กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรมแพทย์ทหารเรือ

มกราคม ๒๕๖๘

กองเวชสารสนเทศ กรมแพทย์ทหารเรือ

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
กรมแพทย์ทหารเรือ

ประวัติการแก้ไขเอกสาร

เวอร์ชัน	รายละเอียดการแก้ไข	วันที่จัดทำ
๐๑	เอกสารเวอร์ชันตั้งต้น	๑๖ มกราคม ๒๕๖๘
๐๒	เอกสารปรับปรุงครั้งที่ ๑	๙ พฤษภาคม ๒๕๖๘

การอนุมัติเอกสาร

ผู้จัดทำ	ผู้ทบทวน	ผู้อนุมัติ
น.ท.ชัยยา จารุภาค (หน.สารสนเทศ)	น.อ.หญิง ปิติยา ปิยะนุช (ผอ.กวส.พร./ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (ISMR))	พล.ร.ต.เรวัตร กิจณรงค์ (รอง จก.พร./ผู้บริหารรักษาความมั่นคงปลอดภัยไซเบอร์ระดับสูง (CISO))

สารบัญ

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และไปในทิศทางเดียวกัน กรมแพทย์ทหารเรือ(พร.) ในฐานะหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล จึงจัดทำ กรอบมาตรฐานด้านการรักษาความปลอดภัยไซเบอร์ถือปฏิบัติ โดยอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงาน ของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔

๑.๒ วัตถุประสงค์

เพื่อกำหนดกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งนำไปใช้ในการดำเนินงานและการจัดการระบบงานเทคโนโลยีสารสนเทศของ พร. ให้มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน

๑.๓ ขอบเขต

เอกสารฉบับนี้ครอบคลุมตามกรอบและวิธีปฏิบัติสำหรับด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ใช้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

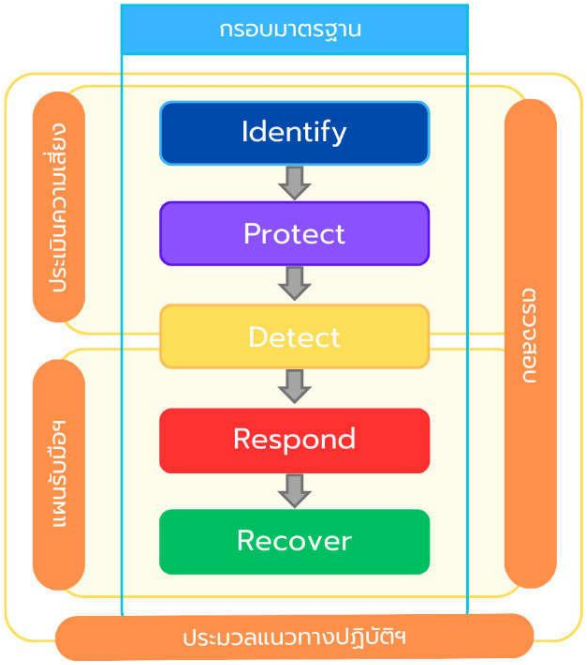
๑.๔ คำนิยาม

๑) หน่วยงาน หรือ องค์กร	หมายถึง	กรมแพทย์ทหารเรือ หรือ พร.
๒) คณะกรรมการ	หมายถึง	คณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์
๓) กกม.	หมายถึง	คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
๔) สกมช.	หมายถึง	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๕) ดัชนีชี้วัดความเสี่ยงที่สำคัญ	หมายถึง	เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์

		เหตุการณ์ และความเสี่ยงในอนาคต และเตรียมมาตรการการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย
๖) คอมไพเลอร์	หมายถึง	โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
๗) แพตช์	หมายถึง	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟแวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟแวร์ ผู้พัฒนาซอฟแวร์หลาย รายได้เผยแพร่แพตช์ (Patch) ออกมาเป็นระยะเช่น บริษัท Microsoft มีการ เผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update
๘) Recovery Time Objective (RTO)	หมายถึง	ระยะเวลาในการกู้คืนระบบ
๙) Recovery Point Objective (RPO)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
๑๐) Maximum Tolerance Period of Disruption (MTPD)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และรองรับการเกิดเหตุการณ์ผิดปกติ ต่างๆ ที่อาจส่งผลให้เกิดการหยุดชะงัก หรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
๑๑) ผู้ใช้งาน	หมายถึง	ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างตามสัญญาจ้าง ในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้ เครื่องคอมพิวเตอร์ และระบบเครือข่าย ของ พร.
๑๒) บุคคลภายนอก	หมายถึง	บุคคลจากหน่วยงานภายนอกที่เข้ามาประชุม หรือปฏิบัติงานร่วมกับหน่วยงาน
๑๓) หน่วยงานภายนอก	หมายถึง	หน่วยงานภายนอกที่หน่วยงานอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูล หรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้งานตาม อำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๔) สิทธิ์ของผู้ใช้งาน	หมายถึง	สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และ สิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
๑๕) ผู้ดูแลระบบ	หมายถึง	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบ ดูแล รักษา หรือจัดการระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบงาน
๑๖) สินทรัพย์	หมายถึง	ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตน อันมีมูลค่าคุณค่าสำหรับหน่วยงาน
๑๗) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	หมายถึง	การขออนุญาต การกำหนดสิทธิ์ หรือมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบสารสนเทศและระบบเครือข่าย
๑๘) ความมั่นคงปลอดภัยด้านสารสนเทศ	หมายถึง	การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ

บทที่ ๒
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



รูปที่ ๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Identify)

รูปที่ ๒ การประเมินความเสี่ยง

๒.๑.๑ การจัดการสินทรัพย์ (Asset Management)

๒.๑.๑.๑ จัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน

๒.๑.๑.๒ ระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๒.๑.๑.๓ มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใดๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๒.๑.๑.๔ มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของ พร. ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ในข้อ ๒.๑.๑.๑ อย่างน้อยปีละ ๑ ครั้ง

๒.๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๒.๑.๒.๑ ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของ พร. ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management)

๒.๑.๒.๒ กำหนดปัจจัยต่างๆ ที่เกี่ยวข้องกับการประเมินความเสี่ยงที่เกิดขึ้นจากปัจจัยภายนอก เช่น การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๑.๒.๓ ปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๒.๑.๓.๑ ตรวจสอบข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่มีการประกาศบนเว็บไซต์ หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่างๆ ที่มีการใช้งานบนระบบสารสนเทศของหน่วยงาน หรือจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติ (ThaiCERT)

๒.๑.๓.๒ ประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยงของ พร. เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญของ พร.

๒.๑.๓.๓ การตรวจสอบขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

๑) ประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

๒) ประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

๓) ตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๒.๑.๓.๔ ประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใดๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใดๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๒.๑.๓.๕ การทดสอบเจาะระบบ (Penetration Testing) สำหรับบริการที่สำคัญ โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๒.๑.๓.๖ ตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ โดยเฉพาะอย่างยิ่งทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๒.๑.๓.๗ พิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อย ๒ ปีครั้ง ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๒.๑.๓.๘ ตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

๒.๑.๓.๙ ตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของ พร.

๒.๑.๓.๑๐ มีกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไข

๒.๑.๓.๑๑ หากได้รับการร้องขอจาก กกม. หรือ สกมช. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานดังกล่าว ไปยัง สกมช. ภายในกำหนด ๓๐ วัน นับแต่วันที่ได้รับหนังสือด้วย

๒.๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

๒.๑.๔.๑ แจ้งผู้ให้บริการภายนอกได้รับทราบถึงรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอก จะดำเนินงานใดๆ ก็ตามในส่วนของบริการที่สำคัญของ พร.

๒.๑.๔.๒ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้อง กับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของ พร. ตามความต้องการทางธุรกิจขององค์กรและโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของ พร. จากภัยคุกคามทางไซเบอร์

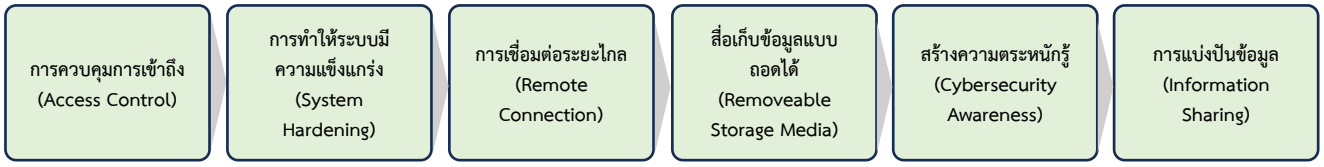
๓) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

๔) สิทธิ์ของ พร. ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๒.๑.๔.๓ สร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สามและการตรวจสอบผลิตภัณฑ์

๒.๑.๔.๔ ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

๒.๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)



รูปที่ ๓ การป้องกันความเสี่ยง

๒.๒.๑ การควบคุมการเข้าถึง (Access Control)

๒.๒.๑.๑ การเข้าถึงบริการที่สำคัญของ พร. ถูกจำกัดไว้ที่

๑) บุคลากร/เจ้าหน้าที่ที่ปฏิบัติงานให้ พร. และกิจกรรมที่ได้รับอนุญาตจาก พร.

๒) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตจาก พร.

๒.๒.๑.๒ ให้แต่ละบุคลากร/เจ้าหน้าที่ กิจกรรมและกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญของ พร. ต้องมีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ

๒.๒.๑.๓ เก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายาม ทั้งหมดในการเข้าถึงบริการที่สำคัญของ พร. และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๒.๒.๑.๔ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) อยู่ภายใต้การดูแลของ พร. เท่านั้น และควรพิจารณาให้ดำเนินการในสถานที่ของ พร. (หากเป็นไปได้)

๒.๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๒.๑ สร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของ พร.

๒.๒.๒.๒ มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒) แบ่งแยกหน้าที่ (Separation of Duties)

๓) บังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๔) ลบบัญชีที่ไม่ได้ใช้

๕) ลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น ลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๖) ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗) การป้องกันมัลแวร์ (Malware)

๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

๙) ปิดการใช้งานอัลกอริทึมที่ไม่มีความปลอดภัย เช่น 3DES, RC4, SSLv2, SSlv3

๒.๒.๒.๓ ตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใดๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ

๒.๒.๒.๔ ตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒.๒.๒.๕ จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ

๒.๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๒.๒.๓.๑ ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของ พร. มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

๑) เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น

๒) ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง

๓) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

๔) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างชัดเจน

๕) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๒.๔.๑ ตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญของ พร. โดยใช้มาตรการอย่างน้อย ดังนี้

๑) ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

๒) สื่อบันทึกข้อมูลทุกประเภท และทุกชนิด ต้องได้รับอนุญาตก่อนนำมาเชื่อมต่อทั้งหมด

๓) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมด ไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ

๒.๒.๔.๒ เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญ บนสื่อบันทึกข้อมูลแบบถอดได้

๒.๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒.๒.๕.๑ ให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สาม ที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๑) มีกิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่ พนักงานใหม่ (New Employees) ผู้ใช้และระดับบริหาร (Users and Management) เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

๒) เผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของ พร.

๓) ให้ความรู้ด้านกฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๔) การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ ผลกระทบและการบรรเทาผลกระทบ

๒.๒.๕.๒ ต้องทบทวนแผนงาน/กิจกรรมในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

๒.๒.๖ การแบ่งปันข้อมูล (Information Sharing)

กำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใดๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญ และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญ) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

รายละเอียด แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงาน และสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่ สกมช. ประกาศกำหนด

๒.๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

ตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
(Cyber Threat Detection and Monitoring)

รูปที่ ๔ ตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

๒.๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๒.๓.๑.๑ มีกลไกและกระบวนการเพื่อตรวจจับ จัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และมีการวิเคราะห์ว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญหรือไม่

๒.๓.๑.๒ ดำเนินการทบทวนกลไกและกระบวนการภายในข้อ ๒.๓.๑.๑ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่างๆ ยังคงมีประสิทธิภาพ

๒.๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

รูปที่ ๕ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

๒.๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๒.๔.๑.๑ มีการจัดทำและสื่อสาร แผนรับมือภัยคุกคามทางไซเบอร์ให้ผู้เกี่ยวข้องทราบ

๒.๔.๑.๒ มีการฝึกซ้อมแผนการรับมือภัยคุกคามไซเบอร์ที่กำหนดขึ้น อย่างน้อยปีละ ๑ ครั้ง

๒.๔.๑.๓ ต้องมีการทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๒.๔.๒.๑ มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒.๔.๒.๒ แผนการสื่อสารในภาวะวิกฤต ประกอบไปด้วย

๑) มีการจัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

๒) มีการระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

๓) มีการระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๔) มีการระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อมีการกล่าวแถลงกับสื่อมวลชน

๕) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๒.๔.๒.๓ ตรวจสอบแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๒.๔.๒.๔ ดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้งเพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒.๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๒.๔.๓.๑ สนับสนุนบุคลากรและเจ้าหน้าที่ ให้เข้าร่วมฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าว อาจดำเนินการได้ ทั้งในระดับชาติหรือระดับภาคส่วน โดยบุคลากรและเจ้าหน้าที่ที่อยู่ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

๒.๔.๓.๒ เข้าร่วมฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ตามที่คณะกรรมการกำหนด อย่างน้อยปีละ ๑ ครั้ง

๒.๔.๓.๓ ปฏิบัติตามคำขอของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้อง กับบริการที่สำคัญเพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการ อาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้น

๒.๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์
(Cybersecurity Resilience and Recovery)

รูปที่ ๖ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

๒.๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๒.๕.๑.๑ เพื่อให้การดำเนินการกู้คืนระบบการให้บริการที่สำคัญ สอดคล้องกับแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) จึงได้กำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ ที่เกี่ยวข้องกับบริการที่สำคัญ ดังนี้

๑) กำหนดบทบาทหน้าที่ความรับผิดชอบให้ชัดเจน

๒) กำหนดเป้าหมายการกู้คืนระบบที่เกี่ยวข้องกับบริการที่สำคัญ โดยระยะเวลาเป้าหมายการกู้คืนระบบการให้บริการที่สำคัญ มีดังนี้

(๑) ระยะเวลาเป้าหมายสำหรับการกู้คืนกระบวนการที่มีความสำคัญ (RTO) ๒๔ ชั่วโมง

(๒) ระยะเวลามากที่สุดที่ยอมให้ข้อมูลสูญหายนับจากมีการแจ้งเหตุฯ (RPO) ๓ วัน

(๓) ระยะเวลานานที่สุดที่องค์กรยอมรับได้หากมีการหยุดชะงัก (MTPD) ๒๔ ชั่วโมง

๓) ความเสี่ยงและมาตรการลดความเสี่ยง อ้างอิงเอกสาร การประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ พร.

๔) แผนกู้คืนระบบที่เกี่ยวข้องกับบริการที่สำคัญ

(กรณีที่ ๑) เมื่อเกิดเหตุการณ์ที่มีการบุกรุกจากภายนอก โดยประเมินแล้วเหตุการณ์มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการตามแผนกู้คืนดังนี้

(๑) ตรวจสอบ log และการตั้งค่า Firewall เพื่อวิเคราะห์หาสาเหตุการเข้ามาและผลกระทบที่เกิดขึ้น

(๒) แจ้งให้หัวหน้ากลุ่มเทคโนโลยีและสารสนเทศทราบ

(๓) ดำเนินการการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆ ที่ถูกบุกรุกเข้ามา

(กรณีที่ ๒) เมื่อเกิดเหตุการณ์ที่มีการมีการแพร่กระจายของไวรัส (Virus) มัลแวร์ (Malware) มัลแวร์เรียกค่าไถ่ หรือแรนซัมแวร์ (Ransomware) โดยประเมินแล้วเหตุการณ์มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการตามแผนกู้คืนดังนี้

(๑) ตัดการเชื่อมต่อทางเครือข่าย สำหรับเครื่องคอมพิวเตอร์ที่โดนมัลแวร์ ระบบสำรองข้อมูล รวมถึงตัดการเชื่อมต่ออุปกรณ์จัดเก็บข้อมูลภายนอก และระบบสารสนเทศที่อยู่ในเครือข่ายเดียวกัน

(๒) แจ้งให้หัวหน้ากลุ่มเทคโนโลยีและสารสนเทศทราบ

(๓) ตรวจสอบเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายเดียวกับเครื่องที่ติดมัลแวร์ เพื่อประเมินสถานการณ์ด้วยวิธีการดังนี้

- ตรวจสอบความผิดปกติภายในเครื่องคอมพิวเตอร์
- Full Scan ใน Anti-Virus และ Anti-Malware

(๔) ประสานเพื่อขอความช่วยเหลือไปยัง ทร. และ/หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เบอร์ติดต่อ ๐๒-๑๔๒๖๘๘๘ และศูนย์ประสานการรักษาความมั่นคง ปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ผ่านทางโทรศัพท์เบอร์ติดต่อ ๐๒-๑๒๓๑๒๑๒

(๕) ปฏิบัติตามคำแนะนำของผู้เชี่ยวชาญ

(๖) กรณีเครื่อง Client ใช้คอมพิวเตอร์สำรอง ข้อมูลที่ถูกสำรองไว้ หรือข้อมูลบน Cloud ในการทำงาน โดยไม่ยุ่งเกี่ยวกับข้อมูลหรือเครื่องคอมพิวเตอร์ที่ติดมัลแวร์จนกว่าการแก้ไข สถานการณ์จะสิ้นสุดลง

(๗) กรณีเครื่อง Server ประสานงานผู้ให้บริการภายนอก เพื่อดำเนินการกู้คืนข้อมูลจากอุปกรณ์ที่ได้ดำเนินการ Backup ไว้

๕) การกลับสู่ภาวะปกติ

(๑) กรณี Client ทำการล้างเครื่องทั้งหมดแบบ Clean format ไม่ให้มีข้อมูลหลงเหลือใน Hard Disk ก่อนทำการลงเครื่องใหม่ ทั้งหมด

(๒) กรณี Server ทำการ Restore Backup Data, Application and Configuration

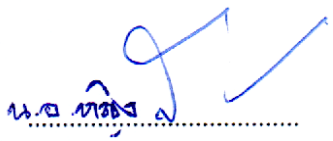
(๓) ดำเนินการ Test Restore

(๔) ตั้งค่าระบบ การกำหนด Vhost เพื่อให้ผู้ใช้งานสามารถใช้เข้าใช้งานได้ตามปกติ

(๕) ทดสอบความพร้อมใช้งานของระบบและความครบถ้วนของข้อมูลที่กู้คืน

(๖) รายงานผลการกู้คืนให้หัวหน้ากลุ่มเทคโนโลยีและสารสนเทศรับทราบ

๒.๕.๑.๒ มีการฝึกซ้อมแผนการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์



(ปิติยา ปิยะนุช)
ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ

แผนกปฏิบัติการเทคโนโลยีสารสนเทศ
กองเวชสารสนเทศ กรมแพทย์ทหารเรือ
โทร. ๕๒๙๖๔