



บันทึกข้อความ

ส่วนราชการ ส่วนบริหารทั่วไป สำนักบริหารจัดการน้ำและอุทกวิทยา โทร. ๐ ๒๒๔๑ ๕๗๒๒ (๒๓๗๖)

ที่ สบอ ๒๕๗๙/๒๕๖๖

วันที่ ๒๔ มีนาคม ๒๕๖๖

เรื่อง ขอเชิญเข้าร่วมกิจกรรมการประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐ (CII and Government Cybersecurity Assessment ๒๐๒๓)

เรียน ผอ.ส่วน ผอช.ภาค ทน.๑-๙ บอ. และหัวหน้าฝ่ายส่วนบริหารทั่วไป

เพื่อโปรดทราบ และแจ้งให้บุคลากรในสังกัดทราบหากมีผู้สนใจเข้าร่วมโครงการฝึกอบรมดังกล่าว ตอบรับการเข้าร่วมกิจกรรมภายในเวลาที่กำหนด

(นางสาววิณา บรรยงนุชวานิช)
งบ.บอ. รักษาราชการแทน ผบท.บอ.



สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ อีเมล saraban@ncsa.or.th

ผ.ช.บอ.

มท 591

ส.ท.ล 2579

ที่ สกนช ๐๖๐๐/ว๑๑๙๑

๐๓/๖๖๕

๒๐ มีนาคม ๒๕๖๖

เรื่อง ขอเชิญเข้าร่วมกิจกรรมการประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงาน
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐ (CII and Government Cybersecurity
Assessment 2023)

เรียน ผู้อำนวยการสำนักบริหารจัดการน้ำและอุทกวิทยา กรมชลประทาน

- สิ่งที่ส่งมาด้วย ๑. รายละเอียดกิจกรรมการอบรมให้ความรู้เกี่ยวกับกรอบ หลักเกณฑ์และเครื่องมือในการ
ประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์
๒. รายละเอียดกิจกรรมการประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ สำหรับ
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐ
๓. แบบฟอร์มหนังสือแต่งตั้งผู้ทำหน้าที่บันทึกข้อมูลเข้าสู่ระบบ

ตามที่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้ดำเนิน
โครงการการออกแบบและประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้าง
พื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐ และจัดทำฐานข้อมูลดัชนีวัดระดับความมั่นคงปลอดภัย
ไซเบอร์กลางของประเทศ (National Cybersecurity Rating Index: NCRI) โดยมีวัตถุประสงค์เพื่อออกแบบ
และประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Rating Index) ที่มีความน่าเชื่อถือ
วัดผลได้อย่างรวดเร็วและมีประสิทธิภาพ ซึ่งจะทำให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
และหน่วยงานของรัฐ สามารถประเมินระดับความมั่นคงปลอดภัยไซเบอร์ได้ด้วยตนเองอย่างสม่ำเสมอ
และสามารถนำไปเปรียบเทียบกับค่าเฉลี่ยระดับความมั่นคงปลอดภัยไซเบอร์ในกลุ่มหน่วยงานเดียวกัน ส่งผลให้
หน่วยงานสามารถยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างสอดคล้องกับระดับความเสี่ยง
ด้านไซเบอร์ของหน่วยงาน รวมถึงพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ต่อไป

ในการนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ขอเชิญ
หน่วยงานของท่านเข้าร่วมกิจกรรม โดยมีกำหนดการ ดังนี้

๑. กิจกรรมการอบรมให้ความรู้เกี่ยวกับกรอบ หลักเกณฑ์และเครื่องมือในการประเมินดัชนีวัดระดับ
ความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐ
ในวันที่ ๓ เมษายน ๒๕๖๖ เวลา ๑๓.๓๐ - ๑๖.๓๐ น. ผ่านสื่ออิเล็กทรอนิกส์ระบบ Zoom Meeting
รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย ๑


๒. กิจกรรมการประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้าง
พื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐ ระหว่างวันที่ ๒๔ เมษายน ถึง ๕ พฤษภาคม ๒๕๖๖
รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย ๒

ทั้งนี้ โปรดตอบรับการเข้าร่วมกิจกรรม ในข้อ ๑ ผ่านทางลิงก์ที่ปรากฏในสิ่งที่ส่งมาด้วย ๑ ภายในวันที่ ๓๑ มีนาคม ๒๕๖๖ และตอบรับการเข้าร่วมกิจกรรมในข้อ ๒ โดยต้องมีหนังสือแต่งตั้งผู้ทำหน้าที่ บันทึกข้อมูลเข้าสู่ระบบเป็นลายลักษณ์อักษร ภายในวันที่ ๑๐ เมษายน ๒๕๖๖ ตามแบบฟอร์มในสิ่งที่ส่งมาด้วย ๓ และขอมอบหมายให้ คุณณภาพร แสนพิศ หมายเลขโทรศัพท์ ๐ ๒๖๗๐ ๘๙๘๐ ต่อ ๔๐๔ ไปรษณีย์อิเล็กทรอนิกส์ naphaphorn@acinfotec.com เป็นผู้ประสานงาน

จึงเรียนมาเพื่อโปรดพิจารณาเข้าร่วมกิจกรรมดังกล่าว

ขอแสดงความนับถือ

พลอากาศตรี



(จเด็จ คุณะก้องกิจ)

ผู้ช่วยเลขาธิการ รักษาการแทน

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

รายละเอียดกิจกรรมการอบรมให้ความรู้เกี่ยวกับกรอบ หลักเกณฑ์และเครื่องมือ
ในการประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์

๑. หลักการและเหตุผล

การโจมตีทางไซเบอร์ในปัจจุบันมุ่งเป้าไปที่ทุกช่องทาง โดยเฉพาะโครงสร้างพื้นฐานสำคัญระดับชาติ ภัยคุกคามทางไซเบอร์เหล่านี้ส่งผลกระทบต่อทั้งภาคเศรษฐกิจและสังคม โดยคาดการณ์ภายในปี พ.ศ. ๒๕๖๘ ความเสียหายที่เกิดขึ้นอาจมีมูลค่าสูงถึง ๑๐.๕ ล้านล้านดอลลาร์ นอกจากนี้ความเสียหายที่เป็นตัวเงินแล้ว ยังทำลายชื่อเสียงและความน่าเชื่อถือของหน่วยงานที่เกี่ยวข้อง รวมทั้งชื่อเสียงของประเทศในภาพรวม

ด้วยเหตุนี้ การพัฒนากลยุทธ์ด้านความปลอดภัยไซเบอร์ในระดับประเทศสำหรับปกป้องพลเมือง ธุรกิจ และโครงสร้างพื้นฐานที่สำคัญในปลอดภัยจากความเสี่ยงที่อาจเกิดขึ้นจึงเป็นเรื่องสำคัญที่ต้องดำเนินการเป็นอันดับต้น ๆ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงประสงค์ให้มีโครงการออกแบบและประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานรัฐ และจัดทำฐานข้อมูลดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์กลางของประเทศ (National Cybersecurity Rating Index: NCRI) เพื่อออกแบบและประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Rating Index) ที่มีความน่าเชื่อถือ วัตถุประสงค์ได้รวดเร็ว แต่ใช้เวลาและทรัพยากรน้อย เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐ สามารถประเมินระดับความมั่นคงปลอดภัยไซเบอร์ได้ด้วยตนเองอย่างสม่ำเสมอ มีความรวดเร็ว ใช้ต้นทุนต่ำ ให้ผลลัพธ์ที่เชื่อถือได้ และสามารถนำไปเปรียบเทียบระหว่างกันได้ ส่งผลให้ลดความเสี่ยงจากภัยไซเบอร์ที่มีต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐ ได้อย่างมีประสิทธิภาพ

๒. วัตถุประสงค์ของการอบรม

เพื่ออธิบายกรอบ หลักเกณฑ์ เครื่องมือ และวิธีการการประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ สำหรับการประเมินโดยหน่วยงานเอง (Self-Assessment) การประเมินโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระ (Expert-Assessment) และการประเมินโดยระบบอัตโนมัติ (Automated-Assessment)

๓. คุณสมบัติของผู้เข้าร่วมการอบรม

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐที่เข้าร่วมกิจกรรมการอบรมและกิจการการประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ต้องส่งบุคลากรที่มีคุณสมบัติ ดังต่อไปนี้

- ๓.๑ เป็นผู้บริหารหรือตัวแทนผู้บริหารด้านเทคโนโลยีสารสนเทศหรือด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (ผู้อนุมัติคำตอบแบบประเมิน) จำนวนอย่างน้อย ๑ คน
- ๓.๒ เป็นผู้ที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศหรือด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (ผู้ตอบแบบประเมิน) จำนวนอย่างน้อย ๑ คน
- ๓.๓ บุคลากรตามข้อ ๓.๑ และ ๓.๒ เป็นบุคคลที่ได้รับแต่งตั้งให้เป็นผู้ทำหน้าที่บันทึกข้อมูลเข้าสู่ระบบ โดยใช้แบบฟอร์มในสิ่งที่ส่งมาด้วย ๓

๔. ระยะเวลาการอบรม

การอบรมจะจัดขึ้นผ่านสื่ออิเล็กทรอนิกส์ระบบ Zoom Meeting ในวันที่ ๓ เมษายน ๒๕๖๖ เวลา ๑๓.๓๐ - ๑๖.๓๐ น.

๕. การลงทะเบียนเข้าร่วมการอบรม

ผู้ที่มีคุณสมบัติตามข้อ ๓ ต้องลงทะเบียนเข้าร่วมการอบรมภายในวันที่ ๓๑ มีนาคม ๒๕๖๖ โดยกรอกแบบฟอร์มผ่านทางลิงก์ <https://forms.gle/ZoqhYcqbSkrUvAgi9> เพื่อรับลิงก์การเข้าร่วมประชุมผ่านทางอีเมลที่ท่านได้ให้ไว้ในแบบฟอร์มดังกล่าว

๖. ช่องทางการติดต่อ

ท่านสามารถสอบถามข้อมูลเพิ่มเติมและประสานงานได้ที่ คุณนภาพร แสนพิศ (ผู้ประสานงาน) โทร ๐ ๒๖๗๐ ๘๙๘๐ ต่อ ๔๐๔ อีเมล naphaphorn@acinfotec.com

กำหนดการ
กิจกรรมการอบรมให้ความรู้เกี่ยวกับกรอบ
หลักเกณฑ์และเครื่องมือในการประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์
วันที่ ๓ เมษายน ๒๕๖๖ เวลา ๑๓.๓๐ - ๑๖.๓๐ น.
ผ่านสื่ออิเล็กทรอนิกส์ระบบ Zoom Meeting

๑๓.๐๐ - ๑๓.๓๐ น.	ผู้เข้าร่วมอบรมเข้าระบบ Zoom Meeting
๑๓.๓๐ - ๑๓.๔๐ น.	ประธานเปิดการอบรม
๑๓.๔๐ - ๑๓.๕๐ น.	อธิบายข้อมูลเบื้องต้นของกรอบการประเมิน
๑๓.๕๐ - ๑๔.๑๕ น.	อธิบายวิธีการ เกณฑ์ และเครื่องมือการประเมินระดับความ มั่นคงปลอดภัยไซเบอร์โดยหน่วยงานเอง (Self- Assessment)
๑๔.๑๕ - ๑๕.๔๕ น.	อธิบายวิธีการ เกณฑ์ และเครื่องมือการประเมินระดับความ มั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบภายในหรือผู้ ตรวจสอบอิสระ (Expert-Assessment)
๑๕.๔๕ - ๑๖.๐๐ น.	ชี้แจงการใช้เครื่องมือสำหรับการประเมินระดับความมั่นคง ปลอดภัยไซเบอร์โดยระบบอัตโนมัติ (Automated- Assessment)
๑๖.๐๐ - ๑๖.๑๕ น.	ชี้แจงกำหนดการการประเมินทั้ง ๓ วิธี
๑๖.๑๕ - ๑๖.๓๐ น.	ตอบข้อซักถามของผู้เข้าร่วมการอบรม

หมายเหตุ: กำหนดการอาจมีการเปลี่ยนแปลงตามความเหมาะสม

CIL and Government Cybersecurity Assessment 2023

ความเป็นมาของ CIL and Government Cybersecurity Assessment 2023

การโจมตีทางไซเบอร์ในปัจจุบันเข้ามามีบทบาทสำคัญมากขึ้น โดยเฉพาะโครงสร้างพื้นฐานสำคัญระดับชาติที่ภัยคุกคามทางไซเบอร์เหล่านี้ส่งผลกระทบต่ออย่างมหาศาล ต่อถึงภาคเศรษฐกิจและสังคมโดยคาดการณ์ภายในปี พ.ศ. 2568 ความเสียหายที่เกิดขึ้นอาจมีมูลค่าสูงถึง 10.5 ล้านล้านบาท นอกจากนี้ภัยคุกคามที่เพิ่มขึ้นแล้ว ยังทำลายชื่อเสียงและความน่าเชื่อถือของหน่วยงานที่เกี่ยวข้อง รวมทั้งชื่อเสียงของประเทศในภาพรวม

ด้วยเหตุนี้การพัฒนาบุคลากรด้านความปลอดภัยไซเบอร์ในระดับประเทศ สำหรับปกป้องพลเมือง ธุรกิจ และโครงสร้างพื้นฐานที่สำคัญให้ปลอดภัยจากความเสี่ยงที่จะเกิดขึ้น จึงเป็นเรื่องสำคัญที่ต้องดำเนินการเป็นอันดับต้น ๆ สู่เป้าหมายการบรรลุเป้าหมายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สมทช.) จึงประสงค์ให้มีโครงการออกแบบและประเมินดัชนีวัดระดับความมั่นคงปลอดภัย ไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานรัฐ และจัดทำฐานข้อมูลดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์กลางของประเทศ (National Cybersecurity Rating Index: NCRI) เพื่อออกแบบและประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Rating Index) ที่มีความน่าเชื่อถือ วัตถุประสงค์รวดเร็ว แต่ใช้เวลาและทรัพยากรน้อย เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐ สามารถประเมินความมั่นคงปลอดภัยไซเบอร์ได้ด้วยตนเองอย่างสม่ำเสมอ มีความรวดเร็วทันคนต่ำให้ผลลัพธ์ที่เชื่อถือได้และสามารถนำไปเปรียบเทียบกับองค์กรที่อื่นได้ ส่งผลให้ลดความเสียหายจากภัยไซเบอร์ที่มีต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐ ได้อย่างมีประสิทธิภาพ

ในขณะนี้ สมทช. จึงขอเชิญชวนเข้าร่วมโครงการดังกล่าว เพื่อความร่วมมือในการจัดทำและพัฒนาระดับชาติที่มีความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับยุทธศาสตร์ชาติและเป็นเป้าหมายของแต่ละหน่วยงานได้อย่างมีประสิทธิภาพ

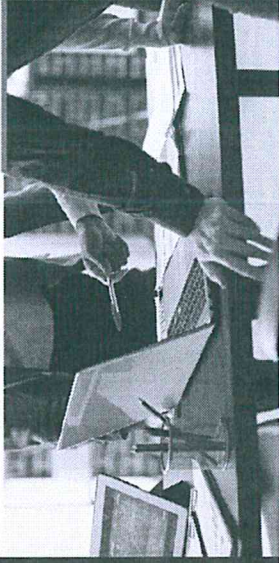


ประโยชน์ของดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์

1. ทราบระดับความมั่นคงปลอดภัยไซเบอร์ขององค์กรของท่าน ที่จุดแข็ง จุดอ่อน และคะแนน
2. ทราบผลการเปรียบเทียบระดับความมั่นคงปลอดภัยไซเบอร์ขององค์กรของท่าน เมื่อเทียบกับค่าเฉลี่ยของกลุ่มอุตสาหกรรม
3. วางแผนกลยุทธ์สำหรับองค์กรของท่านในการปรับปรุงการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ดียิ่งขึ้น และประเมินประสิทธิภาพ
4. กำหนดลำดับความสำคัญและทรัพยากรที่ต้องใช้เพื่อปรับปรุงการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรของท่านอย่างเหมาะสม

สิ่งที่ท่านจะได้รับเมื่อทำการประเมินแล้วเสร็จ

1. คะแนนระดับความมั่นคงปลอดภัยไซเบอร์ขององค์กรท่าน
2. กราฟเปรียบเทียบคะแนนระหว่างองค์กรของท่านกับค่าเฉลี่ยของกลุ่มอุตสาหกรรม
3. คำแนะนำเชิงต้นเพื่อปรับปรุงการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรของท่าน



ขั้นตอนการประเมิน

1. **Self-Assessment**
โดยให้วิศวกรของท่านทำการประเมินระดับความมั่นคงปลอดภัยไซเบอร์ด้วยตนเองตามแบบประเมินที่ สมทช. ได้จัดเตรียมให้
2. **Expert Assessment**
โดยให้วิศวกรสอบภายในหรือผู้ตรวจสอบอิสระประเมินระดับความมั่นคงปลอดภัยไซเบอร์ขององค์กรของท่าน
3. **Automated Assessment**
โดยให้วิศวกรของท่านทำการประเมินระดับความมั่นคงปลอดภัยไซเบอร์ด้วยเครื่องมือที่ สมทช. ได้จัดเตรียมให้

หากท่านมีข้อสงสัยสามารถสอบถามเพิ่มเติมได้ที่
ชื่อ: นภาพร แสงพิศ

อีเมล: naphaphorn@acinfofotec.com
โทร: 02-670-8980 ต่อ 404

**สรุปกำหนดการจัดกิจกรรมการประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์ สำหรับ
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐ
(CII and Government Cybersecurity Assessment 2023)**

วันที่	กิจกรรม
๓๑ มีนาคม ๒๕๖๖	<p>วันสุดท้ายสำหรับการลงทะเบียนเข้าร่วมอบรม โดยมีลงทะเบียนผ่านช่องทาง ดังนี้</p> <ul style="list-style-type: none"> ● ผู้เข้าร่วมอบรมวันที่ ๓ เมษายน ๒๕๖๖ ลงทะเบียนผ่านลิงก์ https://forms.gle/ZoqhYcqBskrUvAgi9 ● ผู้เข้าร่วมอบรมวันที่ ๔ เมษายน ๒๕๖๖ ลงทะเบียนผ่านลิงก์ https://forms.gle/Z54zyzG4nk5YCw8t5
๓ - ๔ เมษายน ๒๕๖๖	<p>การอบรมให้ความรู้เกี่ยวกับกรอบ หลักเกณฑ์และเครื่องมือในการประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์</p>
๑๐ เมษายน ๒๕๖๖	<p>วันสุดท้ายสำหรับการส่งหนังสือแต่งตั้งผู้ทำหน้าที่บันทึกข้อมูลเข้าสู่ระบบเป็นลายลักษณ์อักษร โดยใช้แบบฟอร์มตามสิ่งที่ส่งมาด้วย ๓</p>
๒๔ เมษายน ถึง ๕ พฤษภาคม ๒๕๖๖	<p>การประเมินระดับความมั่นคงปลอดภัยไซเบอร์โดยหน่วยงานเอง (Self-Assessment) โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระ (Expert-Assessment) และโดยระบบอัตโนมัติ (Automated-Assessment)</p> <p>หมายเหตุ: การประเมินระดับความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระจะดำเนินการสุ่มเลือกอย่างน้อย 2 หน่วยงาน จากหน่วยงานที่ตอบรับการเข้าร่วมกิจกรรม</p>

แบบฟอร์มหนังสือแต่งตั้งผู้ทำหน้าที่บันทึกข้อมูลเข้าสู่ระบบ

ข้าพเจ้า นาย/นาง/นางสาว

ตำแหน่ง

ในนามของผู้บริหารสูงสุดของหน่วยงานหรือผู้ได้รับมอบอำนาจ ขอมอบหมายให้บุคคลดังต่อไปนี้ทำหน้าที่นำข้อมูลเกี่ยวกับการประเมินระดับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของข้าพเจ้าเข้าสู่ระบบตามโครงการการออกแบบและประเมินดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐ และจัดทำฐานข้อมูลดัชนีวัดระดับความมั่นคงปลอดภัยไซเบอร์กลางของประเทศ (National Cybersecurity Rating Index: NCRI) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

1. ผู้บริหารหรือตัวแทนผู้บริหารด้านเทคโนโลยีสารสนเทศหรือด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (ผู้อนุมัติคำตอบแบบประเมิน)
 นาย/นาง/นางสาว.....
 ตำแหน่ง.....
 อีเมล.....
2. ผู้ที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศหรือด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (ผู้ตอบแบบประเมิน)
 นาย/นาง/นางสาว.....
 ตำแหน่ง.....
 อีเมล.....
3. บุคลากรสำรอง
 นาย/นาง/นางสาว.....
 ตำแหน่ง.....
 อีเมล.....

ด้วยความยินยอมของข้าพเจ้า บุคคลดังกล่าวข้างต้นจะดำเนินการในนามของหน่วยงานของข้าพเจ้า จะรักษาความมั่นคงปลอดภัยสารสนเทศตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานของข้าพเจ้า จะรักษาความลับของข้อมูลสารสนเทศของหน่วยงานของข้าพเจ้า และจะปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนดโดยเคร่งครัด

ข้าพเจ้าขอรับรองว่าข้อมูลดังกล่าวข้างต้นเป็นจริงทุกประการ

.....
 (.....)

ตำแหน่ง.....

หน่วยงาน.....