BIG DATA INSTITUTE

ประกาศสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)
เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ
(Information Security Policy)

ด้วยสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) (“สถาบัน”) ได้ตระหนักถึงความสำคัญของการบริหารงานด้านระบบเทคโนโลยีและข้อมูลสารสนเทศ รวมทั้งคำนึงถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น ดังนั้น เพื่อให้การดำเนินงานด้านการบริหารจัดการระบบการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย เชื่อถือได้ สอดคล้องกับนโยบายและมาตรฐานของกฎหมายที่เกี่ยวข้อง

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชกฤษฎีกาจัดตั้งสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) พ.ศ. ๒๕๖๖ ประกอบกับมติที่ประชุมคณะทำงานธรรมาภิบาลข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ครั้งที่ ๓/๒๕๖๘ เมื่อวันที่ ๑๓ มีนาคม พ.ศ. ๒๕๖๘ ผู้อำนวยการสถาบันข้อมูลขนาดใหญ่ จึงออกประกาศนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ดังต่อไปนี้

ข้อ ๑ สถาบันได้กำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) โดยมีวัตถุประสงค์ ดังต่อไปนี้

(๑) เพื่อดำเนินการปกป้องทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัยโดยครอบคลุมถึงความลับ (Confidential) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) อย่างเป็นระบบและสอดคล้องตามมาตรฐาน

(๒) เพื่อดำเนินการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้ครอบคลุมในขอบเขตของการจัดทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศอย่างสม่ำเสมอ

(๓) เพื่อบริหารจัดการความเสี่ยงตามแนวทางที่กำหนดให้เกิดผลในการปกป้องทรัพย์สินสารสนเทศอย่างเพียงพอและเหมาะสม

(๔) เพื่อดำเนินการควบคุมการเข้าถึงระบบสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ ระบบปฏิบัติการ โปรแกรมประยุกต์ และสารสนเทศ ทั้งจากการปฏิบัติงานภายในและภายนอกสถาบัน

(๕) เพื่อพิจารณาภัยคุกคามและช่องโหว่ของระบบสารสนเทศอย่างเป็นระบบ เพื่อให้สอดคล้องกับเทคโนโลยีและการดำเนินธุรกิจสมัยใหม่

(๖) เพื่อเป็นการสื่อสารนโยบายความมั่นคงปลอดภัยของสารสนเทศไปยังผู้ใช้งาน ผู้ดูแลระบบ หรือผู้เกี่ยวข้องกับระบบสารสนเทศได้รับทราบ เข้าใจ และนำไปปฏิบัติให้สอดคล้องในทุกระดับ

(๗) เพื่อเป็นการเผยแพร่ความรู้ ความเข้าใจ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเสริมสร้างความตระหนักให้กับผู้ปฏิบัติงานของสถาบันและผู้มีส่วนได้เสียที่เกี่ยวข้อง

(๘) เพื่อดำเนินการดูแลระบบสารสนเทศหลักและระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานระบบสารสนเทศได้อย่างต่อเนื่อง

/ข้อ ๒ ให้ผู้บริหาร...

ข้อ ๒ ให้ผู้บริหารและผู้ปฏิบัติงานทุกระดับมีส่วนร่วมในการส่งเสริมให้ระบบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศได้รับการพัฒนาอย่างต่อเนื่อง (Continual Improvement)

ข้อ ๓ ให้ผู้บริหารและผู้ปฏิบัติงานทุกระดับปฏิบัติตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ข้อกำหนด คำสั่ง หรือสัญญา ที่เกี่ยวกับข้อมูลสารสนเทศอย่างเคร่งครัด รวมถึงการปฏิบัติตามกฎหมายที่เกี่ยวกับการคุ้มครองสารสนเทศส่วนบุคคล และระบบข้อมูลสารสนเทศ เช่น ปฏิบัติตามกฎหมายลิขสิทธิ์ (Copyright) หรือใบอนุญาต (License) ของ Software Product และข้อมูลสารสนเทศอื่น ๆ ที่ต้องการใช้เพื่อประโยชน์ทางธุรกิจให้ถูกต้อง

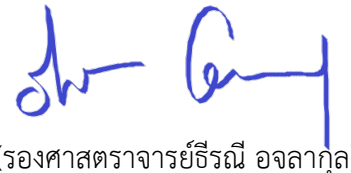
ข้อ ๔ ให้ผู้บริหาร ผู้ปฏิบัติงาน หรือผู้ที่เกี่ยวข้องปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) แนบท้ายประกาศนี้อย่างเคร่งครัด

ข้อ ๕ ให้มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ของสถาบัน ให้มีความทันสมัยเป็นปัจจุบัน และเป็นมาตรฐานที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖ กรณีไม่สามารถปฏิบัติตามประกาศฉบับนี้ หรือไม่สามารถปฏิบัติตามนโยบายมาตรฐานความปลอดภัยของข้อมูลสารสนเทศ อันเนื่องมาจากสภาพหรือสถานการณ์ที่ไม่อาจหลีกเลี่ยงได้ให้เป็นอำนาจของผู้อำนวยการที่จะทำการวินิจฉัยและสั่งการตามความเหมาะสมต่อไป

จึงประกาศให้ทราบโดยทั่วกัน ทั้งนี้ ให้มีผลนับตั้งแต่บัดนี้เป็นต้นไป จนกว่าจะมีประกาศเปลี่ยนแปลง

ประกาศ ณ วันที่ ๒๔ มีนาคม พ.ศ.๒๕๖๘



(รองศาสตราจารย์ธีรณี อจลากุล)
ผู้อำนวยการสถาบันข้อมูลขนาดใหญ่

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ
(Information Security Policy)

---

๑. บททั่วไป

การรักษาความมั่นคงปลอดภัยสารสนเทศของสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) (“สถาบัน”) ใช้กรอบการดำเนินการในรูปแบบวงจรควบคุมคุณภาพ (PDCA Cycle) ซึ่งเป็นการจัดการเชิงกระบวนการ (Process Approach) โดยคำนึงถึงกลไกการควบคุมที่สอดคล้องกับความเสี่ยงของสินทรัพย์ เพื่อตรวจสอบ ประเมินผล ทบทวน และปรับปรุงนโยบาย และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน และเอกสารที่เกี่ยวข้องให้ดีขึ้นอย่างต่อเนื่องและสอดคล้องกับยุทธศาสตร์ของสถาบัน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์ที่สำคัญ

๒. โครงสร้าง บทบาท หน้าที่ และความรับผิดชอบ ในการรักษาความมั่นคงปลอดภัยสารสนเทศ

สถาบันได้แบ่งแยกหน้าที่และความรับผิดชอบให้ชัดเจนในการปฏิบัติงานเพื่อลดโอกาสที่จะทำให้มีการเปลี่ยนแปลงแก้ไขระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ การเปลี่ยนแปลงทรัพย์สินของสถาบัน หรือมีการนำทรัพย์สินไปใช้ผิดวัตถุประสงค์ โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนา โดยบทบาทหน้าที่และความผิดชอบ รวมถึงการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๓. การบริหารจัดการความเสี่ยง

สถาบันมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยมีแผนการจัดการความเสี่ยง ซึ่งกำหนดเกณฑ์ในการประเมิน การแก้ไข และยอมรับความเสี่ยง เพื่อลดโอกาสในการสูญเสียความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของสินทรัพย์ของสถาบัน ซึ่งมีการจัดแบ่งระดับความเสี่ยงเป็น ๓ ระดับ คือ High, Medium และ Low โดยระดับความเสี่ยงที่สถาบัน สามารถยอมรับได้โดยไม่จำเป็นต้องดำเนินการแก้ไขและควบคุมความเสี่ยง คือ ระดับ Low เท่านั้น การยอมรับความเสี่ยงระดับที่สูงกว่า Low ต้องดำเนินการอย่างเป็นลายลักษณ์อักษรและต้องได้รับความเห็นชอบจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารความเสี่ยง (Risk Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๑ ว่าด้วยเรื่องการระบุความเสี่ยง (Identify)

๔. การสร้างความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร

สถาบันมีการสร้างความรู้และความตระหนักในการใช้งานระบบสารสนเทศอย่างมั่นคงปลอดภัยแก่ผู้ใช้งาน ผู้ปฏิบัติงาน โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่เอกสารที่เกี่ยวข้องผ่านระบบเว็บไซต์ภายในของสถาบัน รวมถึงสื่อสารนโยบายด้านความมั่นคงปลอดภัยสารสนเทศให้ผู้ให้บริการภายนอกทราบในเรื่องที่เกี่ยวข้อง รวมถึงการสรรหาบุคลากร ต้องเป็นไปตามเกณฑ์ที่กำหนด และมีการตรวจสอบคุณสมบัติ (Screening) ของผู้สมัครงานทุกคนเป็นไปตามเกณฑ์ที่กำหนด หากผู้สมัครงานได้รับการคัดเลือกและบรรจุเป็น

/ผู้ปฏิบัติงาน...

ผู้ปฏิบัติงานของสถาบันจะมีการตรวจสอบประวัติอาชญากรรมจากสำนักงานตำรวจแห่งชาติและประวัติการทำงานต่าง ๆ รวมถึงคดีความมั่นคงปลอดภัยของสารสนเทศของผู้ที่ผ่านการคัดเลือกกับสถานที่ทำงานเดิมและ/หรือหน่วยงานภาครัฐที่เกี่ยวข้อง เพื่อลดความเสี่ยงที่จะเกิดกับสถาบัน ตลอดจนจัดทำข้อตกลง และเงื่อนไขการจ้างงาน (Terms and conditions of employment) เป็นไปตามเกณฑ์ที่กำหนด โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๕. การสื่อสารในสถาบัน

สถาบันมีการเผยแพร่นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศบนเว็บไซต์ภายใน ทางออนไลน์อื่น ๆ และระบบจัดเก็บเอกสารของสถาบัน เพื่อสื่อสารให้ผู้ปฏิบัติงานภายในสถาบันได้รับทราบถึงข้อมูลข่าวสารต่าง ๆ รวมถึงการเผยแพร่นโยบายผ่านหน้าเว็บไซต์ของสถาบัน เพื่อสื่อสารให้บุคคลภายนอกที่เกี่ยวข้องรับทราบ รวมถึงสามารถเข้าถึงได้อย่างสะดวก โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๖. การจัดการเอกสารสารสนเทศ

สถาบันมีการบริหารจัดการเอกสารที่เกี่ยวข้องกับการปฏิบัติงานภายในของสถาบัน ได้แก่ นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ และขั้นตอนการควบคุมเอกสาร โดยสถาบันจะจัดการและควบคุมเอกสารตามมาตรฐานในการสร้างธรรมาภิบาลสารสนเทศและรักษาความมั่นคงปลอดภัยของสารสนเทศในองค์กร โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการควบคุมเอกสาร (Document Control Procedure) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๗. การทบทวนการบริหารระบบมาตรฐาน

สถาบันมีการทบทวนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของสถาบัน เพื่อให้มั่นใจว่าการดำเนินงานมีความเหมาะสม และมีประสิทธิผล ทั้งนี้ การทบทวนดังกล่าวต้องพิจารณาถึงโอกาสในการปรับปรุงและพัฒนาอย่างต่อเนื่องเพื่อบรรลุวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน โดยมีการรายงานต่อคณะทำงานธรรมาภิบาลข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ในการประชุมทบทวนการบริหารระบบมาตรฐาน (Management Review) หรือการประชุมคณะทำงานธรรมาภิบาลข้อมูลฯ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๘. การปรับปรุงพัฒนา

สถาบันมีการแก้ไขและปรับปรุงนโยบายและการปฏิบัติงานที่ไม่สอดคล้องด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีการกำหนดกระบวนการในการทบทวน การระบุสาเหตุ การแก้ไขหรือเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การทบทวนประสิทธิผลของปฏิบัติการแก้ไข รวมถึงการจัดเก็บเอกสารที่เกี่ยวข้อง เพื่อให้เกิดการพัฒนาอย่างต่อเนื่องและมีประสิทธิภาพ โดยการปฏิบัตินั้นให้เป็นไปตาม

/แนวทางการบริหาร...

แนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ว่าด้วยเรื่อง “การจัดการการเปลี่ยนแปลง (Change Management)” ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๙. การบริหารจัดการสินทรัพย์

สถาบันมีการบริหารจัดการสินทรัพย์เกี่ยวกับเทคโนโลยีสารสนเทศของสถาบัน คือ ประเภทข้อมูล (Information) อุปกรณ์ (Hardware) ซอฟต์แวร์ (Software) บุคลากร (People) บริการ (Service) โดยการจัดทำมาตรการควบคุมการใช้งานสินทรัพย์ที่เหมาะสมตลอดวงจรชีวิตของสินทรัพย์ ตั้งแต่การจัดหา การลงทะเบียน การบำรุงรักษา การจำหน่าย และการทำลายสินทรัพย์ ตามลำดับชั้นความลับของข้อมูลที่อยู่ในสินทรัพย์นั้น ๆ โดยมีการตรวจสอบและทบทวนทะเบียนสินทรัพย์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น เพื่อให้มั่นใจว่าทะเบียนสินทรัพย์เป็นปัจจุบันอยู่เสมอ โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารความเสี่ยง (Risk Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๑ ว่าด้วยเรื่องการระบุความเสี่ยง (Identify)

๑๐. การแบ่งประเภทของข้อมูล และการจัดการสื่อที่ใช้ในการบันทึกข้อมูล

สถาบันมีการแบ่งประเภทของข้อมูล (Data Classification) ทั้งที่อยู่ในรูปแบบกระดาษและอิเล็กทรอนิกส์ แบ่งออกเป็น ๕ ประเภท คือ

(๑) เอกสารเผยแพร่ (Public) หมายถึง ข้อมูลที่สามารถนำไปเปิดเผยนอกองค์กรและสาธารณะ โดยไม่มีความเสี่ยงหรือมีความเสี่ยงน้อยที่องค์กรรับได้

(๒) เอกสารใช้ภายใน (Private) หมายถึง ข้อมูลที่เปิดเผยให้เฉพาะผู้ปฏิบัติงานสามารถเข้าถึงได้และเป็นข้อมูลที่องค์กรไม่ได้เผยแพร่โดยอิสระ ทั้งข้อมูลบุคคลหรือองค์กรและหากเกิดการสูญเสียข้อมูลหรือการเปิดเผยข้อมูลอาจไม่ส่งผลให้เกิดผลกระทบที่สำคัญ แต่ก็ไม่พึงประสงค์ที่ให้เปิดเผยโดยไม่ได้รับอนุญาต เช่น ข้อมูลระเบียน ข้อมูลผู้ปฏิบัติงาน เอกสารประกอบการปฏิบัติงาน และวิธีปฏิบัติภายในหน่วยงาน ฯลฯ

(๓) ลับ (Confidential) หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

(๔) ลับมาก (Secret) หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

(๕) ลับที่สุด (Top Secret) ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการจัดหมวดหมู่และชั้นความลับของข้อมูล (Data Classification) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๑ ว่าด้วยเรื่องการระบุความเสี่ยง (Identify)

๑๑. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

สถาบันมีการกำหนดมาตรการเกี่ยวกับการเข้าถึงทางกายภาพและสภาพแวดล้อมของสถาบันสำหรับพื้นที่ทั่วไปของสถาบัน พื้นที่มั่นคงปลอดภัย รวมถึงพื้นที่ศูนย์ข้อมูลที่สถาบันใช้บริการ โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

/๑๒.การบริหาร...

๑๒. การบริหารจัดการการให้บริการโดยหน่วยงานภายนอก

สถาบันมีการบริหารจัดการการใช้บริการหน่วยงานภายนอก โดยสถาบันมีการกำหนดมาตรฐาน เพื่อใช้บริหารจัดการและตรวจสอบการดำเนินงานของหน่วยงานภายนอกอย่างสม่ำเสมอ เพื่อรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องของสถาบันกับหน่วยงานภายนอก โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการรักษาความมั่นคงปลอดภัย สำหรับผู้ให้บริการภายนอก (Third Party Security) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๑๓. การจัดการความสอดคล้องและการปฏิบัติตามข้อกำหนด

สถาบันมีการปฏิบัติตามข้อกฎหมาย ระเบียบ ข้อบังคับ ข้อผูกพันตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ มาตรฐาน และข้อกำหนดด้านความมั่นคงปลอดภัยที่สถาบันกำหนด เพื่อให้การบริหารจัดการความสอดคล้อง (Compliance) เป็นไปอย่างมีประสิทธิภาพ โดยมีการสื่อสารกับผู้ปฏิบัติงานให้รับทราบและเข้าใจ รวมทั้งมีการทบทวนและตรวจสอบการปฏิบัติตามนโยบายที่สถาบันกำหนด โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๑๔. การบริหารความต่อเนื่องในการดำเนินงานของสถาบัน

สถาบันมีการบริหารความต่อเนื่องด้านความมั่นคงปลอดภัยระบบสารสนเทศและการดำเนินกิจการของสถาบัน โดยคณะทำงานย่อยบริหารความต่อเนื่องในการทำงาน (Business Continuity Plan : BCP) มีหน้าที่ในการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) จัดลำดับความสำคัญของข้อมูลและระบบสารสนเทศที่จำเป็นต้องมีความต่อเนื่องในการใช้งาน กำหนดกระบวนการ กิจกรรมและทรัพยากรที่จำเป็น จัดทำเอกสารที่เกี่ยวข้อง สื่อสารให้ผู้ที่เกี่ยวข้องทราบและตระหนักถึงหน้าที่ของตน ตลอดจนจัดให้มีการซ้อมแผนบริหารความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง โดยการปฏิบัตินั้นให้เป็นไปตามแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) สำหรับการบริหารความพร้อมต่อสภาวะวิกฤตของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๔ ว่าด้วยเรื่อง การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๑๕. การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

สถาบันมีการควบคุมการเข้าถึงระบบสารสนเทศแก่ผู้ใช้งาน ตั้งแต่การลงทะเบียน การกำหนดสิทธิ การเพิกถอนสิทธิ การทบทวนสิทธิการใช้งาน รวมถึงการให้ความคุ้มครองข้อมูลส่วนบุคคลในส่วนที่ไม่พึงเปิดเผยภายใต้บทบัญญัติของกฎหมาย โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการควบคุมการเข้าถึงข้อมูล (Access Control Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๑๖. การจัดการการเข้ารหัสลับ

สถาบันมีการเข้ารหัสลับข้อมูลที่มีระดับชั้นความลับ โดยแบ่งตามการจัดการสื่อที่ใช้ในการบันทึกข้อมูล ประกอบด้วย ข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ส่วนบุคคลของสถาบัน ข้อมูลที่ถูกจัดเก็บอยู่ในเซิร์ฟเวอร์ หรืออยู่ในคลาวด์ของสถาบัน ข้อมูลที่ถูกส่งผ่านเครือข่าย โดยการปฏิบัตินั้นให้เป็นไปตามแนว

/ทางการจัด...

ทางการจัดหมวดหมู่และชั้นความลับของข้อมูล (Data Classification) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๑๗. การบริหารจัดการการเปลี่ยนแปลง

สถาบันมีการบริหารจัดการการเปลี่ยนแปลงขององค์กร (Change Management) ที่มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าการเปลี่ยนแปลงได้รับการวางแผน การจัดลำดับความสำคัญ ประเมินผลกระทบ การอนุมัติจากผู้มีอำนาจ การมอบหมาย ทดสอบ บันทึก และดำเนินการอย่างเหมาะสม เพื่อลดโอกาสหรือผลกระทบของความเสียหายอันเกิดจากการเปลี่ยนแปลงนั้น และรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๑๘. การบริหารจัดการขีดความสามารถสารสนเทศ

สถาบันมีการบริหารจัดการขีดความสามารถสารสนเทศ (Capacity Management) เพื่อตรวจสอบการใช้งานให้มีทรัพยากรเพียงพอต่อความต้องการใช้งานของสถาบัน และระบบสารสนเทศของสถาบันสามารถให้บริการได้อย่างต่อเนื่อง โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๑๙. การควบคุมการติดตั้งซอฟต์แวร์ และการบริหารจัดการช่องโหว่ทางเทคนิค

สถาบันมีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ครอบคลุมในการจัดทำขั้นตอนปฏิบัติงาน การป้องกันมัลแวร์ การควบคุมการใช้งานซอฟต์แวร์ การบริหารจัดการช่องโหว่ และการตรวจสอบระบบสารสนเทศ โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการใช้งานสารสนเทศขององค์กร (Acceptable Use) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๓ ว่าด้วยเรื่องการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๒๐. การสำรองข้อมูลและการกู้คืนระบบสารสนเทศ

สถาบันมีการบริหารจัดการการสำรองข้อมูลสำหรับระบบสารสนเทศ เพื่อป้องกันข้อมูลจากการสูญหาย ถูกทำลาย จากเหตุการณ์ไม่พึงประสงค์หรือเหตุการณ์ที่ไม่คาดคิด พร้อมทั้งจัดทำแผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อให้ระบบสารสนเทศของสถาบันสามารถให้บริการได้อย่างต่อเนื่อง โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๕ ว่าด้วย เรื่องการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๒๑. การบันทึกข้อมูลจราจรทางคอมพิวเตอร์ และเฝ้าระวัง

สถาบันมีการบันทึกเหตุการณ์ที่เกิดขึ้นในระบบสารสนเทศ เช่น กิจกรรมของผู้ดูแลระบบและผู้ใช้งาน ความผิดปกติหรือข้อผิดพลาดของระบบสารสนเทศ การใช้งานต่าง ๆ เป็นต้น โดยได้เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ทั้งนี้ เหตุการณ์ที่

/บันทึกต้อง...

บันทึกต้องได้รับการปกป้องจากการเปลี่ยนแปลงเพื่อทำลายและการเข้าถึงโดยไม่ได้รับอนุญาต โดยต้องมีการตรวจสอบและวิเคราะห์เหตุการณ์ที่บันทึกอย่างสม่ำเสมอ เพื่อป้องกันเหตุการณ์ไม่พึงประสงค์หรือภัยคุกคามที่อาจส่งผลกระทบต่อสถาบัน โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๓ ว่าด้วยเรื่องการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๒๒. การบริหารจัดการการสื่อสารและการใช้งานระบบเครือข่าย

สถาบันมีการควบคุมการสื่อสาร และการส่งข้อมูลผ่านระบบเครือข่ายของสถาบัน เพื่อป้องกันการเข้าถึงระบบสารสนเทศของสถาบันจากผู้ที่ไม่ได้รับอนุญาต ป้องกันภัยคุกคามที่อาจก่อให้เกิดผลกระทบต่อสถาบัน รวมถึงควบคุมการเข้าถึงการใช้งานระบบเครือข่ายเพื่อปฏิบัติงานจากภายนอกสถาบันให้มีความมั่นคงปลอดภัย โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการใช้งานสารสนเทศขององค์กร (Acceptable Use) ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๒๓. การจัดหา พัฒนา และการบำรุงรักษาระบบสารสนเทศ

สถาบันมีกระบวนการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ โดยมีการศึกษาความเป็นไปได้ การวิเคราะห์ผลกระทบ และการตรวจสอบระบบสารสนเทศให้มั่นใจว่าเป็นไปตามแนวทางการปฏิบัติขององค์กรก่อนการโอนย้ายขึ้นสู่สภาพแวดล้อมการใช้งานจริง เพื่อป้องกันผลกระทบต่อการปฏิบัติงานหรือต่อภารกิจของสถาบัน โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

๒๔. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

สถาบันมีการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีการกำหนดหน้าที่ของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการเฝ้าระวัง การรายงานเหตุการณ์ การวิเคราะห์ การเก็บรวบรวมหลักฐานการแก้ปัญหา และการบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น เพื่อให้เกิดการตอบสนองอย่างรวดเร็ว มีประสิทธิภาพและประสิทธิผล เป็นระเบียบแบบแผน และนำความรู้ที่ได้รับจากการวิเคราะห์และแก้ปัญหาไปใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ในอนาคต โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Security Incident Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๔ ว่าด้วยเรื่อง การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๒๕. การประเมินผลการปฏิบัติงาน

สถาบันมีการประเมินผลการปฏิบัติงาน เพื่อทบทวนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของสถาบัน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าการดำเนินงานมีความเหมาะสม และมีประสิทธิผล ทั้งนี้ การทบทวนดังกล่าวต้องพิจารณาถึงโอกาสในการปรับปรุงและพัฒนาอย่างต่อเนื่องเพื่อบรรลุวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน โดยการปฏิบัตินั้นให้เป็นไปตามแนวทางการบริหารจัดการการสื่อสารและการดำเนินงานด้านสารสนเทศขององค์กร (Communications and Operations Management) ของสถาบัน ซึ่งได้สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จาก สกมช. หัวข้อที่ ๒ ว่าด้วยเรื่องการป้องกันความเสี่ยง (Protect)

/๒๖. การเปลี่ยนแปลง...

๒๖. การเปลี่ยนแปลงนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ

สถาบันอาจปรับปรุงนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศนี้ เป็นครั้งคราว เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของการให้บริการ การดำเนินงานของสถาบัน และข้อเสนอแนะความคิดเห็นจากท่าน โดยสถาบันจะประกาศการเปลี่ยนแปลงให้ทราบอย่างชัดเจนบนเว็บไซต์ของสถาบัน

หากท่านมีข้อสงสัยเพิ่มเติม โปรดติดต่อได้ที่ :
สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) ฝ่ายบริหารกลาง
โทร. ๐ ๒๔๘๐ ๘๘๓๓ ต่อ ๙๖๘๒ ไปรษณีย์อิเล็กทรอนิกส์ montree.ch@bdi.or.th