สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ อาคารซี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
เลขรับ: 3735/2569
วันที่รับ: 22/10/2569
เวลารับ: 15:33

ที่ สกมช ๐๕๐๐/ว๓๘๓๙

๒๑ ตุลาคม ๒๕๖๙

เรื่อง ขอเชิญร่วมสนับสนุนและส่งผลงานเข้าร่วม CYBERCONF 2027: Cybersecurity Research & Innovation Forum

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
เลขรับ: 1967/2569
วันที่รับ: 3/11/2569
เวลารับ: 09:55

เรียน อธิการบดีมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

สิ่งที่ส่งมาด้วย ๑. รายละเอียดการจัดงาน CYBERCONF 2027 จำนวน ๑ ฉบับ
๒. ประกาศเชิญชวนส่งบทความและผลงานวิจัย (Call for Papers) จำนวน ๑ ฉบับ

ด้วยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ กำหนดจัดงาน CYBERCONF 2027: Cybersecurity Research & Innovation Forum ภายใต้แนวคิด “Cybersecurity Research for the Resilient Digital Future” ระหว่างวันที่ ๒๐-๒๑ มกราคม ๒๕๗๐ ณ ศูนย์การประชุมแห่งชาติสิริกิติ์ กรุงเทพมหานคร โดยเป็นส่วนหนึ่งของงาน Cybersec Asia x Thailand International Cyber Week 2027 มีวัตถุประสงค์เพื่อเป็นเวทีเผยแพร่และแลกเปลี่ยนองค์ความรู้ ผลงานวิจัย ผลงานวิชาการ และนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีที่เกี่ยวข้อง ตลอดจนส่งเสริมการพัฒนางานวิจัยที่ตอบสนองต่อสถานการณ์ภัยคุกคาม ความต้องการของประเทศ และความท้าทายจากเทคโนโลยีเกิดใหม่ พร้อมทั้งสร้างเครือข่ายความร่วมมือด้านการวิจัยและพัฒนาระหว่างภาครัฐ ภาควิชาการ ภาคอุตสาหกรรม และเครือข่ายทั้งในประเทศและต่างประเทศ

ในการนี้ สกมช. พิจารณาแล้วเห็นว่า หน่วยงาน/สถาบันของท่านมีบุคลากร นักวิจัย และผู้เชี่ยวชาญที่มีศักยภาพในการร่วมขับเคลื่อนงานวิจัยและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ จึงใคร่ขอความอนุเคราะห์จากท่านในการสนับสนุนการดำเนินงาน CYBERCONF 2027: Cybersecurity Research & Innovation Forum ดังนี้

๑. ขอความอนุเคราะห์ประชาสัมพันธ์ Call for Papers ไปยังคณะ หน่วยงาน นักวิจัย คณาจารย์ นิสิต นักศึกษา ผู้เชี่ยวชาญและเครือข่ายที่เกี่ยวข้อง เพื่อเชิญชวนส่งบทความวิชาการ ผลงานวิจัย และผลงานวิจัยประยุกต์เข้าร่วม CYBERCONF 2027: Cybersecurity Research & Innovation Forum

๒. ขอความอนุเคราะห์สนับสนุนและส่งเสริมนักวิจัย คณาจารย์ นิสิต นักศึกษา และบุคลากรที่เกี่ยวข้องให้ส่งผลงานและเข้าร่วมนำเสนอผลงาน ตลอดจนร่วมแลกเปลี่ยนองค์ความรู้และสร้างเครือข่ายความร่วมมือด้านการวิจัยและนวัตกรรมภายในงาน

๓. ขอความอนุเคราะห์เสนอชื่อผู้ทรงคุณวุฒิ นักวิจัย หรือผู้เชี่ยวชาญที่มีความเชี่ยวชาญสอดคล้องกับสาขาหัวข้อการวิจัย (Research Tracks) ของการประชุม เพื่อร่วมเป็นผู้ทรงคุณวุฒิพิจารณากลั่นกรองบทความวิชาการและผลงานวิจัย (Reviewer) ตามกระบวนการและหลักเกณฑ์ที่กำหนด

/๔. ขอความ...

๔. ขอความอนุเคราะห์ใช้ตราสัญลักษณ์ของหน่วยงาน/สถาบันของท่าน ประกอบการประชาสัมพันธ์การจัดงาน CYBERCONF 2027: Cybersecurity Research & Innovation Forum ทั้งในสื่อสิ่งพิมพ์ สื่อออนไลน์ และสื่อประชาสัมพันธ์ที่เกี่ยวข้อง เพื่อแสดงถึงการให้การสนับสนุนและความร่วมมือทางวิชาการในการจัดงานดังกล่าว

ทั้งนี้ CYBERCONF 2027: Cybersecurity Research & Innovation Forum เปิดรับผลงานตั้งแต่วันที่ ๑๕ ตุลาคม ๒๕๖๙ ถึง ๓๐ พฤศจิกายน ๒๕๖๙ และจัดงานระหว่างวันที่ ๒๐-๒๑ มกราคม ๒๕๗๐ ณ ศูนย์การประชุมแห่งชาติสิริกิติ์ กรุงเทพมหานคร ภายใต้งาน Cybersec Asia x Thailand International Cyber Week 2027 ตามรายละเอียดที่แนบมาพร้อมนี้ หากท่านประสงค์สอบถามรายละเอียดเพิ่มเติม สามารถติดต่อได้ที่ นางสาววรวรรณ ศรีศักดิ์ ตำแหน่งหัวหน้างานพัฒนาเครือข่ายวิจัย ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ โทรศัพท์ ๐ ๒๕๐๒ ๗๘๒๓ ไปรษณีย์อิเล็กทรอนิกส์ worawan.s@ncsa.or.th

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

พลตรี

(ธีรวุฒิ วิทยากรณ์)

รองเลขาธิการ รักษาการแทน

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์
โทรศัพท์ ๐ ๒๕๐๒ ๗๘๒๓
ไปรษณีย์อิเล็กทรอนิกส์ research@ncsa.or.th

เรียน คณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
เพื่อโปรดพิจารณา

3 พ.ย. 2569

CYBERCONF 2027

Cybersecurity Research & Innovation Forum

“Cybersecurity Research for the Resilient Digital Future”

ภายใต้งาน Cybersec Asia x Thailand International Cyber Week 2027



วันที่ 20-21 มกราคม 2570

ณ ศูนย์การประชุมแห่งชาติสิริกิติ์ กรุงเทพมหานคร

จัดโดย

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

CYBERCONF 2027

Cybersecurity Research & Innovation Forum

๑. หลักการและเหตุผล

ปัจจุบัน การเปลี่ยนผ่านสู่เศรษฐกิจและสังคมดิจิทัลเกิดขึ้นอย่างรวดเร็ว ควบคู่กับการพัฒนาของเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ระบบอัตโนมัติ การประมวลผลแบบคลาวด์ ศูนย์ข้อมูล เทคโนโลยีควอนตัม ตลอดจนระบบดิจิทัลและโครงสร้างพื้นฐานที่มีการเชื่อมโยงกันมากขึ้น ส่งผลให้รูปแบบและระดับความซับซ้อนของภัยคุกคามทางไซเบอร์เปลี่ยนแปลงอย่างต่อเนื่อง และอาจส่งผลกระทบต่อประชาชน ภาคธุรกิจ หน่วยงานภาครัฐ ตลอดจนโครงสร้างพื้นฐานสำคัญของประเทศในวงกว้าง

การยกระดับขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศจึงมิได้จำกัดอยู่เพียงการป้องกันและรับมือภัยคุกคามเท่านั้น แต่จำเป็นต้องพัฒนาฐานองค์ความรู้ งานวิจัย เทคโนโลยี นวัตกรรม และบุคลากรที่สามารถตอบสนองต่อความเสี่ยงและการเปลี่ยนแปลงของเทคโนโลยีได้อย่างทันท่วงที ควบคู่กับการสร้างกลไกเชื่อมโยงองค์ความรู้และผลงานวิจัยจากภาควิชาการไปสู่การทดสอบ การประยุกต์ใช้ และการพัฒนานวัตกรรม เพื่อให้เกิดการใช้ประโยชน์ในภาครัฐ ภาคอุตสาหกรรม และภาคเศรษฐกิจอย่างเป็นรูปธรรม

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีภารกิจในการส่งเสริมและสนับสนุนการพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมถึงการส่งเสริมการวิจัยและพัฒนาเทคโนโลยีและนวัตกรรม การพัฒนาบุคลากร และการสร้างเครือข่ายความร่วมมือเพื่อเสริมสร้างระบบนิเวศด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถรองรับภัยคุกคามและความท้าทายจากเทคโนโลยีเกิดใหม่ได้อย่างมีประสิทธิภาพ ประกอบกับเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้มีดำริให้ เพิ่มมิติด้านวิชาการ การวิจัย และนวัตกรรมเป็นส่วนหนึ่งของการจัดงาน Cybersec Asia x Thailand International Cyber Week 2027 เพื่อเปิดพื้นที่สำหรับการนำเสนอและแลกเปลี่ยนองค์ความรู้ ผลงานวิจัย เทคโนโลยี และนวัตกรรม ตลอดจนสร้างโอกาสในการเชื่อมโยงนักวิจัย นักวิชาการ ผู้เชี่ยวชาญ ผู้ประกอบการ ภาคอุตสาหกรรม และหน่วยงานที่เกี่ยวข้อง เพื่อผลักดันผลงานวิจัยไปสู่การประยุกต์ใช้และการต่อยอดให้เกิดประโยชน์ต่อประเทศ

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ (ศวจ.) จึงกำหนดจัด CYBERCONF 2027: Cybersecurity Research & Innovation Forum ภายใต้แนวคิด “Cybersecurity Research for the Resilient Digital Future” ให้เป็นเวทีด้านวิชาการ การวิจัย และนวัตกรรมภายใต้งาน Cybersec Asia x Thailand International Cyber Week 2027 (Powered by NCSA) โดยเปิดพื้นที่ให้นักวิจัย คณาจารย์ นิสิต นักศึกษา ผู้เชี่ยวชาญ นักพัฒนา ผู้ประกอบการ และบุคลากรจากภาคอุตสาหกรรมทั้งในประเทศและต่างประเทศได้นำเสนอและแลกเปลี่ยนองค์ความรู้ ผลงานวิจัย ผลงานวิชาการ เทคโนโลยี และนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีที่เกี่ยวข้อง อันจะนำไปสู่การสร้างเครือข่ายความร่วมมือ การต่อยอดผลงานวิจัยสู่การใช้ประโยชน์ และการเสริมสร้างระบบนิเวศด้านการวิจัยและนวัตกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยให้มีความเข้มแข็งและยั่งยืน

๒. ชื่องาน

CYBERCONF 2027: Cybersecurity Research & Innovation Forum

Part of Cybersec Asia x Thailand International Cyber Week 2027

๓. แนวคิดหลัก

Cybersecurity Research for the Resilient Digital Future

๔. วัน เวลา และสถานที่

วันที่ ๒๐-๒๑ มกราคม ๒๕๗๐ ณ ศูนย์การประชุมแห่งชาติสิริกิติ์ กรุงเทพมหานคร

๕. หน่วยงานรับผิดชอบ

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ (ศวจ.)
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

๖. วัตถุประสงค์

๖.๑ เพื่อเป็นเวทีเผยแพร่ นำเสนอ และแลกเปลี่ยนองค์ความรู้ ผลงานวิจัย ผลงานวิชาการ เทคโนโลยี และนวัตกรรม ด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีที่เกี่ยวข้อง ระหว่างนักวิจัย นักวิชาการ นิสิต นักศึกษา ผู้เชี่ยวชาญ หน่วยงานภาครัฐ ภาคอุตสาหกรรม และผู้ประกอบการทั้งในประเทศและต่างประเทศ

๖.๒ เพื่อส่งเสริมการพัฒนางานวิจัยที่ตอบสนองต่อสถานการณ์ภัยคุกคาม ความต้องการ และโจทย์สำคัญด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมถึงความท้าทายจากเทคโนโลยีเกิดใหม่ อาทิ ปัญญาประดิษฐ์ (Artificial Intelligence: AI) เทคโนโลยีควอนตัม (Quantum Technology) ระบบคลาวด์ (Cloud) ศูนย์ข้อมูล (Data Center) อัตลักษณ์ดิจิทัล (Digital Identity) และระบบอัตโนมัติ (Autonomous Systems)

๖.๓ เพื่อสร้างและขยายเครือข่ายความร่วมมือด้านการวิจัยและพัฒนา และส่งเสริมการเชื่อมโยงระหว่างมหาวิทยาลัย สถาบันวิจัย หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภาคเอกชน ผู้ประกอบการ และเครือข่ายวิชาการทั้งในประเทศและต่างประเทศ เพื่อสนับสนุนการนำองค์ความรู้และผลงานวิจัยไปสู่การทดสอบ การประยุกต์ใช้ การพัฒนาเทคโนโลยีและนวัตกรรม ตลอดจนการต่อยอดให้เกิดประโยชน์ในเชิงนโยบาย เศรษฐกิจ และสังคม

๖.๔ เพื่อยกระดับ Cybersec Asia x Thailand International Cyber Week ให้เป็นแพลตฟอร์มด้านองค์ความรู้ การวิจัย และนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาค โดยเชื่อมโยงนโยบายและโจทย์สำคัญของประเทศเข้ากับองค์ความรู้ งานวิจัย เทคโนโลยี นวัตกรรม และความต้องการในการนำไปใช้จริงของภาครัฐและภาคอุตสาหกรรม พร้อมทั้งส่งเสริมและขยายความร่วมมือกับเครือข่ายระดับอาเซียนและนานาชาติ

๗. กลุ่มเป้าหมาย

- นักวิจัย อาจารย์ นักวิชาการ และนิสิต/นักศึกษา
- ผู้เชี่ยวชาญและบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์
- หน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)
- ผู้ประกอบการ บริษัทเทคโนโลยี และภาคอุตสาหกรรม
- มหาวิทยาลัย สถาบันการศึกษา สถาบันวิจัย และสมาคมวิชาชีพ
- เครือข่ายความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ

๘. รูปแบบกิจกรรม

กิจกรรมหลักประกอบด้วย ๒ ส่วน ได้แก่

- CALL FOR PAPERS – เปิดรับบทความวิชาการและผลงานวิจัย ตามหัวข้อที่กำหนด
- RESEARCH PRESENTATION –
  การนำเสนอผลงานที่ผ่านกระบวนการพิจารณากลั่นกรองโดยผู้ทรงคุณวุฒิ ในรูปแบบ Oral Presentation และ Poster Presentation

๙. Research Tracks

ลำดับ	Research Track	Topics of Interest
๑)	**Cybersecurity, Cybercrime & Threat Intelligence**	Cyber Defense, Network Security, SOC, Incident Response, Malware, Vulnerability, Digital Forensics, Cybercrime, Fraud, Threat Intelligence
๒)	**AI Security & Intelligent Autonomous Systems**	AI Security, LLM Security, Generative AI, Agentic AI, Adversarial AI, Deepfake, AI Governance, Autonomous Systems
๓)	**Quantum & Post-Quantum Security**	Post-Quantum Cryptography, Quantum-safe Security, Cryptography, Crypto-agility, Quantum Readiness, Migration Strategy

ลำดับ	Research Track	Topics of Interest
๔)	**Cloud, Data Center & Resilient Digital Infrastructure**	Cloud Security, Data Center Security, Secure & Green Data Center, Physical Security, Power Resilience, Certification & Assurance, Digital Infrastructure
๕)	**Critical Infrastructure, OT, IoT & Cyber-Physical Security**	CII, OT/ICS, Energy, Telecom, Transport, Healthcare, Smart Infrastructure, IoT/Embedded Systems, Cyber-Physical Systems
๖)	**Digital Trust, Privacy, Governance & Cyber Resilience**	Digital Identity, Zero Trust, Data Protection, Privacy, Cyber Resilience, Risk Management, Standards, Regulation, Digital Sovereignty, Cyber Diplomacy
๗)	**Cybersecurity Innovation & Applied Research**	Prototype, PoC, Technology Validation, Cybersecurity Products & Services, Technology Transfer, Research Commercialization, Research-to-Market

๑๐. ประเภทผลงานที่เปิดรับ

CYBERCONF 2027 เปิดรับผลงานด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีที่เกี่ยวข้อง โดยแบ่งประเภทผลงานออกเป็น ๒ ประเภท เพื่อเปิดโอกาสให้ครอบคลุมทั้งงานวิจัยเชิงวิชาการและงานวิจัยประยุกต์ที่สามารถเชื่อมโยงไปสู่การใช้ประโยชน์จริง ดังนี้

๑๐.๑ Full Research Paper

สำหรับผลงานวิจัยที่ดำเนินการแล้วเสร็จหรือมีผลการศึกษาที่สมบูรณ์ โดยมีการกำหนดปัญหาหรือคำถามวิจัย ระเบียบวิธีวิจัย ผลการศึกษา การวิเคราะห์ และข้อสรุปอย่างเป็นระบบ สามารถแสดงถึงองค์ความรู้ใหม่หรือข้อค้นพบที่มีคุณค่าต่อการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีที่เกี่ยวข้อง

รูปแบบผลงาน: Full Paper ความยาวประมาณ ๖–๑๐ หน้า

การพิจารณา: Peer Review

รูปแบบการนำเสนอ: Oral Presentation

กลุ่มเป้าหมาย: Researchers / Faculty / Graduate Students

๑๐.๒ Applied Research / Technical Paper

สำหรับงานวิจัยประยุกต์ ผลการพัฒนาเทคโนโลยี กรณีศึกษา การทดลองใช้ หรือ Technical Solution ที่มุ่งแก้ไขปัญหาหรือตอบสนองต่อความต้องการด้านความมั่นคงปลอดภัยไซเบอร์ และมีผลลัพธ์ บทเรียน หรือแนวทางที่สามารถนำไปประยุกต์ใช้หรือต่อยอดได้

รูปแบบผลงาน: Extended Abstract / Technical Paper ความยาวประมาณ ๓-๕ หน้า

การพิจารณา: Technical & Relevance Review

รูปแบบการนำเสนอ: Oral Presentation หรือ Poster Presentation

กลุ่มเป้าหมาย: Researchers / Government / CII / Industry / Technology Companies

ทั้งนี้ รูปแบบการจัดทำต้นฉบับ (Template) ภาษา รูปแบบการอ้างอิง หลักเกณฑ์การส่งผลงาน และรายละเอียดอื่นที่เกี่ยวข้อง ให้เป็นไปตาม **Call for Papers ของ CYBERCONF 2027** ที่กำหนด

๑๑. การพิจารณาและคัดเลือกผลงาน

ผลงานที่ส่งเข้าร่วม **CYBERCONF 2027** จะได้รับการตรวจสอบความครบถ้วนของเอกสารและความสอดคล้องกับ Research Tracks ก่อนเข้าสู่กระบวนการพิจารณาตามประเภทของผลงาน เพื่อให้การคัดเลือกมีความเหมาะสมกับลักษณะของงานวิจัยและการนำไปใช้ประโยชน์ โดยมีกระบวนการดำเนินงาน ดังนี้

๑๑.๑ การรับและตรวจสอบผลงาน

ผู้สนใจส่งผลงานตามรูปแบบ หลักเกณฑ์ ช่องทาง และระยะเวลาที่กำหนดใน Call for Papers โดยฝ่าย

เลขานุการจะตรวจสอบความครบถ้วนของเอกสาร รูปแบบการจัดทำผลงาน และความสอดคล้องกับขอบเขตของ CYBERCONF 2027 ก่อนส่งเข้าสู่กระบวนการพิจารณา

๑๑.๒ การพิจารณาผลงาน

ผลงานที่ผ่านการตรวจสอบเบื้องต้นจะเข้าสู่กระบวนการพิจารณาตามประเภทของผลงาน ดังนี้

- **Full Research Paper** ผ่านกระบวนการพิจารณาโดยผู้ทรงคุณวุฒิ (**Peer Review**) ที่มีความเชี่ยวชาญในสาขาที่เกี่ยวข้อง โดยพิจารณาคุณภาพทางวิชาการ ความใหม่ ความเหมาะสมของระเบียบวิธีวิจัย ความน่าเชื่อถือของผลการศึกษา และคุณค่าของผลงานต่อสาขาที่เกี่ยวข้อง

- **Applied Research / Technical Paper** ผ่านกระบวนการพิจารณาด้านเทคนิคและความสอดคล้องกับการนำไปใช้ประโยชน์ (**Technical & Relevance Review**) โดยพิจารณาความสำคัญของปัญหา แนวทางหรือเทคโนโลยีที่นำเสนอ ผลการทดลองหรือการประยุกต์ใช้ ความเป็นไปได้ทางเทคนิค และศักยภาพในการนำไปใช้หรือต่อยอด

๑๑.๓ การแจ้งผลและปรับปรุงผลงาน

ฝ่ายเลขานุการจะแจ้งผลการพิจารณาให้ผู้เขียนทราบ และอาจให้ผู้เขียนปรับปรุงผลงานตามข้อเสนอแนะของผู้ทรงคุณวุฒิหรือคณะผู้พิจารณาตามความเหมาะสม ก่อนจัดส่งต้นฉบับฉบับสมบูรณ์ (Camera-ready) ภายในระยะเวลาที่กำหนด

๑๑.๔ การคัดเลือกและนำเสนอผลงาน

ผลงานที่ผ่านเกณฑ์จะได้รับการคัดเลือกให้นำเสนอภายในงาน CYBERCONF 2027 ในรูปแบบ **Oral Presentation หรือ Poster Presentation** ตามประเภท ลักษณะ และความเหมาะสมของผลงาน โดยผลการพิจารณาอาจใช้ประกอบการคัดเลือกผลงานเพื่อรับรางวัลผลงานวิจัยดีเด่นตามหลักเกณฑ์ที่กำหนด

๑๑.๕ การเผยแพร่และต่อยอดผลงาน

ผลงานที่ผ่านกระบวนการพิจารณาโดยผู้ทรงคุณวุฒิ (**Peer Review**) ตามหลักเกณฑ์ที่กำหนดและได้รับการคัดเลือก จะได้รับโอกาสนำเสนอผลงานภายในงาน **CYBERCONF 2027: Cybersecurity Research & Innovation Forum** และได้รับการพิจารณาเผยแพร่ใน **Official Conference Proceedings** ตามหลักเกณฑ์ รูปแบบ และเงื่อนไขที่ผู้จัดงานกำหนด

นอกจากนี้ ผลงานที่ได้รับการคัดเลือก (**Selected Papers**) ซึ่งมีคุณภาพทางวิชาการและมีเนื้อหาสอดคล้องกับขอบเขตของวารสารหรือการประชุมวิชาการที่เกี่ยวข้อง อาจได้รับการเสนอชื่อเพื่อเข้าสู่กระบวนการพิจารณาต่อยอดและเผยแพร่ในช่องทางวิชาการ ดังนี้

๑) RMUTL Engineering Journal - TCI Tier 1

วารสารวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา สำหรับผลงานที่มีเนื้อหาสอดคล้องกับขอบเขตด้านวิศวกรรมศาสตร์ เทคโนโลยี วิศวกรรมคอมพิวเตอร์ (Computer Engineering) และสาขาที่เกี่ยวข้อง ทั้งนี้ การพิจารณาตีพิมพ์เป็นไปตามขอบเขต กระบวนการพิจารณาบทความ และเงื่อนไขการตีพิมพ์ของวารสาร

๒) Journal of Innovative Technology Research (JITR) - TCI Tier 2

สำหรับผลงานที่ได้รับการคัดเลือกและมีเนื้อหาสอดคล้องกับขอบเขตของวารสาร โดยการพิจารณาตีพิมพ์เป็นไปตามกระบวนการพิจารณาบทความ หลักเกณฑ์ และเงื่อนไขของวารสาร JITR

๓) The 31st International Computer Science and Engineering Conference (ICSEC 2027)

สำหรับผลงานที่ได้รับการคัดเลือกในระดับโดดเด่น (**Outstanding Selected Papers**) และมีศักยภาพในการต่อยอดสู่เวทีวิชาการระดับนานาชาติ ทั้งนี้ การส่งผลงานและการพิจารณารับเข้าร่วมหรือตีพิมพ์ให้เป็นไปตามขอบเขตของการประชุม (Scope) กระบวนการ Peer Review หลักเกณฑ์การส่งผลงาน (Submission Requirements) และเงื่อนไขที่ ICSEC 2027 กำหนด

ทั้งนี้ **การได้รับคัดเลือกหรือนำเสนอผลงานใน CYBERCONF 2027 มิได้ถือเป็นการรับรองการตีพิมพ์ในวารสารหรือการประชุมวิชาการข้างต้นโดยอัตโนมัติ** ผลงานที่ได้รับการเสนอชื่อจะต้องผ่านกระบวนการพิจารณาและเป็นไปตามหลักเกณฑ์ของวารสารหรือการประชุมวิชาการแต่ละแห่งอีกครั้ง

๑๒. รางวัลผลงานวิจัยดีเด่น CYBERCONF 2027

เพื่อส่งเสริมคุณภาพของผลงานวิชาการ สร้างแรงจูงใจแก่นักวิจัยและนักวิจัยรุ่นใหม่ ตลอดจนสนับสนุนการต่อยอดผลงานวิจัย เทคโนโลยี และนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ไปสู่การใช้ประโยชน์จริง **CYBERCONF 2027: Cybersecurity Research & Innovation Forum** กำหนดให้มีการพิจารณารางวัลผลงานวิจัยดีเด่น จำนวน **๕ ประเภทรางวัล** ดังนี้

ประเภทรางวัล	จุดเน้นในการพิจารณา
๑. Best Paper Award	ผลงานวิจัยที่มีคุณภาพทางวิชาการโดดเด่น มีความใหม่ ระเบียบวิธีวิจัยเหมาะสม ผลการศึกษาน่าเชื่อถือ และสร้างองค์ความรู้ที่มีคุณค่าต่อสาขาความมั่นคงปลอดภัยไซเบอร์
๒. Best Student Paper Award	ผลงานวิจัยดีเด่นที่มีนักศึกษาเป็นผู้เขียนหลักและผู้นำเสนอ เพื่อส่งเสริมนักวิจัยรุ่นใหม่และการพัฒนากำลังคนด้านความมั่นคงปลอดภัยไซเบอร์
๓. Best Applied Cybersecurity Research Award	งานวิจัยประยุกต์ที่สามารถเชื่อมโยงองค์ความรู้กับโจทย์หรือปัญหาจริง และมีหลักฐานการทดลอง การทดสอบ หรือการประยุกต์ใช้ที่ชัดเจน
๔. Best Innovation & Technology Award	ผลงานที่มีความโดดเด่นด้านนวัตกรรม เทคโนโลยี ต้นแบบ (Prototype) หรือการพิสูจน์แนวคิด (Proof of Concept: PoC) มีความใหม่ ความเป็นไปได้ทางเทคนิค และศักยภาพในการพัฒนาต่อยอด
๕. Best Research-to-Impact Award	ผลงานที่มีศักยภาพในการนำไปใช้แก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หรือภาคอุตสาหกรรม และมีโอกาสต่อยอดไปสู่การใช้งานจริงหรือเชิงพาณิชย์

การพิจารณารางวัลให้เป็นไปตามหลักเกณฑ์ วิธีการ และกระบวนการที่คณะกรรมการหรือคณะผู้ทรงคุณวุฒิของ CYBERCONF 2027 กำหนด โดยคำนึงถึงคุณภาพทางวิชาการ ความใหม่ ความถูกต้องของ

ระเบียบวิธี ความสำคัญของปัญหา ศักยภาพในการประยุกต์ใช้ และผลกระทบที่คาดว่าจะเกิดขึ้นตามลักษณะของแต่ละประเภทรางวัล

๑๓. กรอบระยะเวลาดำเนินงาน

ลำดับ	กิจกรรม	ระยะเวลา
๑	จัดทำประกาศ Call for Papers หลักเกณฑ์ แบบฟอร์ม และประสานคณะกรรมการ/Reviewer	๑ ตุลาคม ๒๕๖๙-๑๔ ตุลาคม ๒๕๖๙
๒	เปิดรับบทความวิชาการและผลงานวิจัย (Call for Papers)	๑๕ ตุลาคม ๒๕๖๙-๓๐ พฤศจิกายน ๒๕๖๙
๓	ตรวจสอบความครบถ้วนของเอกสารและความสอดคล้องกับ Research Tracks (ดำเนินการทยอยตรวจสอบระหว่างเปิดรับสมัคร)	๑๕ ตุลาคม ๒๕๖๙-๒ ธันวาคม ๒๕๖๙
๔	พิจารณากลั่นกรองผลงานโดยผู้ทรงคุณวุฒิ (Peer Review / Technical & Relevance Review)	๑ ธันวาคม ๒๕๖๙-๑๒ ธันวาคม ๒๕๖๙
๕	แจ้งผลการพิจารณาและข้อเสนอแนะสำหรับการปรับปรุงผลงาน	๑๔ ธันวาคม ๒๕๖๙-๑๕ ธันวาคม ๒๕๖๙
๖	ผู้เขียนปรับปรุงและส่งต้นฉบับฉบับสมบูรณ์ (Camera-ready Submission)	๑๖ ธันวาคม ๒๕๖๙-๒๕ ธันวาคม ๒๕๖๙
๗	ยืนยันการตอบรับและการนำเสนอผลงาน (Author Confirmation)	ภายใน ๒๘ ธันวาคม ๒๕๖๙
๘	จัดทำกำหนดการนำเสนอผลงาน (Conference Program) และรวบรวมต้นฉบับสำหรับ Official Conference Proceedings	๒๘ ธันวาคม ๒๕๖๙-๘ มกราคม ๒๕๗๐
๙	ประสานผู้นำเสนอ ตรวจสอบไฟล์นำเสนอ และเตรียมความพร้อมด้านสถานที่และระบบเทคนิค	๙ มกราคม ๒๕๗๐-๑๙ มกราคม ๒๕๗๐
๑๐	จัดงาน CYBERCONF 2027 (Oral / Poster Presentation)	๒๐ มกราคม ๒๕๗๐-๒๑ มกราคม ๒๕๗๐
๑๑	สรุปผลการจัดงาน เผยแพร่ผลงานตามเงื่อนไข และเชื่อมโยงโอกาสการต่อยอดงานวิจัย	ภายหลังการจัดงาน

๑๔. แนวทางการสร้างความร่วมมือ

ศวจ. จะประสานมหาวิทยาลัย สถาบันการศึกษา สถาบันวิจัย หน่วยงานภาครัฐ ภาคเอกชน สมาคมวิชาชีพ และเครือข่ายที่เกี่ยวข้อง เพื่อร่วมสนับสนุนการดำเนินงาน ดังนี้

- ประชาสัมพันธ์ Call for Papers และเชิญชวนส่งผลงานเข้าร่วม CYBERCONF 2027
- สนับสนุนนักวิจัย คณาจารย์ นักศึกษา ผู้เชี่ยวชาญ และบุคลากรที่เกี่ยวข้องให้ส่งผลงานและเข้าร่วมกิจกรรม
- เสนอชื่อผู้ทรงคุณวุฒิ นักวิจัย หรือผู้เชี่ยวชาญเพื่อร่วมทำหน้าที่ Reviewer
- อนุญาตให้ใช้ตราสัญลักษณ์ของหน่วยงานหรือสถาบันที่ให้การสนับสนุนในสื่อประชาสัมพันธ์ภายหลังได้รับอนุญาตจากเจ้าของตราสัญลักษณ์
- ร่วมเชื่อมโยงผลงานวิจัยและนวัตกรรมที่มีศักยภาพไปสู่ผู้ใช้ประโยชน์ ภาคอุตสาหกรรม หรือกลไกสนับสนุน ที่เกี่ยวข้อง

๑๕. ผลผลิตและผลลัพธ์ที่คาดว่าจะได้รับ

๑๕.๑ ผลผลิตที่คาดว่าจะได้รับ (Outputs)

๑) เกิดเวทีสำหรับการเผยแพร่ นำเสนอ และแลกเปลี่ยนองค์ความรู้ ผลงานวิจัย ผลงานวิชาการ เทคโนโลยี และนวัตกรรม ด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีที่เกี่ยวข้อง ภายใต้งาน Cybersec Asia x Thailand International Cyber Week 2027 ซึ่งเป็นพื้นที่เชื่อมโยงนักวิจัย นักวิชาการ นิสิต นักศึกษา ผู้เชี่ยวชาญ ภาครัฐ ภาคอุตสาหกรรม และผู้ประกอบการทั้งในประเทศและต่างประเทศ

๒) เกิดผลงานวิจัยและผลงานวิชาการที่ผ่านกระบวนการพิจารณากลั่นกรองตามหลักเกณฑ์ที่กำหนด และได้รับโอกาสนำเสนอภายในงาน รวมถึงได้รับการพิจารณาเผยแพร่ใน Official Conference Proceedings และต่อยอดสู่ช่องทางเผยแพร่ทางวิชาการที่เกี่ยวข้องตามหลักเกณฑ์และเงื่อนไขของแต่ละแห่ง

๑๕.๒ ผลลัพธ์ที่คาดว่าจะได้รับ (Outcomes)

๑) เกิดการพัฒนาและแลกเปลี่ยนองค์ความรู้และงานวิจัยที่ตอบสนองต่อสถานการณ์ภัยคุกคามโจทย์สำคัญของประเทศ และความท้าทายจากเทคโนโลยีเกิดใหม่ อาทิ AI, Quantum Technology, Cloud, Data Center, Digital Identity และ Autonomous Systems ซึ่งสามารถนำไปใช้เป็นฐานความรู้สำหรับการพัฒนาเทคโนโลยี นวัตกรรม และแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ในอนาคต

๒) เกิดการสร้างและขยายเครือข่ายความร่วมมือด้านการวิจัยและพัฒนา ระหว่างมหาวิทยาลัย สถาบันวิจัย หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภาคเอกชน ผู้ประกอบการ และเครือข่ายวิชาการทั้งในประเทศและต่างประเทศ พร้อมทั้งเพิ่มโอกาสในการเชื่อมโยงผลงานวิจัยไปสู่การทดสอบ การประยุกต์ใช้ และการพัฒนาต่อยอด

๓) เพิ่มโอกาสในการนำองค์ความรู้ ผลงานวิจัย เทคโนโลยี และนวัตกรรมไปใช้ประโยชน์จริง โดยเชื่อมโยงโจทย์และความต้องการของภาครัฐ ภาคอุตสาหกรรม และผู้ใช้ประโยชน์กับนักวิจัยและผู้พัฒนาเทคโนโลยี เพื่อสนับสนุนการต่อยอดในเชิงนโยบาย เศรษฐกิจ และสังคม

๔) สนับสนุนการยกระดับ Cybersec Asia x Thailand International Cyber Week ให้เป็นแพลตฟอร์มด้านองค์ความรู้ การวิจัย และนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาค และเป็นพื้นที่เชื่อมโยงความร่วมมือระหว่างภาครัฐ ภาควิชาการ ภาคอุตสาหกรรม ตลอดจนเครือข่ายระดับอาเซียนและนานาชาติ

๕) สนับสนุนบทบาทของ สกมช. ในการพัฒนาระบบนิเวศด้านการวิจัย เทคโนโลยี และนวัตกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศ ให้เกิดการเชื่อมโยงตั้งแต่การสร้างองค์ความรู้ การพัฒนางานวิจัย การนำเสนอและแลกเปลี่ยนผลงาน ไปจนถึงการนำไปประยุกต์ใช้และต่อยอดให้เกิดประโยชน์อย่างเป็นรูปธรรม

๑๖. การประชาสัมพันธ์

ประชาสัมพันธ์ผ่านเว็บไซต์และสื่อสังคมออนไลน์ของ สกมช. ช่องทางของงาน Cybersec Asia x Thailand International Cyber Week 2027 ตลอดจนมหาวิทยาลัย สถาบันวิจัย หน่วยงานภาครัฐ ภาคเอกชน สมาคมวิชาชีพ และเครือข่ายพันธมิตรที่ร่วมสนับสนุนกิจกรรม

๑๗. ผู้ประสานงาน

นางสาววรวรรณ ศรีศักดิ์ หัวหน้างานพัฒนาเครือข่ายวิจัย
ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ (ศวจ.)
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
ไปรษณีย์อิเล็กทรอนิกส์: research@ncsa.or.th
โทรศัพท์: ๐๒-๕๐๒-๗๘๒๓ ในวันและเวลาราชการ

CYBERCONF
Cybersecurity & Research Research & Innovation Forum

CYBERSEC ASIA X THAILAND INTERNATIONAL CYBER WEEK 2027

NCSA สกมช.

CALL FOR PAPERS
CYBERCONF 2027

Cybersecurity Research & Innovation Forum
เวทีวิชาการด้านความมั่นคงปลอดภัยไซเบอร์
เพื่อสังคมที่มั่นคง ปลอดภัย และยั่งยืน

PEOPLE
POLICY
TECHNOLOGY
TRUST

Research for a Safer Digital Society

20-21 มกราคม 2570

QSNCC ศูนย์สิริกิติ์
กรุงเทพมหานคร ประเทศไทย

RESEARCH | INNOVATION | COLLABORATION | A SAFER DIGITAL THAILAND

TOPICS OF INTEREST

1. **Cybersecurity, Cybercrime & Threat Intelligence**
   Cyber Defense, Network Security, SOC, Incident Respond, Malware, Vulnerability, Digital Forensics, Cybercrime, Fraud, Threat Intelligence
2. **AI Security & Intelligent Autonomous Systems**
   AI Security, LLM Security, Generative AI, Agentic AI, Adversarial AI, Deepfake, AI Governance, Autonomous Systems
3. **Quantum & Post-Quantum Security**
   Post-Quantum Cryptography, Quantum-safe Security, Cryptography, Crypto-agility, Quantum Resilience, Migration Strategy
4. **Cloud, Data Center & Resilient Digital Infrastructure**
   Cloud Security, Data Center Security, Secure & Green Data Center, Physical Security, Power Resilience, Certification & Assurance, Digital Infrastructure
5. **Critical Infrastructure, OT, IoT & Cyber-Physical Security**
   CII, OT/CIS, Energy, Telecom, Transport, Healthcare, Smart Infrastructure, IoT/Embedded Systems, Cyber-Physical Systems
6. **Digital Trust, Privacy, Governance & Cyber Resilience**
   Digital Identity, Zero Trust, Data Protection, Privacy, Cyber Resilience, Risk Management, Standards, Regulation, Digital Sovereignty, Cyber Diplomacy
7. **Cybersecurity Innovation & Applied Research**
   Prototype, Poc, Technology Validation, Cybersecurity Products & Services, Technology Transfer, Research Commercialization, Research-to-Market

ประเภทผลงานที่เปิดรับ (Submission Types)

A Full Research Paper
สำหรับผลงานวิจัยที่ดำเนินการแล้วเสร็จ มีผลการศึกษาที่สมบูรณ์

- **รูปแบบ:** Full Paper 6-10 หน้า
- **พิจารณา:** Peer Review
- **นำเสนอ:** Oral Presentation
- **กลุ่มเป้าหมาย:** นักวิจัย คณาจารย์ นักศึกษาระดับบัณฑิตศึกษา

B Applied Research / Technical Paper
สำหรับงานวิจัยประยุกต์ ผลการพัฒนาเทคโนโลยี กรณีศึกษา หรือ Technical Solution ที่สามารถนำไปประยุกต์ใช้ได้

- **รูปแบบ:** Extended Abstract / Technical Paper 3-5 หน้า
- **พิจารณา:** Technical & Relevance Review
- **นำเสนอ:** Oral หรือ Poster Presentation
- **กลุ่มเป้าหมาย:** นักวิจัย หน่วยงานภาครัฐ หน่วยงาน CII ภาคอุตสาหกรรม ผู้ประกอบการ และบริษัทเทคโนโลยี

รางวัลผลงานวิจัยดีเด่น CYBERCONF 2027
จำนวน 5 ประเภท

1. Best Paper Award
2. Best Student Paper Award
3. Best Applied Cybersecurity Research Award
4. Best Innovation & Technology Award
5. Best Research-to-Impact Award

การเผยแพร่ผลงาน

- RMUTL Engineering Journal — TCI Tier 1
- Journal of Innovative Technology Research (JITR) — TCI Tier 2
- ISESC 2027 The 31st International Computer Scinnce and Engineering Conference (ISEC 2027)

หมายเหตุ:
- การเผยแพร่ผลงานในแต่ละช่องทางเป็นไปตามขอบเขต (Scope) กระบวนการพิจารณา การคัดเลือก มาตรฐาน และเงื่อนไขของแต่ละวารสาร/การประชุม
- การได้รับคัดเลือกให้นำเสนองานใน CYBERONF 2027 มิได้หมายความว่าจะได้รับการตีพิมพ์ในวารสารหรือได้รับการคัดเลือกไป ICSEC 2027 โดยอัตโนมัติ

กำหนดการสำคัญ

เปิดรับบทความวิชาการ	พิจารณาผลงาน (Peer Review)	แจ้งผลการพิจารณา	ส่งต้นฉบับสมบูรณ์ (Camera-ready)	ยืนยันการนำเสนอผลงาน	จัดงาน CYBERCONF 2027
15 ต.ค. - 30 พ.ย. 69	1 - 12 ธ.ค. 69	14 - 15 ธ.ค. 69	16 - 25 ธ.ค. 69	ภายใน 28 ธ.ค. 69	20 - 21 ม.ค. 70

SUBMIT YOUR PAPER
HTTPS://AICYBER.RMUTL.AC.TH/CYBERCONF2027/

สอบถามรายละเอียดเพิ่มเติมได้ที่

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ สกมช.
ผู้ประสานงาน: นางสาววรวรรณ ศรีศักดิ์ หัวหน้างานพัฒนาเครือข่ายวิจัย
อีเมล: research@ncsa.or.th
โทรศัพท์: 02-502-7823 ในวันและเวลาราชการ

TOGETHER FOR A MORE CYBER RESILIENT THAILAND