

นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ฉบับปรับปรุง ปี 2567

1. หลักการและเหตุผล

บริษัท สยามเวลเนสกู๊ป จำกัด(มหาชน) ได้กำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ มีวัตถุประสงค์ดังต่อไปนี้

เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการติดต่อสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กรให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผลและปฏิบัติได้อย่างถูกต้องตามกฎหมายต่างๆ ที่เกี่ยวข้องได้กำหนดไว้

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้ อย่างเคร่งครัด

เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหารเจ้าหน้าที่ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กรตระหนักถึงความสำคัญการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการติดต่อสื่อสารขององค์กรในการดำเนินการและปฏิบัติตามอย่างเคร่งครัด นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้ง ต่อปี

2. วัตถุประสงค์

บริษัท สยามเวลเนสกู๊ป จำกัด(มหาชน) ได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทเป็นไปอย่างเหมาะสมมีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่องและป้องกันภัยคุกคามต่างๆ ปฏิบัติตามเจตนารมณ์ของพระราชบัญญัติดังกล่าวได้อย่างถูกต้องและเหมาะสม

นอกจากนี้ยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่นๆ ที่เกี่ยวข้องรวมถึงการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ด้วย

3. ความหมายและคำจำกัดความ

หน่วยงาน หรือ องค์กร หมายถึง บริษัท สยามเวลเนสกู๊ป จำกัด(มหาชน)

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ ที่เชื่อมต่อการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

ความมั่นคงปลอดภัย หมายถึง ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

ระบบแลน (Local Area Network) และ ระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

คอมพิวเตอร์ หมายถึง คอมพิวเตอร์แบบตั้งโต๊ะและคอมพิวเตอร์แบบพกพา

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำมาใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของบริษัทสยามเวลเนสกรุ๊ป จำกัด(มหาชน)

ผู้ให้บริการ หรือ ผู้ใช้งาน หมายถึง ผู้ใช้ภายในของหน่วยงานที่มีสิทธิ์เข้าถึงข้อมูลสารสนเทศ และหมายรวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้คอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

ผู้ดูแลระบบ (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบเครือข่ายและคอมพิวเตอร์ไม่ว่าส่วนใดส่วนหนึ่ง

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิเฉพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

หน่วยงานภายนอก หมายถึง องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

4. องค์ประกอบของนโยบาย

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ บริษัท สยามเวลเนสกรุ๊ป จำกัด(มหาชน) จัดทำขึ้น เพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้อง และเป็นไปตามนโยบายที่กำหนดไว้โดยแบ่งแนวปฏิบัติออกเป็นส่วนๆ ดังต่อไปนี้

- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Acceptable use Policy)
- โครงสร้างทางด้านการมั่นคงปลอดภัยสารสนเทศ(Organizational Information Security)
- การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human resource security)
- การบริหารจัดการสินทรัพย์ (Asset Management)(Human resource security)
- แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)
- แนวปฏิบัติการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ ไฟร์วอลล์ (Firewall Policy)
- แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail Policy)
- แนวปฏิบัติการใช้งานอินเทอร์เน็ต (Internet Policy)
- แนวปฏิบัติการควบคุมการเข้าถึง (Access Control Policy)
- แนวปฏิบัติการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก (Intrusion Detection System : IDS and Intrusion Prevention System : IPS)
- การกำหนดผู้รับผิดชอบ
- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)
- การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment)
- ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการติดต่อสื่อสารของบริษัท สยามเวลเนสกรุ๊ป จำกัด(มหาชน) แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทฯ เพื่อที่จะช่วยให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการติดต่อสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสี่ยงต่อการปฏิบัติงานทรัพยากรสิน บุคลากรของบริษัทฯ ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการติดต่อสื่อสารของบริษัท สยามเวลเนสกรุ๊ป จำกัด(มหาชน) จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการติดต่อสื่อสารของบริษัทฯ ซึ่งเจ้าหน้าที่ของบริษัทฯ และหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด