แบบสำรวจระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

คำชี้แจงการประเมิน

1. หลักการและเหตุผล

1.1 แบบสำรวจระดับความพร้อมนี้จัดทำขึ้นเพื่อสำรวจระดับการรับรู้ การเตรียมความพร้อม และความก้าวหน้าในการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ให้สอดคล้องกับมาตรฐาน นโยบาย แผน และแนวปฏิบัติที่เกี่ยวข้อง ซึ่งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีการประกาศทั้งที่มีผลบังคับใช้แล้ว อยู่ระหว่างการขับเคลื่อน หรือคาดว่าจะมีผลใช้บังคับในระยะต่อไป รวมถึงการเตรียมความพร้อมเพื่อรองรับเทคโนโลยีอุบัติใหม่และความเสี่ยงทางไซเบอร์ในอนาคต โดยมุ่งเน้นการประเมินตนเอง เพื่อสะท้อนสถานะการดำเนินงานที่แท้จริงของหน่วยงาน และใช้เป็นข้อมูลพื้นฐานสำหรับการพัฒนาอย่างต่อเนื่อง ทั้งนี้ เพื่อให้สอดคล้องกับนโยบายรัฐบาลด้านการพัฒนารัฐบาลดิจิทัล (Government Digital Transformation) ซึ่งมุ่งเน้นการยกระดับการบริหารจัดการภาครัฐด้วยเทคโนโลยีดิจิทัล

1.2 ในคราวการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ครั้งที่ 1/2569 เมื่อวันที่ 25 พฤษภาคม 2569 ที่ประชุมมีมติเห็นชอบนโยบาย AI เพื่อการปกป้องและการปกป้อง AI (AI for Security and Security for AI) การเตรียมความพร้อมระบบสารสนเทศเพื่อเข้าสู่ยุคควอนตัมภายในปี 2573 (Quantum-Ready 2030) รวมถึงหลักการ (ร่าง) แผนบูรณาการเพื่อขับเคลื่อนการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2569 – 2573 โดยมอบหมายให้ สกมช. เป็นหน่วยงานหลักในการขับเคลื่อน

1.3 ผลการสำรวจระดับความพร้อมนี้ สกมช. จะนำไปใช้ในการวิเคราะห์สถานะความพร้อมด้านไซเบอร์ของประเทศในภาพรวม การประเมินระดับความเสี่ยง การจัดกลุ่มหน่วยงานตามระดับความพร้อมและความจำเป็นในการสนับสนุน ตลอดจนการวางแผน กำหนดมาตรการ ส่งเสริมองค์ความรู้ จัดทำแนวทางสนับสนุนเชิงเทคนิค และวางแผนการตรวจติดตามหรือการกำกับดูแลในระยะต่อไป เพื่อยกระดับการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานให้สอดคล้องกับมาตรฐาน เทคโนโลยีที่เปลี่ยนแปลง และภัยคุกคามทางไซเบอร์ในอนาคต ทั้งนี้ แบบสำรวจดังกล่าวมิได้มีวัตถุประสงค์เพียงเพื่อประเมินความพร้อมของหน่วยงานเท่านั้น แต่เพื่อรวบรวมข้อมูลตามข้อเท็จจริงเกี่ยวกับสถานะการดำเนินงาน ปัญหา อุปสรรค ช่องว่าง และความต้องการสนับสนุนของหน่วยงาน เพื่อใช้เป็นข้อมูลประกอบการรายงานเสนอต่อคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) และเป็นข้อมูลพื้นฐานในการกำหนดทิศทางนโยบาย มาตรการ และแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมถึงการกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบบริการให้มีความมั่นคงปลอดภัยไซเบอร์ ตามหน้าที่และอำนาจของคณะกรรมการตามมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2. แนวทางการตอบแบบสำรวจระดับความพร้อม

2.1 ขอความร่วมมือให้หน่วยงานพิจารณาประเมินแต่ละหัวข้อโดยอ้างอิงจากแผนงาน หรือผลการดำเนินงาน โดยให้สะท้อนสถานะการดำเนินงานที่เป็นจริงของหน่วยงาน ทั้งนี้ ในขั้นตอนนี้หน่วยงานไม่จำเป็นต้องจัดส่งเอกสารหลักฐานมายัง สกมช.

2.2 แบบสำรวจนี้ออกแบบให้ตอบได้โดยสะดวก และหลีกเลี่ยงการขอข้อมูลเชิงเทคนิคหรือข้อมูลที่มีความอ่อนไหว

3. รูปแบบการตอบ โปรดทำเครื่องหมายลงในช่องที่ตรงกับสถานะของหน่วยงาน โดยมีความหมาย ดังนี้

- **มี** หมายถึง หน่วยงานมีการดำเนินการครบถ้วน
- **มีบางส่วน** หมายถึง หน่วยงานเริ่มดำเนินการแล้ว แต่ยังไม่ครบถ้วน
- **ไม่มี** หมายถึง หน่วยงานยังไม่ได้ดำเนินการ
- **ไม่เกี่ยวข้อง** หมายถึง หน่วยงานไม่มีบริการ ระบบ หรือบริบทที่เกี่ยวข้องในหัวข้อนั้น

ช่อง **ปัญหาและอุปสรรค** (ถ้ามี) เพื่อให้หน่วยงานระบุรายละเอียดเพิ่มเติม หรือในกรณีที่ต้องการรับการสนับสนุนจาก สกมช.

คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice)

สกมช. ดำเนินการจัดเก็บ รวบรวม เก็บรักษา ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อใช้ในกิจกรรมของ สกมช. และให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดย สกมช. จะเก็บรักษาข้อมูลดังกล่าวเป็นความลับ และใช้ในวัตถุประสงค์ ดังนี้

1. ข้อมูลของท่าน ได้แก่ ชื่อ สกุล ตำแหน่ง หน่วยงาน โทรศัพท์ และอีเมล เพื่อใช้สื่อสารและประชาสัมพันธ์กิจกรรมของ สกมช. โดยจัดเก็บในรูปแบบข้อมูลอิเล็กทรอนิกส์
2. ดำเนินการเก็บรวบรวม เพื่อการประมวลผลทางสถิติ
3. ดำเนินการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตลอดระยะเวลาการคงอยู่ของ สกมช.
4. สิทธิของเจ้าของข้อมูล ท่านมีสิทธิในการขอแก้ไข ลบ หรือทำลาย เข้าถึงข้อมูลส่วนบุคคล โอนข้อมุลส่วนบุคคล คัดค้านการเก็บรวบรวม ใช้ เปิดเผย หรือระงับการใช้ข้อมูลส่วนบุคคลของท่าน โดยแจ้งมายัง สกมช. ท่านสามารถเลือกว่าจะยินยอมให้ข้อมูลส่วนบุคคลหรือไม่ก็ได้ แต่อย่างไรก็ตาม โปรดทราบว่า หากท่านไม่ให้ข้อมูลส่วนบุคคลแก่ สกมช. อาจมีบางกิจกรรมที่ไม่สามารถติดต่อหรือแจ้งข่าวสารให้แก่ท่านได้ หากปราศจากข้อมูลส่วนบุคคลของท่าน ในกรณีที่ สบพ. มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อดำเนินการอื่นนอกเหนือจากวัตถุประสงค์ข้างต้นตามที่ได้ระบุไว้ สกมช. จะแจ้งวัตถุประสงค์ใหม่ให้ท่านทราบและได้รับการยินยอมก่อน **ท่านสามารถอ่านรายละเอียดนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)** ตามลิงก์ https://drive.google.com/file/d/1gxHdTRzSKbfnavtp2Ar57yGqluA7hJZr/view?usp=sharing

ชื่อหน่วยงาน *

มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ประเภทหน่วยงาน *

- (●) หน่วยงานของรัฐ
- ( ) หน่วยงานควบคุมหรือกำกับดูแล

- [ ] หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- [ ] Other

ยศ (ถ้ามี) ชื่อ-สกุล ผู้ประสานงาน *

ผู้ช่วยศาสตราจารย์ ดร.นิสิต ภูครองตา

ตำแหน่ง *

ผู้ช่วยผู้อำนวยการและหัวหน้างานความมั่นคงปลอดภัยดิจิทัล สำนักวิทยบริการและเทคโนโลยีสาร

หมายเลขโทรศัพท์ *

0915429889

อีเมล *

nisit_p@rmutt.ac.th

มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ (มีผลบังคับใช้ 18 ม.ค. 2567)

เอกสารอ้างอิง:
ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 https://ratchakitcha.soc.go.th/documents/17286.pdf

การรับทราบสาระสำคัญของประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 *

หน่วยงานได้รับทราบและเข้าใจสาระสำคัญของมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ บ้างหรือไม่ เช่น รับทราบหนังสือเวียนหรือข่าวสารเกี่ยวกับมาตรฐานการกำหนดคุณลักษณะฯ จาก สกมช. และได้สื่อสารให้ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ เจ้าของระบบ และผู้เกี่ยวข้องทราบ

- (●) มี
- ( ) มีบางส่วน
- ( ) ไม่มี
- ( ) ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

แผนดำเนินการเพื่อกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ *

หน่วยงานมีแผนงาน ผู้รับผิดชอบ และทรัพยากร เพื่อดำเนินการให้สอดคล้องกับมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

- (●) มี
- ( ) มีบางส่วน
- ( ) ไม่มี
- ( ) ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การอบรมหรือเสริมสร้างความรู้เกี่ยวกับประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 *

หน่วยงานมีการเข้าร่วมอบรมที่ สกมช. จัดขึ้น และถ่ายทอดความรู้ให้ผู้เกี่ยวข้องแล้วหรือไม่ เช่น ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ หรือเจ้าหน้าที่ความมั่นคงปลอดภัยไซเบอร์ เจ้าของระบบ ฯลฯ

- ○ มี
- ◉ มีบางส่วน
- ○ ไม่มี
- ○ ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การดำเนินการสอดคล้องตามประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 *

หน่วยงานมีการจัดทำนโยบาย และการดำเนินการที่สอดคล้องตามมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

- ◉ มี

- มีบางส่วน
- ไม่มี
- ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ

มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ (มีผลบังคับใช้ 18 ม.ค. 2567)

เอกสารอ้างอิง:
ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
https://ratchakitcha.soc.go.th/documents/17287.pdf

การรับทราบสาระสำคัญของประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 *

หน่วยงานได้รับทราบและเข้าใจสาระสำคัญของมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ บ้างหรือไม่ เช่น รับทราบหนังสือเวียนหรือข่าวสารเกี่ยวกับมาตรฐานขั้นต่ำฯ จาก สกมช. และได้สื่อสารให้ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ เจ้าของระบบ และผู้เกี่ยวข้องทราบ

- (●) มี
- มีบางส่วน
- ไม่มี
- ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

แผนดำเนินการเพื่อกำหนดมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ *

หน่วยงานมีแผนงาน ผู้รับผิดชอบ และทรัพยากร เพื่อดำเนินการให้สอดคล้องกับมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศพ.ศ. 2566

- (●) มี
- ( ) มีบางส่วน
- ( ) ไม่มี
- ( ) ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การอบรมหรือเสริมสร้างความรู้ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 *

หน่วยงานมีการเข้าร่วมอบรมที่ สกมช. จัดขึ้น และถ่ายทอดความรู้ให้ผู้เกี่ยวข้องแล้วหรือไม่ เช่น ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ หรือเจ้าหน้าที่ความมั่นคงปลอดภัยไซเบอร์ เจ้าของระบบ ฯลฯ

- ( ) มี
- (●) มีบางส่วน

- ไม่มี
- ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การดำเนินการสอดคล้องตามประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

* หน่วยงานมีการจัดทำนโยบาย และการดำเนินการที่สอดคล้องตามมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

- มี
- มีบางส่วน
- ไม่มี
- ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (มีผลบังคับใช้ 10 ก.ย. 2569)

เอกสารอ้างอิง:
1. ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 https://ratchakitcha.soc.go.th/documents/43184.pdf
2. ประกาศ สกมช. เรื่อง กรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ https://drive.ncsa.or.th/s/dGEeLf7sJZSRK6B
3. ประกาศ สกมช. เรื่อง เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลหลักในประเทศไทย พ.ศ. 2567 https://drive.ncsa.or.th/s/WBQjwSfmEkxHC9P

การรับทราบสาระสำคัญของประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

*

หน่วยงานได้รับทราบและเข้าใจสาระสำคัญของมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์บ้างหรือไม่ เช่น รับทราบหนังสือเวียนหรือข่าวสารเกี่ยวกับมาตรฐานคลาวด์ฯ จาก สกมช. และได้สื่อสารให้ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ เจ้าของระบบ และผู้เกี่ยวข้องทราบ

- ○ มี
- ◉ มีบางส่วน
- ○ ไม่มี
- ○ ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

แผนดำเนินการเพื่อยกระดับความมั่นคงปลอดภัยของระบบคลาวด์ *

หน่วยงานมีแผนงาน ผู้รับผิดชอบ และทรัพยากร เพื่อยกระดับระบบคลาวด์ให้สอดคล้องกับมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

- [ ] มี
- [x] มีบางส่วน
- [ ] ไม่มี
- [ ] ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การอบรมหรือเสริมสร้างความรู้เกี่ยวกับประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 *

หน่วยงานมีการเข้าร่วมอบรมที่ สกมช. จัดขึ้น และถ่ายทอดความรู้ให้ผู้เกี่ยวข้องแล้วหรือไม่ เช่น ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ หรือเจ้าหน้าที่ความมั่นคงปลอดภัยไซเบอร์ เจ้าของระบบ ฯลฯ

- [x] มี
- [ ] มีบางส่วน
- [ ] ไม่มี
- [ ] ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การดำเนินการสอดคล้องตามประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

*

หน่วยงานมีการจัดทำนโยบาย และการดำเนินการที่สอดคล้องตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

- ○ มี
- ◉ มีบางส่วน
- ○ ไม่มี
- ○ ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (มีผลบังคับใช้ 16 ก.ย. 2569)

เอกสารอ้างอิง:
ประกาศ กมช. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568
https://ratchakitcha.soc.go.th/documents/86192.pdf

การรับทราบสาระสำคัญของประกาศ กมช. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 *

หน่วยงานได้รับทราบและเข้าใจสาระสำคัญของมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 บ้างหรือไม่ เช่น รับทราบหนังสือเวียนหรือข่าวสารเกี่ยวกับมาตรฐานเว็บไซต์ฯ จาก สกมช. และได้สื่อสารให้ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ เจ้าของระบบ และผู้เกี่ยวข้องทราบ

- ( ) มี
- (•) มีบางส่วน
- ( ) ไม่มี
- ( ) ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

แผนดำเนินการเพื่อยกระดับความมั่นคงปลอดภัยของเว็บไซต์ *

หน่วยงานมีแผนงาน ผู้รับผิดชอบ และทรัพยากร เพื่อยกระดับเว็บไซต์ให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568

- (•) มี
- ( ) มีบางส่วน
- ( ) ไม่มี
- ( ) ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การอบรมหรือเสริมสร้างความรู้เกี่ยวกับประกาศ กมช. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568

*

หน่วยงานมีการเข้าร่วมอบรมที่ สกมช. จัดขึ้น และถ่ายทอดความรู้ให้ผู้เกี่ยวข้องแล้วหรือไม่ เช่น ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ หรือเจ้าหน้าที่ความมั่นคงปลอดภัยไซเบอร์ เจ้าของระบบ ฯลฯ

- ○ มี
- ◉ มีบางส่วน
- ○ ไม่มี
- ○ ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การดำเนินการสอดคล้องตามประกาศ กมช. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568

*

หน่วยงานมีการจัดทำนโยบาย และการดำเนินการที่สอดคล้องตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568

- ◉ มี
- ○ มีบางส่วน

- ไม่มี
- ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย

เอกสารอ้างอิง:
1. แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย https://drive.ncsa.or.th/s/Le37SrkAWo97q6g
2. นโยบายการใช้เทคโนโลยี Generative AI ที่ยอมรับได้ https://drive.ncsa.or.th/s/j5wkBZ4EngLKGKY

การรับทราบสาระสำคัญของแนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย

*

หน่วยงานได้รับทราบและเข้าใจสาระสำคัญของแนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย บ้างหรือไม่ เช่น รับทราบหนังสือเวียนหรือข่าวสารเกี่ยวกับแนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย จาก สกมช. และได้สื่อสารให้ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ เจ้าของระบบ และผู้เกี่ยวข้องทราบ

- มี
- มีบางส่วน
- ไม่มี
- ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

แผนดำเนินการเพื่อยกระดับการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย

*

หน่วยงานมีแผนงาน ผู้รับผิดชอบ และทรัพยากร เพื่อยกระดับการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย

- ○ มี
- ◉ มีบางส่วน
- ○ ไม่มี
- ○ ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การอบรมหรือเสริมสร้างความรู้เกี่ยวกับแนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย

*

หน่วยงานมีการเข้าร่วมอบรมที่ สกมช. จัดขึ้น และถ่ายทอดความรู้ให้ผู้เกี่ยวข้องแล้วหรือไม่ เช่น ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ หรือเจ้าหน้าที่ความมั่นคงปลอดภัยไซเบอร์ ฯลฯ

- ○ มี
- ◉ มีบางส่วน
- ○ ไม่มี

- ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การดำเนินการสอดคล้องตามแนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย

*

หน่วยงานมีการจัดทำนโยบาย แนวปฏิบัติ และการดำเนินการที่สอดคล้องตามแนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย
ทั้งนี้ หน่วยงานสามารถนำนโยบายการใช้เทคโนโลยี Generative AI ที่ยอมรับได้ ซึ่งเผยแพร่โดย สกมช. ไปใช้เป็นแนวทางตั้งต้นในการจัดทำนโยบายของหน่วยงานได้
https://ncsa.or.th/docpdf/view/ba37afc6636334401e000142

- มี
- มีบางส่วน
- ไม่มี
- ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

แนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม

เอกสารอ้างอิง:
1. คำแนะนำเรื่องแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม
https://drive.ncsa.or.th/s/52GYxAqMfDNZjEZ
2. แพลตฟอร์มควอนตัมเพื่อการเรียนรู้ ประเมิน และติดตามระดับชาติ https://pqc-learn.ncsa.or.th/

การรับทราบสาระสำคัญของแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม

*

หน่วยงานได้รับทราบและเข้าใจสาระสำคัญของแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม บ้างหรือไม่ เช่น รับทราบหนังสือเวียนหรือข่าวสารเกี่ยวกับแนวปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัมฯ จาก สกมช. และได้สื่อสารให้ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ เจ้าของระบบ และผู้เกี่ยวข้องทราบ

- ( ) มี
- ( ) มีบางส่วน
- (•) ไม่มี
- ( ) ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

แผนดำเนินการเพื่อยกระดับการเตรียมความพร้อมสำหรับยุคควอนตัม

*

หน่วยงานมีแผนงาน ผู้รับผิดชอบ และทรัพยากร เพื่อยกระดับการเตรียมความพร้อมสำหรับยุคควอนตัมอย่างมั่นคงปลอดภัย

- ( ) มี
- ( ) มีบางส่วน
- (•) ไม่มี

- [ ] ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การอบรมหรือเสริมสร้างความรู้เกี่ยวกับแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม

*

หน่วยงานมีการเข้าร่วมอบรมที่ สกมช. จัดขึ้น และถ่ายทอดความรู้ให้ผู้เกี่ยวข้องแล้วหรือไม่ เช่น ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ หรือเจ้าหน้าที่ความมั่นคงปลอดภัยไซเบอร์ เจ้าของระบบ ฯลฯ

- [ ] มี
- [ ] มีบางส่วน
- [ ] ไม่มี
- [ ] ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การดำเนินการสอดคล้องตามแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม

*

หน่วยงานมีการจัดทำแนวปฏิบัติ และการดำเนินการที่สอดคล้องตามแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม

- [ ] มี
- [ ] มีบางส่วน
- [x] ไม่มี
- [ ] ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

แนวปฏิบัติการใช้ซีโร่ทรัสต์ (Zero Trust Guidelines)

เอกสารอ้างอิง:
แนวปฏิบัติการใช้ซีโร่ทรัสต์ (Zero Trust Guidelines) https://drive.ncsa.or.th/s/Qepi4xeNFQ2iBJG

การรับทราบสาระสำคัญของแนวปฏิบัติการใช้ซีโร่ทรัสต์ (Zero Trust Guidelines)

*
หน่วยงานได้รับทราบและเข้าใจสาระสำคัญของแนวปฏิบัติการใช้ซีโร่ทรัสต์ (Zero Trust Guidelines) บ้างหรือไม่ เช่น รับทราบหนังสือเวียนหรือข่าวสารเกี่ยวกับแนวการใช้ซีโร่ทรัสต์ (Zero Trust Guidelines) จาก สกมช. และได้สื่อสารให้ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ เจ้าของระบบ และผู้เกี่ยวข้องทราบ

- [ ] มี
- [x] มีบางส่วน
- [ ] ไม่มี

- ( ) ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

แผนดำเนินการเพื่อยกระดับการใช้ซีโร่ทรัสต์

* หน่วยงานมีแผนงาน ผู้รับผิดชอบ และทรัพยากร เพื่อยกระดับการใช้ซีโร่ทรัสต์อย่างมั่นคงปลอดภัย

- ( ) มี
- (•) มีบางส่วน
- ( ) ไม่มี
- ( ) ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การอบรมหรือเสริมสร้างความรู้เกี่ยวกับแนวทางการปฏิบัติการใช้ซีโร่ทรัสต์ (Zero Trust Guidelines)

*

หน่วยงานมีการเข้าร่วมอบรมที่ สกมช. จัดขึ้น และถ่ายทอดความรู้ให้ผู้เกี่ยวข้องแล้วหรือไม่ เช่น ผู้บริหาร เจ้าหน้าที่เทคโนโลยีสารสนเทศ หรือเจ้าหน้าที่ความมั่นคงปลอดภัยไซเบอร์ เจ้าของระบบ ฯลฯ

- (●) มี
- ( ) มีบางส่วน
- ( ) ไม่มี
- ( ) ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

การดำเนินการสอดคล้องตามแนวปฏิบัติการใช้ซีโร่ทรัสต์ (Zero Trust Guidelines)

*

หน่วยงานมีการจัดทำแนวปฏิบัติ และการดำเนินการที่สอดคล้องตามแนวปฏิบัติการใช้ซีโร่ทรัสต์ (Zero Trust Guidelines)

- ( ) มี
- (●) มีบางส่วน
- ( ) ไม่มี
- ( ) ไม่เกี่ยวข้อง

ปัญหาและอุปสรรค (ถ้ามี)

Enter your answer

ข้อเสนอแนะ ปัญหา และอุปสรรคในการดำเนินงานในภาพรวม

(เช่น ด้านงบประมาณ บุคลากร เทคโนโลยี หรือประเด็นอื่นที่เกี่ยวข้อง)

งบประมาณในด้านการพัฒนากำลังคนให้เท่าทันเทคโนโลยีสมัยใหม่