แผนการปฏิบัติการ

ด้านความมั่นคงปลอดภัยทางไซเบอร์

มหาวิทยาลัยมหาสารคาม พ.ศ.2566-2569

สารบัญ

ส่วนที่ 1 บทนำ

1.1 หลักการและเหตุผล

การใช้บริการอินเทอร์เน็ตได้ขยายตัวในทุกด้านทั้งจำนวนผู้ใช้บริการ จำนวนเครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ในการเชื่อมต่อกับอินเทอร์เน็ต ตลอดจนมีการพัฒนาแอปพลิเคชันหรือบริการใหม่ ๆ เกิดขึ้นอยู่ตลอดเวลา ในปัจจุบันยังมีการนำเครือข่ายการสื่อสารของอินเทอร์เน็ตไปใช้ให้เกิดประโยชน์มากที่สุด เพื่อให้เกิดการสื่อสารที่เป็นหนึ่งเดียว ทั้งการส่งภาพ ภาพเคลื่อนไหว เสียง และอื่น ๆ มหาวิทยาลัยมหาสารคามโดยสำนักคอมพิวเตอร์ได้ให้บริการอินเทอร์เน็ตทั้งในเขตพื้นที่ขามเรียง (ม.ใหม่) พื้นที่ในเมือง (ม.เก่า) พื้นที่นาสีนวนและในเขตพื้นที่นาดูน โดยมีเกตเวย์ในการเชื่อมต่ออินเทอร์เน็ตที่ห้องศูนย์กลางข้อมูลจำนวน 2 เส้นทาง ประกอบด้วยการเชื่อมต่อผ่านเครือข่าย UniNet และการเชื่อมต่อผ่านบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) โดยมีอัตราการรับ-ส่งข้อมูลเส้นทางละ 10 Gbps แสดงให้เห็นว่าการให้บริการอินเทอร์เน็ตของมหาวิทยาลัยมหาสารคามมีพื้นที่กว้างขวาง มีจุดให้บริการทั้งเครือข่ายใช้สายสัญญาณและเครือข่ายไร้สาย (ไวไฟ) เป็นจำนวนมาก นอกจากนั้นในปัจจุบันมหาวิทยาลัยมีผู้ใช้บริการจำนวนมากเช่นกัน ทั้งบุคลากรและนิสิตระดับปริญญาตรีและระดับบัณฑิตศึกษา ประกอบกับเทคโนโลยีทางด้านคอมพิวเตอร์และอุปกรณ์การสื่อสารข้อมูลมีการพัฒนาอย่างรวดเร็ว แพร่หลาย และมีราคาถูกลง ทำให้ผู้ใช้บริการสามารถใช้อุปกรณ์ต่าง ๆ ในการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตหลากหลายมากขึ้น ทั้งแล็ปท็อป แท็บเล็ต และสมาร์ตโฟน เมื่อมีการใช้บริการอย่างแพร่หลายทุกพื้นที่ของมหาวิทยาลัย และมีผู้ใช้บริการเป็นจำนวนมาก ทำให้มีภัยคุกคามต่าง ๆ กับผู้ใช้บริการอินเทอร์เน็ตจำนวนมาก และมีความเสี่ยงทางไซเบอร์ (Cyber Risk) เกิดขึ้นทั้งกับข้อมูลของคณะ/หน่วยงาน หรือกับข้อมูลส่วนบุคคล มหาวิทยาลัยจึงมีความจำเป็นที่จะต้องมีนโยบายและแผนปฏิบัติการทางด้านความมั่นคงไซเบอร์ (Cybersecurity) เพื่อสร้างความมั่นใจและแนวปฏิบัติที่ดีสำหรับการจัดการความมั่นคงทางไซเบอร์ให้กับคณะ/หน่วยงาน บุคลากร และนิสิต มหาวิทยาลัยมหาสารคาม

ความมั่นคงทางไซเบอร์หมายถึงการป้องกันฮาร์ดแวร์ ซอฟต์แวร์ แหล่งข้อมูลที่เชื่อมต่อและจัดเก็บบนอินเทอร์เน็ต (Thakur & Pathan, 2020, p. 31) นอกจากนั้นยังมีรวมถึงการป้องกันข้อมูลที่จัดเก็บ ส่งต่อ และประมวลผลในระบบเครือข่ายของคอมพิวเตอร์ อุปกรณ์ดิจิทัลอื่น ๆ อุปกรณ์เครือข่ายและและสายสัญญาณในการส่ง รวมถึงอินเทอร์เน็ต โดยการคุ้มครองจะครอบคลุมถึงการรักษาความลับ ความคงสภาพ ความพร้อมใช้งาน ความถูกต้อง และการตรวจสอบได้ วิธีการป้องกันรวมถึงนโยบายและขั้นตอนขององค์กร เช่นเดียวกับวิธีการทางเทคนิค เช่น การเข้ารหัสและโพรโทคอลการสื่อสารที่มีความปลอดภัย (Stallings, 2023, p. 23) ความมั่นคงทางไซเบอร์เป็นการศึกษาในระดับกว้าง ที่ครอบคลุมเทคโนโลยีและแนวทางการป้องกันคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ และข้อมูลจากอันตรายต่าง ๆ วิทยาการความมั่นคงทางไซเบอร์มี

ความสำคัญในแง่ของการทำความเข้าใจ การพัฒนา และแนวทางปฏิบัติที่ดีที่สุดของความปลอดภัยบนโลกไซเบอร์ เพราะว่าปัญหาที่เกิดขึ้นสร้างผลกระทบในแนวกว้างทั้งทางด้านธุรกิจ สังคม และส่วนบุคคล ในปัจจุบันภัยคุกคามบนโลกไซเบอร์ได้สร้างผลกระทบและกระจายไปทั่วโลก มีความซับซ้อนมากขึ้นและมีความยุ่งยากในการตรวจสอบและป้องกัน

การกำหนดมาตรการด้านความมั่นคงไซเบอร์ไว้ในกฎหมายหรือพระราชบัญญัติต่าง ๆ ที่เกี่ยวข้อง เช่น พ.ร.บ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA และมาตรการอื่น ๆ โดยเน้นให้ความสำคัญในด้านมาตรการป้องกันและลดความเสี่ยง การสร้างผู้เชี่ยวชาญด้านความมั่นคง การกำหนดความผิดและการลงโทษ ซึ่งอาจครอบคลุมเพียงบางมิติของการรักษาความมั่นคงทางไซเบอร์เท่านั้น จึงมีความจำเป็นต้องยกระดับความเข้มแข็งเพื่อเตรียมความพร้อมของประเทศในด้านดังกล่าวให้ครอบคลุมถึงมิติของการเฝ้าระวังภัยคุกคาม หรือการดำเนินการใด ๆ ที่จำเป็นเมื่อถูกโจมตีหรือเกิดวิกฤติต่อความมั่นคงทางไซเบอร์ ตลอดจนมาตรการที่ทำงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง เมื่อถูกโจมตีหรือเกิดวิกฤติทางไซเบอร์ขึ้น ในการประชุมคณะรัฐมนตรี (ครม.) เมื่อวันที่ 23 กันยายน 2565 ได้มีมติเห็นชอบร่างนโยบายและแผนปฏิบัติการว่าด้วยความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565-2570 ที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ได้จัดทำและเสนอมา เพื่อทำให้บริการที่สำคัญของประเทศไทยมีความมั่นคงปลอดภัยไซเบอร์ และมีความยั่งยืนทางเศรษฐกิจและสังคม โดยร่างนโยบายและแผนปฏิบัติการฯ เป็นการดำเนินการตามบทบัญญัติมาตรา 9(1) และมาตรา 9(3) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่จะทำให้บรรลุวัตถุประสงค์ของพระราชบัญญัติดังกล่าว

แผนการปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม พ.ศ.2566-2569 ร่างขึ้นโดยอ้างอิงจากระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Management Systems: ISMS) ตามมาตรฐาน ISO/IEC 27001:2013 และกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากล NIST Cybersecurity Framework เพื่อสนับสนุนแผนพัฒนาการศึกษามหาวิทยาลัยมหาสารคาม ฉบับที่ 13 (พ.ศ. 2565-2569) และแผนการพัฒนาดิจิทัลเพื่อเป็น Smart University ของมหาวิทยาลัยมหาสารคาม ระยะ 5 ปี (พ.ศ.2565-2569) ซึ่งจะทำให้มหาวิทยาลัยมหาสารคามมีแผนปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติ และเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยมหาสารคาม โดยกรอบ

แนวทางดำเนินการมีเป้าหมายดังนี้

1. กำหนดวัตถุประสงค์การดำเนินงานสอดคล้องตามพ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2. กำหนดแนวทางการดำเนินการตามมาตรฐาน ISO/IEC 27001:2013 และกรอบการทำงานของ NIST (NIST Cybersecurity Framework)

3. จัดทำนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม

4. เผยแพร่แผนการปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ให้กับคณะ/หน่วยงานได้รับทราบเพื่อนำไปปรับใช้และสามารถแก้ไขปัญหาที่เกิดขึ้นได้

5. พัฒนาและปรับปรุงกระบวนงานตามนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม

6. จัดการองค์กร โครงสร้าง อำนาจ หน้าที่ ขีดความสามารถในการป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยทางไซเบอร์

7. กำหนดระบบบริหารจัดการภายในมหาวิทยาลัยในแต่ละระดับให้ชัดเจน

8. เสริมสร้างและพัฒนาระบบการรายงานในสถานการณ์ฉุกเฉิน

9. ควบคุม กำกับ ติดตามและประเมินผล อย่างต่อเนื่อง

10. ยกระดับแนวความคิดในการปกป้องโครงสร้างพื้นฐานสำคัญทางดิจิทัลของมหาวิทยาลัย

11. พัฒนาการป้องกันแก้ไขปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงทางไซเบอร์

12. สร้างความตระหนักรู้ให้แก่คณะ/หน่วยงาน บุคลากร และนิสิตของมหาวิทยาลัย

13. พัฒนาศักยภาพบุคลากร นิสิต และเทคโนโลยีดิจิทัลให้ทันสมัย เพื่อให้มีความพร้อมในการรองรับการถูกโจมตีหรือเกิดวิกฤติต่อความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัย

ดังนั้นเพื่อการกำหนดทิศทาง หลักการและแนวทางด้านแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์ที่ครอบคลุมในทุกมิติ สำนักคอมพิวเตอร์ มหาวิทยาลัยมหาสารคามจึงได้ดำเนินการจัดทำแผนการปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม พ.ศ.2566-2569 เพื่อให้ผู้ปฏิบัติงาน คณะหน่วยงานภายในมหาวิทยาลัยใช้ดำเนินการตามอย่างเคร่งครัดต่อไป

1.2 วัตถุประสงค์

1.2.1 เพื่อกำหนดกรอบ ทิศทาง แนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม

1.2..2 เพื่อกำหนดมาตรการ นโยบาย และกลไกในการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และตอบโต้ในภาวะฉุกเฉินเพื่อแก้ไขปัญหา

1.2.3 เพื่อสร้างความมั่นใจให้กับนิสิต บุคลากรและผู้เกี่ยวข้อง ในการได้รับการปกป้องจากภัยคุกคามทางไซเบอร์ในทุกรูปแบบ

1.2.4 เพื่อเป็นแนวทางในการดำเนินงานของมหาวิทยาลัยมหาสารคาม ในการพัฒนาให้ความรู้แก่บุคลากรทางไซเบอร์และผู้ใช้งานทั่วไป ได้รับการปลูกฝังให้ตระหนักในการร่วมมือกันป้องกันภัยไซเบอร์

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 มหาวิทยาลัยมีเครื่องมือและกลไกในการป้องกัน เฝ้าระวังและติดตามภัยคุกคามทางไซเบอร์

1.3.2 หน่วยงานภายในมหาวิทยาลัยมหาสารคามมีแนวทางการดำเนินงานในการป้องกันและแก้ไขปัญหาที่จะเกิดขึ้นเมื่อเกิดภัยคุกคามทางไซเบอร์

1.3.3 นิสิต บุคลากรและผู้เกี่ยวข้อง มีความเชื่อมั่นในการใช้บริการระบบอินเทอร์เน็ตของมหาวิทยาลัยมหาสารคาม

ส่วนที่ 2 นโยบายและกฎหมายที่เกี่ยวข้อง

2.1 ยุทธศาสตร์ชาติ (พ.ศ.2561-2580)

สำหรับการจัดทำแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัยมหาสารคาม ได้ศึกษายุทธศาสตร์ชาติ (พ.ศ. 2561 - 2580) ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560 – 2564) (National Cyber security Strategy 2517 - 2021) แผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อเป็นกรอบแนวทางการดำเนินงานของมหาวิทยาลัยมหาสารคามรวมทั้งได้กล่าวถึงสถานการณ์ด้านกฎหมายในประเทศไทย และการจัดตั้งองค์กรกำกับดูแลด้านไซเบอร์ของประเทศไทย โดยยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 – 2580) เป็นยุทธศาสตร์ชาติของประเทศไทยซึ่งจะต้องนำไปสู่การปฏิบัติเพื่อให้ประเทศไทยบรรลุวิสัยทัศน์ “ประเทศมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามปรัชญาของเศรษฐกิจพอเพียง” นำไปสู่การพัฒนาให้คนไทยมีความสุข และตอบสนองต่อการบรรลุซึ่งผลประโยชน์แห่งชาติ ในการที่จะพัฒนาคุณภาพชีวิตสร้างรายได้ระดับสูงเป็นประเทศพัฒนาแล้ว และสร้างความสุขของคนไทย สังคมมีความมั่นคง เสมอภาค เป็นธรรมและมีระบบเศรษฐกิจที่มีศักยภาพและสามารถแข่งขันได้ ประกอบด้วย 6 ยุทธศาสตร์
ได้แก่

1. ยุทธศาสตร์ชาติด้านความมั่นคง
2. ยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน
3. ยุทธศาสตร์ชาติด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์
4. ยุทธศาสตร์ชาติด้านการสร้างโอกาสและความเสมอภาคทางสังคม
5. ยุทธศาสตร์ชาติด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม
6. ยุทธศาสตร์ชาติด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

2.2 ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560 – 2564)

สำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี ได้จัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560 – 2564) เพื่อเป็นแนวนโยบายระดับชาติฉบับแรกของประเทศไทยในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้รับกับสภาพสังคมที่เข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบในอนาคต โดยมีเป้าหมายหลักคือการสร้างความพร้อมของประเทศไทย ในการรับมือกับภัยคุกคามทางไซเบอร์ที่จะทวีความรุนแรงมากขึ้น ให้ครอบคลุมรอบด้านตามสภาวะแวดล้อม เอื้ออำนวย เสริมขีดความสามารถของไทยให้มีความเข้มแข็งยิ่งขึ้น โดยมุ่งเน้นการมีกลไกกลางในการบริหารจัดการการรักษาความมั่นคงปลอดภัย

ไซเบอร์แห่งชาติ การปกป้องโครงสร้างสาธารณูปโภคพื้นฐาน การสร้างความตระหนักในทุกภาคส่วนและสร้างความร่วมมือกับต่างประเทศ โดยมีเป้าหมายเชิงยุทธศาสตร์ คือ ประเทศเทศไทยมีความมั่นคงปลอดภัยและมีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ ประกอบด้วย 2 ตัวชี้วัด คือ 1. ระดับความพร้อมของไทยในการป้องกันความเสี่ยงจากการโจมตีด้านไซเบอร์ที่สอดคล้องกับหลักสากล และ 2. ระบบป้องกันทางไซเบอร์ที่มีประสิทธิภาพ สามารถปกป้องข้อมูลอิเล็กทรอนิกส์ของรัฐบาล ตลอดจนโครงสร้างพื้นฐานสำคัญทางไซเบอร์ และมีการกำหนดกลยุทธ์เพื่อให้การดำเนินงานทั้งหมด 6 กลยุทธ์ ได้แก่

กลยุทธ์ที่ 1 พัฒนาขีดความสามารถทั้งองค์กรภาครัฐ ทั้งฝ่ายทหาร พลเรือนและตำรวจ และภาคส่วนต่าง ๆ ภายในประเทศ เพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ ตลอดจนรองรับสังคมดิจิทัล

กลยุทธ์ที่ 2 พัฒนากรอบความร่วมมือระหว่างประเทศและอาเซียนเพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

กลยุทธ์ที่ 3 พัฒนาทรัพยากรมนุษย์ องค์ความรู้ และความตระหนักรู้ถึงความสำคัญ ของภัยคุกคามความมั่นคงทางไซเบอร์

กลยุทธ์ที่ 4 ปกป้อง ป้องกัน ภัยคุกคามทางไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยทางไซเบอร์ โดยบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ และเสริมสร้างเครือข่ายความร่วมมือกับทุกภาคส่วนทั้งภายในและภายนอกประเทศ

กลยุทธ์ที่ 5 พัฒนาการบังคับใช้กฎหมาย ระเบียบต่าง ๆ เพื่อความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์

กลยุทธ์ที่ 6 ส่งเสริมการพัฒนาขีดความสามารถขององค์กรทุกภาคส่วน/บุคลากรที่เกี่ยวข้อง ให้มีความรู้ ความชำนาญด้านไซเบอร์อย่างต่อเนื่อง

พร้อมทั้งกำหนดประเด็นยุทธศาสตร์เพื่อเป็นกรอบการดำเนินงานที่ใช้กับทุกภาคส่วน ทั้งภาครัฐ ภาคธุรกิจ และภาคประชาชน โดยเน้นความสมดุลระหว่างสิทธิเสรีภาพของประชาชนและการใช้อำนาจของรัฐเชิงนโยบายในการควบคุมและรักษาความสงบเรียบร้อยของสังคม และเพื่อให้บรรลุตามเป้าหมายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560 - 2564) และบรรลุวิสัยทัศน์ ที่ได้กำหนดไว้ว่า ไซเบอร์สเปซของไทยมีความมั่นคงปลอดภัย ทุกภาคส่วนมั่นใจความพร้อมรับมือกับภัยคุกคามทางไซเบอร์และร่วมมือกันใช้ไซเบอร์อย่างสร้างสรรค์ เพื่อส่งเสริมความมั่นคงทางเศรษฐกิจและคุณภาพชีวิตที่ดี ได้กำหนดประเด็นยุทธศาสตร์ไว้ 8 ประเด็นยุทธศาสตร์ ดังนี้

ประเด็นยุทธศาสตร์ที่ 1 : เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

เป้าหมาย

1. รัฐบาลให้ความสำคัญและสนับสนุนการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

2. ภาคธุรกิจและประชาชนมั่นใจในการใช้เทคโนโลยีดิจิทัล อินเทอร์เน็ตและไซเบอร์สเปซที่ได้มาตรฐาน ทั้งจากการใช้บริการภาครัฐ ภาคธุรกิจและส่วนบุคคล

แนวทางการดำเนินการ

1. ระดับนโยบายให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สนับสนุนการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

2. พัฒนาโครงสร้างองค์กรในภาครัฐ เพื่อรองรับสังคมดิจิทัลและรับมือภัยคุกคามทางไซเบอร์เพื่อเสริมสร้างความไว้วางใจแก่ภาคส่วนต่าง ๆ ที่ติดต่อประสานงานกับรัฐ

3. ส่งเสริมการใช้เทคโนโลยีดิจิทัลและอินเทอร์เน็ต เพื่อการบริการประชาชนของหน่วยงานรัฐและประชาสัมพันธ์เชิงรุกให้ประชาชนรับทราบและมั่นใจในการใช้บริการ ของหน่วยงานของรัฐ

4. ส่งเสริมให้ภาครัฐมีความโปร่งใส โดยใช้เทคโนโลยีและดำเนินกิจกรรมทางไซเบอร์โดยคำนึงถึงหลักการคุ้มครองสิทธิและเสรีภาพ ตลอดจนความเป็นส่วนตัวของผู้ใช้บริการออนไลน์ของภาครัฐ

5. สร้างความเชื่อมั่นและความไว้วางใจในภาคส่วนต่าง ๆ นอกเหนือจากภาครัฐ โดยการเปิดโอกาสและจัดหาช่องทางให้ประชาชนเข้ามามีส่วนร่วมกับหน่วยงานของรัฐ ในการพัฒนา ปรับปรุงเทคโนโลยีและการดำเนินกิจกรรมทางไซเบอร์ เพื่อให้ตรงตามความต้องการและวัตถุประสงค์ของ ผู้รับบริการ

6. ส่งเสริมให้ภาคเอกชนในธุรกิจสาขาต่าง ๆ ในทุกระดับดำเนิน ธุรกิจโดยใช้เทคโนโลยีดิจิทัล อินเทอร์เน็ต และไซเบอร์สเปซในวงกว้างและได้มาตรฐาน โดยประชาสัมพันธ์เชิง รุกและขอความร่วมมือจากภาคเอกชน

ประเด็นยุทธศาสตร์ที่ 2 : ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบ สารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

เป้าหมาย

1. ประเทศไทยมีการบูรณาการการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

2. ประเทศไทยมีหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ และมีการกำหนดบทบาทและหน้าที่หน่วยงานต่าง ๆ ของรัฐอย่างชัดเจน เพื่อดูแลการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศทั้งของภาครัฐและเอกชน

3. มีการทำงานขององค์กรต่าง ๆ ในรูปแบบที่สามารถทำงานที่พร้อมรับมือกับภัยคุกคามทางไซเบอร์ในแบบ CERT มากขึ้น

แนวทางการดำเนินการ

1. จัดทำกรอบนโยบาย/ยุทธศาสตร์ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 สำหรับการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและทบทวนประเมินผลการดำเนินการตามนโยบายเพื่อการปรับปรุงนโยบายให้ทันกับสถานการณ์ที่เปลี่ยนไป

2. ให้มีการจัดตั้งหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ เพื่อทำหน้าที่เป็นศูนย์กลางระดับนโยบายที่ขึ้นตรงต่อนายกรัฐมนตรี โดยเป็นศูนย์กลางด้านความมั่นคงปลอดภัยไซเบอร์และประสานการปฏิบัติ ทั้งในด้านการประสานงาน เฝ้าระวัง การ ตอบสนอง บริหารจัดการภัยคุกคามทางไซเบอร์ สร้างความตระหนักตลอดจนประสานความร่วมมือทั้งในและต่างประเทศ และส่งเสริมการพัฒนาขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานต่าง ๆ โดย อาจพิจารณาจัดตั้งหน่วยปฏิบัติขึ้นเพื่อสนับสนุนการดำเนินงานตามความเหมาะสม

3. จัดทำรายงานการเตรียมความพร้อมของหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศทั้งของภาครัฐและเอกชน พร้อมจัดลำดับความสำคัญ เพื่อประกอบการจัดทำแผนปฏิบัติการและแผนเผชิญเหตุ

4. กำหนดบทบาทและหน้าที่ของหน่วยงานต่าง ๆ ของรัฐ ในด้าน การปกป้องโครงสร้างพื้นฐานสำคัญที่มีการบริหารจัดการด้วยระบบสารสนเทศให้มีความชัดเจน เพื่อการรับมือภัย คุกคามทางไซเบอร์ทั้งในยามปกติ ยามเกิดเหตุ การฟื้นตัว และฟื้นฟูหลังเกิดเหตุ รวมทั้งการเยียวยา แก้ไข ผลกระทบ รวมทั้งมีกลไกประสานความร่วมมือกับภาคเอกชนและผู้มีส่วนเกี่ยวข้องเพื่อปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศของไทยจากภัยคุกคามทางไซเบอร์

5. ส่งเสริมการจัดทำแผนการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศทั้งในภาครัฐและเอกชน โดยให้แต่ละองค์กรยึดถือหลักการปกป้อง โครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศของหน่วยงานโดยอาศัยศักยภาพของหน่วยงาน และในกรณีที่สถานการณ์ยกระดับหรือเป็นเหตุฉุกเฉินที่เกินความสามารถของหน่วยงาน สามารถประสานขอความสนับสนุนได้ทันต่อสถานการณ์

6. ส่งเสริมการจัดการฝึกเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ เพื่อเตรียมพร้อมการรับมือกับสถานการณ์ทางไซเบอร์ในรูปแบบต่าง ๆ รวมทั้งในสภาวะวิกฤติ

7. จัดทำร่างและปรับปรุงกฎหมาย ระเบียบปฏิบัติ และข้อกำหนดเพื่อกำกับและวางกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณากำหนดบทคุ้มครองและบทลงโทษเหมาะสม

8. พัฒนาศักยภาพของบุคลากรในภาครัฐผ่านการศึกษา ฝึกอบรม ในรูปแบบต่าง ๆ และส่งเสริมการถ่ายทอดความรู้ภายในภาครัฐหรือระหว่างภาครัฐกับเอกชน ตลอดจนให้ ความสำคัญกับการพัฒนาตำแหน่งงานในภาครัฐที่สนับสนุนการเติบโตของบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสม เพื่อเป็นการรักษาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้อยู่ในระบบราชการ

9. พัฒนาศักยภาพการวิจัยและพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนแสวงหาความร่วมมือกับเอกชนทั้งในและต่างประเทศ เพื่อสามารถเข้าถึงแหล่งเทคโนโลยีและแหล่งเงินทุน ตลอดจนการพัฒนาตลาดสำหรับอุตสาหกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย เพื่อนำไปสู่การลดการพึ่งพาจากต่างประเทศ

10. ส่งเสริมการมีส่วนร่วมของภาคเอกชนอย่างจริงจังในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในด้านการพัฒนาองค์ความรู้และเทคโนโลยี การพัฒนาบุคลากร การรักษาความ มั่นคงปลอดภัยเพื่อยกระดับขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศแบบองค์รวม

11. พัฒนามาตรฐานและกระตุ้นให้มีกลไกการตรวจสอบประเมินมาตรฐานความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศ

12. ส่งเสริมให้มีการทำงานด้วยการปรับใช้มาตรการทางเทคนิคในลักษณะการทำงานแบบศูนย์ประสานความมั่นคงปลอดภัยทางไซเบอร์ หรือ CERT โดยเฉพาะอย่างยิ่ง ในกลุ่มโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อให้มีการประสานการทำงานรับมือกับภัยคุกคามทางไซเบอร์ ในทางปฏิบัติให้มีความเข้มแข็งมากยิ่งขึ้น

ประเด็นยุทธศาสตร์ที่ 3 : ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

เป้าหมาย

1. มีการวิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ทันสมัย ครอบคลุมรอบด้าน ต่อเนื่องและถูกต้องแม่นยำเพื่อประโยชน์ในการตัดสินใจทางนโยบายและปฏิบัติที่เหมาะสม

2. กองทัพและหน่วยงานความมั่นคงที่เกี่ยวข้องมีความพร้อมรับมือภัยคุกคามทางไซเบอร์ทั้งในรูปแบบเดิมและภัยคุกคามในรูปแบบใหม่ ๆ

3. มีแผนเผชิญภัยคุกคามทางไซเบอร์เมื่อเกิดสถานการณ์วิกฤติทางไซเบอร์ระดับชาติหรือสงครามไซเบอร์

แนวทางการดำเนินการ

1. ศึกษา ติดตาม และวิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องอย่างสม่ำเสมอ ทั้งภัยคุกคามในรูปแบบเดิมและรูปแบบใหม่ เพื่อทราบถึงแนวโน้มความเป็นไปได้ที่จะเกิดภัยคุกคาม รวมถึงเป็นประโยชน์ต่อการหาทางป้องกันไม่ให้เกิดเหตุหรือลดความเสียหายให้น้อยลงมากที่สุด

2. หน่วยงานความมั่นคงที่เกี่ยวข้องพิจารณาจัดทำนโยบาย/ยุทธศาสตร์เพื่อรับมือกับภัยคุกคามทางไซเบอร์และบริหารจัดการการเก็บรักษาข้อมูล ป้องกันการโจมตี หรือเจาะระบบ การใช้เครื่องมือทางไซเบอร์เพื่อสร้างความขัดแย้ง รวมทั้งประเมินสถานการณ์และทบทวนนโยบาย/ยุทธศาสตร์ด้านไซเบอร์ให้ทันสมัย

3. กำหนดบทบาทให้กองทัพดูแลรับผิดชอบการป้องกันประเทศในมิติทางไซเบอร์และเป็นฝ่ายสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อได้รับการมอบหมายจากรัฐบาล โดยเฉพาะเมื่อเกิดสถานการณ์วิกฤติทางไซเบอร์ระดับชาติหรือสงครามไซเบอร์

ประเด็นยุทธศาสตร์ที่ 4 : เสริมสร้างระบบเศรษฐกิจดิจิทัล

เป้าหมาย

1. ประเทศไทยเปลี่ยนผ่านเข้าสู่เศรษฐกิจดิจิทัลอย่างราบรื่นและมีความยั่งยืน

2. มีการใช้เทคโนโลยีดิจิทัลในวงกว้างมากขึ้นในภาคเอกชน

3. มียุทธศาสตร์/แผนงาน กฎระเบียบที่มีประสิทธิภาพ เหมาะสมต่อระบบเศรษฐกิจดิจิทัลได้มาตรฐาน และเอกชนมีส่วนร่วม

แนวทางการดำเนินการ

1. ส่งเสริมการพัฒนาขีดความสามารถหรือการดำเนินการที่สนับสนุนต่อการเปลี่ยนผ่านสู่เศรษฐกิจดิจิทัลอย่างสมดุล ราบรื่น คุณภาพและนำไปสู่เศรษฐกิจดิจิทัลที่ยั่งยืน

2. สนับสนุนการมีส่วนร่วมของภาคเอกชน ในการส่งเสริมเศรษฐกิจดิจิทัลกับภาครัฐ ทั้งในกลุ่มผู้ที่ใช้เทคโนโลยีดิจิทัลเพื่อดำเนินธุรกิจอยู่แล้ว และส่งเสริมการใช้เทคโนโลยีดิจิทัลในวงกว้าง

3. พัฒนา ปรับปรุงยุทธศาสตร์ แผนหรือแผนงานตลอดจนกฎหมายระเบียบปฏิบัติที่เหมาะสมสอดคล้องและเอื้ออำนวยต่อเศรษฐกิจดิจิทัล พร้อมทั้งมีการประเมินผลและทบทวนอย่างสม่ำเสมอโดยเน้นการมีส่วนร่วมของภาคเอกชนในกระบวนการจัดทำยุทธศาสตร์แผนหรือแผนงานดังกล่าว

ประเด็นยุทธศาสตร์ที่ 5 : สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เป้าหมาย

1. ประชาชนทั่วไปทุกระดับ ทุกเพศและวัยที่เป็นผู้ใช้อินเทอร์เน็ตมีความตระหนักถึงภัยคุกคามทางไซเบอร์ และมีความรู้เรื่องการรักษาความปลอดภัยทางไซเบอร์

2. รัฐ ภาคเอกชน และประชาสังคมร่วมมือกันในการรักษาความมั่นคงปลอดภัยไซเบอร์

3. ช่องทาง/กลไกการสื่อสารแนวนโยบายสู่การปฏิบัติในภาคเอกชนและภาคประชาสังคม

แนวทางการดำเนินการ

1. ส่งเสริมการเผยแพร่ข้อมูลข่าวสารแก่ทุกภาคส่วนโดยทั่วถึง ผ่านสื่อและกลไกต่าง ๆ ของภาครัฐ ภาคเอกชน และภาควิชาการ เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์และความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อการใช้เทคโนโลยีดิจิทัลและการดำเนินกิจกรรมทางไซเบอร์ได้อย่างปลอดภัยและเกิดประโยชน์ รวมทั้งส่งเสริมความร่วมมือด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ในรูปแบบการรวมกลุ่ม ทั้งในระดับบุคคลและองค์กร

2. ส่งเสริมความร่วมมือกับสถาบันวิจัยและสถาบันการศึกษาต่างๆ ในการแลกเปลี่ยนความรู้ การวิจัยร่วมกันและ/หรือการนำเสนองานวิจัย ตลอดจนการจัดทำคู่มือเผยแพร่ ความรู้เกี่ยวข้องกับด้านไซเบอร์ เช่น มหาวิทยาลัย สถาบันวิชาการ เป็นต้น

3. ส่งเสริมและพัฒนาหลักสูตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในการศึกษาตามระบบตั้งแต่ขั้นพื้นฐาน ทั้งสายสามัญและอาชีวะ โดยให้เนื้อหาของหลักสูตร มีความแตกต่างกันไปในแต่ละระดับการศึกษา

4. ส่งเสริมการให้ความรู้ด้านการรักษาความมั่นคงปลอดภัย ทางไซเบอร์แก่ประชาชนผู้ใช้อินเทอร์เน็ตทั่วไป ผู้สูงอายุ เด็ก สตรีและเยาวชน ชุมชน ท้องถิ่น โดยร่วมมือกับ สถานศึกษา องค์การบริหารส่วนท้องถิ่นและหน่วยงานที่เกี่ยวข้อง เพื่อเผยแพร่ความรู้และสร้างความตระหนัก อย่างเป็นระบบและต่อเนื่อง

5. ส่งเสริมและประสานความร่วมมือระหว่างรัฐกับเอกชนและภาคประชาสังคม เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในลักษณะองค์กรรวมที่มีความเข้มแข็ง โดยจัดให้มีกลไกและช่องทางการสื่อสารระหว่างกัน เพื่อประโยชน์ในการทำความเข้าใจในแนวนโยบายจากรัฐสู่เอกชน และภาคประชาสังคมสู่การปฏิบัติ การมีส่วนร่วมของภาคเอกชนและภาคประชาสังคมในการสะท้อนปัญหาประเมินผลการดำเนินนโยบายและการเสนอแนะนโยบาย ตลอดจนการสนับสนุนและการเป็นผู้ร่วมรักษาความมั่นคงปลอดภัยไซเบอร์

ประเด็นยุทธศาสตร์ที่ 6 : เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

เป้าหมาย

1. ให้มีกลไกที่มีการปลูกฝังจิตสำนึกที่ดีในการใช้ไซเบอร์สเปซไปในทางที่เหมาะสม และเคารพสิทธิและเสรีภาพขั้นพื้นฐานของผู้อื่นบนโลกไซเบอร์

2. ส่งเสริมให้เกิดเครือข่ายผู้ใช้อินเทอร์เน็ตที่ช่วยกันดูแลการใช้ไซเบอร์สเปซไปในทางที่เหมาะสม

3. ส่งเสริมการเรียนรู้ โดยเฉพาะอย่างยิ่งในกลุ่มเด็กและเยาวชนให้รู้เท่าทันและมีความตระหนักเกี่ยวกับภัยคุกคามที่กระทบต่อความมั่นคงปลอดภัยของไซเบอร์สเปซ

แนวทางการดำเนินการ

1. ส่งเสริมค่านิยมอันดีงามของชาติบนโลกไซเบอร์ โดยส่งเสริมการใช้เทคโนโลยีสารสนเทศและการสื่อสารของประชาชนให้เป็นไปเพื่อการธำรงไว้ซึ่ง ชาติ ศาสนา และพระมหากษัตริย์

2. ส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซ (Cyber Space) ด้วยความรับผิดชอบและมีจิตสำนึกต่อผู้อื่นและสังคมโดยรวม เคารพสิทธิเสรีภาพขั้นพื้นฐานบนโลกไซเบอร์ และไม่ละเมิดกฎหมาย

ประเด็นยุทธศาสตร์ที่ 7 : ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

เป้าหมาย

1. บุคลากรด้านการสืบสวนและงานข่าวมีขีดความสามารถสูงขึ้น

2. หน่วยงานของไทยมีเทคโนโลยีที่ทันสมัยยิ่งขึ้นในการช่วยในงานสืบสวนและงานข่าว

แนวทางการดำเนินการ

1. ยกระดับและกำหนดบทบาทของผู้บังคับใช้กฎหมาย ได้แก่ เจ้าหน้าที่ตำรวจ เจ้าหน้าที่กรมสอบสวนคดีพิเศษ และเจ้าหน้าที่หรือหน่วยงานที่เกี่ยวข้อง ในการสืบสวนทางไซเบอร์เพื่อค้นหาตัวผู้กระทำผิดมาลงโทษ

2. ส่งเสริมการพัฒนาขีดความสามารถบุคลากรด้านการสืบสวนและงานข่าว ตลอดจนส่งเสริมการใช้เทคโนโลยีที่ทันสมัยเข้ามาช่วยในงานสืบสวนและงานข่าว

3. ส่งเสริมการพัฒนางานข่าวทางไซเบอร์อย่างเป็นรูปธรรมเพื่อเพิ่มประสิทธิภาพการจัดการภัยคุกคามทางไซเบอร์ได้อย่างทันต่อสถานการณ์

4. ส่งเสริมความร่วมมือด้านการแลกเปลี่ยนข้อมูลข่าวสาร ตลอดจนประสบการณ์และแนวปฏิบัติที่ดีกับต่างประเทศ ทั้งในระดับทวิภาคีและกับองค์การระหว่างประเทศที่ เกี่ยวข้อง อาทิ ตำรวจสากล เพื่อการพัฒนาขีดความสามารถในการป้องกันและปราบปรามอาชญากรรมของไทย โดยเฉพาะประโยชน์ในการสืบสวนและการข่าว

5. ส่งเสริมและสนับสนุนการพัฒนาระเบียบ และกฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมไซเบอร์

ประเด็นยุทธศาสตร์ที่ 8 : ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในความร่วมมือเพื่อการ รักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคและระดับนานาชาติ

เป้าหมาย

1. ไทยมีบทบาทที่สร้างสรรค์ในการพัฒนาหรือผลักดันให้เกิดบรรทัดฐาน มาตรฐาน และการสร้างความวางใจหรือความเชื่อมั่นในการร่วมกันใช้ไซเบอร์สเปซ ทั้งในระดับภูมิภาคและระดับระหว่างประเทศ

2. มีการแลกเปลี่ยนองค์ความรู้และแนวปฏิบัติที่ดีกับต่างประเทศอย่างต่อเนื่อง

แนวทางการดำเนินการ

1. สนับสนุนให้มีการใช้ไซเบอร์สเปซ (Cyber Space) ในทางสันติโดยไม่ใช้เทคโนโลยีสารสนเทศเพื่อการสร้างความขัดแย้ง ตลอดจนร่วมมือกับมิตรประเทศ ในการต่อต้านการใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการก่ออาชญากรรมข้ามชาติหรือการกระทำที่สร้างความเสียหาย

2. สนับสนุนการแลกเปลี่ยนองค์ความรู้ ข้อมูล แนวปฏิบัติ ที่ดีด้านไซเบอร์กับต่างประเทศ ทั้งในระดับทวิภาคีระดับภูมิภาคและระดับพหุภาคี

3. มีช่องทางการสื่อสารแลกเปลี่ยนข้อมูลและแนวทางปฏิบัติที่ชัดเจนในการร่วมมือกับต่างประเทศในการตอบสนองและรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

4. มีบทบาทในการส่งเสริมการหารือเกี่ยวกับบรรทัดฐาน มาตรฐานและมาตรการสร้างความไว้วางใจหรือความเชื่อมั่นระหว่างประเทศในมิติไซเบอร์ รวมถึงการมีท่าทีร่วมกันในระดับภูมิภาค เพื่อให้บรรทัดฐานระหว่างประเทศเป็นที่ยอมรับและสะท้อนผลประโยชน์ของไทยและประเทศในภูมิภาค

2.3 นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565-2570

นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565-2570 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับสมบูรณ์นี้ ได้กำหนดวิสัยทัศน์การรักษาความมั่นคงปลอดภัยไซเบอร์ คือ “บริการที่สำคัญของประเทศไทยมีความมั่นคง ปลอดภัยไซเบอร์ เพื่อความยั่งยืนทางเศรษฐกิจและสังคม”

นโยบายและแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565-2570 เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติ และในสถานการณ์ที่อาจจะ เกิดหรือเกิดภัยคุกคามทางไซเบอร์ ซึ่งสอดคล้องกับนโยบายยุทธศาสตร์และแผนระดับชาติ และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

เพื่อให้บรรลุวิสัยทัศน์และเป้าหมายการขับเคลื่อนยุทธศาสตร์ด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ จึงได้**กำหนดยุทธศาสตร์การดำเนินงาน 4 ยุทธศาสตร์ ดังนี้**

ยุทธศาสตร์ที่ 1 : สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัย ไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Capacity)

วัตถุประสงค์

เพื่อเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ ของประเทศ โดยบูรณาการบุคลากร องค์ความรู้ และเทคโนโลยี นำไปสู่การพัฒนาผลิตภัณฑ์ด้านความมั่นคง ปลอดภัยไซเบอร์ที่เป็นนวัตกรรมของประเทศ

เป้าหมาย

1. พัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับความต้องการของประเทศ
2. ส่งเสริมให้บุคลากรทุกภาคส่วนมีความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์
3. ส่งเสริมให้เกิดการมีส่วนร่วมในการสร้างความแข็งแกร่งด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ
4. ส่งเสริมการพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นนวัตกรรมของประเทศ

กลยุทธ์

1. เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์
2. สร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์
3. ส่งเสริมการวิจัยและพัฒนาและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 2 : บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)

วัตถุประสงค์

เพื่อบูรณาการความร่วมมือในการเตรียมความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์ และการฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้อย่างรวดเร็วกับทุกภาคส่วน ทั้งภายในประเทศและระหว่างประเทศ

เป้าหมาย

1. มีการประสานความร่วมมือทั้งภาครัฐและภาคเอกชนภายในประเทศ เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์และการฟื้นคืนสู่สภาพปกติ
2. มีการประสานความร่วมมือระหว่างประเทศ เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์และการฟื้นคืนสู่สภาพปกติ

กลยุทธ์

1. ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและภาคเอกชน

2. ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม

ยุทธศาสตร์ที่ 3 : สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้(Resilience)

วัตถุประสงค์

เพื่อส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์ และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้

เป้าหมาย

1. มีการกำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2. มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

3. มีการปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ

กลยุทธ์

1. กำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

2. กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

3. ปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ

ยุทธศาสตร์ที่ 4 : สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน (Standard)

วัตถุประสงค์

มุ่งสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

เป้าหมาย

1. มีการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แบบบูรณาการในระดับชาติ

2. มีหน่วยงานหลักและหน่วยงานรองที่มีคุณภาพและมาตรฐาน สามารถทำงานร่วมกันแบบบูรณาการได้

3. มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

4. มีการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

5. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ มีมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เข้มแข็ง

กลยุทธ์

1. เพิ่มขีดความสามารถการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

2. ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม

3. ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์

2.4 กฎหมายที่เกี่ยวข้อง

2.4.1 กฎหมายว่าด้วยธุรกรรมการอิเล็กทรอนิกส์

ประเทศไทยได้มีการประกาศใช้กฎหมายเกี่ยวกับการทำธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วย พระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ซึ่งได้กำหนดมาตรการเพื่อลดความเสี่ยงและทำให้เกิดความน่าเชื่อถือต่อการใช้งานระบบคอมพิวเตอร์และอินเทอร์เน็ต ในการทำธุรกรรมทางอิเล็กทรอนิกส์ และมีการกำหนดบทลงโทษสำหรับการก่ออาชญากรรมคอมพิวเตอร์ นอกจากนี้ยังได้มีการกำหนดกฎกระทรวง ประกาศ ระเบียบ เพื่อการบังคับใช้กฎหมายดังกล่าว อาทิ กฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. 2551 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง กำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

2.4.2 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อป้องกันระบบคอมพิวเตอร์และโรงข่ายเทคโนโลยีสารสนเทศของโครงสร้างพื้นฐานที่สำคัฐทางสารสนเทศ หรือบริการที่สำคัญของประเทศมีความมั่นคงปลอดภัยสามารถให้บริการได้เป็นและหน่วยงานสามารถรับมือกับภัยคุกคาม

ทางไซเบอร์ได้อย่างทันท่วงที รวมถึงป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ มีการกำหนดให้มีการจัดตั้งองค์กร เพื่อรับผิดชอบในการขับเคลื่อนนโยบายความมั่นคงปลอดภัยไซเบอร์ไปสู่การปฏิบัติ การจัดทำแผนและนโยบายแห่งชาติ และการประสานการดำเนินการระหว่างหน่วยงานที่เกี่ยวข้องในลักษณะองค์รวมของประเทศทั้งภาครัฐ ภาคเอกชน และภาคประชาชน ในสถานการณ์ทั่วไป หรือสถานการณ์ภัยต่อความมั่นคง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพจึงได้มีการพยายามออกกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งนี้ เพื่อเป็นการดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

สาระสำคัญกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

1. กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐมีมาตรฐานและมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

2. มีการเฝ้าระวังภัยคุกคามและมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ

3. มีการร่วมมือและประสานงานกันกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อมีภัยร้ายแรงที่ทำให้การบริการที่สำคัญไม่สามารถให้บริการได้

ส่วนที่ 3 แนวทางการดำเนินงาน

มหาวิทยาลัยมหาสารคาม ได้นำแนวทางการดำเนินงานของสภาความมั่นคงแห่งชาติ และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มาพิจารณากำหนดขั้นตอนและวิธีการดำเนินงาน พร้อมจัดทำแผนงานโครงการและกิจกรรม ที่จะสนับสนุนการดำเนินงานตามกลยุทธ์เพื่อให้บรรลุเป้าหมายที่กำหนด และเป็นแนวทางการดำเนินงานให้หน่วยงานในสังกัดมหาวิทยาลัยมหาสารคามนำไปปรับปรุงแผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน

3.1 แนวความคิดในการแก้ปัญหาแบบบูรณาการ

ขั้นตอนที่ 1 การเตรียมการ

เป็นการเตรียมความพร้อมด้านเครื่องมือ อุปกรณ์ และโครงสร้างพื้นฐานด้านไอที รวมไปถึงบุคลากรให้มีความพร้อมและรับมือกับเหตุการณ์ภัยคุกคามต่าง ๆ ได้ โดยกำหนดแนวทางไว้ ดังนี้

1. กำหนดบุคคลรับผิดชอบ ทำหน้าที่ในการบริหารจัดการ กำหนดมาตรการ/มาตรฐาน โดยให้เป็นไปตามที่สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Agency: NCSA) กำหนด โดยมีมาตรการดังนี้

1.1 Identify คือ การระบุและเข้าใจเพื่อการบริหารจัดการความเสี่ยงภัยคุกคามทางไซเบอร์

1.2 Protect คือ การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร

1.3 Detect คือ การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ผิดปกติที่เกิดขึ้น

1.4 Respond คือ การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น

1.5 Recovery คือ การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ดำเนินการได้อย่างต่อเนื่องและฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

2. การกำหนดมาตรการป้องกัน โดยการจัดทำมาตรการป้องกันและรับมือภัยคุกคามทางไซเบอร์ทั้งในระดับภายในและระหว่างหน่วยงาน

3. การจัดเตรียมเครื่องมือและบุคลากร โดยจัดให้มีอุปกรณ์และเครื่องมือเทคโนโลยีที่ทันสมัย และมีความพร้อมในการรับมือภัยคุกคามต่าง ๆ ได้แก่ การมีระบบแจ้งเตือนเหตุ การป้องปรามและป้องกัน การแก้ไขและฟื้นฟู การตอบโต้ รวมถึงการฝึกอบรมเพื่อพัฒนาบุคลากรในทุกระดับ (ระดับปฏิบัติการ/เชี่ยวชาญ/

บริหาร)

4. จัดเตรียมอุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น เครื่องคอมพิวเตอร์หรืออุปกรณ์สำรองข้อมูล (Backup Device) เครื่องมือสำหรับตรวจจับและวิเคราะห์ข้อมูลในเครือข่ายคอมพิวเตอร์ (Packet Sniffers and Protocol Analyzers) เพื่อใช้ศึกษาพฤติกรรมของ Malware หรือความผิดปกติของเครือข่ายเครื่องคอมพิวเตอร์สำรอง และอุปกรณ์ที่ใช้ในการรวบรวมหลักฐาน เป็นต้น

5. ซอฟต์แวร์สำหรับการบรรเทาเหตุภัยคุกคาม เช่น ไฟล์ disk image ของระบบปฏิบัติการ (OS) และ แอปพลิเคชัน (Application) เพื่อใช้ในการกู้คืนและฟื้นฟูระบบ เป็นต้น

6. Backup Device สำหรับใช้ในการเก็บข้อมูลต่างๆ ที่จำเป็นและเกี่ยวข้องกับ Incident เช่น log file, screen capture เป็นต้น

7. รายการทรัพย์สินสารสนเทศที่สำคัญ โดยอย่างน้อยควรประกอบด้วย Hardware, Software, Data, Network Diagram, Data Flow Diagram

8. การประเมินความเสี่ยง (Risk Assessment) ควรทำการประเมินความเสี่ยง เพื่อพิจารณาว่ามีความเสี่ยงใดบ้างที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์หรือช่องโหว่ด้านความมั่นคงปลอดภัยเพื่อประเมินผลกระทบและมูลค่าความเสียหายที่แท้จริง และเป็นข้อมูลประกอบการพิจารณาทบทวนหรือปรับปรุงแนวทางในการรับมือและการตอบสนองต่อภัยคุกคามทางไซเบอร์ต่อไป

9. การกำหนดแนวทางรักษาความมั่นคงปลอดภัยของระบบแม่ข่าย (Implement Host Security Control) และการควบคุมพื้นฐานในระดับ Endpoint ที่ควรมีรวมทั้งควรกำหนดให้มีการรักษาความมั่นคงปลอดภัยที่เหมาะสมและมีมาตรฐาน ควรมีการกำหนดสิทธิ์ของผู้ใช้งานโดยให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น รวมทั้งระบบแม่ข่ายควรบันทึกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่สำคัญของหน่วยงานและได้รับการติดตามตรวจสอบอย่างสม่ำเสมอ

10. การรักษาความปลอดภัยของเครือข่าย (Network Security: Implement Network Security Control) เป็นการตั้งค่าอุปกรณ์ทางเครือข่ายที่จำเป็น เช่น Router ACL, Firewall, IPDS เป็นต้น ให้ปฏิเสธการเข้าถึงของกิจกรรมทั้งหมดที่ไม่ได้รับอนุญาตรวมทั้งอุปกรณ์เครือข่ายทั้งหมดของหน่วยงานที่เชื่อมต่อกับเครือข่ายภายนอกเพื่อป้องกันและแจ้งเตือนการบุกรุก

11. การจัดทำแนวปฏิบัติเพื่อรองรับการการเกิดภัยคุกคาม โดยการจัดทำรายละเอียดแนวปฏิบัติเพื่อเตรียมความพร้อมกับสถานการณ์ที่เกิดขึ้นจริง เช่น การจัดทำแผนสำรองและกู้คืนข้อมูล แผนฟื้นฟูระบบเมื่อเกิดสถานการณ์ภัยคุกคาม เป็นต้น โดยกำหนดให้มีการซักซ้อมการรับมือ แลกเปลี่ยนข้อมูล รวมถึงการติดตามข่าวเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อเตรียมความพร้อมรับมือในภาวะวิกฤต

ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection & Analysis)

1. การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident การตรวจจับ Incidentจะขึ้นอยู่กับระบบที่ใช้งานอยู่และรูปแบบของความพยายามในการโจมตีประกอบกับกลไกต่างๆ ที่ทำการปกป้องระบบอยู่ เพราะโดยทั่วไประบบการป้องกันจะทำการแจ้งเตือน (Alert) หรือ เก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์หาความผิดปกติ

2. การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้งการวิเคราะห์เหตุภัยคุกคาม

3. การบันทึกข้อมูลเหตุการณ์ภัยคุกคามซึ่งจะช่วยให้การรับมือและตอบสนองภัยคุกคามมีประสิทธิภาพและเป็นระบบมากขึ้น โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้นตั้งแต่การตรวจพบจนถึงการสิ้นสุดของเหตุการณ์ภัยคุกคามเพื่อประโยชน์ในการติดตามเหตุการณ์ ขั้นตอนการจัดการ และแก้ไขเหตุภัยคุกคาม

4. การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident การวิเคราะห์ผลกระทบและความรุนแรงเพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจเพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสม

5. การติดต่อประสานงานและแจ้งข้อมูลให้กับบุคลากรด้านอื่น ๆ ทราบ รายงานต่อผู้บริหารหน่วยงานและผู้อำนวยการสำนักคอมพิวเตอร์

ขั้นตอนที่ 3 การรับมือเมื่อเกิดเหตุ

สำนักคอมพิวเตอร์ มหาวิทยาลัยมหาสารคาม เป็นหน่วยงานหลักในการรับผิดชอบโครงสร้างพื้นฐานเทคโนโลยีดิจิทัลและสารสนเทศ มีระบบสารสนเทศที่เป็นโครงสร้างพื้นฐานที่สำคัญของมหาวิทยาลัย จึงต้องปฏิบัติตามแนวทางการปฏิบัติการรับมือภัยคุกคามทางไซเบอร์ ซึ่งต้องดำเนินการดังต่อไปนี้

1. แนวทางการดำเนินการในระดับหน่วยงานและระดับมหาวิทยาลัย

ระดับที่ 1 (ปกติ) ทุกหน่วยงาน

- มีหน้าที่ป้องกันและรับมือตามแนวทางที่กำหนด
- จัดทำแนวปฏิบัติ มีระบบและระเบียบปฏิบัติ รวมถึงแนวปฏิบัติการสำรองข้อมูลและการกู้คืนข้อมูลพร้อมการซักซ้อมและรายงานผลการดำเนินงานต่อมหาวิทยาลัย
- เมื่อเกิดเหตุการณ์ให้รับมือด้วยตนเอง แต่หากเกินกว่าจะรับมือได้ให้ขอความช่วยเหลือไปยังคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคาม หรือผู้อำนวยการสำนักคอมพิวเตอร์ มหาวิทยาลัยมหาสารคาม

ระดับที่ 2 สถานการณ์เกิดขึ้นในระดับมหาวิทยาลัย

- เป็นเหตุการณ์ที่เกิดขึ้นกับหน่วยงานในกำกับดูแล
- จัดให้มีหัวหน้าหน่วยงานกำกับดูแลในระดับมหาวิทยาลัย เพื่อกำหนดนโยบาย ระเบียบปฏิบัติที่เกี่ยวข้อง และจัดทำแผนปฏิบัติการในระดับมหาวิทยาลัยเพื่อเป็นแนวทางบริหารจัดการ
- กำหนดผู้รับผิดชอบในการป้องกันและรับมือในฐานะหน่วยงานกำกับดูแล
- สำหรับแผนปฏิบัติการระดับมหาวิทยาลัยจะต้องมีการซักซ้อมเป็นประจำทุกปี
- จะต้องรักษาข้อมูลของผู้ใช้บริการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
- เมื่อเกิดเหตุการณ์ที่เกินกว่าจะรับมือได้ให้ร้องขอความช่วยเหลือไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

2. การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery)

2.1 พิจารณาวิธีการในการควบคุมความเสียหาย การควบคุมความเสียหายมีความจำเป็นอย่างยิ่งที่จะป้องกันไม่ให้ความเสียหายกระจายออกไปเป็นวงกว้างและสร้างผลกระทบต่อการดำเนินงานอื่น ๆ โดยแนวทางการควบคุมความเสียหายโดยวิธีการทั่วไปมีดังนี้

- ปิดระบบ (Shut Down)
- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ ปลายทางแบบเรียลไทม์)
- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot

2.2 การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือเพื่อให้การแก้ไข Incident ส่งผลกระทบต่อการดำเนินงานให้น้อยที่สุด

2.3 การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ ตัวอย่างเช่น

- การปิดช่องโหว่ของระบบ
- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน
- การลบโปรแกรมประเภท Backdoor ออกจากระบบ

- การใช้ข้อมูล Indicator of Compromise (IoC) ในการสแกนหา Malware หรือร่องรอยอื่น ๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด

2.4 หลังจากดำเนินการควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติ โดยควรเตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่างๆจาก Master Image ที่ปลอดภัย

- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

ขั้นตอนที่ 4 การดำเนินการหลังถูกภัยคุกคาม (Post Incident Activity)

แนวทางการปฏิบัติการรับมือภัยคุกคามทางไซเบอร์ การฟื้นฟู/กู้คืน ให้ผู้ใช้งานสามารถใช้งานได้อย่างต่อเนื่อง จะต้องดำเนินการดังต่อไปนี้

1) การกู้คืนข้อมูล

- จัดทำและตรวจสอบความพร้อมของแนวปฏิบัติการกู้คืนข้อมูล และฟื้นฟูระบบ ให้เป็นไปตามมาตรฐานสากล

2) การกำหนด ทบทวน ข้อมูลที่เกี่ยวข้อง

- กำหนด/ทบทวนบัญชีเป้าหมายที่เกี่ยวข้องกับการเกิดหรือการแพร่กระจายของข้อมูลที่เป็นภัยคุกคามทางไซเบอร์

- กำหนด/ทบทวนกระบวนการเฝ้าตรวจ/รายงาน ระหว่างบุคคลหรือหน่วยงานที่เกี่ยวข้อง

- กำหนด/ทบทวนเครื่องมือหรืออุปกรณ์ต่าง ๆ ในการตรวจพบข้อมูลที่เป็นภัยคุกคาม

- กำหนด/ทบทวนบุคลากรที่เกี่ยวข้องในการรับมือกับการเกิดภัยคุกคามทางไซเบอร์

- เก็บข้อมูลและจัดทำฐานข้อมูลเพื่อสนับสนุนให้การแก้ปัญหาหน่วยงาน

3) ปรับปรุงมาตรการ/อุปกรณ์และเครื่องมือ/บุคลากร

- ทบทวนกลไกการทำงาน

- เตรียมพร้อมเครื่องมือ บุคลากร เพื่อนำความรู้ที่ได้รับมาประยุกต์ใช้ตลอดเวลา

- กำหนด/ทบทวนมาตรการของหน่วยงาน โดยการศึกษา/หารือ แนวทางการดำเนินงานจากภายในหน่วยงานทั้งในและต่างประเทศ เพื่อแลกเปลี่ยน ความรู้ และวิธีการแก้ไขปัญหาภัยไซเบอร์ เพื่อเป็นองค์ความรู้ให้กับบุคลากรด้านไอซีที

3.2 กรอบแนวทางการดำเนินงาน

ในการจัดทำแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม ได้กำหนดกรอบแนวทางการดำเนินงาน ไว้ดังนี้

3.2.1 กำหนดแผนการดำเนินงาน

3.2.2 วิเคราะห์ความสอดคล้องของกลยุทธ์ที่เกี่ยวข้อง

3.2.3 กำหนดแผนงาน/โครงการ/กิจกรรม ให้สอดคล้องกับกลยุทธ์ตามแผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัยมหาสารคาม ในการจัดทำแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคามได้กำหนดกรอบแนวทางการดำเนินงานและระยะเวลาในการดำเนินงานไว้ดังนี้

ตารางที่ 1 แผนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม

กิจกรรม	ระยะเวลาดำเนินการ (ปีงบประมาณ)
1.จัดทำ ปรับปรุง แก้ไข แผนการปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ฯ	ตุลาคม -พฤศจิกายน
2.จัดทำ ปรับปรุง แก้ไข และตรวจสอบนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยฯ	ตุลาคม -พฤศจิกายน
3.เสนอนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยฯ แก่คณะ/หน่วยงานภายในมหาวิทยาลัยเพื่อนำไปสู่การปฏิบัติ	พฤศจิกายน -ธันวาคม
4.จัดกิจกรรมส่งเสริมให้ความรู้แก่นิสิตและบุคลากรของมหาวิทยาลัย	มกราคม-สิงหาคม
5. คณะ/หน่วยงาน รับการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จากผู้ตรวจประเมิน	มีนาคม-เมษายน
6. รายงานสรุปผลการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่คณะ/หน่วยงานสำหรับนำไปปรับปรุงแก้ไข	กรกฎาคม
7.ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	สิงหาคม-กันยายน
8.ประเมินผลและสรุปรายงานการดำเนินงานเสนอผู้บริหาร	กันยายน

3.3 ความสอดคล้องของกลยุทธ์ที่เกี่ยวข้อง

จากการวิเคราะห์กลยุทธ์ตามแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคามได้กำหนดกลยุทธ์หลักที่จะต้องดำเนินการ จำนวน 6 กลยุทธ์ ได้แก่

กลยุทธ์ที่ 1 กำหนดแนวความคิด มาตรการ มาตรฐาน ระบบบริหารจัดการในการป้องกันความมั่นคงปลอดภัยไซเบอร์ในภาพรวม

กลยุทธ์ที่ 2 กำหนดระบบบริหารจัดการในแต่ละระดับชัดเจน

กลยุทธ์ที่ 3 ระบบการตอบโต้ต่อสถานการณ์ฉุกเฉิน

กลยุทธ์ที่ 4 ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ที่ 5 สร้างความตระหนักรู้ประชาชนและหน่วยงาน

กลยุทธ์ที่ 6 พัฒนาศักยภาพเทคโนโลยีและบุคลากร

สรุปการดำเนินงานในแต่ละกลยุทธ์ได้ ดังนี้

กลยุทธ์ที่ 1 กำหนดแนวความคิด มาตรการ มาตรฐาน ระบบบริหารจัดการในการป้องกันความมั่นคงปลอดภัยไซเบอร์ในภาพรวม ผ่านผู้บริหารระดับสูงด้านสารสนเทศ (Chief Information Officer: CIO) ทำหน้าที่ในการกำกับ ดูแล บริหารจัดการในส่วนที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

กลยุทธ์ที่ 2 กำหนดระบบบริหารจัดการในแต่ละระดับ เป็นกลยุทธ์หน่วยงานรับผิดชอบโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องดำเนินการจัดทำแนวปฏิบัติเพื่อเตรียมรับมือความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยสำนักคอมพิวเตอร์ มหาวิทยาลัยมหาสารคาม รับผิดชอบหลักในส่วนของโครงสร้างพื้นฐานสารสนเทศ จึงได้จัดทำแผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ พร้อมให้หน่วยงานในสังกัดมหาวิทยาลัยมหาสารคาม ดำเนินการตามแผนปฏิบัติการฯ พร้อมทั้งจัดทำแผนปฏิบัติการฯ ของหน่วยงานเพื่อเป็นแนวทางในการดำเนินการเมื่อเกิดภัยคุกคาม และมีการซักซ้อมแผนปฏิบัติการฯ อย่างต่อเนื่อง

กลยุทธ์ที่ 3 ระบบการตอบโต้ต่อสถานการณ์ฉุกเฉิน เช่น การจัดแนวทางในการบริหารความเสี่ยง แนวทางบริหารความต่อเนื่องทางการดำเนินงาน แนวทางแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ เป็นต้น ซึ่งมีการอธิบายเหตุการณ์ หรือภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศ ขั้นตอนการดำเนินงาน ผู้รับผิดชอบ หน่วยงานที่เกี่ยวข้อง ระยะเวลาในการแก้ไขปัญหาและวิธีการในการทำให้ระบบสามารถกลับมาใช้ได้เช่นเดิม รวมไปถึงการนำบทเรียน เหตุการณ์ หรือประสบการณ์ต่าง ๆ ที่เกี่ยวข้อง มาประกอบการพิจารณาทบทวนเพื่อรองรับเหตุการณ์ภัยคุกคามด้านไซเบอร์

กลยุทธ์ที่ 4 ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยการจัดทำแผนงาน/โครงการ/กำหนดนโยบายในการใช้งานอุปกรณ์และระบบสารสนเทศภายในหน่วยงาน เพื่อป้องกันภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมไปถึงกฎ ระเบียบ ข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับการป้องกันภัยทางไซเบอร์ การทดสอบความพร้อมในการถูกคุมคามทางไซเบอร์ จัดหาเครื่องมือ หรืออุปกรณ์ที่จำเป็นสำหรับการควบคุม ตรวจสอบการเข้าถึงระบบสารสนเทศของหน่วยงาน การตรวจสอบการทางานของซอร์สโค้ดของระบบงาน

กลยุทธ์ที่ 5 สร้างความตระหนักรู้แก่บุคลากร นิสิต และผู้ปฏิบัติงานของคณะ หน่วยงาน โดยการจัดทำสื่อประชาสัมพันธ์เกี่ยวกับ กฎ ระเบียบ ที่เกี่ยวข้องกับภัยทางไซเบอร์ ทั้งผ่านทางเว็บไซต์ภายในหน่วยงาน

กลยุทธ์ที่ 6 พัฒนาศักยภาพเทคโนโลยีและบุคลากร โดยการจัดทำแผนพัฒนาบุคลากรในหน่วยงานให้มีความรู้เกี่ยวกับการความปลอดภัยทางไซเบอร์ และการพัฒนาบุคลากรด้านไอทีของหน่วยงานมีความรู้และเข้าใจเกี่ยวกับภัยคุกคามและการรักษาความปลอดภัยทางไซเบอร์

3.4 แผนกลยุทธ์และแผนที่นำทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

3.4.1 แผนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อ้างอิงมาตรฐาน NIST (National Institute of Standards and Technology)

ตารางที่ 2 แผนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การระบุ (IDENTIFY)	**การป้องกัน (PROTECT)**	**การตรวจจับ (DETECT)**	**การตอบสนอง (RESPOND)**	**การกู้คืน (RECOVERY)**
การบริหารจัดการทรัพย์สิน (Asset Management)	การบริหารจัดการผู้ใช้งาน การพิสูจน์ตัวตน และการควบคุมการเข้าถึง (Identity Management, Authentication and Access Control)	ความผิดปกติและเหตุการณ์ (Anomalies and Events)	การวางแผนการตอบสนอง (Response Planning)	การวางแผนการกู้คืน (Recovery Planning)
สภาพแวดล้อมทางการดำเนินการ	การสร้างความตระหนัก และการอบรม (Awareness and Training)	การติดตามความปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring)	การสื่อสาร (Communications)	การปรับปรุง (Improvements)
Governance	ความปลอดภัยของข้อมูล (Data Security)	ขั้นตอนการตรวจจับ (Detection Processes)	การวิเคราะห์ (Analysis)	การสื่อสาร (Communications)
การประเมินความเสี่ยง (Risk Assessment)	ขั้นตอนและแนวทางปฏิบัติในการป้องกันสารสนเทศ (Information Protection Processes & Procedures)		การบรรเทา (Mitigation)	
กลยุทธ์ในการบริหารจัดการความเสี่ยง (Risk Management Strategy)	การซ่อมบำรุง (Maintenance)		การปรับปรุง (Improvements)	
Supply Chain Risk Management	เทคโนโลยีในการป้องกัน (Protective Technology)			

3.4.2 กลยุทธ์ที่เกี่ยวข้องกับการระบุสภาพแวดล้อมพื้นฐานเพื่อให้มีความมั่นคงปลอดภัย (IDENTIFY)

ตารางที่ 3 กลยุทธ์ที่เกี่ยวข้องกับการระบุสภาพแวดล้อมพื้นฐานเพื่อให้มีความมั่นคงปลอดภัย (IDENTIFY)

การระบุ (IDENTIFY)	**เอกสารอ้างอิง**
การบริหารจัดการทรัพย์สิน (Asset Management)	-หมวด 4 การบริหารจัดการทรัพย์สิน -หมวด 3 ความมั่นคงปลอดภัยทางกายภาพ คณะ/หน่วยงาน และสภาพแวดล้อม -หมวด 5 ความมั่นคงปลอดภัยในการดำเนินงาน
สภาพแวดล้อมทางการดำเนินการ	- ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก
การกำกับดูแล (Governance)	- นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์
การประเมินความเสี่ยง (Risk Assessment)	- แนวทางปฏิบัติการประเมินความเสี่ยง
กลยุทธ์ในการบริหารจัดการความเสี่ยง (Risk Management Strategy)	- แนวทางปฏิบัติการประเมินความเสี่ยง
การบริหารจัดการความเสี่ยงห่วงโซ่อุปทาน (Supply Chain Risk Management)	- แนวทางปฏิบัติการประเมินความเสี่ยง

3.4.3 กลยุทธ์ที่เกี่ยวข้องกับการป้องกันไม่ให้มีการละเมิดความมั่นคงปลอดภัย (PROTECT)

ตารางที่ 4 กลยุทธ์ที่เกี่ยวข้องกับการป้องกันไม่ให้มีการละเมิดความมั่นคงปลอดภัย (PROTECT)

การป้องกัน (PROTECT)	**อ้างอิงเอกสาร**
การบริหารจัดการผู้ใช้งาน การพิสูจน์ตัวตนและการควบคุมการเข้าถึง (Identity Management, Authentication and Access Control)	- หมวด 7 การควบคุมการเข้าถึง (Access Control)
การสร้างความตระหนัก และการอบรม (Awareness and Training)	- จัดให้มีการสร้างความตระหนักการสื่อสารความมั่นคงปลอดภัยไซเบอร์ เป็นประจำ อย่างสม่ำเสมอ
ความปลอดภัยของข้อมูล (Data Security)	-หมวด 8 นโยบายการเข้ารหัสข้อมูล (Cryptography)

การป้องกัน (PROTECT)	อ้างอิงเอกสาร
ขั้นตอนและแนวทางปฏิบัติในการป้องกันสารสนเทศ (Information Protection Processes & Procedures)	-หมวด 4 การบริหารจัดการทรัพย์สิน -หมวด 3 ความมั่นคงปลอดภัยทางกายภาพ คณะ/หน่วยงาน และสภาพแวดล้อม -หมวด 5 ความมั่นคงปลอดภัยในการดำเนินงาน -หมวด 6 การควบคุมอุปกรณ์พกพาและปฏิบัติงานจากระยะไกล -หมวด 7 การควบคุมการเข้าถึง -หมวด 8 การเข้ารหัสข้อมูล
การซ่อมบำรุง (Maintenance)	-หมวด 10 การจัดหา การพัฒนา และบำรุงรักษาระบบ
เทคโนโลยีในการป้องกัน (Protective Technology)	-หมวด 4 การบริหารจัดการทรัพย์สิน -หมวด 3 ความมั่นคงปลอดภัยทางกายภาพ คณะ/หน่วยงาน และสภาพแวดล้อม -หมวด 5 ความมั่นคงปลอดภัยในการดำเนินงาน -หมวด 6 การควบคุมอุปกรณ์พกพาและปฏิบัติงานจากระยะไกล -หมวด 7 การควบคุมการเข้าถึง -หมวด 8 การเข้ารหัสข้อมูล

3.4.4 กลยุทธ์ที่เกี่ยวข้องกับการตรวจจับเหตุการณ์ละเมิดความมั่นคงปลอดภัย (DETECT)

ตารางที่ 5 กลยุทธ์ที่เกี่ยวข้องกับการตรวจจับเหตุการณ์ละเมิดความมั่นคงปลอดภัย (DETECT)

การตรวจจับ (DETECT)	อ้างอิงเอกสาร
ความผิดปกติและเหตุการณ์ (Anomalies and Events)	- หมวด 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
การติดตามความปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring)	-หมวด 11 นโยบายการบริหารจัดการเพื่อสร้างความต่อเนื่องทางการดำเนินงาน

การตรวจจับ (DETECT)	**อ้างอิงเอกสาร**
	-หมวด 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
ขั้นตอนการตรวจจับ (Detection Processes)	- หมวด 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

3.4.5 กลยุทธ์ที่เกี่ยวข้องกับการตอบสนองเหตุการณ์ละเมิดความมั่นคงปลอดภัย (RESPOND)

ตารางที่ 6 กลยุทธ์ที่เกี่ยวข้องกับการตอบสนองเหตุการณ์ละเมิดความมั่นคงปลอดภัย (RESPOND)

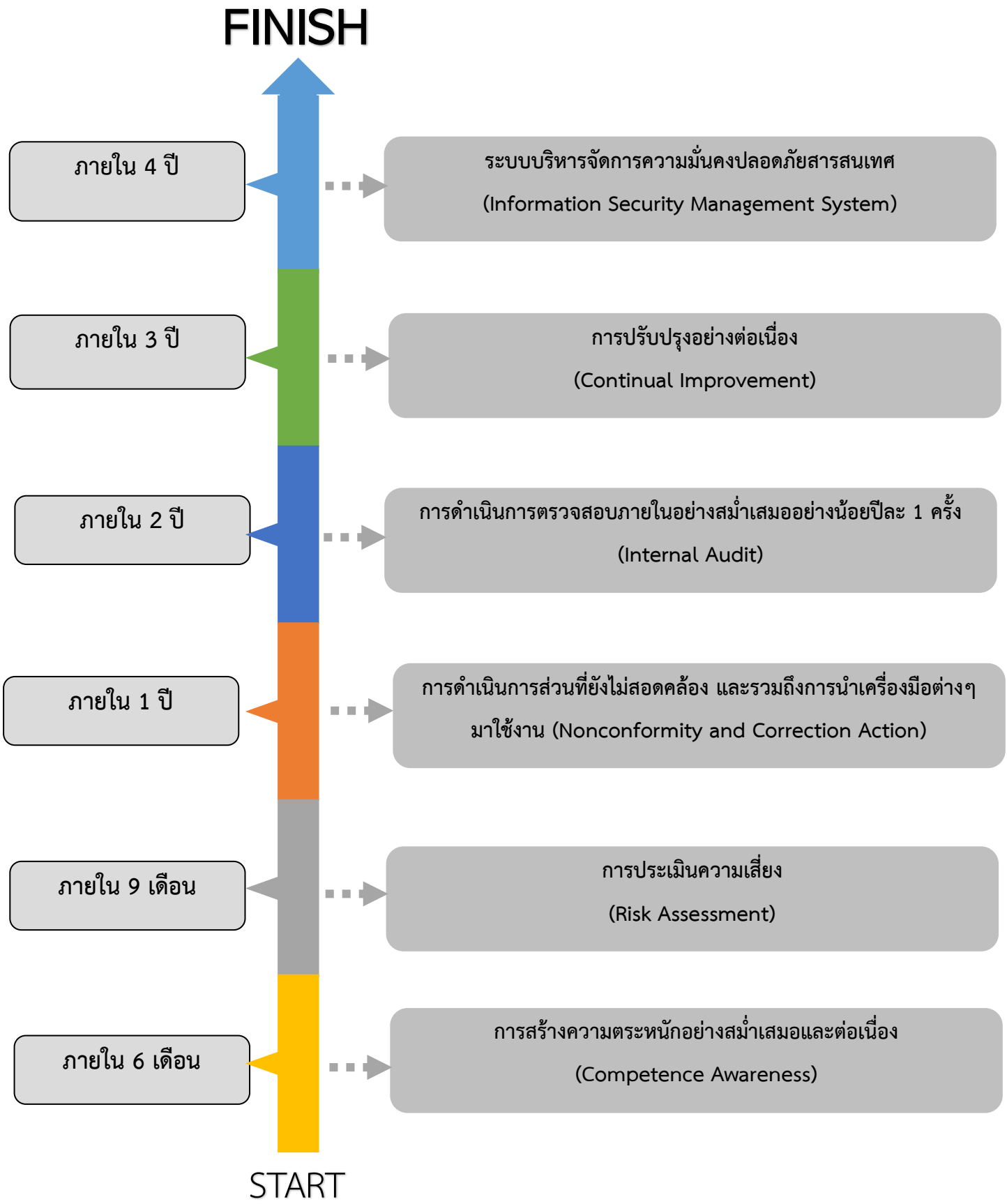
การตอบสนอง (RESPOND)	**อ้างอิงเอกสาร**
การวางแผนการตอบสนอง (Response Planning)	- หมวด 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
การสื่อสาร (Communications)	- หมวด 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
การวิเคราะห์ (Analysis)	- หมวด 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
การบรรเทา (Mitigation)	- หมวด 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
การปรับปรุง (Improvements)	- หมวด 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

3.4.6 กลยุทธ์ที่เกี่ยวข้องกับการกู้คืนเพื่อกลับไปสู่สภาวะปกติ (RECOVERY)

ตารางที่ 7 กลยุทธ์ที่เกี่ยวข้องกับการกู้คืนเพื่อกลับไปสู่สภาวะปกติ (RECOVERY)

การกู้คืน (RECOVERY)	**อ้างอิงเอกสาร**
การวางแผนการกู้คืน (Recovery Planning)	-หมวด 11 นโยบายการบริหารจัดการเพื่อสร้างความต่อเนื่องทางการดำเนินงาน
การปรับปรุง (Improvements)	-หมวด 11 นโยบายการบริหารจัดการเพื่อสร้างความต่อเนื่องทางการดำเนินงาน
การสื่อสาร (Communications)	-หมวด 9 ความมั่นคงปลอดภัยในการสื่อสาร

3.4.7 แผนที่นำทาง (Roadmap)



แผนที่นำทาง ประกอบด้วย 3 ระยะ ดังนี้

1. แผนระยะสั้น ในช่วง 6-9 เดือน มหาวิทยาลัยมหาสารคามต้องสร้างความตระหนักอย่างสม่ำเสมอและต่อเนื่องตลอดไปให้กับบุคลากรที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศทุกระดับเพื่อให้ความรู้ ความเข้าใจ และเสริมสร้างการป้องกันภัยคุกคามทางไซเบอร์ได้

2. แผนระยะกลาง ในช่วง 9 เดือน ถึง 3 ปี มหาวิทยาลัยมหาสารคามต้องดำเนินการส่วนที่ยังไม่สอดคล้องจากผลการประเมินความเสี่ยงช่องว่าง (GAP) ทั้งหมดที่เกิดขึ้นรวมถึงการนำ เครื่องมือหรือเทคโนโลยี มาเสริมสร้างการควบคุมและการป้องกันภัยคุกคามไซเบอร์ได้และต้องการวัดผลการบริหารจัดการในกระบวนการเพื่อให้ได้ผลลัพธ์การปฏิบัติงานที่มีประสิทธิภาพและประสิทธิผล และต้องมีการตรวจสอบภายในอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เพื่อเป็นการ ตรวจสอบการดำเนินการให้มีความสอดคล้องให้มากยิ่งขึ้น

3. แผนระยะยาว ในช่วง 2 - 4 ปี มหาวิทยาลัยมหาสารคามต้องมีการทบทวนผลการประเมินความเสี่ยง และผลการตรวจสอบภายในเพื่อให้ได้การปรับปรุงอย่างต่อเนื่อง และให้ได้ระบบบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์อย่างสมบูรณ์

3.5 แผนปฏิบัติงาน (Action Plan / Implementation Plan)

เพื่อรับมือจากภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ ในระยะสั้น ระยะกลาง และระยะยาว

ตารางที่ 8 แผนปฏิบัติงาน (Action Plan / Implementation Plan)

แผนปฏิบัติงานรับมือภัยคุกคาม ทางไซเบอร์	**ระยะสั้น**	**ระยะกลาง**	**ระยะยาว**
ภัยคุกคามระดับไม่ร้ายแรง	**People** -จัดเตรียมคนให้มีความรู้เพื่อพร้อมรับมือกับภัยคุกคามทางไซเบอร์	**People** -จัดเตรียมคนให้มีความรู้เพื่อพร้อมรับมือกับภัยคุกคามทางไซเบอร์ **Process** -จัดเตรียมคู่มือปฏิบัติงานสำหรับรับมือกับภัยคุกคามทางไซเบอร์	**People** -จัดเตรียมคนให้มีความรู้เพื่อพร้อมรับมือกับภัยคุกคามทางไซ เบอร์ **Process** -จัดเตรียมคู่มือปฏิบัติงานสำหรับรับมือกับภัยคุกคามทางไซเบอร์ **Technology** -จัดเตรียมอุปกรณ์หรือเครื่องมือให้พร้อมรับมือกับภัยคุกคามทางไซเบอร์
ภัยคุกคามระดับร้ายแรง	**People** -จัดเตรียมคนให้มีความรู้และทักษะเพื่อพร้อมรับมือกับภัยคุกคามทางไซเบอร์	**People** -จัดเตรียมคนให้มีความรู้และทักษะเพื่อพร้อมรับมือกับภัยคุกคามทางไซเบอร์ **Process** -จัดเตรียมคู่มือปฏิบัติงานสำหรับรับมือกับภัยคุกคามทางไซเบอร์ -จัดเตรียมแผนรองรับภัยคุกคามทางไซเบอร์	**People** -จัดเตรียมคนให้มีความรู้และทักษะเพื่อพร้อมรับมือกับภัย คุกคามทางไซเบอร์ **Process** -จัดเตรียมคู่มือปฏิบัติงานสำหรับรับมือกับภัยคุกคามทางไซเบอร์ -จัดให้มีการซ้อมแผนรองรับภัยคุกคามทางไซเบอร์ **Technology** -จัดเตรียมอุปกรณ์หรือเครื่องมือให้พร้อมรับมือกับภัยคุกคามทางไซเบอร์

ส่วนที่ 4 การขับเคลื่อนและการติดตามการดำเนินงาน

เพื่อให้แผนปฏิบัติการป้องกันและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ประสบผลสำเร็จตามเป้าหมายที่กำหนดไว้ จึงต้องมีการกำหนดแนวทางและวิธีการขับเคลื่อนทั้งในส่วนของระดับนโยบายและระดับปฏิบัติ รวมไปถึงต้องการติดตามผลการดำเนินงาน เพื่อมีประกอบการพิจารณาทบทวนแผนปฏิบัติการให้มีความทันต่อการเปลี่ยนแปลงของเทคโนโลยีและภัยคุกคามในอนาคต

4.1 แนวทางการขับเคลื่อนแผนลงสู่การปฏิบัติ

เพื่อให้การดำเนินงานเกิดผลเป็นรูปธรรม จึงได้จัดทำข้อเสนอแนะขึ้นทั้งในระดับนโยบาย และระดับปฏิบัติที่มีความเกี่ยวข้องกับมิติด้านไซเบอร์ ไว้ ดังนี้

4.1.1 ข้อเสนอแนะต่อระดับนโยบาย ได้แก่

1) การนำนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยไปดำเนินการในระดับหน่วยงาน
2) การเชื่อมโยงการทำงานด้านไซเบอร์ในภาพรวมมหาวิทยาลัยมหาสารคาม โดยการแต่งตั้งคณะทำงานหรือทีมงาน เพื่อแลกเปลี่ยนเรียนรู้เกี่ยวกับภัยคุกคามที่หน่วยงานเคยโดนโจมตี เพื่อหาวิธีการป้องกันการถูกคุกคาม
3) ให้หน่วยงานภายในมหาวิทยาลัยมหาสารคามบรรจุเรื่องความมั่นคงปลอดภัยทางไซเบอร์เข้าบรรจุในแผนปฏิบัติราชการของหน่วยงาน

4.1.2 ข้อเสนอแนะต่อระดับปฏิบัติที่มีความเกี่ยวข้องกับมิติด้านไซเบอร์ ได้แก่

1) การสร้างเครือข่ายไซเบอร์ในภาพรวมทั้งภายในและภายนอกมหาวิทยาลัย
2) การสนับสนุนของหน่วยงานที่เกี่ยวข้อง
3) ส่งเสริมให้หน่วยวิจัยที่เกี่ยวข้อง รวมถึงการพัฒนาบุคลากรด้านเทคโนโลยีดิจิทัลของมหาวิทยาลัยมหาสารคามให้มีการวิจัย และผลิต Software Hardware ทางไซเบอร์ใช้งานภายในหน่วยงาน
4) การฝึกร่วมกันระหว่างหน่วยงานด้านกลางด้านไซเบอร์ของประเทศไทย
5) การเตรียมความพร้อมในการตอบสนองต่อสถานการณ์ฉุกเฉินได้ทันท่วงที และฟื้นคืนระบบกลับสู่ภาวะปกติโดยเร็วที่สุด (Cyber Resilience)
6) การแบ่งปันข้อมูลระหว่างหน่วยงานในประเด็นที่เกี่ยวข้องกับไซเบอร์
7) การผลิตและพัฒนาบุคลากรด้านไซเบอร์
8) หน่วยงานทางด้านไซเบอร์ควรมีกระบวนการรับมือกับภัยคุกคามด้านไซเบอร์หลายรูปแบบ

4.2 แนวทางการติดตามและประเมินผล

4.2.1 ให้หน่วยงานในสังกัดมหาวิทยาลัยมหาสารคาม รายงานผลการดำเนินงานของกิจกรรม/แผนงาน/โครงการที่เกี่ยวข้องกับการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ได้ดำเนินการไปแล้วให้มหาวิทยาลัยมหาสารคามทราบเพื่อใช้ประกอบการติดตามและประเมินผล

4.2.2 จัดตั้งคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคาม เพื่อกำกับ ติดตามการดำเนินงานและให้ข้อเสนอแนะ เพื่อเป็นแนวทางการดำเนินงานให้กับหน่วยงานในสังกัดต่อไป

คำสั่งมหาวิทยาลัยมหาสารคาม

ที่ 1231 /2566

เรื่อง แต่งตั้งคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคาม

เพื่อให้การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคามเป็นไปด้วยความเรียบร้อย เพื่อรองรับกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และให้สอดคล้องกับการดำเนินงานตามแผนการพัฒนาดิจิทัลเพื่อเป็น Smart University ของมหาวิทยาลัยมหาสารคาม ระยะ 5 ปี (พ.ศ. 2565-2569) อาศัยอำนาจตามความในมาตรา 17 และมาตรา 20 (1) แห่งพระราชบัญญัติมหาวิทยาลัยมหาสารคาม พ.ศ. 2537 จึงแต่งตั้งคณะกรรมการดำเนินงานการจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม พ.ศ. 2566-2569 ดังรายชื่อต่อไปนี้

1. คณะกรรมการฝ่ายอำนวยการ

1.1 อธิการบดีมหาวิทยาลัยมหาสารคาม	ประธานกรรมการ
1.2 รองอธิการบดีฝ่ายบริหารและพัฒนาศักยภาพองค์กร	กรรมการ
1.3 รองอธิการบดีฝ่ายพัฒนาโครงสร้างพื้นฐาน วิจัย และนวัตกรรม	กรรมการ
1.4 รองอธิการบดีฝ่ายแผนงานและพัฒนาองค์กรดิจิทัล	กรรมการ
1.5 รองอธิการบดีฝ่ายการคลังและพัสดุ	กรรมการ
1.6 คณบดีคณะแพทยศาสตร์	กรรมการ
1.7 คณบดีคณะวิศวกรรมศาสตร์	กรรมการ
1.8 คณบดีคณะวิทยาศาสตร์	กรรมการ
1.9 คณบดีคณะศึกษาศาสตร์	กรรมการ
1.10 รองศาสตราจารย์สุชาติ คุ้มมะณี	กรรมการ
1.11 รองศาสตราจารย์พยุง มีสัจ	กรรมการ
1.12 ผู้ช่วยศาสตราจารย์มณีรัตน์ วงษ์ซื่ม	กรรมการ
1.13 ผู้ช่วยศาสตราจารย์อนัตต์ เจ่าสกุล	กรรมการ
1.14 ผู้อำนวยการสำนักคอมพิวเตอร์	กรรมการและเลขานุการ
1.15 รองผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายพัฒนาระบบนวัตกรรมดิจิทัล	กรรมการและผู้ช่วยเลขานุการ
1.16 รองผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายบริการวิชาการและนวัตกรรมการเรียนรู้	กรรมการและผู้ช่วยเลขานุการ

หน้าที่.../2

หน้าที่รับผิดชอบ

กำกับดูแล ให้คำปรึกษาในการดำเนินงานตามแผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม พ.ศ. 2566-2569 ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ

2. คณะกรรมการฝ่ายดำเนินงาน

2.1 ผู้อำนวยการสำนักคอมพิวเตอร์	ประธานกรรมการ
2.2 รองผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายพัฒนาระบบนวัตกรรมดิจิทัล	รองประธานกรรมการ
2.3 รองผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายบริการวิชาการและนวัตกรรมการเรียนรู้	รองประธานกรรมการ
2.4 ผู้ช่วยผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายโครงสร้างพื้นฐานและระบบเครือข่าย	กรรมการ
2.5 ผู้ช่วยผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายนโยบายและแผนพัฒนาดิจิทัล	กรรมการ
2.6 รองศาสตราจารย์สุชาติ คุ้มมะณี	กรรมการ
2.7 อาจารย์สมโภช ทองน้ำเที่ยง	กรรมการ
2.8 อาจารย์อิทธิพล เอี่ยมภูงา	กรรมการ
2.9 นางสิริวรรณ ดติยรัตน์	กรรมการ
2.10 นายสิทธิ์ เอมดี	กรรมการ
2.11 นายวงศวัฒน์ เทพาศักดิ์	กรรมการ
2.12 นางสาวสุกัญญา สิดวัน	กรรมการ
2.13 นายสุรเชษฐ์ ตั้งทรัพย์สกุล	กรรมการ
2.14 นายวีระศักดิ์ ศรีวงยาง	กรรมการ
2.15 ผู้ช่วยผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายพัฒนาระบบดิจิทัลและถ่ายทอดเทคโนโลยี	กรรมการและเลขานุการ

หน้าที่รับผิดชอบ

1. ตรวจสอบและให้คำแนะนำในการดำเนินการตามแผนปฏิบัติการด้านความมั่นคงไซเบอร์ มหาวิทยาลัยมหาสารคาม พ.ศ. 2566-2569 กับหน่วยงานภายในมหาวิทยาลัย
2. ป้องกันและแก้ไขปัญหาด้านความมั่นคงไซเบอร์ ให้กับหน่วยงานภายในมหาวิทยาลัยมหาสารคาม
3. เผยแพร่องค์ความรู้ด้านความมั่นคงไซเบอร์ให้กับบุคลากรและนิสิต มหาวิทยาลัยมหาสารคาม
4. สร้างความตระหนักรู้ด้านความมั่นคงไซเบอร์ให้กับบุคลากรและนิสิต มหาวิทยาลัยมหาสารคาม

ทั้งนี้.../3

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ 12 พฤษภาคม พ.ศ. 2566

(รองศาสตราจารย์ประยุกต์ ศรีวิไล)
อธิการบดีมหาวิทยาลัยมหาสารคาม

ผู้จัดทำ

แผนการปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์

มหาวิทยาลัยมหาสารคาม พ.ศ.2566-2569

ที่ปรึกษา

รองศาสตราจารย์ ดร.ประยุกต์ ศรีวิไล	อธิการบดีมหาวิทยาลัยมหาสารคาม
ผู้ช่วยศาสตราจารย์ ดร.จรวย สาวิถี	ผู้อำนวยการสำนักคอมพิวเตอร์
อาจารย์ ดร.ณัฐกานต์ ชุติมารังสรรค์	รองผู้อำนวยการฝ่ายบริการวิชาการและนวัตกรรมการเรียนรู้
อาจารย์ ดร.สมหมาย ขันทอง	รองผู้อำนวยการฝ่ายพัฒนาระบบนวัตกรรมดิจิทัล
นางสาวพัตชบูล กิ่งพุ่ม	หัวหน้าสำนักงานเลขานุการ

ผู้จัดทำ

อาจารย์ ดร.ณัฐกานต์ ชุติมารังสรรค์	รองผู้อำนวยการฝ่ายบริการวิชาการและนวัตกรรมการเรียนรู้
นางสิรีวรรณ ตติยรัตน์	หัวหน้ากลุ่มงานบริหาร

ออกแบบปก

นางสาวพรพรรณ โตจำเริญ

ปีที่พิมพ์

ธันวาคม 2566 จำนวน 40 เล่ม

แผนการปฏิบัติการ

ด้านความมั่นคงปลอดภัยทางไซเบอร์

มหาวิทยาลัยมหาสารคาม พ.ศ.2566-2569