คำนำ

ด้วยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลใช้บังคับเมื่อวันที่ 18 กรกฎาคม พ.ศ. 2550 ที่ผ่านมา โดยมีเจตนารมณ์เพื่อกำหนดฐานความผิด บทลงโทษ และอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ ซึ่งมีความรู้และความเชี่ยวชาญในการสืบสวนสอบสวนเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ร่วมกับหน่วยงานอื่นที่เกี่ยวข้อง รวมทั้งกำหนดหน้าที่ของผู้ให้บริการ ซึ่ง มีบทบาทสำคัญอย่างยิ่งในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ อันจะใช้เป็นพยานหลักฐานที่สำคัญในการนำตัวผู้กระทำความผิดมาลงโทษ

การบังคับใช้กฎหมายฉบับนี้ จึงนับเป็นโครงสร้างพื้นฐานทางกฎหมายที่มีคุณประโยชน์อย่างยิ่ง หากแต่ก็อาจส่งผลกระทบต่อการดำเนินวิถีชีวิตของผู้คนในสังคมได้เช่นกัน ดังนั้น เพื่อให้กฎหมายมีความยืดหยุ่นและสามารถบังคับใช้ได้อย่างมีประสิทธิภาพและประสิทธิผล ในกฎหมายฉบับนี้หลายมาตราจึงได้กำหนดให้มีการตรากฎหมายลำดับรองหรือกฎหมายลูก เพื่อกำหนดรายละเอียดที่มีความสำคัญไว้หลายเรื่องด้วยกัน รวมทั้งเพื่อให้กฎหมายลูกนั้นสามารถปรับปรุงให้ทันสมัยตลอดเวลา ในหนังสือเล่มนี้จึงได้รวมเอาทั้งกฎหมายแม่ และร่างกฎหมายลูก ที่กำลังจะประกาศใช้บังคับเร็วๆ นี้ไว้ด้วยกัน เพื่อประโยชน์ในการเผยแพร่สร้างความรู้ความเข้าใจและเตรียมความพร้อมของทุกภาคส่วนในสังคมที่เกี่ยวข้องต่อไป

คณะผู้จัดทำ
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

เป็นปีที่ ๖๒ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ

จะต้องรับโทษภายในราชอาณาจักร

หมวด ๒
พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้วพนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา ๒๐ ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา ๒๑ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวงทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

Unofficial

Computer-Related Crime Act

B.E. 2550 (2007)

BHUMIBOL ADULYADEJ, REX.

Given on the 10th of June B.E. 2550;

Being the 62nd Year of the Present Reign.

His Majesty King Bhumibol Adulyadej is graciously pleased to proclaim that:

Whereas it is expedient to have the law on computer related crime;

Be it, therefore, enacted by the King, by and with the advice and consent of the National Legislative Assembly, as follows:

……..

Section 1 This Act shall be called the "Computer-Related Crime Act B.E. 2550"

Section 2 This Act shall come into force after thirty days following the date of its publication in the Government Gazette

Section 3 In this Act:

"computer system" means any device or a group of interconnected or related devices, one or more of which pursuant to a program or instruction or anything else, performs automatic processing of data.

“computer data” means information, messages and concepts or instruction, a program or anything else in a form suitable for processing in a computer system and shall include electronic data under the law on electronic transaction.

“traffic data” means any data relating to communication by means of a computer system, indicating the communication’s origin, destination, route, time, date, size, duration, type of underlying service, or other information relating to communication of such a computer system.

ขอขอบคุณดร.ดวงทิพย์ สุรินทาธิป และบริษัท ชวลิต แอนด์เอสโซ่วิเอทส์ จำกัดที่ได้ช่วยตรวจแก้และปรับปรุงร่างกฎหมายฉบับแปลของสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติจนแล้วเสร็จ ขณะนี้ร่างกฎหมายฉบับแปลอยู่ระหว่างการตรวจพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา เพื่อให้เป็น Official Translation ต่อไป

"service provider" means:

(1) a person who, either in his own name or in the name or for the benefit of another person, provides to other persons with access to the internet or the ability to communicate by other means through a computer system.

(2) a person who stores computer data for the benefit of other persons.

"user" means a person who uses the service of the service provider with or without pay.

"competent official" means a person appointed by the minister for the execution of this Act.

"Minister" means the Minister having charge and control of this Act.

Section 4 The Minister of the Information and Communication Technology Ministry shall have charge and control of this Act and shall have the power to issue Ministerial Regulations for the execution of this Act.

Such Ministerial Regulations shall come into force upon their publication in the Government Gazette.

Part 1

Computer-Related Offences.

Section 5 Whoever illegally accesses to a computer system that has specific security measures and such security measures are not intended for his use, shall be liable to imprisonment for a term not exceeding six months or to a fine not exceeding ten thousand Baht or to both.

Section 6 Whoever having knowledge of the security measures to access to a computer system created specifically by another person ,discloses, without right, such security measures in a manner that is likely to cause damage to another person, shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand Baht or to both.

Section 7 Whoever illegally accesses to a computer data that has specific security measures which are not intended for his use, shall be liable to imprisonment for a term not exceeding two years or to a fine not exceeding forty thousand Baht or to both.

Section 8 Whoever illegally makes, by any electronic means, an interception of computer data of another person that is being transmitted in a computer system and such computer data is not for the benefit of the public or is not available for other persons to utilize, shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both.

Section 9 Whoever illegally acts in a manner that causes damage, impairment, deletion, alteration or addition either in whole or in part of computer data of another person, shall be liable to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or to both.

Section 10 Whoever illegally acts in a manner that causes suspension, deceleration, obstruction or interference of a computer system of another person so that it cannot function normally shall be liable to imprisonment for a term not exceeding five years or a fine not exceeding one hundred thousand Baht or to both.

Section 11 Whoever sends computer data or an electronic mail to another person while hiding or faking its sources, in a manner that interferes with such another person's normal utilization of the computer system, shall be liable to a fine not exceeding one hundred thousand Baht.

Section 12 If the offences under Section 9 or 10

(1) result in damage to the general public, whether the damage takes place immediately or afterwards or simultaneously, the offender shall be liable to imprisonment for a term not exceeding ten years, or to a fine not exceeding two hundred thousand Baht.

(2) are committed in a manner that is likely to cause damage to computer data or computer systems relating to national security, public safety, economic stability or public utilities, or committed against computer data or a computer system that is available for the benefit of the public, the offender shall be liable to imprisonment for a term from three to fifteen years and to a fine from sixty thousand Baht to three hundred thousand Baht.

If the offence under (2) causes death to another person, the offender shall be liable to imprisonment for a term from ten to twenty years.

Section 13 Whoever sells or disseminates a program specifically designed for the purpose of committing offences under Section 5 to Section 10 or Section 11 shall be liable to imprisonment for a term not exceedting one year or to a fine not exceeding twenty thousand Baht or to both.

Section 14 Whoever commits the following acts shall be liable to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or both:

(1) input into a computer system wholly or partially fake or false computer data that is likely to cause damage to another person or the public;

(2) input into a computer system false computer data in a manner that is likely to undermine national security or to cause public panic;

(3) input into a computer system computer data that is an offence against national security or terrorism according to the Criminal Code.

(4) input into a computer system pornographic computer data that is accessible to the public;

(5) publish or forward any computer data with the full knowledge that such computer data is under paragraph (1), (2) (3) or (4);

Section 15 Any service provider, who intentionally supports or gives consent to the commission of an offence under Section 14 in the computer system in his control, shall be liable to the same penalty as provided in Section 14.

Section 16 Any person inputs into a computer system, that is available to the public, photographs of another person and such photographs are developed, edited, added or altered by electronic or any other means in a manner that is likely to impair the reputation of that other person, to expose that other person to hatred, contempt or humiliation, shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both.

If any person acts under paragraph one with honest intent, he is not guilty.

The offence under paragraph one is a compoundable offence.

If the aggrieved party dies before lodging a complaint, the parents, spouse or children of the aggrieved party shall be entitled to lodge the complaint and shall be deemed to be an injured party.

Section 17 Whoever commits an offence pursuant to this Act outside the Kingdom , whether

(1) the offender be a Thai person, and there be a request for punishment by the Government of the country where the offence has occurred or by the injured person ; or

(2) the offender be an alien, and the Royal Thai Government or a Thai person be the injured person, and there be a request for punishment by the injured person,

shall be punished in the Kingdom.

Part 2
Competent Officials

Section 18 Subject to Section 19, for the purpose of investigation and interrogation, in case where there is reasonable ground for believing that an offence has been committed under this Act, the competent official shall have the following powers, as deemed necessary for the purpose of providing evidence related to the offence or of the search for the offender :

(1) to notify or summon in writing any person who is involved in the offence prescribed by this Act to give statement or to submit declaration letter, documents, information or other evidence in an understandable form;

(2) to require traffic data from the service provider who is in charge of communications through the computer system or other relevant;

(3) to require the service provider to submit to the competent official user's information that is required to be kept under Section 26 or is in his possession or control;

(4) to copy the computer data and traffic data from the computer system that is suspected of having been used for committing the offence under this Act., in case where the computer system is not in the possession of the competent official;

(5) to require the possessor or controller of the computer data or equipment storing the computer data to deliver to him such computer data or equipment;

(6) to access the computer system, traffic data, or computer data of any person in order to ascertain the offender and in case where it is required, the competent official may also instruct such a person to deliver to him all relevant computer data as deemed necessary;

(7) to decrypt any person's computer data or to require a person who is involved in encryption of computer data to decrypt it or to co-operate with the competent official in carrying out the decryption;

(8) to seize or attach as necessary the computer system for the purpose of identifying details of the offence or the offender under this Act.

Section 19 In exercising his power under Section 18 (4) (5) (6) (7) and (8) the competent official shall submit a request to the competent court for a permission to implement the request. The request should identify reasonable grounds for believing that any person has committed or about to commit an offence under this Act, reasons for exercising this power, the manner of the offence, details of devices used in committing the offence and of the offender to the extent possible. In determining the request, the court shall proceed in a speedy manner.

After the court has granted the permission, the competent official shall, before implementing the court's order, send a copy of a note stating the reasonable grounds for the exercise of his powers under Section 18 (4) (5) (6) (7) and (8) to the owner or possessor of the computer system as evidence. In the absence of the owner or possessor, the competent official shall send a copy of the note to the said owner or possessor promptly.

The competent official who is the chief implementer under Section 18 (4) (5) (6) (7) and (8) shall submit to the competent court a copy of records detailing implementation and its reasons within forty-eight hours as evidence.

A copy of computer data under Section 18 (4) could be made only when there are reasonable grounds to believe that an offence has been committed under this Act. It should not pose unnecessary obstacles to the operations of the owner or possessor of the computer data.

The competent official must send a copy of the seizure or attachment under Section 18 (8), to the owner or the possessor of the computer system as evidence. However, the seizure or attachment shall not last longer than thirty days. If it is necessary to extend the period of seizure or attachment, a request could be submitted to the competent court for such an extension. The court shall allow a maximum period of sixty days extension either for one or several requests put together.

When it is no longer necessary to seize or to attach or upon the expiry of such period, the competent official must proceed to return the computer system promptly

Summons of seizure or attachment under paragraph five shall be in accordance with the rules and procedures prescribed in the Ministerial Regulations.

Section 20 In the case where an offence committed under this Act involves disseminating computer data that could undermine national security as prescribed in the Criminal Code, or is against the public peace or good morals, the competent official, with the Minister's approval, may submit a request with evidence to the competent court for an order to suspend/block the dissemination of such computer data.

Section 21 In case where the competent official finds that any computer data comprises undesirable programs, the competent official has the power to prohibit its sale or dissemination or to instruct the owner or the possessor of the computer data to cease using, to destroy or to alter such computer data or may specify conditions of use, possession, or dissemination of such undesirable programs.

An undesirable program in paragraph one shall mean any program which causes damage to computer data, computer systems, or other computer programs by destroying, altering, changing or corrupting them, and rendering them unable to function as instructed or being in conditions as specified by the Ministerial Regulations. However, exception is made for a program which aims at protecting or modifying such undesirable programs as stipulated by the Minister in the Government Gazette.

Section 22 The competent official is prohibited from disclosing or delivering computer data, traffic data or user's data that have been obtained under Section 18 to any person.

Paragraph one shall not apply to the acts carried out for the benefit of legal actions against the offender under this Act or for the benefit of legal actions against the competent official on the ground of wrongful exercise of his power or the act done in accordance with the court's order.

The competent official who is in breach of paragraph two shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both.

Section 23 Any competent official commits an act by negligence and thereby causing another person to gain a knowledge of computer data, traffic data or user's information obtained by means provided in Section 18, shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand Baht or to both.

Section 24 Whoever having gained a knowledge of the computer data, traffic data or user's information which the competent official has obtained according to Section 18, discloses the same to a third party, shall be liable to imprisonment for a term not exceeding two years or to a fine not exceeding forty thousand Baht or to both.

Section 25 Data, computer data, traffic data or user's information, obtained by the competent official under this Act, shall be used and admissible as evidence according to the provision of the Criminal Procedure Code or other laws that have relevant provision on taking evidence except that such evidence must not be obtained by means of persuasion, promises, threat, swindling or other illegal actions.

Section 26 A service provider shall keep traffic data for not less than ninety days from the day when such data has been entered into a computer system. If necessary, the competent official shall, as a particular case and time, instruct any service provider to keep traffic data for over ninety days but not exceeding one year.

A service provider shall keep user's data as necessary for the purpose of identifying the user from the first day of such a service and store such user data for not less than ninety days from its expiry date.

The Minister shall prescribe the type of service providers, how and when the provisions in paragraph one shall apply by promulgation in the Government Gazette,

Any service provider, who fails to comply with this Section, shall be liable to a fine not exceeding five hundred thousand Baht.

Section 27 Whoever fails to comply with an order of the court or the competent official pursuant to Section 18 or Section 20 or fails to comply with the court order pursuant to Section 21, shall be liable to a fine not exceeding two hundred thousand Baht and a daily fine not exceeding five thousand Baht until the order or condition is properly complied with.

Section 28 Under this Act, the Minister shall appoint the competent officials who have knowledge and expertise in computer systems and other qualifications as determined by the Minister.

Section 29 In performing his duties under this Act, the competent official designated by the Minister shall be deemed to be a senior administrative officer or a senior police officer under the Criminal Procedure Code having the authority to receive complaint or accusation, and to investigate and interrogate only of offences under this Act.

In arresting, confining, searching, investigating and instituting criminal prosecution against the offender under this Act within the authorities prescribed by the Criminal Procedure Code of a senior administrative officer or a senior police officer or an investigating officer, the competent official shall coordinate with the investigating officer who will proceed further within his authority.

The Prime Minister whose mandate is to control and supervise the National Police Bureau, together with the Minister, shall jointly stipulate those regulations relating to the guidelines and procedural methods for the action described in paragraph two.

Section 30 In carrying out his duties under this Act, the competent official shall present his identity card to the person involved.

The identity card under paragraph one shall be in the form as prescribed by the Minister by promulgation in the Government Gazette.

Countersigned by

General Surayud Chulanont

Prime Minister

Rationale: Nowadays computer systems play a significant role in business operations and people's lifestyle. If a person commits any act in a manner that causes computer malfunctioning as programmed or failing to perform as instructed or illegally accesses, compromises , alters or destroys data belonging to another person in the computer system or uses the computer system for dissemination of false or pornographic computer data, it will cause damage and adverse effects to the society, economy and national security including public peace and good morals. It is therefore expedient to impose measures for prevention and suppression of such acts, and to promulgate this Act.

(ร่าง)

กฎกระทรวง

ว่าด้วยการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. ....

อาศัยอำนาจตามความในมาตรา ๔ มาตรา ๑๘ และมาตรา ๑๙ วรรค ๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ออกกฎกระทรวงไว้ ดังต่อไปนี้

ข้อ ๑ เมื่อศาลมีคำสั่งอนุญาตให้ยึดหรืออายัดระบบคอมพิวเตอร์แล้ว ก่อนทำการยึดหรืออายัดให้พนักงานเจ้าหน้าที่แสดงบัตรประจำตัว และส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ดำเนินการยึดหรืออายัดโดยให้เจ้าพนักงานตำรวจหรือพนักงานฝ่ายปกครองแห่งท้องที่นั้นมาร่วมเป็นพยานด้วย

ข้อ ๒ ให้พนักงานเจ้าหน้าที่ดำเนินการยึดหรืออายัดระบบคอมพิวเตอร์ได้ทุกวันในเวลาระหว่างพระอาทิตย์ขึ้นถึงพระอาทิตย์ตก เว้นแต่ในกรณีที่มีเหตุอันควรเชื่อได้ว่าหากไม่ดำเนินการทันที ระบบคอมพิวเตอร์นั้นจะสูญหายหรือถูกยักย้าย ให้มีอำนาจดำเนินการยึดหรืออายัดในเวลาอื่นได้

ข้อ ๓ ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการยึดหรืออายัด ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

ข้อ ๔ ให้พนักงานเจ้าหน้าที่ทำบัญชีแสดงรายละเอียดเกี่ยวกับระบบคอมพิวเตอร์ที่ตรวจยึดหรืออายัด เช่น ประเภทอุปกรณ์ ชนิด รุ่น หมายเลขเครื่อง(S/N) จำนวน โดยกรอกข้อมูลลงในแบบ ทก.ยค. ที่แนบท้ายกฎกระทรวงนี้ และให้ถ่ายสำเนาแบบนั้น ติดที่บรรจุภัณฑ์ ตามลำดับหมายเลขไว้และให้แสดงเครื่องหมายไว้ที่ระบบคอมพิวเตอร์นั้นให้เห็นเป็นที่ประจักษ์แจ้งว่าได้มีการยึดหรืออายัดแล้ว ตามวิธีที่เห็นสมควร

ข้อ ๕ เมื่อยึดหรืออายัดระบบคอมพิวเตอร์แล้ว ให้พนักงานเจ้าหน้าที่จัดการให้เจ้าของ หรือผู้ครอบครองระบบคอมพิวเตอร์นั้นลงลายมือชื่อรับรองในแบบ ทก.ยค. แนบท้ายกฎกระทรวงนี้ หากผู้นั้นไม่ยินยอมลงลายมือชื่อ หรือในกรณีที่ไม่มีบุคคลดังกล่าวให้จดแจ้งลงในแบบนั้น และให้เจ้าพนักงานตำรวจหรือพนักงานฝ่ายปกครองแห่งท้องที่นั้นลงลายมือชื่อรับรองแทน

ข้อ ๖ เมื่อยึดหรืออายัดระบบคอมพิวเตอร์แล้ว ให้พนักงานเจ้าหน้าที่จัดให้มีบรรจุภัณฑ์ที่เหมาะสมสำหรับการจัดเก็บระบบคอมพิวเตอร์นั้น เพื่อป้องกันความเสียหายและการเปลี่ยนแปลงของข้อมูลที่อาจเกิดขึ้น แล้วทำการปิดผนึก (Seal) ด้วยวัสดุที่สามารถป้องกันการเปิดบรรจุภัณฑ์โดยไม่ได้รับอนุญาตได้

ข้อ ๗ ในกรณีที่พนักงานเจ้าหน้าที่ดำเนินการยึดหรืออายัดระบบคอมพิวเตอร์ใดแล้วไม่สามารถขนย้ายมาเก็บรักษาไว้ ณ สำนักงาน หรือสถานที่เก็บรักษาได้ หรือระบบคอมพิวเตอร์นั้นมีสภาพไม่เหมาะสมที่จะนำมาเก็บรักษา ให้รายงานพนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าพร้อมเสนอความเห็นเพื่อพิจารณาสั่งการตามที่เห็นสมควร

ในกรณีที่พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้ายังไม่สั่งการตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ผู้ดำเนินการยึดหรืออายัดนั้นจัดการเก็บรักษาทรัพย์สินไว้ตามที่เห็นสมควรไปพลางก่อน

ข้อ ๘ ในการดำเนินการยึดหรืออายัดระบบคอมพิวเตอร์ ให้พนักงานเจ้าหน้าที่มีหนังสือแจ้งแก่เจ้าของ ผู้มีสิทธิหรือผู้ครอบครองระบบคอมพิวเตอร์นั้น

ข้อ ๙ ถ้ามูลค่าแห่งระบบคอมพิวเตอร์ที่ได้ยึดหรืออายัดไว้นั้น ต้องเสื่อมเสียไปเพราะความผิดของบุคคลภายนอกเนื่องจากการไม่ปฏิบัติตามคำสั่งยึดหรืออายัดไม่ว่าด้วยประการใด ๆ ให้พนักงานเจ้าหน้าที่ เรียกให้บุคคลภายนอกนั้นรับผิดชดใช้ค่าสินไหมทดแทนเพื่อความเสียหายใดๆ อันเกิดขึ้นแต่การนั้น

ให้ไว้ ณ วันที่ พ.ศ. ....

(นายสิทธิชัย โภไคยอุดม)

รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ทก.ยค.

หนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์

(แนบท้ายกฎกระทรวงว่าด้วยการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. ....)

เขียนที่.....

วันที่.....

ข้าพเจ้า.....ตำแหน่ง.....

พนักงานเจ้าหน้าที่ผู้ซึ่งรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร แต่งตั้งตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พร้อมด้วย

(๑).....ตำแหน่ง.....

(๒).....ตำแหน่ง.....

ได้มาทำการยึดหรืออายัดระบบคอมพิวเตอร์เพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ซึ่งมี.....เป็นผู้ถูกกล่าวหา

และมีภูมิลำเนาอยู่ที่ เลขที่.....ตรอก/ซอย.....หมู่ที่.....ถนน.....

ตำบล/แขวง.....อำเภอ/เขต.....จังหวัด.....

ตามคำสั่งให้ทำการยึดหรืออายัดของศาล.....เลขที่.....

ลงวันที่.....

ในการดำเนินการยึดหรืออายัด ดังกล่าว ปรากฏว่ามี ระบบคอมพิวเตอร์ และหลักฐานอื่นๆ ดังต่อไปนี้ ที่เชื่อว่ามีส่วนเกี่ยวข้องกับการกระทำความผิดดังกล่าว จึงได้ยึดหรืออายัดไปเพื่อดำเนินการตรวจสอบ มีรายการแสดงชื่อและปริมาณของสิ่งที่ยึดหรืออายัดไว้ทั้งหมด.....รายการ ดังต่อไปนี้

(๑).....

.....

และตามบัญชีต่อท้ายหนังสือนี้อีก .....รายการ

บรรดาเอกสารหรือพยานหลักฐานที่ยึดหรืออายัดไปนี้ หากท่านประสงค์จะตรวจสอบเพื่อดำเนินกิจการของท่าน ขอให้ท่านติดต่อได้.....

ลงชื่อ.....ผู้ยึดหรืออายัด

(.....)

ลงชื่อ.....เจ้าของ หรือ

(.....)ผู้ครอบครอง

ลงชื่อ.....พยาน

(.....)

ลงชื่อ.....พยาน

(.....)

ทก.ยค.

บัญชีรายละเอียดแสดงการยึดหรืออายัดระบบคอมพิวเตอร์

บัญชีลำดับที่.....ยึดหรืออายัด เมื่อวันที่.....เวลา.....

บ้านเลขที่.....หมู่ที่.....ซอย.....ถนน.....

ตำบล/แขวง.....อำเภอ.....จังหวัด.....

พนักงานเจ้าหน้าที่ผู้ยึดหรืออายัด.....เลขที่บัตรประจำตัว.....

โดยมี.....เป็นผู้นำยึดหรืออายัด

ลำดับที่	รายการ	จำนวน	ราคา		เจ้าของ/ผู้ครอบครอง	หมายเหตุ
			บาท	สต.		

และตามบัญชีรายละเอียดระบบคอมพิวเตอร์ที่ยึดหรืออายัด ต่อท้ายบัญชีนี้อีก .....รายการ

ข้าพเจ้า.....ในฐานะ ผู้นำการยึดหรืออายัด ได้ตรวจนับทรัพย์สินดังกล่าวแล้ว พร้อมกับได้อ่านแล้ว รับว่า ถูกต้อง และเป็นจริง จึงขอลงลายมือชื่อไว้เป็นหลักฐาน

(ลงชื่อ).....ผู้นำยึดหรืออายัด

(.....)

(ลงชื่อ).....พนักงานเจ้าหน้าที่/บันทึก/อ่าน

(.....)

(ลงชื่อ).....ผู้ยึดหรืออายัด

(.....)

(ลงชื่อ).....พยาน

(.....)

ทก.ยค.

บัญชีรายละเอียดระบบคอมพิวเตอร์ที่ยึดหรืออายัด

(ต่อท้ายบัญชีรายละเอียดแสดงการยึดหรืออายัดระบบคอมพิวเตอร์)

1.ประเภทอุปกรณ์ Computer ที่ยึดหรืออายัด มีจำนวนทั้งหมด.....เครื่องได้แก่

1.1.1. ชนิด.....รุ่น(Model)……หมายเลขเครื่อง(S/N)……..

Case Type:☐ Mini Tower ☐ Mid Tower ☐ Full Tower ☐ อื่นๆ.....

หรือมีเอกลักษณะเป็น ☐ PC.Stand-alone ☐ Sever…… ☐ Client

☐ Workstation ☐ Mainframe ☐ อื่นๆ.....

ยี่ห้อ.....ติดตั้งอยู่บริเวณ…… ……

……..

1.1.2. มี Drives ดังนี้

5 ¼" Floppy drive(s)……3 ½" Floppy drive(s)…… Zip drive(s)……. Jazz drive(s)…….

Tape drive(s)…… Speakers……CD-Rom drive(s)…….CD-Rom types……..

Parallel port(s)…… Serial Port(s)……USB Port(s)…….Sound Card/port……..

Modem card/port……Video card/port……. .External SCSI port/card…….NIC card/port…….

Monitor……

Printer…….

อุปกรณ์เพิ่มเติมอื่นๆ.....

.....

1.2.1. ชนิด.....รุ่น(Model)……หมายเลขเครื่อง(S/N)…….

Case Type:☐ Mini Tower ☐ Mid Tower ☐ Full Tower ☐ อื่นๆ.....

หรือมีเอกลักษณะเป็น ☐ PC.Stand-alone ☐ Sever…… ☐ Client

☐ Workstation ☐ Mainframe ☐ อื่นๆ.....

ยี่ห้อ.....ติดตั้งอยู่บริเวณ.....

.....

1.2.2. มี Drives ดังนี้

5 ¼" Floppy drive(s)……3 ½" Floppy drive(s)…… Zip drive(s)……. Jazz drive(s)…….

Tape drive(s)…… Speakers……CD-Rom drive(s)…….CD-Rom types……

Parallel port(s)…… Serial Port(s)……USB Port(s)…….Sound Card/port……

Modem card/port……Video card/port……. .External SCSI port/card…….NIC card/port…….

Monitor……

Printer……..

อุปกรณ์เพิ่มเติมอื่นๆ.....

ทก.ยค.

1.3.1. ชนิด.....รุ่น(Model)……หมายเลขเครื่อง(S/N)…….

Case Type:☐ Mini Tower ☐ Mid Tower ☐ Full Tower ☐ อื่นๆ.....

หรือมีเอกลักษณะเป็น ☐ PC.Stand-alone ☐ Sever…… ☐ Client

☐ Workstation ☐ Mainframe ☐ อื่นๆ.....

ยี่ห้อ.....ติดตั้งอยู่บริเวณ……..

……

1.3.2. มี Drives ดังนี้

5 ¼" Floppy drive(s)……3 ½" Floppy drive(s)…… Zip drive(s)……. Jazz drive(s)……...

Tape drive(s)…… Speakers……CD-Rom drive(s)…….CD-Rom types……..

Parallel port(s)…… Serial Port(s)……USB Port(s)…….Sound Card/port……..

Modem card/port……Video card/port……. .External SCSI port/card…….NIC card/port……..

Monitor…….

Printer……..

อุปกรณ์เพิ่มเติมอื่นๆ.....

.....

1.4.1. ชนิด.....รุ่น(Model)……หมายเลขเครื่อง(S/N)…….

Case Type:☐ Mini Tower ☐ Mid Tower ☐ Full Tower ☐ อื่นๆ.....

หรือมีเอกลักษณะเป็น ☐ PC.Stand-alone ☐ Sever…… ☐ Client

☐ Workstation ☐ Mainframe ☐ อื่นๆ.....

ยี่ห้อ.....ติดตั้งอยู่บริเวณ.....

.....

1.4.2. มี Drives ดังนี้

5 ¼" Floppy drive(s)……3 ½" Floppy drive(s)…… Zip drive(s)……. Jazz drive(s)……

Tape drive(s)…… Speakers……CD-Rom drive(s)…….CD-Rom types……

Parallel port(s)…… Serial Port(s)……USB Port(s)…….Sound Card/port……...

Modem card/port……Video card/port……. .External SCSI port/card…….NIC card/port……

Monitor…….

Printer……..

อุปกรณ์เพิ่มเติมอื่นๆ.....

.....

.....

2.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

ข้าพเจ้าขอรับรองว่า รายละเอียดที่ให้ไว้ดังกล่าวข้างต้น เป็นความสัตย์จริงทุกประการ เจ้าพนักงานได้สอบถามข้าพเจ้าอย่างสุภาพ ไม่มีการข่มขู่ ไม่ได้ขัดขวางการประกอบกิจการหรือหน้าที่การงานของข้าพเจ้าแต่อย่างไร พนักงานฯได้อ่านข้อความดังกล่าวข้างต้นทั้งหมด และข้าพเจ้าเข้าใจข้อความดังกล่าวดีแล้ว จึงขอลงลายมือชื่อไว้เป็นหลักฐานต่อหน้าพนักงานและหน้าพยาน

(ลงชื่อ).....ผู้นำการยึดหรืออายัด (ลงชื่อ).....พยาน

(.....) (.....)

(ลงชื่อ).....พนักงานเจ้าหน้าที่ (ลงชื่อ).....ร่วมสอบสวน

(.....) (.....)

ลงชื่อ).....ร่วมสอบสวน /พิมพ์ (ลงชื่อ).....ร่วมสอบสวน

(.....) (.....)

(ร่าง)

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

พ.ศ. ๒๕๕๐

.....

ด้วยในปัจจุบันการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์เริ่มเข้าไปมีบทบาทและทวีความสำคัญเพิ่มขึ้นตามลำดับต่อระบบเศรษฐกิจและคุณภาพชีวิตของประชาชน แต่ในขณะเดียวกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีแนวโน้มขยายวงกว้าง และทวีความรุนแรงเพิ่มมากขึ้น ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดี อันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สวนสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ จึงสมควรกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว

อาศัยอำนาจตามความในมาตรา ๒๖ วรรค ๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ดังนั้น รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้กำหนดหลักเกณฑ์ไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามประกาศนี้

ข้อ ๔ ในประกาศนี้

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนด คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

ข้อ ๕ ภายใต้บังคับของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แบ่งได้ ดังนี้

(๑) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ ๔ ประเภท ดังนี้

ก.ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ข.ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ค.ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ (Host Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ง.ผู้ให้บริการร้านอินเทอร์เน็ต (Internet Café) และผู้ให้บริการร้านเกมออนไลน์ ดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

(๒) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (๑) (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Application Service Provider) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก. แนบท้ายประกาศนี้

ข้อ ๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการต้องเก็บรักษาปรากฏดังภาคผนวก ข. แนบท้ายประกาศนี้

ข้อ ๗ ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๑

(๒) ผู้ให้บริการตามข้อ ๕ (๑) ข. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒ ตามประเภท ชนิดและหน้าที่การให้บริการ

(๓) ผู้ให้บริการตามข้อ ๕ (๑) ค. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒ ตามประเภท ชนิดและหน้าที่การให้บริการ

(๔) ผู้ให้บริการตามข้อ ๕ (๑) ง. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๓

(๕) ผู้ให้บริการตามข้อ ๕ (๒) มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๔

ทั้งนี้ ในการเก็บรักษาข้อมูลจราจรตามภาคผนวกต่างๆ ที่กล่าวไปข้างต้นนั้น ให้ผู้ให้บริการเก็บเพียงเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น

ข้อ ๘ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือ ทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กร กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

(๓) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้การส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

(๔) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

(๕) ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ ๑ ถึงข้อ ๔ ข้างต้น ได้ให้บริการในนามตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุให้ผู้ให้บริการในข้อ ๑ ถึงข้อ ๔ ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการเช่นว่านั้นต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

ข้อ ๙. ผู้ให้บริการต้องเทียบเวลาประเทศไทยให้ตรงกับเครื่องให้บริการเวลา (Time Server) ที่เปิดให้บริการสาธารณะโดยใช้ Network Time Protocol (NTP)

ข้อ ๑๐. ผู้ให้บริการซึ่งมีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ ๗ เริ่มเก็บข้อมูลดังกล่าวตามลำดับดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก.เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นสามสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

(๒) ให้ผู้ให้บริการตามข้อ ๕ (๑) ข. เฉพาะผู้ให้บริการเครือข่ายสาธารณะหรือผู้ให้บริการอินเทอร์เน็ต (ISP) เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งร้อยแปดสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

ผู้ให้บริการอื่นนอกจากที่กล่าวมาในข้อ ๑๐ (๑) และข้อ ๑๐ (๒) ข้างต้นให้เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งปีนับจากวันประกาศในราชกิจจานุเบกษา

ประกาศ ณ วันที่ เดือน พ.ศ.

.....

รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ภาคผนวก ก
แนบท้ายประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ
พ.ศ. ๒๕๕๐

.....

๑. ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น ตามข้อ ๕ (๑) จำแนกได้ ๔ ประเภท ดังนี้

ประเภท	ตัวอย่างของผู้ให้บริการ
ก.ผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier)	๑) ผู้ให้บริการโทรศัพท์พื้นฐาน (Fixed Line Service Provider) ๒) ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Service Provider) ๓) ผู้ให้บริการวงจรเช่า (Leased Circuit Service Provider) เช่น ผู้ให้บริการ Leased Line, ผู้ให้บริการสายเช่า Fiber Optic, ผู้ให้บริการ ADSL (Asymmetric Digital Subscriber Line), ผู้ให้บริการ Frame Relay, ผู้ให้บริการ ATM (Asynchronous Transfer Mode), ผู้ให้บริการ MPLS (Multi Protocol Label Switching) เป็นต้น เว้นแต่ผู้ให้บริการนั้น ให้บริการแต่เพียง Physical Media หรือสายสัญญาณอย่างเดียว (Cabling) เท่านั้น (เช่น ผู้ให้บริการ Dark Fiber, ผู้ให้บริการสายใยแก้วนำแสง ซึ่งอาจไม่มีสัญญาน Internet หรือไม่มี IP Traffic) ๔) ผู้ให้บริการดาวเทียม (Satellite Service Provider)

ประเภท	ตัวอย่างของผู้ให้บริการ
ข.ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)	๑) ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย ๒) ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด ๓) ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือสถาบันการศึกษา
ค.ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider)	๑) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting),การให้บริการเช่า Web Server ๒) ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing) ๓) ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider) ๔) ผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Internet Data Center)
ง.ผู้ให้บริการร้านอินเทอร์เน็ต	๑.ผู้ให้บริการร้านอินเทอร์เน็ต (Internet Café) ๒.ผู้ให้บริการร้านเกมออนไลน์

๒.ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม ข้อ ๕ (๒) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก แนบท้ายประกาศนี้

ประเภท	ตัวอย่างของผู้ให้บริการ
ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Content and Application Service Provider)	๑) ผู้ให้บริการเว็บบอร์ด (Web board) หรือ ผู้ให้บริการบล็อค (Blog) ๒) ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Electronic Payment Service Provider) ๓) ผู้ให้บริการเว็บเซอร์วิส (Web Services) ๔) ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือธุรกรรมทางอิเล็กทรอนิกส์ (e-Transactions)

ภาคผนวก ข
แนบท้ายประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ
พ.ศ. ๒๕๕๐

.....

๑.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ก. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก.ข้อมูลที่สามารถระบุและติดตามถึงแหล่งกำเนิดต้นทาง ปลายทาง และทางสายที่ผ่านของการติดต่อสื่อสารของระบบคอมพิวเตอร์	-ข้อมูลระบบชุมสายโทรศัพท์พื้นฐาน โทรศัพท์วิทยุมือถือ และระบบตู้โทรศัพท์สาขา (Fixed Network Telephony and Mobile Telephony)
	-หมายเลขโทรศัพท์ หรือ เลขหมายวงจร รวมทั้งบริการเสริมอื่นๆ เช่น บริการโอนสาย และหมายเลขโทรศัพท์ที่ได้โอนสาย รวมทั้งหมายเลขโทรศัพท์ซึ่งถูกเรียกจากโทรศัพท์ที่มีการโอน
	-ชื่อ ที่อยู่ของผู้ใช้บริการหรือผู้ใช้งานที่ลงทะเบียน (Name and Address of Subscriber or Registered User)

ประเภท	รายการ
	- ข้อมูลเกี่ยวกับวันที่, เวลา และที่ตั้งของ Cell ID ซึ่งมีการใช้บริการ (Date and Time of the Initial Activation of the Service and the Location Label (Cell ID))
ข.ข้อมูลที่สามารถระบุวันที่ เวลา และระยะเวลาของการติดต่อสื่อสารของระบบคอมพิวเตอร์	วันที่ รวมทั้งเวลาเริ่มต้นและสิ้นสุดของการใช้งาน (Fixed Network Telephony and Mobile Telephony, the Date and Time of the Start and End of the Communication)
ค.ข้อมูลซึ่งสามารถระบุที่ตั้งในการใช้โทรศัพท์มือถือหรืออุปกรณ์ติดต่อสื่อสารแบบไร้สาย (Mobile Communication Equipment)	๑) ที่ตั้ง label ในการเชื่อมต่อ (Cell ID) ณ สถานที่เริ่มติดต่อสื่อสาร
	๒) ข้อมูลซึ่งระบุที่ตั้งทางกายภาพของโทรศัพท์มือถืออันเชื่อมโยงกับข้อมูลที่ตั้งของ Cell ID ขณะที่มีการติดต่อสื่อสาร
	๓) จัดให้มีระบบบริการตรวจสอบบุคคลผู้ใช้บริการ

๒.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ข. ถึง ค. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	๑) ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย (Access Logs Specific to Authentication and Authorization Servers เช่น TACACS (Terminal Access Controller Access-Control System) or RADIUS (Remote Authentication Dial-In User Service) or DIAMETER (Used to Control Access to IP Routers or Network Access Servers)
	๒) ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
	๓) ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)
	๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (Assigned IP Address)
	๕) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification)
ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมาย	๑) ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (Simple Mail Transfer Protocol : SMTP Log)
	๒) ข้อมูลจดหมายอิเล็กทรอนิกส์ที่บันทึกการใช้บริการเรียก

ประเภท	รายการ
อิเล็กทรอนิกส์ (e-mail servers)	ข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิกโดยยังคงจัดเก็บข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้น ไว้ที่เครื่องให้บริการ (POP3 (Post Office Protocol version 3) Log or IMAP4 (Internet Message Access Protocol Version 4) Log)
	๓) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server)
	๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP Address of Sending Computer)
	๕) ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID)
	๖) ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender E-mail Address)
	๗) ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver E-mail Address)
	๘) ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status Indicator)
	๙) ข้อมูลที่บอกถึงวันเวลาในการเชื่อมต่อของเครื่องที่เข้าใช้บริการเชื่อมกับเครื่องให้บริการ (Date and Time of Connection of Client to Server)

ประเภท	รายการ
	๑๐) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (IP Address of Client Connected to Server)
	๑๑) ชื่อผู้ใช้งาน (User ID) (ถ้ามี)
	๑๒) ข้อมูลจดหมายอิเล็กทรอนิกส์ที่ถูกส่งคืน
ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล
	๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
	๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP Source Address)
	๔) ข้อมูลชื่อผู้ใช้งาน (User ID) (ถ้ามี)
	๕) ข้อมูลตำแหน่ง (Path) และ ชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการ ส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป (Path and Filename of Data Object Uploaded or Downloaded)
ง. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ
	๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ
	๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น

ประเภท	รายการ
	๔) ข้อมูลคำสั่งการใช้งานระบบ
	๕) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI: Uniform Resource Identifier) เช่น ตำแหน่งของเว็บเพ็จ
จ. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP (Network News Transfer Protocol) Log)
	๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
	๓) ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID)
	๔) ข้อมูลชื่อเครื่องให้บริการ (Host Name)
	๕) ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted Message ID)
ฉ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น	ข้อมูล Log เช่น ข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and Time of Connection of Client to Server) และ ข้อมูลชื่อเครื่องบนเครือข่าย และ หมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (Hostname and IP Address) เป็นต้น

๓.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ง. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ผู้ให้บริการร้านอินเทอร์เน็ต	๑) ข้อมูลที่สามารถระบุตัวบุคคล ๒) เวลาของการเข้าใช้ และเลิกใช้บริการ ๓) หมายเลขเครื่องที่ใช้ IP Address (Internet Protocol address)

๔.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๒) มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)	๑) ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ หรือ เลขประจำตัว (User ID) ของผู้ขายสินค้าหรือบริการ หรือ เลขประจำตัวผู้ใช้บริการ (User ID) และ ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ
	๒) บันทึกข้อมูลการเข้าใช้บริการ
	๓) กรณีผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อค (Blog) ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล

(ร่าง)

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

.....

เพื่อให้การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ มีความชัดเจนและเป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้กำหนดหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

“รัฐมนตรี” หมายความว่า รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๒ พนักงานเจ้าหน้าที่ ต้องมีคุณสมบัติ ดังต่อไปนี้

(๑) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์

(๒) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์

(๓) ผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) สืบสวน สอบสวน และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ตามภาคผนวกท้ายประกาศนี้ และ

(๔) มีคุณสมบัติอื่นอย่างหนึ่งอย่างใด ดังต่อไปนี้

ก.รับราชการหรือเคยรับราชการไม่น้อยกว่าสองปีในตำแหน่งเจ้าหน้าที่ตรวจพิสูจน์พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์

ข.สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาตรี และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสี่ปี

ค.สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาโท หรือสอบไล่ได้เป็นเนติบัณฑิตตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา หากเป็นสาขานิติศาสตร์ และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสามปี

ง.สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาเอก หรือมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงาน ตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสองปี

จ.เป็นบุคคลที่ทำงานเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือมีประสบการณ์ในการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ไม่น้อยกว่าสองปี

ข้อ ๓ ในกรณีที่มีความจำเป็นเพื่อประโยชน์ของทางราชการในการสืบสวนและสอบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จำเป็นต้องมีบุคลากรซึ่งมีความรู้ ความชำนาญ หรือประสบการณ์สูง เพื่อดำเนินการสืบสวนและสอบสวนการกระทำผิดหรือคดีเช่นว่านั้น หรือเป็นบุคลากรในสาขาที่ขาดแคลน รัฐมนตรีอาจยกเว้นคุณสมบัติตามข้อ ๒ ไม่ว่าทั้งหมดหรือบางส่วนสำหรับการบรรจุและแต่งตั้งบุคคลใดเป็นการเฉพาะก็ได้

ข้อ ๔ การแต่งตั้งบุคคลหนึ่งบุคคลใดเป็นพนักงานเจ้าหน้าที่ให้แต่งตั้งจากบุคคลซึ่งมีคุณสมบัติตามข้อ ๒ หรือ ข้อ ๓ โดยบุคคลดังกล่าวต้องผ่านการประเมินความรู้ความสามารถหรือทดสอบตามหลักสูตรและหลักเกณฑ์ที่รัฐมนตรีประกาศกำหนด

การแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ ดำรงตำแหน่งในวาระคราวละ ๔ ปี และการแต่งตั้งให้ประกาศในราชกิจจานุเบกษา

ข้อ ๕ พนักงานเจ้าหน้าที่ต้องไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) เป็นบุคคลล้มละลาย บุคคลไร้ความสามารถ หรือบุคคลเสมือนไร้ความสามารถ

(๒) เป็นสมาชิกสภาผู้แทนราษฎร สมาชิกวุฒิสภา ข้าราชการการเมือง สมาชิกสภาท้องถิ่น ผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งที่รับผิดชอบ

ในการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ในพรรคการเมือง

(๓) เป็นผู้อยู่ระหว่างถูกสั่งให้พักราชการหรือถูกสั่งให้ออกจากราชการไว้ก่อน

(๔) ถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐหรือรัฐวิสาหกิจเพราะทำผิดวินัย หรือรัฐมนตรีให้ออกจากการเป็นพนักงานเจ้าหน้าที่เพราะมีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่หรือหย่อนความสามารถ

(๕) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่กระทำโดยประมาทหรือความผิดลหุโทษ

(๖) ต้องคำพิพากษาหรือคำสั่งของศาลให้ทรัพย์สินตกเป็นของแผ่นดินเพราะร่ำรวยผิดปกติหรือมีทรัพย์สินเพิ่มขึ้นผิดปกติ

ข้อ ๖ พนักงานเจ้าหน้าที่พ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) ถูกจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก

(๔) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามข้อ ๕

(๕) รัฐมนตรีให้ออก เพราะมีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่หรือหย่อนความสามารถ

(๖) ครบวาระการดำรงตำแหน่ง

ข้อ ๗ ประกาศนี้มีผลใช้บังคับตั้งแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ เดือน พ.ศ.๒๕๕๐

(นายสิทธิชัย โภไคยอุดม)
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ภาคผนวก
ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่
ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. ๒๕๕๐

.....

ผู้ที่จะได้รับการแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ จะต้องผ่านการอบรมด้านจริยธรรม สืบสวน สอบสวนความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) แล้วแต่กรณี ดังต่อไปนี้

๑. หลักสูตรมาตรฐานสากล (International Standard Courses)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดอบรมให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีทั่วไป (หลักสูตรเต็มเวลาประมาณ ๑ เดือน ทั้งภาคทฤษฎีและปฏิบัติ ทั้งนี้ ไม่รวมด้านที่สาม ข. และด้านที่สี่ ข. ซึ่งเป็นหลักสูตรความเชี่ยวชาญเฉพาะทาง)

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่ของพนักงานเจ้าหน้าที่

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๒.	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓.	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๔.	การสืบสวนทางเทคนิค เช่น การตรวจสอบหมายเลข IP Address หรือแหล่งที่มาของการกระทำความผิด การขอข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ให้บริการ การวิเคราะห์และเชื่อมโยงข้อมูล/พยานหลักฐานข้างต้น
๕.	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยานหลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การเก็บรักษาพยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการ การเปรียบเทียบปรับ และการดำเนินคดี เป็นต้น
๖.	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security)

ก. เนื้อหาหลักสูตรภาคบังคับสำหรับพนักงานเจ้าหน้าที่

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) **Compulsory Course**
๑.	General security concepts
๒.	Security Architecture
๓.	Access Controls
๔.	Applications Security
๕.	Operation Security
๖.	Security Management
๗.	Cryptography
๘.	Physical Security
๙.	Telecommunications and Network Security
๑๐.	Business Continuity Planning
๑๑.	Law, Investigations, and Ethics

ข. หลักสูตรความมั่นคงปลอดภัยของระบบสารสนเทศขั้นสูง (Advanced Information Security Course) สำหรับพนักงานเจ้าหน้าที่สายผู้เชี่ยวชาญด้านเทคนิค

ลำดับ	เนื้อหาหลักสูตร (ความชำนาญเฉพาะทาง)
๑.	Audit and Monitoring
๒.	Risk, Response and Recovery
๓.	Malicious Code Analysis
๔.	Vulnerabilities Assessment & Penetration Testing

ด้านที่สี่ การพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ก.ความรู้ด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	The needs for Computer Forensics
๒.	Principles of Computer Forensics and Digital/Electronic Evidence
๓.	Crime scene, Digital/Electronic Evidence and Chain of Custody
๔.	Capturing the Data Image and Volatile Data
๕.	Extracting Information from Captured Data
๖.	Breaking Password and Encryption
๗.	Using Computer Forensics Tools
๘.	Investigation and Interrogation
๙.	Digital/Electronic Evidence Analysis and Synthesis
๑๐.	Testify in Court, Admissibility requirements

๑๑.	Different between Computer Forensics and Network/Internet Forensics
๑๒.	Network/Internet Forensics
๑๓.	Using Network/Internet Forensics Tools

ข.ความเชี่ยวชาญเฉพาะทางด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Professional Computer Forensics และ Certified Forensic Computer Examiner (CFCE))

ลำดับ	เนื้อหาหลักสูตร (ความชำนาญเฉพาะทาง)
๑.	Using Computer Forensic Tools เช่น Encase, Forensics Toolkits, lLook
๒.	Using Network / Internet Forensic Tools เช่น Encase Field Intelligence Model (FIM)
๓.	Wireless Forensic Tools เช่น Netstumbler, Kismet, Aircrack
๔.	Using Handheld Forensics Tools (Cell & PDA) Paraben, MobilEdit, Vogon
๕.	Cryptology ได้แก่ Cryptography และ Cryptanalysis

๒. หลักสูตรเร่งรัด (Intensive Courses) (๕ วัน)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดการอบรมระยะสั้นแบบเร่งรัดให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีพิเศษ ซึ่งได้รับการยกเว้นตามหลักเกณฑ์ในการกำหนดคุณสมบัติของพนักงานเจ้าหน้าที่ตามปกติทั่วไป

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่ของพนักงานเจ้าหน้าที่

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๒.	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓.	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๓.	การสืบสวนทางเทคนิค เช่น การตรวจสอบหมายเลข IP Address หรือแหล่งที่มาของการกระทำความผิด, การขอข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ให้บริการ, การวิเคราะห์และเชื่อมโยงข้อมูล/ พยานหลักฐานข้างต้น
๕.	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่

	เกี่ยวข้อง การรวบรวม พยาน หลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การเก็บรักษาพยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการ การเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๖.	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม การพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer orensics)

ลำดับ	เนื้อหาหลักสูตรภาคบังคับ Compulsory Course
๑.	The needs for Computer Forensics
๒.	Principles of Computer Forensics and Digital/Electronic Evidence
๓.	Crime scene, Digital/Electronic Evidence and Chain of Custody
๔.	Capturing the Data Image and Volatile Data
๕.	Extracting Information from Captured Data
๖.	Breaking Password and Encryption
๗.	Using Computer Forensics Tools
๘.	Investigation and Interrogation
๙.	Digital/Electronic Evidence Analysis and Synthesis
๑๐.	Testify in Court, Admissibility requirements
๑๑.	Different between Computer Forensics and Network/Internet Forensics
๑๒.	Network/Internet Forensics
๑๓.	Using Network/Internet Forensics Tools

(ร่าง)

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง กำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ.๒๕๕๐

อาศัยอำนาจตามความในมาตรา ๓๐ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่ไว้ ดังต่อไปนี้

ข้อ ๑ บัตรประจำตัวพนักงานเจ้าหน้าที่ให้มีพื้นสีขาว ขนาดและลักษณะตามแบบท้ายประกาศนี้

ข้อ ๒ ให้ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้ออกบัตรประจำตัวพนักงานเจ้าหน้าที่

ข้อ ๓ ให้พนักงานเจ้าหน้าที่ยื่นคำขอมีบัตรประจำตัว พร้อมกับแนบรูปถ่ายไม่เกินหกเดือนก่อนวันยื่นคำขอมีบัตร ขนาด ๒.๕ x ๓ เซนติเมตร ครึ่งตัว หน้าตรง ไม่สวมหมวก แต่งเครื่องแบบปฏิบัติราชการหรือเครื่องแบบพิธีการหรือแต่งกายสุภาพ จำนวน ๒ รูป ต่อสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๔ คำขอมีบัตรตามข้อ ๓ ให้เป็นไปตามแบบท้ายประกาศนี้

ข้อ ๕ บัตรประจำตัวตามประกาศนี้ ให้ใช้ได้สี่ปีนับแต่วันออกบัตร

ข้อ ๖ เมื่อได้ออกบัตรประจำตัวให้แก่ผู้ใด ให้ผู้ออกบัตรประจำตัวจัดให้มีสำเนาข้อความและรายการบัตรประจำตัวซึ่งติดรูปถ่ายของผู้นั้นไว้ด้วยหนึ่งฉบับ และเก็บไว้เป็นหลักฐานที่สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๗ การออกบัตรประจำตัว ในกรณีบัตรประจำตัวหมดอายุ สูญหาย หรือชำรุดในสาระสำคัญ หรือผู้ถือบัตรประจำตัวนั้นได้ย้ายสังกัด ให้นำความในข้อ ๑ ข้อ ๒ ข้อ ๓ ข้อ ๔ ข้อ ๕ และข้อ ๖ มาบังคับใช้โดยอนุโลม

ข้อ ๘ ผู้ใดได้รับบัตรประจำตัวใหม่ หรือผู้ถือบัตรไม่มีสิทธิใช้บัตรประจำตัวนั้นต่อไป ให้คืนบัตรต่อสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารโดยพลัน ในวันที่ได้รับบัตรประจำตัวใหม่หรือไม่มีสิทธิใช้บัตรประจำตัวนั้น

ประกาศ ณ วันที่ พ.ศ. ๒๕๕๐

(นายสิทธิชัย โภไคยอุดม)
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

แบบคำขอมีบัตรประจำตัวพนักงานเจ้าหน้าที่
ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. ๒๕๕๐

เขียนที่……
วันที่.....เดือน.....พ.ศ.....

ข้าพเจ้า.....เกิดวันที่.....เดือน.....พ.ศ.....
อายุ.....ปี เลขที่บัตรประจำตัวประชาชน.....มีชื่ออยู่ในทะเบียนบ้านเลขที่.....ซอย.....ถนน.....
ตำบล/แขวง.....อำเภอ/เขต.....จังหวัด.....
รหัสไปรษณีย์.....โทรศัพท์.....โทรศัพท์มือถือ.....

ที่อยู่ตามภูมิลำเนา บ้านเลขที่.....ซอย.....ถนน.....
ตำบล/แขวง.....อำเภอ/เขต.....จังหวัด.....
รหัสไปรษณีย์.....

หน่วยงาน.....

ทำคำขอยื่นต่อปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อขอมีบัตรประจำตัวพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และได้แนบรูปถ่ายสองรูปมาพร้อมกับคำขอนี้แล้ว

ข้าพเจ้าขอรับรองว่าข้อความดังกล่าวข้างต้นเป็นความจริงทุกประการ

(ลายมือชื่อ).....ผู้ทำคำขอ

(.....)

ลงชื่อ .....

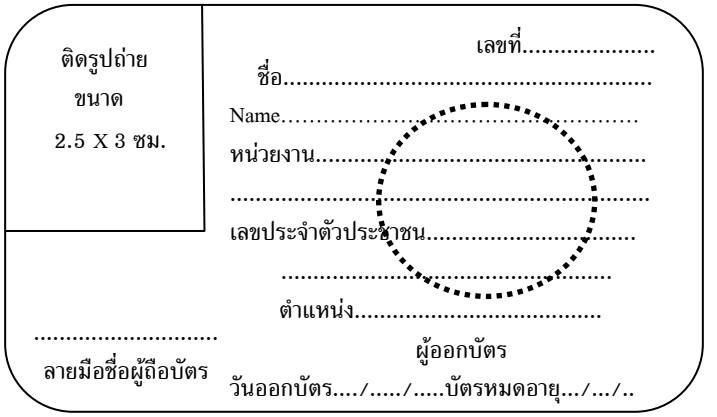
ตำแหน่ง.....

(ผู้บังคับบัญชา ผู้ให้ความยินยอม)

(...../...../.....)

แบบบัตรประจำตัวพนักงานเจ้าหน้าที่

ด้านหน้า



กว้าง 5.4 ซม.

ยาว 8.5 ซม.

ด้านหลัง

หากเก็บบัตรนี้ได้กรุณาส่งคืนกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร หรือ โทร. 1111

หมายเหตุ

(1) ด้านหน้าบัตรแสดงข้อมูลผู้ถือบัตรได้แก่ ชื่อ ชื่อภาษาอังกฤษ หมายเลขบัตรประจำตัวประชาชน ชื่อหน่วยงานต้นสังกัด ภาพถ่าย ลายมือชื่อผู้ถือบัตร และแสดงเลขที่บัตรพร้อมวันที่ออกและวันที่หมดอายุ

(2) ด้านหน้าบัตรมีตราครุฑสีแดง เป็นวงกลมสองวงซ้อนกัน ขนาดเส้นผ่าศูนย์กลาง 3.5 ซม. วงใน 2.5 ซม. ล้อมครุฑขนาดตัวครุฑ 2 ซม. ระหว่างวงนอกและวงใน ให้มีอักษรไทยระบุกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารอยู่ขอบล่างของตรา

(3) ด้านหลังมีแถบแม่เหล็กสำหรับบรรจุข้อมูล

(4) ด้านหลังระบุว่าเป็นบัตรประจำตัวพนักงานเจ้าหน้าที่ตามพระราชบัญญัติฯ

(5) ด้านหลังบัตรด้านล่างมีข้อความระบุว่าหากเก็บบัตรนี้ได้กรุณาส่งคืนกระทรวงฯ หรือ
โทร. 1111

(ร่าง)

บันทึกข้อตกลงระหว่าง
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงกลาโหม กระทรวงยุติธรรม
สำนักข่าวกรองแห่งชาติ สำนักงานตำรวจแห่งชาติ และ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
เรื่อง การประสานงานร่วมมือกันตามพระราชบัญญัติว่าด้วย
การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

โดยที่เป็นการสมควรเพื่อให้การประสานงานร่วมมือกันระหว่างหน่วยงานที่เกี่ยวข้องกับการใช้อำนาจตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นที่หน่วยงานซึ่งเกี่ยวข้องกับพระราชบัญญัตินี้ อันประกอบด้วย กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกระทรวงกลาโหม กระทรวงยุติธรรม สำนักข่าวกรองแห่งชาติ สำนักงานตำรวจแห่งชาติ และศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ต้องทำบันทึกข้อตกลงระหว่างเจ้าหน้าที่ของทั้งหกหน่วยงานในการให้ความช่วยเหลือสนับสนุนซึ่งกันและกัน อันจะยังให้เกิดความคล่องตัวในการทำงาน และมีแนวทางในการปฏิบัติตามกฎหมายไปในทิศทางเดียวกัน

ข้อ ๑ บันทึกข้อตกลงนี้เรียกว่า “บันทึกข้อตกลงระหว่าง กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงกลาโหม กระทรวงยุติธรรม สำนักข่าวกรองแห่งชาติ สำนักงานตำรวจแห่งชาติ และศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เรื่อง การประสานงานร่วมมือกันตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

ข้อ ๒ บันทึกข้อตกลงนี้ให้มีผลตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ในบันทึกข้อตกลงนี้

(๑) พระราชบัญญัติ หมายถึง “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

(๒) พนักงานเจ้าหน้าที่ หมายถึง “พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

(๓) เจ้าพนักงานตำรวจ หมายถึง “ข้าราชการตำรวจตามพระราชบัญญัติตำรวจแห่งชาติ พ.ศ.๒๕๔๗”

(๔) เจ้าพนักงานกรมสอบสวนคดีพิเศษ หมายถึง “พนักงานสอบสวนคดีพิเศษ และ เจ้าหน้าที่คดีพิเศษ ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. ๒๕๔๗”

(๕) หน่วยงานที่เกี่ยวข้อง หมายถึง “กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงกลาโหม กระทรวงยุติธรรม สำนักข่าวกรองแห่งชาติ สำนักงานตำรวจแห่งชาติ และศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ”

ข้อ ๔ ให้มีคณะกรรมการกำหนดแนวทางปฏิบัติ การประสานงานและมาตรการปฏิบัติงานของหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามพระราชบัญญัติและบันทึกข้อตกลงฉบับนี้ คณะกรรมการประกอบด้วย

(๑) ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นประธานกรรมการ

(๒) ผู้แทนกระทรวงกลาโหม เป็นกรรมการ

(๓) ผู้แทนสำนักงานตำรวจแห่งชาติ เป็นกรรมการ

(๔) ผู้แทนกรมสอบสวนคดีพิเศษ เป็นกรรมการ

(๕) ผู้แทนสำนักข่าวกรองแห่งชาติ เป็นกรรมการ

(๖) ผู้แทนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เป็นกรรมการ

(๗) ผู้แทนกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นกรรมการและเลขานุการ

ในการนี้ ให้เลขานุการแต่งตั้งผู้ช่วยเลขานุการจำนวนสองคน

ข้อ ๕ คณะกรรมการตามข้อ ๔ มีอำนาจหน้าที่ ดังนี้

(๑) วางมาตรการในการประสานงานระหว่างหน่วยงานที่เกี่ยวข้องกับการใช้อำนาจและแนวทางการปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ตลอดจนให้คำปรึกษา หรือให้คำแนะนำเกี่ยวกับปัญหาและข้อขัดข้อง ในการปฏิบัติตามพระราชบัญญัติดังกล่าว

(๒) วางแนวปฏิบัติในการร้องทุกข์กล่าวโทษ การสืบสวนสอบสวน และดำเนินคดี รวมถึงการประสานงานในเรื่องดังกล่าวระหว่างหน่วยงานที่เกี่ยวข้องตลอดจนรายละเอียดในการใช้อำนาจและปฏิบัติงานของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติฉบับนี้

(๓) กำหนดมาตรฐานในการปฏิบัติงานของพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

(๔) พิจารณาให้คำแนะนำแก่รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อแต่งตั้งพนักงานเจ้าหน้าที่ ซึ่งผ่านการตรวจสอบคุณสมบัติเรียบร้อยแล้ว

(๕) ให้คำแนะนำอื่นใดแก่รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อพิจารณาปรับปรุงแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ตลอดจน ประกาศ ระเบียบ ข้อบังคับ และกฎหมายอื่นๆ ที่เกี่ยวข้อง

(๖) แต่งตั้งคณะอนุกรรมการ หรือ คณะทำงาน เพื่อช่วยงานของคณะกรรมการ

ข้อ ๖ ให้หน่วยงานที่เกี่ยวข้องที่มิใช่กระทรวงกลาโหมและสำนักข่าวกรองแห่งชาติ รับคำร้องทุกข์และคำกล่าวโทษจากผู้เสียหาย ตลอดจนประสานงานกับหน่วยงานอื่นๆ เพื่อดำเนินการสืบสวนสอบสวน และดำเนินคดีต่อไป

ข้อ ๗ ในกรณีที่ต้องการจะจับกุม ควบคุม ค้น สืบสวน หรือสอบสวน พนักงานเจ้าหน้าที่อาจร้องขอต่อเจ้าพนักงานตำรวจ หรือพนักงานสอบสวนคดีพิเศษผู้มีอำนาจ แล้วแต่กรณี ให้ช่วยดำเนินการและให้การสนับสนุนเครื่องมืออุปกรณ์ และกำลังพล แก่พนักงานเจ้าหน้าที่ในการดำเนินการดังกล่าว

ทั้งนี้ ในการขอหมายค้นหรือหมายจับให้เป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ทำการสืบสวน สอบสวนร่วมกับพนักงานสอบสวนหรือพนักงานสอบสวนคดีพิเศษ

เมื่อได้ตัวผู้กระทำความผิดมาแล้ว การควบคุม และการขอฝากขังผู้ต้องหาต่อศาลตามประมวลกฎหมายวิธีพิจารณาความอาญาให้เป็นหน้าที่ของพนักงานสอบสวนหรือพนักงานสอบสวนคดีพิเศษ และให้พนักงานเจ้าหน้าที่ร่วมกับพนักงานสอบสวนผู้รับผิดชอบ หรือพนักงานสอบสวนคดีพิเศษ ร่วมกันทำความเห็นเสนอพนักงานอัยการเพื่อดำเนินคดีต่อไป

ข้อ ๘ การค้น การรวบรวบพยานหลักฐาน การเก็บรักษาของกลาง ให้เป็นไปตามแนวปฏิบัติและมาตรฐานที่คณะกรรมการกำหนด

ข้อ ๙ ในระยะเริ่มต้นของการใช้ใช้พระราชบัญญัติ ให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติพัฒนาหลักสูตรที่มีเนื้อหาเกี่ยวกับการตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์และอิเล็กทรอนิกส์ เพื่อจัดอบรมแก่หน่วยงานที่เกี่ยวข้องหรือหน่วยงานอื่น

ข้อ ๑๐ ให้แต่ละหน่วยงานที่เกี่ยวข้องออกระเบียบของตนให้เป็นไปตามบันทึกข้อตกลงนี้ ภายใน 30 วัน

บันทึกข้อตกลงนี้ได้ทำขึ้นเมื่อ วัน/เดือน/ปี

ลงชื่อ
( )
ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ลงชื่อ พลเอก
( )
ปลัดกระทรวงกลาโหม

ลงชื่อ
( )
ปลัดกระทรวงยุติธรรม

ลงชื่อ
( )
ผู้อำนวยการสำนักข่าวกรองแห่งชาติ

ลงชื่อ พลตำรวจเอก
( )
ผู้บัญชาการตำรวจแห่งชาติ

ลงชื่อ
( )
ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

(ร่าง)

ระเบียบว่าด้วยการประสานงานเพื่อการดำเนินการตาม
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

.....

อาศัยอำนาจตามพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และมาตรา ๒๙ วรรคสาม แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และมาตรา ๑๐ (๔) แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.๒๕๔๗ สมควรออกระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบว่าด้วยการประสานงานเพื่อการดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันที่มีการลงนามท้ายระเบียบฉบับนี้เป็นต้นไป

ข้อ ๓ ในกรณีที่พนักงานสอบสวนได้รับคำร้องทุกข์ หรือคำกล่าวโทษแล้ว ให้พนักงานสอบสวนประสานงานกับพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ในกรณีที่ต้องการใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ เพื่อทำการสืบสวนและสอบสวนความผิดตามพระราชบัญญัตินี้ร่วมกัน

ความในวรรคหนึ่งให้ใช้กับกรณีที่พนักงานเจ้าหน้าที่เป็นผู้รับคำร้องทุกข์หรือรับคำกล่าวโทษด้วย

ข้อ ๔ ในการจับ ควบคุม และค้น เมื่อพนักงานเจ้าหน้าที่ประสานงานมายังพนักงานสอบสวนผู้รับผิดชอบแล้ว ให้พนักงานสอบสวนผู้รับผิดชอบดำเนินการตามอำนาจหน้าที่ต่อไป

ข้อ ๕ ให้พนักงานเจ้าหน้าที่ส่งมอบพยานหลักฐานที่รวบรวมได้มาทั้งหมดให้พนักงานสอบสวนผู้รับผิดชอบ และร่วมกันสอบสวนจนกว่าการสอบสวนเสร็จสิ้น

ข้อ ๖ ให้พนักงานสอบสวนผู้รับผิดชอบเป็นผู้ทำความเห็นตามสำนวนการสอบสวนว่า ควรสั่งฟ้องหรือสั่งไม่ฟ้อง ส่งไปยังพนักงานอัยการพร้อมด้วยสำนวน

ประกาศ ณ วันที่ พ.ศ. ๒๕๕๐

(พลเอกสุรยุทธ์ จุลานนท์)
นายกรัฐมนตรี

(นายสิทธิชัย โภไคยอุดม)
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

(นายชาญชัย ลิขิตจิตถะ)
รัฐมนตรีว่าการกระทรวงยุติธรรม