รายละเอียดเอกสาร

ชื่อเอกสาร (ไทย)	นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของศูนย์ข้อมูลสารสนเทศ
ชื่อเอกสาร (English)	Information Security Management System Policy
วันที่มีผลบังคับใช้	4 เมษายน 2568
รอบการทบทวนเอกสาร	ทบทวนปีละ 1 ครั้ง

การอนุมัติเอกสาร

ผู้จัดทำเอกสาร	**ลงชื่อ** 	**ชื่อ** **ตำแหน่ง** **วันที่**	นายทวีศักดิ์ นาเมืองรักษ์ นักวิชาการคอมพิวเตอร์ 4 เมษายน 2568
ผู้ตรวจทานเอกสาร	**ลงชื่อ** 	**ชื่อ** **ตำแหน่ง** **วันที่**	นายพฤทธิ์ แกะกระโทก ผู้อำนวยการกลุ่มบริหารจัดการเทคโนโลยีสารสนเทศและเครือข่าย 4 เมษายน 2568
ผู้อนุมัติเอกสาร	**ลงชื่อ** 	**ชื่อ** **ตำแหน่ง** **วันที่**	นางสาวจันทนา วงศ์เยาว์ฟ้า ผู้อำนวยการกองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม 4 เมษายน 2568

ประวัติปรับปรุงเอกสาร

เวอร์ชั่น	ผู้จัดทำเอกสาร	วันที่มีผลบังคับใช้	รายละเอียดการแก้ไข
1	นายพฤทธิ์ แกะกระโทก	4 ตุลาคม 2561	**เอกสารอนุมัติใช้ครั้งแรก**
2	นายพฤทธิ์ แกะกระโทก	6 มีนาคม 2563	- ปรับปรุงชื่อหน่วยงาน - ปรับปรุงสัญลักษณ์หน่วยงาน - ปรับปรุงชื่อศูนย์ข้อมูลระบบสารสนเทศ (MHESI Data Center) แก้ไขคำประกาศนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
3	นายทวีศักดิ์ นาเมืองรักษ์	29 มกราคม 2564	- ปรับปรุงสัญลักษณ์หน่วยงาน - แก้ไขคำจำกัดความ หน้าที่ 6 ข้อที่ 3 ลำดับที่ 1 เพิ่มเติม (ด้าน ววน.)
4	นายทวีศักดิ์ นาเมืองรักษ์	1 ธันวาคม 2564	- ปรับปรุงชื่อหน่วยงาน - ปรับปรุงสัญลักษณ์หน่วยงาน - ปรับปรุงรหัสเอกสาร อ้างอิงชื่อย่อ ภาษา English ของหน่วยงานตามโครงสร้างใหม่ - ปรับปรุงคำจำกัดความ ลำดับที่ 1 – 3 (หน้าที่ 6 ข้อที่ 3) - แก้ไขคำประกาศนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (หน้าที่ 7 ข้อที่ 4) จากเดิม ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม เป็น “กองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม”
5	นายทวีศักดิ์ นาเมืองรักษ์	9 มกราคม 2566	- ตัดข้อความ (อาคารพระจอมเกล้า) ในขอบเขต (หน้าที่ 6 ข้อที่ 2) - ปรับปรุงคำจำกัดความ ลำดับที่ 2 – 3 (หน้าที่ 6 ข้อที่ 3) - ตัด OBJ03: กิจกรรมด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปตามกฎ ระเบียบ นโยบายและกฎหมาย (หน้าที่ 8)

เวอร์ชั่น	ผู้จัดทำเอกสาร	วันที่มีผลบังคับใช้	รายละเอียดการแก้ไข
6	นายทวีศักดิ์ นาเมืองรักษ์	14 กุมภาพันธ์ 2566	- เพิ่ม OBJ06 -กิจกรรมด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปตามกฎ ระเบียบ นโยบาย และกฎหมาย (หน้าที่ 6 ข้อที่ 4) - แก้ไขข้อความ หน้าที่ 8 ข้อที่ 4 จาก “คณะกรรมการ/คณะทำงาน” เป็น “ทีมบริหารจัดการ/ทีมทำงาน”
7	นายทวีศักดิ์ นาเมืองรักษ์	4 เมษายน 2568	- แก้ไขข้อความ**จากเดิม**“มาตรฐาน ISO/IEC27001:2013” **เป็น** “มาตรฐาน ISO/IEC27001:2022” (หน้าที่ 6 ข้อที่ 1-2 และหน้าที่ 7 ข้อที่ 4) - แก้ไขข้อความคำจำกัด**ความ จากเดิม** “อุปกรณ์โครงสร้างพื้นฐาน **เป็น** โครงสร้างพื้นฐาน” และคำจำกัดความ **จากเดิม** “เครื่องปรับอากาศแบบควบคุมความชื้น เครื่องสำรองไฟฟ้า (UPS) และชุดแบตเตอรี่สำรองไฟฟ้า ระบบตรวจจับการรั่วซึมของน้ำ ระบบเฝ้าดู และระบบแจ้งเตือนอัตโนมัติ ระบบดับเพลิงอัตโนมัติ ระบบตรวจจับควันความไวสูง อุปกรณ์เครือข่าย” **เป็น** “อุปกรณ์ที่อยู่ภายในศูนย์ข้อมูลสารสนเทศ เช่น เครื่องปรับอากาศแบบควบคุมความชื้น เครื่องสำรองไฟฟ้า (UPS) และชุดแบตเตอรี่สำรองไฟฟ้า ระบบตรวจจับการรั่วซึมของน้ำ ระบบเฝ้าดู และระบบแจ้งเตือนอัตโนมัติ ระบบดับเพลิงอัตโนมัติ ระบบตรวจจับควันความไวสูง อุปกรณ์เครือข่าย เป็นต้น” (หน้าที่ 7 ลำดับที่ 5) - ปรับปรุงวัตถุประสงค์ของการดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัย (หน้าที่ 8) **จากเดิม** ดังนี้ **OBJ01 -** บุคลากรของ สป.อว. มีความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ และสามารถปฏิบัติ ตามกฎ ระเบียบ นโยบาย และขั้นตอนปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ **OBJ02 -** นโยบาย และแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัย สารสนเทศมีการทบทวนตามความถี่ที่กำหนดไว้

เวอร์ชั่น	ผู้จัดทำเอกสาร	วันที่มีผลบังคับใช้	รายละเอียดการแก้ไข
			OBJ03 – ระบบบริการเครื่องแม่ข่ายแบบเสมือนมีความมั่นคงปลอดภัยและพร้อมใช้ตามที่กำหนด **OBJ04 -** โครงสร้างพื้นฐานของศูนย์ข้อมูลสารสนเทศมีความมั่นคงปลอดภัย และพร้อมใช้ตามที่กำหนด **OBJ05 -** ระบบเครือข่ายมีความมั่นคงปลอดภัยและพร้อมใช้ตามที่กำหนด **OBJ06 -** กิจกรรมด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปตามกฎระเบียบ นโยบายและกฎหมาย **เป็น** **OBJ01 -** เพื่อบริหารจัดการโครงสร้างพื้นฐานของศูนย์ข้อมูลสารสนเทศ ระบบเครือข่ายและระบบบริการเครื่องแม่ข่ายให้มีความมั่นคงปลอดภัย และพร้อมใช้ และเป็นไปตามกฎระเบียบ/นโยบาย/กฎหมายที่เกี่ยวข้อง **OBJ02 -** เพื่อส่งเสริมให้บุคลากร สป.อว. มีความรู้ และความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ - แก้ไขข้อความ**จากเดิม**“ทรัพย์สินสารสนเทศจะต้องถูกเข้าถึงจากผู้มีสิทธิ์เท่านั้นถูกป้องกันจากผู้ไม่มีสิทธิ์ในการเข้าถึง (Unauthorized access)” **เป็น** “ทรัพย์สินสารสนเทศ จะต้องถูกเข้าถึงจากผู้มีสิทธิ์เท่านั้น (Authorized Access)” (หน้าที่ 9 ข้อ 2) - แก้ไขข้อความชื่อเอกสารภาษาอังกฤษ**จากเดิม** “ISMS for information security of Information Technology Center” **เป็น** “Information Security Management System Policy” (หน้าที่ 1) - แก้ไขข้อความ**จากเดิม** “ต้องมีการแต่งตั้งทีมบริหารจัดการ/ทีมทำงาน” **เป็น** “ต้องมีการแต่งตั้งทีมบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและทีมงานด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ” (หน้าที่ 9 ข้อ 4)

สารบัญ

1. วัตถุประสงค์

เอกสารนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของศูนย์ข้อมูลสารสนเทศ เป็นเอกสารแสดงความมุ่งมั่นและความคาดหวังในการดำเนินการ ISMS ของผู้บริหาร รวมถึงการชี้แจงวัตถุประสงค์ของระบบ ISMS ให้เป็นไปตามมาตรฐาน ISO/IEC 27001:2022

2. ขอบเขต

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ของศูนย์ข้อมูลสารสนเทศ สำนักงานปลัดกระทรวงการอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม ครอบคลุมขอบเขต และหลักเกณฑ์การดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อขอการรับรองตามมาตรฐาน ISO/IEC 27001:2022 ของหน่วยงาน

3. คำจำกัดความ

ลำดับที่	คำศัพท์	คำจำกัดความ
1	กรข.สป.อว.	กองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
2	ศูนย์ข้อมูลสารสนเทศ	ศูนย์ข้อมูลสารสนเทศ (อาคารพระจอมเกล้า และอาคารอุดมศึกษา 2)
3	Data Center	Data Center (Phrachomklao Building and Udom Building 2)
4	ทรัพย์สินสารสนเทศ	ครอบคลุมถึง 1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 2) อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

5	โครงสร้างพื้นฐาน	อุปกรณ์ที่อยู่ภายในศูนย์ข้อมูลสารสนเทศ เช่น เครื่องปรับอากาศแบบควบคุมความชื้น เครื่องสำรองไฟฟ้า (UPS) และชุดแบตเตอรี่สำรองไฟฟ้า ระบบตรวจจับการรั่วซึมของน้ำ ระบบเฝ้าดู และระบบแจ้งเตือนอัตโนมัติ ระบบดับเพลิงอัตโนมัติ ระบบตรวจจับควันความไวสูง อุปกรณ์เครือข่าย เป็นต้น
6	บุคลากร	ผู้ใช้งานที่เกี่ยวข้อง และผู้ดูแลระบบของ สป.อว.

4. นโยบายและวัตถุประสงค์ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System policy and objectives)

เป้าหมายของนโยบายเพื่อป้องกันทรัพย์สินสารสนเทศ (Information Assets) ที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศและการสื่อสารของศูนย์ข้อมูลสารสนเทศ จากภัยคุกคามภายในและภายนอกที่อาจเกิดขึ้นทั้งที่โดยเจตนาหรือไม่เจตนาก็ตาม และเพื่อแสดงถึงข้อผูกพันด้านคุณภาพและความมุ่งมั่นของหน่วยงาน ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จึงได้ประกาศนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้

“กองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม มุ่งมั่นในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารของศูนย์ข้อมูลสารสนเทศ จะเป็นไปอย่างต่อเนื่อง มีเสถียรภาพ มั่นคงปลอดภัย และมีความสอดคล้องตามมาตรฐาน ISO/IEC 27001:2022 ตลอดจนดำเนินการพัฒนาอย่างต่อเนื่อง”

วัตถุประสงค์ของการดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีดังนี้

OBJ01 - เพื่อบริหารจัดการโครงสร้างพื้นฐานของศูนย์ข้อมูลสารสนเทศ ระบบเครือข่าย และระบบบริการเครื่องแม่ข่ายให้มีความมั่นคงปลอดภัย และพร้อมใช้ และเป็นไปตามกฎระเบียบ/นโยบาย/กฎหมายที่เกี่ยวข้อง

OBJ02 - เพื่อส่งเสริมให้บุคลากร สป.อว. มีความรู้ และความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ

เพื่อให้บรรลุตามนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังกล่าว กรข.สป.อว. จะดำเนินการดังนี้

1. กำหนดนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และให้การสนับสนุนในเรื่องนโยบาย งบประมาณ ทรัพยากรและอื่นๆ ที่จำเป็นเพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีการพัฒนาและปรับปรุงอย่างต่อเนื่อง
2. นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องสร้างความมั่นใจดังนี้
    - ทรัพย์สินสารสนเทศ จะต้องถูกรักษาสถานภาพด้านความลับ (Confidentiality)
    - ทรัพย์สินสารสนเทศ จะต้องถูกรักษาสถานภาพด้านความถูกต้องสมบูรณ์ (Integrity)
    - การเข้าถึงทรัพย์สินสารสนเทศ จะต้องมีความพร้อมใช้งาน (Availability)
    - ทรัพย์สินสารสนเทศ จะต้องถูกเข้าถึงจากผู้มีสิทธิ์เท่านั้น (authorized access)
    - นโยบาย ขั้นตอน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารต่างๆ จะต้องถูกกำหนดเพื่อสนับสนุนนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
    - มีการปฏิบัติตามคำสั่ง ระเบียบ ข้อบังคับ กฎหมาย และข้อตกลงที่มีผลต่อความมั่นคงปลอดภัยสารสนเทศ
    - บุคลากรซึ่งเป็นผู้ใช้และผู้ดูแลระบบของ สป.อว. จะต้องได้รับการฝึกอบรมด้านความตระหนักและความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ
    - ทุกเหตุการณ์ที่เกิดขึ้นที่มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศจะต้องถูกบันทึก ตรวจสอบ จัดการ และรายงาน
    - แผนบริหารจัดการความต่อเนื่องของธุรกิจจะต้องถูกพัฒนา ปรับปรุง และทดสอบ

- ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จะต้องมีการตรวจสอบ การประเมิน และมีกระบวนการปรับปรุงอย่างต่อเนื่องให้เหมาะสมกับสถานการณ์ที่เปลี่ยนไป

3. การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ตามขั้นตอนปฏิบัติการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Management Procedure) ที่ได้รับการอนุมัติ
4. ต้องมีการแต่งตั้งทีมบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและทีมงานด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อรับผิดชอบในการขับเคลื่อนและธำรงไว้ ซึ่งระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
5. นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จะต้องถูกนำไปปฏิบัติอย่างเคร่งครัด