UAC Global Public Company Limited
บริษัท ยูเอซี โกลบอล จำกัด (มหาชน)
www.uac.co.th | 02-936-1701-6

นโยบายและแนวปฏิบัติ
ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อให้บริษัทมีนโยบายและแนวปฏิบัติในการจัดการด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมและมีประสิทธิภาพ มีความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศและสามารถดำเนินงานได้อย่างต่อเนื่อง และให้ผู้ที่เกี่ยวข้องกับบริษัททุกส่วน ทั้งผู้บริหาร พนักงาน และบุคคลภายนอกที่เข้ามาเกี่ยวข้อง ได้มีแนวปฏิบัติและกรอบการปฏิบัติที่ชัดเจน อันจะนำไปสู่การประสานงานให้บริการที่มีประสิทธิภาพ ความปลอดภัยในการให้บริการสูงสุดและมีมาตรฐานยิ่งขึ้น

ระเบียบปฏิบัติการใช้งานระบบเครือข่าย

1. การใช้งานระบบเครือข่ายจะต้องใช้งานผ่านเครื่องคอมพิวเตอร์ของบริษัทเท่านั้น
2. การใช้งานระบบเครือข่ายจากเครื่องคอมพิวเตอร์ที่ไม่ใช่เครื่องคอมพิวเตอร์ของบริษัท จะต้องได้รับอนุญาตจากผู้ดูแลระบบก่อน และหากพบว่ามีการใช้งานโดยไม่ได้รับอนุญาต ผู้ดูแลระบบสามารถตัดการใช้งานออกจากระบบเครือข่ายได้ทันที
3. ห้ามใช้หรือเข้าเว็บไซต์ต้องห้ามต่าง ๆ ได้แก่ เว็บไซต์ที่ขัดกับหลักการสำคัญของบริษัท และ/หรือขัดต่อผลประโยชน์ทางธุรกิจ เว็บไซต์ที่มีเนื้อหาลามก อนาจาร เว็บไซต์เกี่ยวกับการละเมิดลิขสิทธิ์ เว็บไซต์เกี่ยวกับแฮคเกอร์ เว็บไซต์การพนันทุกประเภท
4. ห้ามพนักงานใช้อินเตอร์เน็ตบริษัทเพื่อแสวงหาประโยชน์ส่วนตนหรือทำธุรกิจ
5. ห้ามโพสต์หรือแชร์ข้อมูลอันเป็นเท็จและส่งผลกระทบต่อภาพลักษณ์ชื่อเสียงบริษัท
6. ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น
7. ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัท และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์
8. ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก
9. ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้
10. ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นจ้าของข้อมูลนั้น ๆ.

แนวปฏิบัติการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อให้การบริหารงานด้านความปลอดภัยระบบสารสนเทศ มีประสิทธิภาพและประสิทธิผล มีกลไกในการควบคุมดูแลด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ นำไปสู่การปฏิบัติให้เป็นไปในทิศทางเดียวกัน จึงกำหนดให้ผู้ที่มีอำนาจรับผิดชอบ เป็นผู้กำกับดูแลด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

โดยมีบทบาทหน้าที่ความรับผิดชอบดังนี้

1. กำหนดเป้าหมาย จัดการพัฒนานโยบายด้านการรักษาความปลอดภัยข้อมูล Policy Standard Procedure and guideline เพื่อให้องค์กรได้มาซึ่ง การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ
2. กำกับดูแลการปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ
3. จัดการบริหารความเสี่ยง วิเคราะห์ความเสี่ยง ที่อาจทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุรกิจของบริษัท
4. ควบคุมบริหารทีม Incident response เพื่อให้สามารถปฏิบัติงานในยามที่ภาวะฉุกเฉินด้านเทคโนโลยีสารสนเทศในองค์กร เช่น การระบาดไวรัสคอมพิวเตอร์
5. เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ ๆ ทางด้าน Information Security อย่างสม่ำเสมอ
6. ให้คำปรึกษาด้านระบบความปลอดภัยข้อมูลให้กับแผนกอื่น ๆ ที่ต้องใช้ไอทีในการปฏิบัติงาน

การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการตอบสนองความเสี่ยง

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ
2. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มี เสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
3. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่องและสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศมีทั้งปัจจัยภายในและปัจจัยภายนอก ได้แก่

1. ระบบเครือข่ายอินเตอร์เน็ตขัดข้อง
2. ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ
3. การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่าง ๆ
4. การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต
5. การเข้าถึงระบบข้อมูลโดยไม่ได้รับอนุญาต

การบริหารความเสี่ยง

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือองค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนและกระบวนการดำเนินงานด้านการบริหารความเสี่ยงสอดคล้องกับ COSO ERM 2017

แนวปฏิบัติการบริหารจัดการความปลอดภัยของข้อมูล

วัตถุประสงค์

ข้อมูลสารสนเทศเป็นสินทรัพย์สำคัญทางธุรกิจ ที่ต้องจัดการด้านความปลอดภัยของข้อมูลและป้องกันอย่างดี บริษัทได้กำหนดความปลอดภัยระบบข้อมูลสารสนเทศ โดยการนำเทคโนโลยีความปลอดภัยที่สำคัญมาใช้ในองค์กร เพื่อช่วยในการทำงานและลดความเสี่ยงด้านความปลอดภัย ในระดับที่เหมาะสม และเกิดประสิทธิภาพต่อการทำงานสูงสุด บริษัทได้ตระหนักถึงความสำคัญข้อมูลสารสนเทศ โดยให้มีการบริหารจัดการให้ระบบข้อมูลมีลักษณะคงความเป็น CIA ดังนี้

1. การรักษาความลับ (Confidentiality) ให้บุคคลมีสิทธิ์เท่านั้น เข้าถึงเรียกดูข้อมูล ข้อมูลความลับ ต้องไม่เปิดเผยกับผู้ไม่มีสิทธิ์
2. ความถูกต้องแท้จริง (Integrity) ป้องกันความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล มีการควบคุมความผิดพลาด ไม่ให้ผู้ไม่มีสิทธิ์มาเปลี่ยนแปลง แก้ไข ข้อมูล
3. ความสามารถพร้อมใช้เสมอ (Availability) ให้บุคคลมีสิทธิ์เท่านั้นเข้าถึงข้อมูลได้ทุกเมื่อที่ต้องการ ต้องมีการควบคุมไม่ให้ระบบล้มเหลว มีสมรรถภาพทำงานต่อเนื่อง ไม่ให้ผู้ไม่มีสิทธิ์มาทำให้ระบบหยุดทำงาน

มาตรการลงโทษการฝ่าฝืนระเบียบด้านการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

บริษัทได้จัดทำ คู่มือความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ขึ้นเพื่อเป็นแนวปฏิบัติการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ไม่ให้บุคคลใดบุคคลหนึ่งฝ่าฝืนข้อบังคับต่างๆ ที่ได้กำหนดไว้ เพื่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท หากพนักงานหรือผู้ใช้งานฝ่าฝืน ทำให้มาตรการรักษาความมั่นคงปลอดภัยของระบบและเครือข่ายของบริษัทอยู่ในความเสี่ยง ซึ่งอาจนำไปสู่การตกเป็นผู้ต้องสงสัยต้องถูกดำเนินคดีภายใต้กฎหมายและบริษัทจะพิจารณาลงโทษตามระเบียบบริษัท พร้อมทั้งให้ความร่วมมือกับเจ้าหน้าที่ตำรวจที่ทำหน้าที่สืบสวนกิจกรรมต้องสงสัย