นโยบายการรักษาความมั่นคงและความปลอดภัย

ด้านสารสนเทศและการสื่อสาร

1. Purpose (วัตถุประสงค์)

1.เพื่อกำหนดนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับ บริษัท เอเชียน มารีน เซอร์วิสส์ จำกัด(มหาชน) ตระหนักถึงความสำคัญของการรักษาความมั่นคงและความปลอดภัยด้านสารสนเทศ และปฏิบัติตามอย่างเหมาะสม

2.เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศของ องค์กร ว่าสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีความพร้อมใช้งาน (Availability)

3.เพื่อเผยแพร่ให้เจ้าหน้าที่และผู้ใช้งานสารสนเทศของ บริษัท เอเชียน มารีน เซอร์วิสส์ จำกัด (มหาชน) ได้รับทราบและปฏิบัติอย่างเคร่งครัด

2. Scope (ขอบข่าย)

1.จัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติในการรักษาความมั่นคงและความปลอดภัยด้านสารสนเทศ เป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการมาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.จัดให้ข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ สถานที่และสิ่งแวดล้อมที่เกี่ยวข้องกับ สารสนเทศ การพัฒนาและบำรุงรักษาระบบสารสนเทศ และสิ่งใดๆที่เกี่ยวข้องกับสารสนเทศ มีการรักษาความมั่นคงปลอดภัยอย่าง เหมาะสมและเพียงพอ และมีการควบคุมการเข้าถึงที่กำหนดอย่างชัดเจนตามหลักการของความต้องการในการใช้งานที่เหมาะสม และมั่นคงปลอดภัย

3.จัดให้มีระบบสำรองข้อมูล ระบบกู้คืนข้อมูล และระบบสำรองที่ใช้ทดแทนระบบเทคโนโลยีสารสนเทศหลักในกรณีฉุกเฉิน โดยระบบสำรองต้องอยู่ในสภาพพร้อมใช้งาน และมีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

4.จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยมีแนวทางสอดคล้องกับการบริหารความเสี่ยงของทางแผนก IT

5.จัดให้มีการตรวจสอบและดำ

เนินการแก้ไข เมื่อมีเหตุการละเมิดความมั่นคงปลอดภัยเกิดขึ้น พร้อมทั้งดำเนินการป้องกันไม่ให้เกิดซ้ำ และให้รายงานและบันทึกไว้อย่างชัดเจน

6.จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย แนวทางปฏิบัติ มาตรฐาน และระเบียบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

นโยบายการควบคุมการเข้าถึงสารสนเทศ (Access control)

บริษัท เอเชียน มารีน เซอร์วิสส์ จำกัด(มหาชน) มีการควบคุมการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เพื่อ กำหนดมาตรการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศโดยไม่ได้รับอนุญาต ป้องกันการบุกรุกทั้งด้านกายภาพ ผ่านระบบเครือข่าย และจากโปรแกรม ที่จะสร้างความเสียหายแก่ข้อมูลหรือทำให้ระบบหยุดชะงัก และสามารถตรวจสอบติดตามการพิสูจน์ตัวบุคคลที่ใช้งาน ข้อมูลหรือระบบสารสนเทศขององค์กรได้อย่างถูกต้องโดยยึดหลักดังนี้

1. การรักษาความลับ (Confidentiality) ให้บุคคลผู้มีสิทธิ์เท่านั้น เข้าถึงข้อมูลได้ และมีการควบคุมการเข้าถึงโดยข้อมูลที่เป็นความลับ จะได้ไม่ถูกเปิดเผยกับผู้ไม่มีสิทธิ์

2. ความถูกต้องครบถ้วน (Integrity) ให้มีการรักษาความถูกต้องครบถ้วนของข้อมูล และควบคุมความผิดพลาด ไม่ให้ข้อมูลถูกแก้ไข ลบทิ้ง เปลี่ยนแปลงโดยผู้ไม่มีสิทธิ

3. ความสามารถในการเข้าถึงและใช้งานได้ (Availability) ให้ผู้มีสิทธิ์ใช้ข้อมูลเท่านั้นสามารถที่จะเข้าถึงข้อมูลได้ตามเวลาที่ตกลงไว้ ผู้รับผิดชอบต้องควบคุมไม่ให้ระบบหยุดชะงัก มีสมรรถภาพในการทำงานต่อเนื่อง และมีการป้องกันไม่ให้มีสิ่งใดทำให้ระบบหยุดทำงาน

วัตถุประสงค์ของการควบคุมการเข้าถึงสารสนเทศ

1. เพื่อกำหนดแนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงาน ให้กับองค์กร ตระหนักถึงความสำคัญของการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ

2. เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ว่า สามารถเข้าถึงได้เฉพาะผู้มีสิทธิ (Confidentiality) มี ความครบถ้วนสมบูรณ์ (Integrity) และมีความพร้อมใช้งาน (Availability)

3. เพื่อให้สามารถตรวจสอบย้อนหลังการเข้าถึงระบบสารสนเทศต่างๆ ของผู้ใช้งานได้

แนวทางปฏิบัติ

1. จัดให้มีแนวทางปฏิบัติ และขั้นตอนปฏิบัติด้านการใช้งานและการเข้าถึงข้อมูลและระบบสารสนเทศ เป็นลายลักษณ์อักษร โดย สอดคล้องตามกฎหมาย หลักการ มาตรฐานสากล ของการรักษาความมั่นคงปลอดภัยสารสนเทศ

2. จัดให้มีข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ สถานที่และสิ่งแวดล้อมที่เกี่ยวข้องกับ สารสนเทศ การพัฒนาและบำรุงรักษาระบบสารสนเทศ และสิ่งใดๆที่เกี่ยวข้องกับสารสนเทศ มีการรักษาความมั่นคงปลอดภัยอย่าง เหมาะสมและเพียงพอ และมีการกำหนดการควบคุมการใช้งานและการเข้าถึงที่อย่างชัดเจนตามหลักการของความต้องการในการ ใช้งานที่เหมาะสมและมั่นคงปลอดภัย

3. จัดให้มีแนวทางปฏิบัติในการพัฒนาการซอฟต์แวร์ ที่ต้องควบคุมการเข้าถึงและสิทธิ์ในการใช้ข้อมูลในระบบ ไปจนกระทั่งการ ควบคุมการเข้าถึงด้วยระบบปฏิบัติการ ซึ่งรวมถึงการใช้ข้อมูลในส่วนต่างๆภายในคอมพิวเตอร์ของผู้ใช้งาน

4. จัดให้มีแนวทางปฏิบัติในการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ และอุปกรณ์สารสนเทศ

5. จัดให้มีแนวทางปฏิบัติในการการควบคุมการเข้าถึงห้องเครื่องแม่ข่าย หรือศูนย์ข้อมูล บนอินเทอร์เน็ต รวมทั้งอุปกรณ์สารสนเทศให้ เข้าได้เฉพาะผู้มีสิทธิ์เท่านั้น

6. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย ข้อกำหนด แนวทางปฏิบัติ ระเบียบ และขั้นตอนปฏิบัติเกี่ยวกับการใช้งานข้อมูลและระบบ สารสนเทศ โดยผู้ใช้งานต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด