สำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี

รายละเอียดเอกสาร

ชื่อเอกสาร	นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ สป.วท. (OPS Information Security Management System Policy)
วันที่มีผลบังคับใช้	4 ตุลาคม 2561
รอบการทบทวนเอกสาร	รอบปีละ 1 ครั้ง

การอนุมัติเอกสาร

ผู้จัดทำ	ลงชื่อ 	**ชื่อ** นาย พฤทธิ์ แกะกระโทก **ตำแหน่ง** ผู้อำนวยการส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศ **วันที่** 2 ตุลาคม 2561
ผู้ตรวจทาน	ลงชื่อ 	**ชื่อ** นางสาว จันทนา วงศ์เยาว์ฟ้า **ตำแหน่ง** ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร **วันที่** 3 ตุลาคม 2561
ผู้อนุมัติ	ลงชื่อ 	**ชื่อ** นาย ปฐม สวรรค์ปัญญาเลิศ **ตำแหน่ง** รองปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี **วันที่** 4 ตุลาคม 2561

ประวัติการปรับปรุงเอกสาร

เวอร์ชั่น	ผู้ดำเนินการ	วันที่มีผลบังคับใช้	รายละเอียด
1	นาย พฤทธิ์ แกะกระโทก	4 ตุลาคม 2561	เอกสารอนุมัติใช้ครั้งแรก

สารบัญ

1. วัตถุประสงค์

เอกสารนโยบายระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ของสำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี เป็นเอกสารแสดงความมุ่งมั่นและความคาดหวังในการดำเนินการ ISMS ของผู้บริหาร รวมถึงชี้แจงวัตถุประสงค์ของระบบ ISMS

2. ขอบเขต

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC 27001:2013 ครอบคลุมขอบเขต และหลักเกณฑ์การดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อขอการรับรองตามมาตรฐาน ISO/IEC 27001:2013 ของสำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี

3. คำจำกัดความ

ลำดับที่	คำศัพท์	คำจำกัดความ
1	สป.วท.	สำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี (Office of the Permanent Secretary: OPS)
2	อุปกรณ์โครงสร้างพื้นฐาน	เครื่องปรับอากาศแบบควบคุมความชื้น เครื่องสำรองไฟฟ้า (UPS) และชุดแบตเตอรี่สำรองไฟฟ้า ระบบตรวจจับการรั่วซึมของน้ำ ระบบเฝ้าดู และระบบแจ้งเตือนอัตโนมัติ ระบบดับเพลิงอัตโนมัติ ระบบตรวจจับควันความไวสูง อุปกรณ์เครือข่าย
3	ทรัพย์สินสารสนเทศ	ครอบคลุมถึง 1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 2) อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
4	MOST Data Center	ศูนย์ข้อมูลระบบสารสนเทศ (Data Center) ของ สป.วท.

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

เป้าหมายของนโยบายเพื่อป้องกันทรัพย์สินสารสนเทศ (Information Assets) ที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศและการสื่อสารของศูนย์ข้อมูลระบบสารสนเทศ (MOST Data Center) สป.วท. จากภัยคุกคามภายในและภายนอกที่อาจเกิดขึ้นทั้งที่โดยเจตนาหรือไม่เจตนาก็ตาม

เพื่อแสดงถึงข้อผูกพันด้านคุณภาพและความมุ่งมั่นของ สป.วท. ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จึงได้ประกาศนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังนี้

“สำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี มุ่งมั่นในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารของศูนย์ข้อมูลระบบสารสนเทศ (MOST Data Center) จะเป็นไปอย่างต่อเนื่อง มีเสถียรภาพ มั่นคงปลอดภัย และมีความสอดคล้องตามมาตรฐาน ISO/IEC 27001:2013 ตลอดจนดำเนินการพัฒนาอย่างต่อเนื่อง”

วัตถุประสงค์ของการดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีดังนี้

OBJ01 – บุคลากรของ สป.วท. มีความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและสามารถปฏิบัติ ตามกฎ ระเบียบ นโยบาย และขั้นตอนปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

OBJ02 - นโยบาย และแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศมีการทบทวนตามความถี่ที่กำหนดไว้

OBJ03 - กิจกรรมด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปตามกฎ ระเบียบ นโยบาย และกฎหมาย

OBJ04 - ระบบบริการเครื่องแม่ข่ายแบบเสมือน มีความพร้อมใช้ตามข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)

OBJ05 – อุปกรณ์โครงสร้างพื้นฐาน ระบบคอมพิวเตอร์เครื่องแม่ข่ายของศูนย์ข้อมูลระบบสารสนเทศ (MOST Data Center) ห้องปฏิบัติการเครือข่ายสื่อสาร (Network Operation Center : NOC) มีการบำรุงรักษา และมีความพร้อมใช้ตามข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)

เพื่อให้บรรลุตามนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดังกล่าว สป.วท. จะดำเนินการดังนี้

1. กำหนดนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และให้การสนับสนุนในเรื่องนโยบาย งบประมาณ ทรัพยากรและอื่น ๆ ที่จำเป็นเพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีการพัฒนาและปรับปรุงอย่างต่อเนื่อง
2. นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องสร้างความมั่นใจดังนี้
    - ทรัพย์สินสารสนเทศ จะต้องถูกรักษาสถานภาพด้านความลับ (Confidentiality)
    - ทรัพย์สินสารสนเทศ จะต้องถูกรักษาสถานภาพด้านความถูกต้องสมบูรณ์ (Integrity)
    - การเข้าถึงทรัพย์สินสารสนเทศ จะต้องมีความพร้อมใช้งาน (Availability)
    - ทรัพย์สินสารสนเทศ จะต้องถูกป้องกันจากผู้ไม่มีสิทธิในการเข้าถึง (Unauthorized access)
    - นโยบาย ขั้นตอน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารต่าง ๆ จะต้องถูกกำหนดเพื่อสนับสนุนนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
    - มีการปฏิบัติตามคำสั่ง ระเบียบ ข้อบังคับ กฎหมาย และข้อตกลงที่มีผลต่อความมั่นคงปลอดภัยสารสนเทศ
    - บุคลากรซึ่งเป็นผู้ใช้และผู้ดูแลระบบของ สป.วท. จะต้องได้รับการฝึกอบรมด้านความตระหนักและความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ
    - ทุก ๆ เหตุการณ์ที่เกิดขึ้นที่มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศจะต้องถูกบันทึก ตรวจสอบ จัดการและรายงาน
    - แผนบริหารจัดการความต่อเนื่องของธุรกิจจะต้องถูกพัฒนา ปรับปรุง และทดสอบ
    - ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จะต้องมีการตรวจสอบ การประเมิน และมีกระบวนการปรับปรุงอย่างต่อเนื่องให้เหมาะสมกับสถานการณ์ที่เปลี่ยนไป
3. การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ตามขั้นตอนปฏิบัติการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Management Procedure) (PCD-ICT-001) ที่ได้รับการอนุมัติ
4. ต้องมีการแต่งตั้งคณะกรรมการ/คณะทำงาน เพื่อรับผิดชอบในการขับเคลื่อนและธำรงไว้ซึ่งระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
5. นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จะต้องถูกนำไปปฏิบัติอย่างเคร่งครัด