการรับประกันหรือไม่

(3.4.3) หากอุปกรณ์ไม่อยู่ในเงื่อนไขการรับประกัน สามารถดำเนินการซ่อมเองหรือนำอุปกรณ์จัดส่งไปร้านบริการรับซ่อมและให้เจ้าหน้าที่ติดตามการสถานการณ์ซ่อมเป็นระยะ

(3.4.4) หากอุปกรณ์ไม่สามารถซ่อมได้หรือซ่อมแล้วก็ยังใช้งานไม่ได้ ให้ทำการจัดซื้ออุปกรณ์ใหม่ทดแทน

(3.4.5) ในกรณีที่อุปกรณ์ที่ไม่สามารถใช้งานได้แล้ว จะต้องดำเนินการขออนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศในการแยกชิ้นส่วนเพื่อนำอะไหล่มาใช้ในการซ่อมแซมอุปกรณ์อื่นๆต่อไป

(3.4.6) เครื่องคอมพิวเตอร์ที่ไม่สามารถใช้งานได้ให้ดำเนินการจำหน่ายออกเป็นมือสอง หรือบริจาคให้องค์กรอื่นๆได้ใช้ประโยชน์ต่อไป

(3.4.7) เจ้าหน้าที่จัดทำสรุปรายงานเสนอหัวหน้าแผนกเทคโนโลยีสารสนเทศ ดังนี้

- รายงานสรุปการแจ้งซ่อมเป็นประจำทุกเดือน
- รายงานสรุปการยืม - คืน เป็นประจำทุกเดือน
- รายงานสรุปการเบิกวัสดุอุปกรณ์ เป็นประจำทุกเดือน
- รายงานสรุปการสำรวจวัสดุอุปกรณ์ เป็นประจำทุกปี

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มการแจ้งซ่อม หมายเลขเอกสาร : ITG-16-65-01

(4.2) แบบฟอร์มขอยืมคืนทรัพย์สินอุปกรณ์คอมพิวเตอร์ หมายเลขเอกสาร : ITG-03-65-00

(4.3) แบบฟอร์ม เบิกวัสดุสิ้นเปลือง จากแผนก IT หมายเลขเอกสาร : ITG-10-65-00

(4.4) แบบฟอร์ม ตรวจสอบเครื่องคอมพิวเตอร์ หมายเลขเอกสาร : ITG-07-65-00

(4.5) บัญชีรายการคอมพิวเตอร์ และอุปกรณ์ต่างๆ หมายเลขเอกสาร : ITG-01-65-00

13) นโยบายการบริหารจัดการโปรแกรมคอมพิวเตอร์ (Software Management Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการบริหารจัดการโปรแกรมคอมพิวเตอร์ เพื่อให้การใช้งานโปรแกรมมีประสิทธิภาพ และปลอดภัย ป้องกันการใช้โปรแกรมเถื่อนที่อาจมีโปรแกรมประสงค์ร้ายแฝงเข้ามา หากไม่มีแนวทางปฏิบัติที่ดีอาจทำให้องค์กรเสียหายจากการถูกปรับหากพบเจอการใช้โปรแกรมที่ละเมิดลิขสิทธิ์ในองค์กร

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมีการมอบหมายให้แผนกเทคโนโลยีสารสนเทศ ทำหน้าที่บริหารจัดการโปรแกรมคอมพิวเตอร์

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดูแล และจัดการโปรแกรมคอมพิวเตอร์

(3) แนวทางปฏิบัติ

(3.1) การขอติดตั้ง ปรับปรุง ถอนการติดตั้งโปรแกรม

(3.1.1) เจ้าหน้าที่รับเรื่องการขอติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์จากผู้ใช้งาน

(3.1.2) เจ้าหน้าที่ตรวจสอบโปรแกรมที่จะทำการติดตั้งว่าถูกต้องตามลิขสิทธิ์หรือไม่ และที่มาของไฟล์ติดตั้งปลอดภัยหรือไม่

(3.1.3) เจ้าหน้าที่นำเสนอหัวหน้าแผนกเพื่ออนุมัติให้ดำเนินการติดตั้ง

(3.1.4) เจ้าหน้าที่ดำเนินการติดตั้งโปรแกรม

(3.1.5) กรณีที่ผู้ใช้งานทำการติดตั้งโปรแกรมที่ไม่ได้มาจากเจ้าหน้าที่ ต้องรับผิดชอบทั้งในด้านลิขสิทธิ์ และความมั่นคงปลอดภัยของการใช้งาน

(3.2) การใช้งานโปรแกรมคอมพิวเตอร์

(3.2.1) การกำหนดให้เจ้าหน้าที่ของแผนกเทคโนโลยีสารสนเทศเป็นผู้ควบคุมการติดตั้ง และการใช้งานโปรแกรมบนเครื่องคอมพิวเตอร์ขององค์กร เพื่อควบคุม และตรวจสอบการใช้งานโปรแกรมที่เหมาะสม และถูกต้องตามลิขสิทธิ์

(3.2.2) การใช้โปรแกรมที่ต้องทำการติดตั้งลงบนเครื่องแม่ข่ายหรือลูกข่าย จำเป็นต้องใช้โปรแกรมที่ถูกต้องตามลิขสิทธิ์

(3.2.3) การใช้โปรแกรมประเภท Open Source หรือ Freeware จะต้องมาจากแหล่งที่น่าเชื่อถือ และปลอดภัยต่อระบบคอมพิวเตอร์ขององค์กร ทั้งในการติดตั้ง และใช้งาน

(3.2.4) การใช้โปรแกรมประเภทที่เปิดผ่าน Browser จะต้องเข้าถึงเว็บไซต์ที่มีความน่าเชื่อถือ และปลอดภัยต่อระบบคอมพิวเตอร์ในองค์กรเพื่อป้องกันไม่ให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ และข้อมูลสำคัญขององค์กร

(3.2.5) ติดตั้งโปรแกรมตรวจจับ และป้องกันมัลแวร์บนเครื่องคอมพิวเตอร์ขององค์กร และเครื่องคอมพิวเตอร์ส่วนตัวที่พนักงานนำเข้ามาใช้เอง

(3.2.6) การใช้งานจากที่ไกล (Remote) ต้องใช้ช่องทางที่ปลอดภัยเพื่อป้องกันการถูกเข้าถึงข้อมูล และระบบโดยไม่ได้รับอนุญาต เช่น VPN (Virtual Private Network) ซึ่งเป็นวิธีการเชื่อมต่อที่ปลอดภัยที่ใช้งานได้ทั่วไป ทั้งนี้การใช้งานควรปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

(3.2.7) การเช่าใช้โปรแกรมหรือซื้อขาดจะต้องมีการกำหนดนโยบาย และกระบวนการที่ชัดเจนในการขออนุมัติสั่งซื้อโปรแกรม โดยแผนกหรือบุคคลที่ต้องการใช้งานจะต้องยื่นคำขออนุมัติ และระบุวัตถุประสงค์การใช้งานโปรแกรม การเช่าใช้โปรแกรมหรือซื้อขาดให้ทางแผนกเทคโนโลยีสารสนเทศ เป็นผู้ดำเนินการติดตั้ง และจัดเก็บข้อมูลโปรแกรมที่ใช้งานในที่เหมาะสมเพื่อการเข้าถึงและใช้งานได้รวดเร็ว

(3.3) การบำรุงรักษา และการสอบทาน

(3.3.1) เจ้าหน้าที่สำรวจโปรแกรมคอมพิวเตอร์ในองค์กรเพื่อตรวจสอบว่ายังมีการใช้งาน และอยู่ในความดูแลของใคร และส่งสรุปผลรายงานการสำรวจให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบเป็นประจำทุกปี

(3.3.2) เจ้าหน้าที่ต้องอัพเดทโปรแกรมอย่างสม่ำเสมอ เพื่อให้เหมาะสมกับการใช้งานในองค์กร

(3.4) การจัดหาโปรแกรมเช่า/ซื้อขาด และการต่ออายุโปรแกรม

(3.4.1) กำหนดให้เจ้าหน้าที่เป็นผู้จัดเก็บรักษา License KEY

(3.4.2) กำหนดให้เจ้าหน้าที่เป็นผู้ควบคุมการติดตั้งโปรแกรมให้กับเครื่องผู้ใช้งาน

(3.4.3) ไม่อนุญาตให้ผู้ใช้งานทำการค้นหา License Key จากเครื่องที่ติดตั้ง และนำไปใช้งาน เพราะจะส่งผลต่อการละเมิดสิทธิการใช้งาน และอาจทำให้เกิดความเสียหายต่อผู้พัฒนาซอฟต์แวร์หรือแอปพลิเคชัน

(3.4.4) ไม่อนุญาตให้เผยแพร่ หรือแจกจ่าย License Key ให้กับบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้พัฒนาซอฟต์แวร์หรือแอปพลิเคชัน

(3.4.5) โปรแกรมที่มีสัญญาการบำรุงรักษา เจ้าหน้าที่จะต้องติดตามการอัพเดตโปรแกรม แจ้งเตือนผู้ใช้งานเมื่อมีการปรับปรุงหรือแก้ไขข้อบกพร่องของโปรแกรม และประสานงานกับผู้พัฒนาโปรแกรมในการแก้ไขปัญหาได้ทันท่วงที เพื่อให้โปรแกรมทำงานได้อย่างมีประสิทธิภาพ และปลอดภัยต่อระบบ

(3.4.6) โปรแกรมที่ต้องต่ออายุสัญญา กำหนดให้เจ้าหน้าที่ดำเนินการต่ออายุสัญญาโปรแกรม

(3.5) การบริหารจัดการ

(3.5.1) เจ้าหน้าที่สามารถทำการติดตั้งโปรแกรม ปรับปรุงโปรแกรม และถอนการติดตั้งโปรแกรมบนเครื่องผู้ใช้งานได้ หากได้รับการร้องขอจากผู้ใช้งาน โดยต้องปฏิบัติตามกระบวนการ และนโยบายขององค์กร

(3.5.2) เจ้าหน้าที่จะต้องทำสรุปรายงานการขอติดตั้ง ปรับปรุง และถอนการติดตั้งโปรแกรม ทุกครั้งที่มีการดำเนินการ

(3.5.3) เจ้าหน้าที่ควรสอบทานการใช้งานโปรแกรมของผู้ใช้งานเป็นประจำทุกปี เพื่อตรวจสอบว่าผู้ใช้งานใช้โปรแกรมอย่างถูกต้องตามขั้นตอน และกฎระเบียบที่กำหนดไว้หรือไม่

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มขอติดตั้งโปรแกรม หมายเลขเอกสาร : ITG-19-65-00

(4.2) สรุปรายงานการขอติดตั้งโปรแกรม หมายเลขเอกสาร : ITG-19-65-01

(4.3) บัญชีรายชื่อโปรแกรมลิขสิทธิ์ที่ใช้ในองค์กร หมายเลขเอกสาร : ITG-01-65-00

14) นโยบายการบริหารจัดการทรัพยากรผู้ใช้งาน (Resource Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยการบริหารจัดการทรัพยากร เมื่อมีการเพิ่มพนักงานใหม่ พนักงานลาออก หรือมีการย้ายแผนกเกิดขึ้น องค์กรจำเป็นต้องมีการกำหนดแนวทางปฏิบัติที่ดีเพื่อความคุ้มครองข้อมูล และทรัพยากรที่เกี่ยวข้องกับผู้ใช้งานหรือพนักงานขององค์กร

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมีการมอบหมายให้แผนกเทคโนโลยีสารสนเทศทำหน้าที่บริหารจัดการทรัพยากรผู้ใช้งาน

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดูแลจัดการทรัพยากรของผู้ใช้งาน

(3) แนวทางปฏิบัติ

(3.1) เมื่อมีผู้ใช้งานเข้าใหม่

(3.1.1) เจ้าหน้าที่ทำการจัดเตรียมทรัพยากรคอมพิวเตอร์ และโปรแกรมที่เหมาะสมกับงาน และความต้องการของผู้ใช้งาน โดยให้คำปรึกษา และแนะนำให้ผู้ใช้งานเลือกใช้เครื่องมือที่เหมาะสมที่สุดสำหรับการทำงาน

(3.1.2) กำหนดให้เครื่องคอมพิวเตอร์ของพนักงานใหม่ต้องผ่านกระบวนการล้างฮาร์ดดิสก์ หรือใช้เครื่องมือสำหรับลบข้อมูลอย่างถูกต้อง เพื่อลบข้อมูลทั้งหมดออกจากเครื่องคอมพิวเตอร์

(3.2) เมื่อมีผู้ใช้งานลาออก

(3.2.1) เจ้าหน้าที่ตรวจสอบประวัติการยืม – คืนเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ

(3.2.2) เจ้าหน้าที่ทำการเรียกคืนอุปกรณ์ทั้งหมดที่เป็นขององค์กร รวมถึงระงับสิทธิการเข้าใช้บัญชีต่างๆ ในองค์กรเพื่อป้องกันการรั่วไหลของข้อมูล (Data Breach)

(3.2.3) เจ้าหน้าที่ทำการตรวจสอบอุปกรณ์สื่อบันทึกข้อมูล (Storage Device) หรือตัวเครื่องคอมพิวเตอร์ของผู้ใช้งานเพื่อตรวจสอบข้อมูลสำคัญ

(3.2.4) เจ้าหน้าที่ทำการสำเนาข้อมูลในกรณีที่ข้อมูลอาจมีการสูญหายหรือเกิดปัญหาเกี่ยวกับการเข้าถึงข้อมูลในอนาคต ทั้งนี้ให้หัวหน้าแผนกเทคโนโลยีสารสนเทศร่วมพิจารณาเพื่อช่วยจัดการเกี่ยวกับการเก็บสำเนาข้อมูลได้ถูกต้อง และมีความเหมาะสมกับการใช้งานของผู้ใช้งานในองค์กร

(3.2.5) เจ้าหน้าที่ทำเรื่องขออนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ เพื่อขอทำลายข้อมูลแบบถาวรในเครื่องผู้ใช้งานเพื่อนำไปใช้งานใหม่

(3.2.6) องค์กรจะไม่ทำการเก็บหรือสำเนาข้อมูลส่วนบุคคลของผู้ใช้งานที่ลาออก

(3.2.7) ยกเลิกสิทธิการใช้งานของผู้ใช้งานที่ลาออกควรมีการดำเนินการเป็นไปตามข้อกำหนด และนโยบายขององค์กรอย่างเคร่งครัด

(3.3) เมื่อพนักงานย้ายแผนกหรือเปลี่ยนตำแหน่งงานภายในองค์กร

(3.3.1) เจ้าหน้าที่ผู้ดูแลระบบทำการปรับปรุงสิทธิตามความเหมาะสม และสอดคล้องกับการทำงานของแผนกหรือตำแหน่งใหม่

(3.3.2) เจ้าหน้าที่ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น โปรแกรม หรือแอปพลิเคชันต่างๆ (Application), จดหมายอิเล็กทรอนิกส์ (E-Mail), ระบบเครือข่ายไร้สาย (Wireless LAN), ระบบอินเตอร์เน็ต (Internet) รวมถึงการเข้าถึงข้อมูลสำคัญต่างๆ เป็นต้น โดยต้องให้ สิทธิเฉพาะการปฏิบัติงานในหน้าที่

(3.4) เมื่อผู้ใช้งานมีการเปลี่ยนเครื่องคอมพิวเตอร์

(3.4.1) กำหนดให้ผู้ใช้งานทำการย้ายหรือโอนย้ายข้อมูลออกจากเครื่องคอมพิวเตอร์ภายในระยะเวลา 15 วัน ทั้งนี้สามารถขอให้เจ้าหน้าที่อำนวยความสะดวกในการโอนย้ายได้

(3.4.2) เจ้าหน้าที่ทำเรื่องขออนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ เพื่อขอทำลายข้อมูลแบบถาวรในเครื่อง ผู้ใช้งานเพื่อนำไปใช้งานใหม่

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มการขอทำลายข้อมูล หมายเลขเอกสาร : ITG-18-65-00

(4.2) รายชื่อพนักงานปัจจุบัน/เข้าใหม่/ลาออก หมายเลขเอกสาร : ITG-27-65-00

15) นโยบายการบริหารจัดการผู้ให้บริการองค์กรภายนอกในการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ (Outsource & Information System Change Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับผู้ให้บริการองค์กรภายนอก ในการเพิ่มประสิทธิภาพการทำงานให้ระบบสารสนเทศที่องค์กรว่าจ้างเพื่อดำเนินการปรับปรุงระบบ รวมถึงการพัฒนา และปรับปรุงระบบที่องค์กรพัฒนาขึ้นเอง หากไม่มีแนวทางปฏิบัติที่ดีอาจส่งผลให้ระบบสารสนเทศมีการเปลี่ยนแปลงไม่ถูกต้อง และไม่สอดคล้องกับการใช้งาน

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมีการมอบหมายให้แผนกเทคโนโลยีสารสนเทศทำหน้าที่บริหารจัดการผู้ให้บริการองค์กรภายนอกในการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ควบคุมดูแลผู้ให้บริการองค์กรภายนอกในการปรับปรุงระบบสารสนเทศ

(2.3) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ควบคุมดูแลการปรังปรุงระบบสารสนเทศที่พัฒนาขึ้นเอง

(3) แนวทางปฏิบัติ

(3.1) การรายงานปัญหาการใช้งานเพื่อขอให้มีการแก้ไขหรือการปรับปรุงระบบสารสนเทศ

(3.1.1) ผู้ใช้งานแจ้งปัญหาการที่เกิดขึ้น และยื่นคำร้องต่อเจ้าหน้าที่เพื่อขอปรับปรุงระบบสารสนเทศ

(3.1.2) เจ้าหน้าที่รายงานปัญหาให้หัวหน้าแผนกเทคโนโลยีสารสนเทศรับทราบ

(3.1.3) เจ้าหน้าที่ดำเนินการประสานงานกับผู้พัฒนาระบบ หรือผู้ให้บริการจากองค์กรภายนอกเพื่อปรับปรุงระบบ

(3.2) การทดสอบระบบสารสนเทศ

(3.2.1) กำหนดให้ผู้พัฒนาระบบสารสนเทศ หรือผู้ให้บริการจากองค์กรภายนอกทำการติดต่อเจ้าหน้าที่เมื่อต้องการเข้าทดสอบระบบภายในองค์กร

(3.2.2) เจ้าหน้าที่ทำเรื่องขออนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ และกำหนดช่วงเวลาในการทดสอบระบบ

(3.2.3) เจ้าหน้าที่ประสานงานกับผู้พัฒนาระบบ หรือผู้ให้บริการจากองค์กรภายนอกในการวางแผนทดสอบระบบ รวมถึงวางแผนการกู้คืนเมื่อการทดสอบระบบผิดพลาด

(3.2.4) เจ้าหน้าที่จัดเตรียมการสภาพแวดล้อมสำหรับทดสอบระบบ โดยมีห้องปฏิบัติงาน และอุปกรณ์สำหรับการทดสอบ

(3.3) การปรับปรุงหรือขึ้นระบบใช้งานจริง

(3.3.1) ระบบต้องผ่านการทดสอบเพื่อตรวจสอบความเสถียร และหาข้อผิดพลาดที่อาจเกิดขึ้น ก่อนการนำระบบขึ้นใช้งานจริง

(3.3.2) เจ้าหน้าที่ทำเรื่องขออนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ เพื่อกำหนดช่วงเวลาในการปรับปรุงหรือขึ้นระบบใช้งานจริง

(4) แบบฟอร์ม และเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มขออนุญาตปรับปรุง/แก้ไขระบบสารสนเทศ หมายเลขเอกสาร : ITG-17-65-00

(4.2) เอกสารบันทึกการปรับปรุง/แก้ไขระบบสารสนเทศ หมายเลขเอกสาร : ITG-17-65-01

(4.3) แบบฟอร์มขออนุญาตทดสอบ/ปรับปรุงระบบ หมายเลขเอกสาร : ITG-20-65-00

(4.4) เอกสารบันทึกการขอทดสอบ/ปรับปรุงระบบ หมายเลขเอกสาร : ITG-20-65-01

16) นโยบายการรักษาความมั่นคงปลอดภัยของการใช้สื่อบันทึก และการโอนย้ายข้อมูล (Media Data Store & Transfer Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของการใช้สื่อบันทึก และการโอนย้ายข้อมูล เพื่อให้ผู้ใช้งานบริหารจัดการไฟล์ได้อย่างมีประสิทธิภาพ และใช้พื้นที่ในการจัดเก็บอย่างเหมาะสมตามนโยบายรักษาความปลอดภัยของข้อมูล หากไม่มีแนวทางปฏิบัติที่ดีอาจส่งผลให้ข้อมูลไม่ปลอดภัย รวมถึงปัญหาพื้นที่การจัดเก็บข้อมูลไม่เพียงพอต่อความต้องการ

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมอบหมายให้แผนกเทคโนโลยีสารสนเทศทำหน้าที่บริหาร และรักษาความมั่นคงปลอดภัยของการใช้สื่อบันทึก และการโอนย้ายข้อมูล

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมาย ให้เจ้าหน้าที่ในแผนกเป็นผู้ดูแล รวมถึงแนะนำการใช้สื่อบันทึก และการโอนย้ายข้อมูล

(3) แนวทางปฏิบัติ

(3.1) การใช้สื่อบันทึกข้อมูลภายในเครื่องคอมพิวเตอร์ของผู้ใช้งาน

(3.1.1) ผู้ใช้งานควรเก็บไฟล์งานส่วนตัวที่มีความสำคัญ และต้องการรักษาเป็นความลับในพื้นที่จัดเก็บไฟล์ของตนเอง โดยจัดเก็บไฟล์เหล่านี้ในโฟลเดอร์ที่มีการรักษาความปลอดภัย และมีการเข้ารหัสเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(3.1.2) ผู้ใช้งานควรมีการจัดการไฟล์ที่ไม่จำเป็น เช่น ลบหรือย้ายไปยังพื้นที่จัดเก็บไฟล์ที่เหมาะสม รวมถึงการบีบอัดเพื่อลดขนาดของไฟล์จะทำให้ประหยัดพื้นที่ในการจัดเก็บข้อมูล

(3.1.3) ผู้ใช้งานควรปฏิบัติตามนโยบาย และข้อกำหนดขององค์กรในการจัดเก็บไฟล์ เพื่อป้องกันการเกิดความเสียหายต่อระบบคอมพิวเตอร์ขององค์กร เช่น การไม่จัดเก็บไฟล์ที่สงสัยว่าอาจก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ขององค์กร

(3.2) การใช้สื่อบันทึกข้อมูลภายนอกเครื่องคอมพิวเตอร์ผู้ใช้งาน

(3.2.1) ผู้ใช้งานสามารถจัดเก็บข้อมูลบนสื่อบันทึกข้อมูลของตนเองได้ เช่น USB Drive หรือฮาร์ดดิสก์ภายนอก (External hard disk) อีกทั้งยังต้องจัดการข้อมูลอย่างเหมาะสมเพื่อป้องกันการสูญหายหรือการเข้าถึงจากบุคคลภายนอก

(3.2.2) การจัดเก็บข้อมูลบนสื่อบันทึกข้อมูลเป็นการสำรองข้อมูลเท่านั้น ควรจัดเก็บข้อมูลต้นฉบับไว้ในเครื่องคอมพิวเตอร์เสมอเพื่อป้องกันการสูญหายของข้อมูล กรณีหากสื่อบันทึกข้อมูลเกิดความเสียหาย

(3.2.3) การเชื่อมต่อสื่อบันทึกข้อมูลต้องมีการตรวจสอบว่าไม่เป็นอันตรายต่อระบบคอมพิวเตอร์ขององค์กร ทั้งนี้ผู้ใช้งานยังสามารถขอให้เจ้าหน้าที่ติดตั้งโปรแกรมตรวจสอบเพิ่มเติมลงบนระบบคอมพิวเตอร์ เพื่อช่วยตรวจสอบความปลอดภัยของระบบ และสื่อบันทึกข้อมูล

(3.3) การใช้สื่อบันทึกรูปแบบแชร์ไดรฟ์ (Shared Drive)

(3.3.1) ในการแชร์ไดรฟ์ให้เจ้าหน้าที่เป็นผู้ทำการแชร์ และกำหนดสิทธิการเข้าถึงไฟล์ต่างๆ

(3.3.2) ไม่อนุญาตให้ผู้ใช้งานแชร์ข้อมูลจากพื้นที่ไดรฟ์ (Drive Storage) ส่วนตัว

(3.3.3) ผู้ใช้งานจะต้องมีบัญชีผู้ใช้ (Account) เพื่อเข้าถึงข้อมูลในแชร์ไดรฟ์ได้ โดยบัญชีผู้ใช้จะต้องได้รับสิทธิการเข้าถึงอย่างเหมาะสม ทั้งนี้ต้องใช้บัญชีของตนเองเท่านั้นในการเข้าถึงข้อมูล

(3.3.4) ผู้ใช้งานควรเก็บไฟล์งานส่วนตัวที่ใช้ในการทำงาน และจัดการไฟล์ที่ไม่จำเป็น เพื่อประสิทธิภาพของพื้นที่จัดเก็บไฟล์

(3.3.5) ผู้ใช้งานไม่ควรจัดเก็บไฟล์ที่สงสัยว่าอาจก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ขององค์กร

(3.4) การใช้สื่อบันทึกบนระบบคลาวด์ (Cloud Storage)

(3.4.1) ผู้ใช้งานจะต้องใช้บัญชี (Account) ของตนเองในการจัดเก็บไฟล์ที่เกี่ยวกับงานขององค์กร และควรจัดเก็บไฟล์ในพื้นที่ที่องค์กรกำหนดให้เท่านั้น

(3.4.2) กำหนดให้ผู้ใช้งานแยกพื้นที่สำหรับเก็บไฟล์ส่วนตัว และเก็บไฟล์ที่เกี่ยวข้องกับงานขององค์กร

(3.4.3) กำหนดให้ผู้ใช้งานกำหนดสิทธิการเข้าถึงให้เหมาะเมื่อมีการแชร์ไปยังผู้ใช้งานอื่นๆ

(3.4.4) กรณีที่ต้องการแชร์ข้อมูลต่อไปยังบุคคลภายนอกองค์กร ควรขออนุญาตจากผู้มีอำนาจที่เกี่ยวข้องหรือผู้บริหารในองค์กร

(3.4.5) กรณีได้รับอนุญาตแชร์ต่อไปยังบุคคลภายนอกองค์กร ต้องมีการกำหนดสิทธิ และจำกัดระยะเวลาในการเข้าถึงให้เหมาะสม

17) นโยบายการรักษาความมั่นคงปลอดภัยของการบริหารจัดการข้อมูล (Data Management Policy)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของการบริหารจัดการข้อมูล เนื่องจากข้อมูล (Data) เป็นสิ่งที่องค์กร รวบรวม จัดหา หรือสร้างขึ้น และนำมาเป็นสารสนเทศ (Information) ที่ใช้ในองค์กร ดังนั้นการบริหารจัดการเกี่ยวกับข้อมูลจึงเป็นสิ่งที่ต้องมีการควบคุม หากไม่มีแนวทางปฏิบัติที่ดีอาจส่งผลให้ข้อมูลที่เป็นความลับขององค์กรรั่วไหล

(2) การกำหนดหน้าที่ และความรับผิดชอบ

(2.1) องค์กรมีการมอบหมายให้แผนกเทคโนโลยีสารสนเทศทำหน้าที่บริหาร การรักษาความมั่นคงปลอดภัยของการบริหารจัดการข้อมูลในระบบสารสนเทศ

(2.2) หัวหน้าแผนกเทคโนโลยีสารสนเทศมอบหมายให้เจ้าหน้าที่ในแผนกเป็นผู้ดำเนินการดูแลการจัดเก็บรักษาข้อมูล

(3) แนวทางปฏิบัติ

(3.1) การแบ่งประเภทชั้นข้อมูล

(3.1.1) ลับที่สุด (Top Secret) คือ ข้อมูลที่ห้ามเปิดเผยทั้งหมดหรือบางส่วน เพราะอาจทำให้เกิดความเสียหายต่อองค์กรอย่างร้ายแรง

(3.1.2) ลับมาก (Secret) คือ ข้อมูลที่ห้ามเปิดเผยทั้งหมดหรือบางส่วน เพราะอาจทำให้เกิดความเสียหาย

(3.1.3) ลับ (Confidential) คือ ข้อมูลที่ห้ามเปิดเผยทั้งหมดหรือบางส่วน เพราะอาจทำให้เสียโอกาสหรือผลประโยชน์

(3.1.4) ใช้ภายใน (Internal Use) คือ ข้อมูลที่ห้ามเปิดเผยต่อบุคคลภายนอก และรับรู้กันเฉพาะภายในองค์กรเท่านั้น

(3.1.5) ทางการ (Official) คือ ข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้

(3.2) การกำหนดหน้าที่ผู้รับผิดชอบข้อมูล

(3.2.1) กำหนดให้เจ้าหน้าที่ที่เกี่ยวข้องเป็นผู้กำหนดสิทธิการเข้าถึงข้อมูลในระบบสารสนเทศ

(3.2.2) การกำหนดสิทธิให้กับบุคลากรในองค์กร ประกอบไปด้วย สิทธิการเป็นเจ้าของข้อมูล สิทธิการมองเห็น สิทธิในการแก้ไข สิทธิในการลบข้อมูล

(4) แบบฟอร์มและเอกสารที่เกี่ยวข้อง

(4.1) แบบฟอร์มขอหรือยกเลิกสิทธิการเข้าถึงระบบสารสนเทศ หมายเลขเอกสาร : ITG-12-65-00

(4.2) รายงานการขอหรือยกเลิกสิทธิเข้าถึงระบบสารสนเทศ หมายเลขเอกสาร : ITG-12-65-01

(4.3) รายงานการตรวจสอบสิทธิที่มีการใช้งานในระบบให้เป็นปัจจุบัน หมายเลขเอกสาร : ITG-12-65-03

18) การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Cyber Security Awareness)

(1) วัตถุประสงค์

เป็นการกำหนดแนวทางปฏิบัติเพื่อสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ใช้งานในองค์กรมีความระมัดระวังในการใช้เทคโนโลยี สามารถใช้งานได้อย่างปลอดภัย

(2) การให้ความรู้

(2.1) องค์กรมีการมอบหมายให้แผนกเทคโนโลยีสารสนเทศทำหน้าที่ให้ความรู้ และสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(2.2) จัดให้มีการแลกเปลี่ยนการเรียนรู้ด้านการรักษาความมั่นคงปลอดภัยในการใช้งานสารสนเทศเป็นประจำ

(3) หัวข้อสำคัญในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับผู้ใช้งาน

(3.1) หลักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(3.2) การเชื่อมต่อเครือข่าย

(3.3) การใช้อินเทอร์เน็ต

(3.4) การป้องกันมัลแวร์

(3.5) การใช้รหัสผ่าน

(3.6) การใช้โปรแกรมสำหรับรับ - ส่งข้อมูล

(3.7) การจัดเก็บไฟล์ข้อมูล

อนุมัติโดย

มติที่ประชุมคณะกรรมการบริษัทครั้งที่ 1/2566 เมื่อวันที่ 25 กรกฎาคม 2566 และมีผลบังคับใช้ในวันเดียวกัน

บริษัท ไลท์อัพ โทเทิล โซลูชั่น จำกัด (มหาชน)

_____

(ผศ.ดร. พร วิรุฬห์รักษ์)

ประธานกรรมการบริษัท