ประกาศกองบังคับการปราบปราม
เรื่อง แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของ กองบังคับการปราบปราม พ.ศ. .....

เพื่อให้กองบังคับการปราบปรามเป็นหน่วยงานที่มีมาตราฐานเป็นที่เชื่อถือ มีความมั่นคงปลอดภัย และมีประสิทธิภาพในการทำงาน สามารถรับมือกับภัยคุกคามที่ทวีจำนวนและรูปแบบที่ซับซ้อนขึ้นในปัจจุบัน จึงจัดทำแนวนโยบายและแนวปฏิบัติเพื่อใช้เป็นแนวทางและมาตรฐาน ให้บุคลากรและผู้เกี่ยวข้องทุกภาคส่วนได้ปฏิบัติและยึดถือ ซึ่งสอดคล้องและมุ่งสู่การมีมีความมั่นคงปลอดภัยและเชื่อถือได้ ต่อไป

ข้อ ๑ ในประกาศนี้

“กองบังคับการ” หมายถึง กองบังคับการปราบปราม

“นโยบาย” หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในรูปแบบของการสืบสวนและสอบสวนที่กองบังคับการจัดไว้ให้บริการประชาชน ซึ่งกองบังคับการประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของกองบังคับการที่เกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

“แนวปฏิบัติ” หมายถึง ขั้นตอนวิธีการที่กองบังคับการได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของเจ้าหน้าที่และผู้ปฏิบัติงานของกองบังคับการที่เกี่ยวข้องกับการสืบสวน โดยมีจุดมุ่งหมายเพื่อให้การสืบสวนนั้น มีวิธีการที่มั่นคงปลอดภัย

“ผู้ใช้งาน” หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบของกองบังคับการ ผู้บริหารกองบังคับการ ผู้ใช้บริการ และผู้ใช้งานที่ใช้บริการระบบเทคโนโลยีสารสนเทศของกองบังคับการ

“บัญชีผู้ใช้งาน” หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกองบังคับการ

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับระบบสารสนเทศของกองบังคับการ

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“สินทรัพย์” หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

“สินทรัพย์คอมพิวเตอร์” หมายความว่า โปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีด้วย

“สารสนเทศ” หมายถึง ข้อมูลในรูปแบบต่างๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจ หรือใช้ประโยชน์ต่างๆ ตามภารกิจของกองบังคับการ

“เครือข่าย” หมายความว่า ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ ๒ เครื่องขึ้นไปเข้าด้วยกัน เพื่อสะดวกต่อการร่วมใช้ข้อมูล โปรแกรม หรือเครื่องพิมพ์ และอำนวยความสะดวกในการติดต่อแลกเปลี่ยนข้อมูลระหว่างเครื่องได้ตลอดเวลา

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของกองบังคับการถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“ผู้บริหารระดับสูงสุด” หมายความว่า ผู้บังคับการกองบังคับการปราบปราม

ข้อ ๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองบังคับการ แบ่งเป็น ๒ ส่วน ได้แก่

ส่วนที่ ๑ แนวนโยบาย

ส่วนที่ ๒ แนวปฏิบัติ

รายละเอียดภายในของทั้งสองส่วน ประกอบด้วยเนื้อหาสาระสำคัญในประเด็นต่อไปนี้

(๑) การรักษาความปลอดภัยทางกายภาพ

(๒) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย

(๓) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์

(๔) การควบคุมการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน

(๕) การสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

(๖) การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

(๗) การจัดซื้อจัดจ้างระบบสารสนเทศ

(๘) การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น

(๙) การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

(๑๐) การแบ่งแยกอำนาจหน้าที่

(๑๑) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

(๑๒) การเผยแพร่ข้อมูลต่อสาธารณะ

(๑๓) การพัฒนาและบำรุงรักษาระบบ

ข้อ ๓ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองบังคับการให้เป็นไปตามที่กำหนดไว้ในแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองบังคับการปราบปราม พ.ศ. .....

ข้อ ๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบ และควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ และตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกองบังคับการอย่างน้อยปีละ ๑ ครั้ง ด้วยผู้ตรวจสอบภายในหน่วยงานของกองบังคับการ

ข้อ ๕ สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานของกองบังคับการ เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ด้วยวิธีการ ดังนี้

(๑) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์กองบังคับการและบอร์ดประชาสัมพันธ์ให้แก่ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

(๒) จัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงโดยผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ ๖ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ

ข้อ ๗ ให้กองบังคับการปราบปรามเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้รวมถึงกำหนดให้มีการปฏิบัติที่ชัดเจนและให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง ทั้งนี้หากมีความเสี่ยงที่เกิดขึ้นอย่างเด่นชัด ได้แก่ การนำระบบสารสนเทศใหม่เข้ามาใช้งาน กฎหมาย หรือข้อบังคับใหม่ เป็นต้น อันมีผลกับการดำเนินการของกองบังคับการ หรือหากนโยบายและแนวปฏิบัติปัจจุบันยังไม่ตอบสนองต่อภารกิจและความเสี่ยงเหล่านี้ได้อย่างเหมาะสม กองบังคับการต้องมีทบทวนปรับปรุงนโยบายและข้อปฏิบัติ เพื่อปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย และรับมือกับความเสี่ยงเหล่านี้ได้อย่างเหมาะสม ทันการณ์

ข้อ ๘ ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ

(๑) การควบคุมการเข้าถึงสารสนเทศ

(๒) การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๙ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้เจ้าหน้าที่ทุกภาคส่วนในองค์กร ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของกองบังคับการ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ เดือน พ.ศ. ๒๕๖๓

ยศ

(.....)

ผู้บังคับการปราบปราม