



นโยบายการรักษา

ความมั่นคงปลอดภัยไซเบอร์จังหวัดศรีสะเกษ

จังหวัดศรีสะเกษได้ให้ความสำคัญในด้านภัยคุกคามไซเบอร์ที่เกิดขึ้นอย่างต่อเนื่อง และต้องเร่งตรวจสอบแก้ไขให้สอดคล้องและเป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 **เพื่อป้องกันความเสี่ยงจากภัยคุกคาม** ทางไซเบอร์ที่อาจกระทบต่อความมั่นคงของภาครัฐและความสงบเรียบร้อยภายในประเทศ



การดำเนินการของจังหวัดศรีสะเกษ

- 1. แต่งตั้งผู้บริหาร**ความมั่นคงปลอดภัยสารสนเทศของจังหวัดศรีสะเกษโดยผู้ว่าราชการจังหวัดศรีสะเกษเป็นประธาน รองผู้ว่าราชการจังหวัดศรีสะเกษ (ที่กำกับดูแล) เป็นรองประธาน
- 2. แต่งตั้งคณะกรรมการ**ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัด ซึ่งมีหัวหน้าส่วนราชการเป็นกรรมการ หัวหน้าสำนักงานจังหวัดศรีสะเกษเป็นกรรมการและเลขานุการ โดยมีอำนาจหน้าที่ ดังนี้



- **กำหนดนโยบาย**ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดศรีสะเกษ
- **พิจารณาทบทวนนโยบาย**ความมั่นคงปลอดภัยไซเบอร์ตามที่คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ประกาศใช้
- **กำหนดกรอบมาตรฐานและแนวทาง**ส่งเสริมการพัฒนาระบบให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดศรีสะเกษ
- **พิจารณาให้ความเห็นชอบแผน**ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดศรีสะเกษ สำหรับเป็นแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติ และสถานการณ์ที่อาจจะเกิดขึ้น หรือเกิดภัยคุกคามทางไซเบอร์

โดยจะต้อง**สอดคล้อง**กับนโยบาย ยุทธศาสตร์ และแผนระดับชาติ และกรอบนโยบาย และแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาพความมั่นคงแห่งชาติ

- 3. แต่งตั้งผู้ประสานงานด้านการรักษาความมั่นคงปลอดภัย**ไซเบอร์ในการประสานงานกับส่วนกลางเพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์

การป้องกันและรับมือภัยคุกคามไซเบอร์ด้วย NIST Cybersecurity Framework และ พ.ร.บ. ไซเบอร์ พ.ศ. 2562

1. การป้องกันและรับมือภัยคุกคามไซเบอร์ด้วย NIST Cybersecurity Framework
NIST Cybersecurity Framework เป็นกรอบแนวทางปฏิบัติที่ดีที่สุดสำหรับการป้องกันและรับมือกับภัยคุกคามไซเบอร์ รวมถึง การบริหารจัดการความเสี่ยง มีอยู่ 5 ขั้นตอน ดังนี้



1) การระบุ (Identify) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบททรัพยากร และกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูลและขีดความสามารถ



2) การป้องกัน (Protect) เป็นการดำเนินการตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐาน โดยมีวัตถุประสงค์เพื่อลดผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ ครอบคลุมการฝึกอบรมด้านความตระหนักมาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี



3) การตรวจจับ (Detect) เป็นการดำเนินการเพื่อเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตามต่อเนื่อง



4) การตอบสนอง (Respond) เป็นการดำเนินการเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ตรวจพบครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยงและการปรับปรุง



5) การคืนสภาพ (Recover) เป็นการดำเนินการตามแผนงานเพื่อรองรับการดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนทั้งด้านขีดความสามารถและบริการให้ได้ตามที่กำหนด

“การขับเคลื่อนการป้องกันและรับมือ (Incidence and Response) ภัยคุกคามไซเบอร์ ด้วย NIST Cybersecurity Framework ให้ได้มาตรฐานเป็นที่ยอมรับตามแบบสากล เพื่อยกระดับการให้บริการด้านดิจิทัลให้พร้อมใช้งานอย่างมีประสิทธิภาพ”

2. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีการกำหนดวิธีการและมาตรฐานไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 13 สอดคล้องกับ NIST Cybersecurity Framework ตามแนวทางของจังหวัดศรีสะเกษ ดังนี้



- การ**ระบุความเสี่ยง**ที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทรัพย์สินและชีวิตร่างกายของบุคคล
- มาตรการ**ป้องกันความเสี่ยง**ที่อาจจะเกิดขึ้น
- มาตรการ**ตรวจสอบและเฝ้าระวังภัย**คุกคามทางไซเบอร์
- **มาตรการเผชิญเหตุ**เมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์
- มาตรการ**รักษาและฟื้นฟูความเสียหาย**ที่เกิดจากภัยคุกคามทางไซเบอร์



ติดต่อสอบถาม สำนักงานจังหวัดศรีสะเกษ ศาลากลางจังหวัดศรีสะเกษ ชั้น 4

ถนนเทพา อำเภอเมืองศรีสะเกษ จังหวัดศรีสะเกษ 33000



โทร. 0 4561 1139 โทรสาร. 0 4561 2527



ไปรษณีย์อิเล็กทรอนิกส์ (E-mail) : sisaket@moi.go.th