



คณะวิศวกรรมศาสตร์
มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย
เลขรับ 1372
วันที่ 29-02-2567
เวลา 09.36 น.

บันทึกข้อความ

ส่วนราชการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

โทร. ๐๗-๔๓๑๗-๑๔๖ เบอร์ภายใน ๑๑๖๑, ๓๐๓๐

ที่ อว ๐๖๕๕.๑๒/๒๓๕ วันที่ ๒๙ กุมภาพันธ์ ๒๕๖๗

เรื่อง ประชาสัมพันธ์ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

เรียน หัวหน้าหน่วยงานในสังกัดมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

ตามที่ มหาวิทยาลัยได้รับหนังสือจาก สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ สกมช ๐๙๐๐/ว๖๙๕ ลงวันที่ ๒๒ กุมภาพันธ์ ๒๕๖๗ เรื่อง ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีวัตถุประสงค์เพื่อให้หน่วยงานของรัฐหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ นำไปใช้เป็นแนวทางในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงาน ในการดำเนินการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานให้สอดคล้องตามนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงเพื่อนำไปใช้เป็นแนวทางในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานได้อย่างถูกต้องครบถ้วนต่อไป นั้น

ในการนี้ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงขอส่งหนังสือมายังหน่วยงานของท่าน เพื่อประชาสัมพันธ์ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฯ ดังกล่าวข้างต้น รายละเอียดดังเอกสารที่แนบมาพร้อมหนังสือฉบับนี้

จึงเรียนมาเพื่อโปรดทราบ

เรียน คณบดี

เพื่อโปรดทราบ

สวส. แจ้งหนังสือจาก สกมช. เรื่อง แนวทางการ

จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

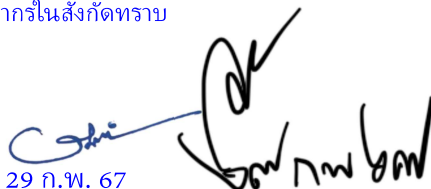
ของหน่วยงาน

เห็นควรมอบนายศุภสัณฑ์ ชัยอนันตกุล

ถือปฏิบัติ และ ปชส. ใ้ห้บุคลากรในสังกัดทราบ

นพพรดา

29 ก.พ. 67


29 ก.พ. 67


(ผู้ช่วยศาสตราจารย์สิทธิโชค อุ่นแก้ว)

ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ทราบและมอบฯ



29 ก.พ. 67



สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

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

ที่ สกมช ๐๙๐๐/ว๖๙๕

๒๒ กุมภาพันธ์ ๒๕๖๗

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย
763
เลขรับ
วันที่ 27/02/2567
เวลา 11.27 น.

เรื่อง ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทาง
การจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

เรียน หัวหน้าหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศ

สิ่งที่ส่งมาด้วย ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

ด้วยในคราวการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)
ครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๘ พฤศจิกายน ๒๕๖๖ ที่ประชุมฯ ได้มีมติเห็นชอบประกาศสำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัย
ไซเบอร์ พ.ศ. ๒๕๖๗ และเมื่อวันที่ ๑๘ ธันวาคม ๒๕๖๖ เลขาธิการคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ ได้ลงนามในประกาศดังกล่าว และได้นำไปประกาศในราชกิจจานุเบกษาเล่มที่ ๑๔๑
ตอนพิเศษ ๓๗ ง ลงวันที่ ๘ กุมภาพันธ์ ๒๕๖๗ เรียบร้อยด้วยแล้ว รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ขอเรียนว่า
ประกาศดังกล่าว มีผลใช้บังคับตั้งแต่วันที่ ๙ กุมภาพันธ์ ๒๕๖๗ เป็นต้นไป มีวัตถุประสงค์เพื่อให้หน่วยงานของรัฐ
หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ นำไปใช้เป็นแนวทาง
ในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงาน
ในการดำเนินการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ให้สอดคล้องตามนโยบาย
การบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ในการนี้ เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้าง
พื้นฐานสำคัญทางสารสนเทศ ทราบถึงผลบังคับใช้ วัตถุประสงค์และรายละเอียดสาระสำคัญของประกาศ
ดังกล่าว สกมช. จึงขอแจ้งเวียนประกาศดังกล่าวมายังท่าน เพื่อนำไปใช้เป็นแนวทางในการจัดทำแผนการรักษา
ความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานได้อย่างถูกต้องครบถ้วน อีกทั้งยังเป็นการเสริมสร้างความรู้
ความเข้าใจและเตรียมการดำเนินการต่าง ๆ ให้เป็นไปตามที่กฎหมายกำหนด ต่อไป

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

พลอากาศตรี

(อมร ชมเชย)

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โทรศัพท์ ๐ ๒๕๐๒ ๗๘๒๖

ไปรษณีย์อิเล็กทรอนิกส์ cii@ncsa.or.th

เรียน อธิการบดี

ด้วย สกมช. ได้ เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗ และประกาศในราชกิจจานุเบกษาเล่มที่ ๑๔๑ ตอนพิเศษ ๓๗ ง ลงวันที่ ๘ กุมภาพันธ์ ๒๕๖๗ เรียบร้อย ด้วยแล้ว มีผลใช้บังคับตั้งแต่วันที่ ๙ กุมภาพันธ์ ๒๕๖๗ เป็นต้นไป มีวัตถุประสงค์เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ นำไปใช้เป็นแนวทาง ในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงาน ในการดำเนินการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ให้สอดคล้องตามนโยบาย การบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงเพื่อนำไปใช้เป็นแนวทางในการจัดทำ แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานได้อย่างถูกต้องครบถ้วนต่อไป

เพื่อโปรดทราบ และมอบ สวส. ดำเนินการในส่วนที่เกี่ยวข้องและประชาสัมพันธ์ต่อไป



๒๗ ก.พ. ๖๗

ทบทวน + ปิดด้วยเรื่อง ปี
๖๖๖๖๖๖

ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

พ.ศ. ๒๕๖๗

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และให้สำนักงานโดยความเห็นชอบของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของตนและเพื่อให้เป็นไปตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในหัวข้อที่ ๓ นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จึงสมควรกำหนดแนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ อันเป็นการกำหนดรายละเอียดในการจัดทำเอกสารที่ระบุข้อกำหนดและมาตรการการควบคุมเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานเพื่อประโยชน์ในการดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๒๒ (๒) และ (๓) และมาตรา ๔๔ วรรคสามแห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยความเห็นชอบของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุม ครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๘ พฤศจิกายน ๒๕๖๖ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“แผนการรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เอกสารที่ระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศในภาพรวม และการควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศที่ดำเนินการอยู่หรือที่จะดำเนินการ เพื่อให้เป็นไปตามข้อกำหนดเหล่านั้น

“การควบคุมความมั่นคงปลอดภัยไซเบอร์” หมายความว่า การป้องกันหรือมาตรการที่กำหนดขึ้น เพื่อดำเนินการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการ รักษาสภาพพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ

ข้อ ๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับการจัดทำประมวลแนวทาง ปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยให้ใช้แนวทางการจัดทำ แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ท้ายประกาศนี้ และเก็บรักษาไว้ที่หน่วยงานและส่งให้สำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเมื่อสำนักงานร้องขอ

ข้อ ๕ ในกรณีที่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศได้จัดทำและดำเนินการตามแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ อยู่ในวันก่อนวันที่ประกาศนี้ใช้บังคับ ให้หน่วยงานดำเนินการตามแผนการรักษาความมั่นคงปลอดภัย ไซเบอร์ดังกล่าวได้ต่อไป จนกว่าจะสิ้นสุดระยะเวลาที่กำหนดไว้ในแผน ในกรณีที่หน่วยงานไม่ได้กำหนด ระยะเวลาไว้ในแผนให้หน่วยงานดำเนินการตามแผนดังกล่าวได้ต่อไปอีกหนึ่งปีนับตั้งแต่วันที่ประกาศนี้ ใช้บังคับ

ข้อ ๖ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รักษาการ ตามประกาศนี้ และให้มีอำนาจกำหนดแบบและออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติ ตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้เลขาธิการมีอำนาจตีความและวินิจฉัยชี้ขาด แล้วรายงานให้คณะกรรมการการรักษาความมั่นคงปลอดภัย ไซเบอร์แห่งชาติทราบ ทั้งนี้ การตีความ และคำวินิจฉัยของเลขาธิการให้เป็นที่สิ้นสุด

ประกาศ ณ วันที่ ๒๕ มกราคม พ.ศ. ๒๕๖๗

พลอากาศตรี อมร ชมเชย

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์
ท้ายประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

บทนำ

เพื่อให้เป็นไปตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในหัวข้อที่ ๓ นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จึงสมควรกำหนดแนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อประโยชน์ในการดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วัตถุประสงค์

เพื่อเป็นแนวทางในการดำเนินการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

ขอบเขตการใช้

หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

การจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยควรประกอบด้วยรายละเอียด ๓ ส่วน ได้แก่

ส่วนที่ ๑ รายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง

ส่วนที่ ๒ การควบคุมความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๓ การบริหารแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

โดยมีรายละเอียดแต่ละส่วน ดังต่อไปนี้

ส่วนที่ ๑ รายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง ประกอบด้วย ๑๑ หัวข้อ ดังนี้

๑.๑ ชื่อและหมายเลขอ้างอิงระบบสารสนเทศ โดยหน่วยงานต้องกำหนดชื่อและหมายเลขอ้างอิงเฉพาะระบบ (Unique Identifier) ให้แก่ระบบสารสนเทศทุกระบบ

๑.๒ คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ ได้แก่ คำอธิบาย การทำงาน (Function) และวัตถุประสงค์ของระบบสารสนเทศ

๑.๓ เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ (Senior Information Security Officer) ให้ระบุรายละเอียดของผู้บริหารระดับสูงของหน่วยงานซึ่งเป็นผู้มีหน้าที่และอำนาจบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) (หรือ Head of Information Security ในกรณีที่หน่วยงานไม่มี CISO) หรือผู้ที่ได้รับมอบหมายให้รับผิดชอบในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศเป็นผู้มีหน้าที่และอำนาจจัดทำและทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยประสานงานร่วมกับเจ้าของระบบสารสนเทศ เจ้าของสารสนเทศ และผู้ที่เกี่ยวข้องกับระบบสารสนเทศ รวมถึงเป็นผู้ประสานงานกับบุคลากรของหน่วยงานในการกำหนดและตรวจสอบการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่มีการใช้งานร่วมกัน โดยต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

- (๑) ชื่อ
- (๒) ตำแหน่ง
- (๓) หน่วยงาน/ส่วนงาน
- (๔) ที่อยู่สำหรับการติดต่อ
- (๕) หมายเลขโทรศัพท์
- (๖) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

๑.๔ เจ้าของระบบสารสนเทศ (Information System Owner) ให้ระบุรายละเอียดของผู้รับผิดชอบระบบสารสนเทศ ซึ่งทำหน้าที่เกี่ยวกับการจัดซื้อ พัฒนา บูรณาการ เปลี่ยนแปลงหรือแก้ไขดำเนินงาน และบำรุงรักษาระบบสารสนเทศในภาพรวม โดยเจ้าของระบบสารสนเทศเป็นผู้มีส่วนในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกับเจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ ในการช่วยระบุและตรวจสอบการควบคุมความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ รวมถึงดำเนินการตามแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ และหากมีการเปลี่ยนแปลงที่สำคัญที่เกี่ยวข้องกับระบบสารสนเทศเกิดขึ้น เจ้าของระบบสารสนเทศต้องดำเนินการแจ้งเจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศทราบ โดยต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

- (๑) ชื่อ
- (๒) ตำแหน่ง
- (๓) หน่วยงาน/ส่วนงาน
- (๔) ที่อยู่สำหรับการติดต่อ
- (๕) หมายเลขโทรศัพท์
- (๖) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

๑.๕ เจ้าของสารสนเทศ (Information Owner) ให้ระบุรายละเอียดของผู้มีอำนาจโดยกฎหมายหรือโดยการได้รับมอบหมายให้ดำเนินงานเกี่ยวกับสารสนเทศนั้น หรือรายละเอียดของผู้มีหน้าที่รับผิดชอบกำหนดมาตรการควบคุมสำหรับการสร้าง การรวบรวม การประมวลผล การเผยแพร่ และการทำลายสารสนเทศดังกล่าว โดยเจ้าของสารสนเทศควรมีส่วนในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกับเจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ ในการให้ข้อมูลเกี่ยวกับความต้องการด้านความมั่นคงปลอดภัยของสารสนเทศ และร่วมพิจารณากำหนดหรืออนุญาตสิทธิและประเภทของสิทธิในการเข้าถึงสารสนเทศให้แก่บุคคล (หรือผู้ดำรงตำแหน่ง) หรือหน่วยงาน รวมทั้งช่วยในการระบุและตรวจสอบการควบคุมความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ โดยต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

- (๑) ชื่อ
- (๒) ตำแหน่ง
- (๓) หน่วยงาน/ส่วนงาน
- (๔) ที่อยู่สำหรับการติดต่อ
- (๕) หมายเลขโทรศัพท์
- (๖) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

๑.๖ เจ้าหน้าที่ที่มีอำนาจ (Authorizing Official) ให้ระบุรายละเอียดของผู้บริหารระดับสูงขององค์กรซึ่งมีหน้าที่รับผิดชอบในการดำเนินงานระบบสารสนเทศ ในระดับความเสี่ยง (ต่อการดำเนินงานภารกิจ หน้าที่ ภาพลักษณ์ หรือทรัพย์สินของหน่วยงานหรือของบุคคล) ที่หน่วยงานยอมรับได้และมีอำนาจอนุมัติหรือรับรองแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือผู้ที่ได้รับมอบหมาย โดยต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

- (๑) ชื่อ
- (๒) ตำแหน่ง
- (๓) หน่วยงาน/ส่วนงาน
- (๔) ที่อยู่สำหรับการติดต่อ
- (๕) หมายเลขโทรศัพท์
- (๖) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคนให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด

๑.๗ ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ (Other Designated Contact) ให้ระบุรายละเอียดของบุคคลที่มีความเกี่ยวข้องกับระบบสารสนเทศ ดังต่อไปนี้

- (๑) ผู้ที่สามารถให้ข้อมูลเกี่ยวกับการดำเนินการและคุณลักษณะของระบบสารสนเทศ
- (๒) ผู้ที่มีส่วนร่วมในการดำเนินการพัฒนาและปรับปรุงแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) ผู้ที่ได้รับมอบหมายจากบุคคลตาม (๑) หรือ (๒) ให้กระทำการแทนรายละเอียดของบุคคลตามวรรคหนึ่ง ต้องมีอย่างน้อยดังต่อไปนี้

- (๑) ชื่อ
- (๒) ตำแหน่ง
- (๓) หน่วยงาน/ส่วนงาน
- (๔) ที่อยู่สำหรับการติดต่อ
- (๕) หมายเลขโทรศัพท์
- (๖) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

๑.๘ การกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์ ให้ระบุรายละเอียดเกี่ยวกับการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ (Security Category) ให้แก่ระบบสารสนเทศจากการประเมินและจัดระดับผลกระทบต่อการดำเนินงานของหน่วยงาน ทรัพย์สินของหน่วยงาน หรือความปลอดภัยของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงาน หรือประชาชน ในกรณีที่มีเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หรือเหตุภัยคุกคามทางไซเบอร์เกิดขึ้น โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ของระบบย่อยแต่ละระบบภายใต้ระบบสารสนเทศในเรื่อง (๑) การรักษาความลับ (Confidentiality) (๒) การรักษาความถูกต้องครบถ้วน (Integrity) และ (๓) การรักษาสภาพพร้อมใช้งาน (Availability) และใช้ระดับผลกระทบของประเภทข้อมูลตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ในแต่ละเรื่องที่มีระดับผลกระทบมากที่สุด

การกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศตามวรรคหนึ่ง ให้ดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

๑.๙ สถานะของระบบสารสนเทศ ให้ระบุสถานะของระบบโดยเลือกจากสถานะใดสถานะหนึ่งดังต่อไปนี้

(๑) สถานะอยู่ระหว่างการพัฒนา หมายถึง ระบบใหม่ที่อยู่ระหว่างขั้นตอนการออกแบบพัฒนา หรือทดสอบการใช้งาน

(๒) สถานะดำเนินการ หมายถึง ระบบดำเนินการหรือใช้งานในปัจจุบัน

(๓) สถานะอยู่ระหว่างการปรับปรุง หมายถึง ระบบอยู่ระหว่างการปรับปรุง แก้ไขหรือเปลี่ยนแปลง และไม่มีการใช้งาน

๑.๑๐ การเชื่อมต่อระบบสารสนเทศและการใช้งานข้อมูลร่วมกัน ให้ระบุรายละเอียดที่เกี่ยวข้องกับการเชื่อมต่อกับระบบสารสนเทศอื่นในเรื่อง ดังต่อไปนี้

(๑) ชื่อระบบสารสนเทศที่เชื่อมต่อ ชื่อหน่วยงานของระบบสารสนเทศที่เชื่อมต่อ และชนิดของการเชื่อมต่อ (เช่น ผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น)

(๒) รายละเอียดการให้สิทธิในการเชื่อมต่อ ได้แก่ วันที่ การกำหนดคุณลักษณะของระบบสารสนเทศที่เชื่อมต่อ การรับรองมาตรฐานด้านความมั่นคงปลอดภัยและสถานะการรับรองมาตรฐานด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่เชื่อมต่อ และชื่อและตำแหน่งของผู้ได้รับมอบอำนาจของระบบสารสนเทศที่เชื่อมต่อ

๑.๑๑ นโยบาย ระเบียบ หรือกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศ ให้ระบุนโยบาย ระเบียบ หรือกฎหมายที่ส่งผลโดยตรงกับการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ

ส่วนที่ ๒ การควบคุมความมั่นคงปลอดภัยไซเบอร์

ให้ระบุรายละเอียดการดำเนินการที่เป็นมาตรฐานขั้นต่ำสำหรับการควบคุมความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ (Minimum Security Control) ตามหลักเกณฑ์ที่กำหนดในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ เพื่อให้เหมาะสมกับการกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศตามข้อ ๑.๘

ส่วนที่ ๓ การบริหารงานแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย

๓.๑ วันที่จัดทำและลายมือชื่อผู้จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒ วันที่ที่อนุมัติและลายมือชื่อผู้อนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๓ กำหนดเวลาทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ และชื่อผู้รับผิดชอบ

ในการติดตามการทบทวนแผน

๓.๔ สาเหตุการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเลือกจากสาเหตุใดสาเหตุหนึ่ง ดังต่อไปนี้

(๑) จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับแรก หมายถึง การจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นใหม่เป็นครั้งแรก หรือจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นใหม่ทั้งฉบับแทนฉบับเดิม

(๒) ทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ตามรอบที่กำหนด หมายถึง การทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่กำหนดไว้ในแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับที่ใช้บังคับอยู่ในขณะนั้น

(๓) ทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์เนื่องจากการเปลี่ยนแปลง หมายถึง การทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์เนื่องจากการเปลี่ยนแปลงที่สำคัญ โดยต้องระบุความเปลี่ยนแปลงดังกล่าวด้วย

ทั้งนี้ กระบวนการทบทวนแผนควรดำเนินการทุกปี หรือดำเนินการก่อนรอบหนึ่งปี หากมีการเปลี่ยนแปลงที่สำคัญ เช่น มีการเปลี่ยนแปลงระดับความเสี่ยงเพิ่มขึ้นเกินกว่าระดับความเสี่ยงที่ยอมรับได้ กฎหมายที่เกี่ยวข้องกับการจัดทำหรือดำเนินการตามแผนการรักษาความมั่นคงปลอดภัยไซเบอร์มีการเปลี่ยนแปลงในสาระสำคัญ มีการเปลี่ยนแปลงลักษณะของภัยคุกคามทางไซเบอร์ มีการเปลี่ยนแปลงเกี่ยวกับบุคคลที่เกี่ยวข้องกับแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ (เช่น การเปลี่ยนแปลงเจ้าของระบบสารสนเทศ ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ หรือเจ้าหน้าที่ที่มีอำนาจ เป็นต้น) ระบบสารสนเทศมีการเปลี่ยนแปลง สถานะของระบบสารสนเทศ มีการเปลี่ยนแปลง หรือการเชื่อมต่อระบบสารสนเทศมีการเปลี่ยนแปลง เป็นต้น

สัญลักษณ์หน่วยงาน
(หากมี)

แผนรักษาความมั่นคงปลอดภัยไซเบอร์

ชื่อระบบ

หมายเลขอ้างอิง

Version	Changes	Changed by On Date	Reviewed by/Approved by On Date

หมายเลขอ้างอิง - version ...

ส่วนที่ ๑ รายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง

ชื่อ	
หมายเลขอ้างอิง	
คำอธิบายและวัตถุประสงค์ของระบบสารสนเทศ	
เจ้าหน้าที่ระดับอาวุโสด้านความมั่นคงปลอดภัยของสารสนเทศ*	
ชื่อ	
ตำแหน่ง	
หน่วยงาน	
ที่อยู่สำหรับการติดต่อ	
หมายเลขโทรศัพท์	
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	
เจ้าของระบบสารสนเทศ*	
ชื่อ	
ตำแหน่ง	
หน่วยงาน/ส่วนงาน	
ที่อยู่สำหรับการติดต่อ	
หมายเลขโทรศัพท์	
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	

หมายเหตุ *สามารถระบุผู้ที่เกี่ยวข้องได้มากกว่า ๑ ท่าน

เจ้าของสารสนเทศ*	
ชื่อ	
ตำแหน่ง	
หน่วยงาน/ส่วนงาน	
ที่อยู่สำหรับการติดต่อ	
หมายเลขโทรศัพท์	
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	
เจ้าหน้าที่ที่มีอำนาจ* (Authorizing Official)	
ชื่อ	
ตำแหน่ง	
หน่วยงาน/ส่วนงาน	
ที่อยู่สำหรับการติดต่อ	
หมายเลขโทรศัพท์	
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	
หมายเหตุ	เจ้าหน้าที่ที่มีอำนาจต้องไม่เป็นเจ้าของระบบสารสนเทศ และในกรณีมีเจ้าหน้าที่ที่มีอำนาจมากกว่าหนึ่งคน ให้กำหนดแนวทางการอนุมัติแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ด้วย เช่น ต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจทุกคน หรือต้องได้รับความเห็นชอบจากเจ้าหน้าที่ที่มีอำนาจไม่น้อยกว่ากึ่งหนึ่งของจำนวนเจ้าหน้าที่ที่มีอำนาจทั้งหมด
ผู้ที่เกี่ยวข้องกับระบบสารสนเทศ* (Other Designated Contact)	
ชื่อ	
ตำแหน่ง	
หน่วยงาน/ส่วนงาน	
ที่อยู่สำหรับการติดต่อ	
หมายเลขโทรศัพท์	
ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)	

หมายเหตุ *สามารถระบุผู้ที่เกี่ยวข้องได้มากกว่า ๑ ท่าน

การกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์

.....

.....

(ดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติว่าด้วยมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ)

สถานะของระบบสารสนเทศ

สถานะอยู่ระหว่างการพัฒนา

สถานะดำเนินการ

สถานะอยู่ระหว่างการปรับปรุง

การเชื่อมต่อระบบสารสนเทศและการใช้งานข้อมูลร่วมกัน

ชื่อระบบ	หน่วยงาน	ชนิดการเชื่อมต่อ	การให้สิทธิ์ในการเชื่อมต่อ	วันที่	การกำหนดคุณลักษณะของระบบที่เชื่อมต่อ	การรับรองและสถานะการรับรอง	ชื่อระบบ

นโยบาย ระเบียบ หรือกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศ

.....

.....

ส่วนที่ ๒ การควบคุมความมั่นคงปลอดภัยไซเบอร์

(รายละเอียดการดำเนินการที่เป็นมาตรฐานขั้นต่ำสำหรับการควบคุมความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ (Minimum Security Control) ตามหลักเกณฑ์ที่กำหนดในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ เพื่อให้เหมาะสมกับการกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศ)

ส่วนที่ ๓ การบริหารงานแผนการรักษาความมั่นคงปลอดภัยไซเบอร์

สาเหตุในการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์	
<input type="checkbox"/> จัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับแรก <input type="checkbox"/> ครั้งแรก <input type="checkbox"/> แทนฉบับเดิม..... <input type="checkbox"/> ทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ตามรอบที่กำหนด <input type="checkbox"/> ทบทวนแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ เนื่องจากมีความเปลี่ยนแปลงที่สำคัญ (ระบุ)..... 	
การจัดทำแผน	
วันที่	ลายมือชื่อผู้จัดทำแผน
การอนุมัติแผน	
วันที่	ลายมือชื่อผู้อนุมัติแผน
การทบทวนแผน	
ทบทวนภายในวันที่	ผู้รับผิดชอบในการดำเนินการทบทวนแผน ชื่อ ตำแหน่ง หน่วยงาน/ส่วนงาน..... ที่อยู่สำหรับการติดต่อ..... เบอร์โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ (e-mail).....