



อธิบดีกรมตรวจบัญชีสหกรณ์
รับที่... ๓๕๙๘
วันที่... ๗ ต.ค. ๒๕๕๗
เวลา... ๑๐.๒๐

รตส.1
รับที่... ๑๖๑๖
วันที่... ๖ ต.ค. ๕๗
เวลา... ๑๕.๕๖ น.

ศูนย์เทคโนโลยีสารสนเทศ
รับที่... ๕๗๒๑, 4967
วันที่... ๖ ต.ค. ๒๕๕๗
เวลา... ๑๔.๒๗

บันทึกข้อความ

ส่วนราชการ กลุ่มระบบเครือข่ายคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศ โทร.๒๓๒๔

ที่ กษ ๐๔๐๓.๔/๑๖๐

วันที่ ๖ ตุลาคม ๒๕๕๗

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์

เรียน อธิบดีกรมตรวจบัญชีสหกรณ์

ตามหนังสือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ ทท ๐๒๐๙.๔/๗๕๘๔ ลงวันที่ ๒๙ กันยายน ๒๕๕๗ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ โดยแจ้งให้กรมตรวจบัญชีสหกรณ์ทราบว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้มีมติในการประชุม ครั้งที่ ๒/๒๕๕๗ เมื่อวันที่ ๒๘ กรกฎาคม ๒๕๕๗ เห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ โดยชี้แจงและให้ความเห็นเพิ่มเติมว่าการพิจารณาให้ความเห็นชอบดังกล่าว เป็นเพียงมาตรการขั้นต่ำที่ช่วยลดความเสี่ยงจากภัยคุกคามของระบบสารสนเทศ เพื่อก่อให้เกิดความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งหน่วยงานต้องให้ความสำคัญและจัดให้มีการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยในทางปฏิบัติ รวมทั้งควรปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสมด้วย นั้น

ปัจจุบันกรมตรวจบัญชีสหกรณ์ ได้ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๕๗ ประกาศ ณ วันที่ ๒๙ เมษายน ๒๕๕๗ ซึ่งฉบับดังกล่าวยังไม่มีผลตามมาตรา ๗ เป็นเพียงการเผยแพร่ประชาสัมพันธ์ให้บุคลากรในสังกัดกรมตรวจบัญชีสหกรณ์ทราบและถือปฏิบัติเป็นการภายใน โดยขณะนั้นนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ พ.ศ.๒๕๕๗ ผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเป็นไปตามเงื่อนไขภายใต้มาตรา ๗ ของพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ.๒๕๔๙ ศูนย์เทคโนโลยีสารสนเทศ เห็นสมควรประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ พ.ศ.๒๕๕๗ ฉบับที่มีผลบังคับใช้ตามมาตรา ๗

จึงเรียนมาเพื่อโปรดพิจารณาลงนามประกาศกรมตรวจบัญชีสหกรณ์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๗ ที่แนบมาพร้อมนี้ เพื่อที่จะได้ทำการเผยแพร่ให้ทุกหน่วยงานทราบต่อไป

กลุ่มระบบเครือข่ายคอมพิวเตอร์
รับที่... ๕๕๙
วันที่... ๖ ต.ค. ๒๕๕๗
เวลา... ๐๙.๑๗

ลงนามแล้ว

(ลายเซ็น)

๗๓๐๕๗

(นายวิณะโรจน์ ทรัพย์ส่งสุข)
อธิบดีกรมตรวจบัญชีสหกรณ์

(ลายเซ็น)

(นางสาวอิสริยา ตันติพิพัฒน์)

นักวิชาการคอมพิวเตอร์ชำนาญการ

(ลายเซ็น)

(นางสาวกนกพรพรรณ ขำนาญกิจ)

ผู้อำนวยการกลุ่มระบบเครือข่ายคอมพิวเตอร์

(ลายเซ็น)

(นางกฤษณา กฤษณวรรณ)

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

นพ ๐๓๓.

ใหญ่ กตส.๑๐๓๓

(ลายเซ็น)

(นางนฤมล พนาวงศ์)

รองอธิบดีกรมตรวจบัญชีสหกรณ์



ประกาศกรมตรวจบัญชีสหกรณ์
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๕๗

ด้วยกรมตรวจบัญชีสหกรณ์ตระหนักถึงปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศ และเพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมตรวจบัญชีสหกรณ์เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหาย จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้มีมาตรฐาน แนวปฏิบัติ และขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

“กรมฯ” หมายความว่า กรมตรวจบัญชีสหกรณ์

“หน่วยงาน” หมายความว่า ศูนย์ สำนัก กอง หรือที่เรียกชื่อเป็นอย่างอื่นในสังกัดกรมตรวจบัญชีสหกรณ์

“ผู้บริหารระดับสูงสุด” หมายความว่า อธิบดีกรมตรวจบัญชีสหกรณ์

“ผู้บังคับบัญชา” หมายความว่า ผู้มีอำนาจในการตัดสินใจทางด้านเทคโนโลยีสารสนเทศ
ในส่วนกลางและส่วนภูมิภาค

- ส่วนกลาง หมายความว่า ผู้บริหารระดับสูง (CIO)
- ส่วนภูมิภาค หมายความว่า ผู้อำนวยการสำนักงานตรวจบัญชีสหกรณ์/หัวหน้าสำนักงานตรวจบัญชีสหกรณ์

“ผู้ใช้งาน” หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ พนักงานจ้างเหมาที่ปรึกษาโครงการ ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

“สินทรัพย์” หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

“สารสนเทศ” หมายความว่า ข้อมูลในรูปแบบต่างๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจ หรือใช้ประโยชน์ต่างๆ ตามภารกิจของกรมฯ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

“แนวนโยบาย” หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมอิเล็กทรอนิกส์ ซึ่งกรมตรวจบัญชีสหกรณ์ประกาศไว้เพื่อให้ผู้ใช้งานของกรมฯ ได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกัน

“แนวปฏิบัติ” หมายถึง ขั้นตอนวิธีการที่กรมตรวจบัญชีสหกรณ์ได้กำหนดไว้สำหรับการปฏิบัติงานของผู้ใช้งานของกรมฯ โดยมีจุดมุ่งหมายเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีวิธีการที่มั่นคงปลอดภัย

ข้อ ๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ แบ่งเป็น ๒ ส่วน ได้แก่

ส่วนที่ ๑ แนวนโยบาย

ส่วนที่ ๒ แนวปฏิบัติ

รายละเอียดภายในของทั้งสองส่วน ประกอบด้วยเนื้อหาสาระสำคัญในประเด็นดังต่อไปนี้

(๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๑.๑) การเข้าถึงระบบสารสนเทศ เพื่อควบคุมและป้องกันการเข้าถึง การเปิดเผย และการแก้ไขสารสนเทศและระบบสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต

(๑.๒) การเข้าถึงระบบเครือข่าย เพื่อกำหนดมาตรการการควบคุมการเข้าถึงระบบเครือข่ายของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกหรือจากโปรแกรมประสงค์ร้ายที่จะสร้างความเสียหายแก่ข้อมูลหรือทำให้ระบบเครือข่ายหยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามระบบพิสูจน์ตัวตนได้อย่างถูกต้อง

(๑.๓) การเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

(๑.๔) การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ เพื่อป้องกันและควบคุมการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ ให้เป็นไปตามที่ปฏิบัติไว้ในแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมตรวจบัญชีสหกรณ์ พ.ศ. ๒๕๕๗

ข้อ ๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีวิธีการตรวจสอบและควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ และดำเนินการตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมฯ อย่างน้อยปีละ ๑ ครั้ง โดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๕ สร้างความรู้ความเข้าใจให้กับผู้ใช้งานของกรมตรวจบัญชีสหกรณ์ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการดังนี้

(๑) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศทางเว็บไซต์กรมฯ ให้แก่ผู้ใช้งานและบุคคลทั่วไป

(๒) จัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

ข้อ ๖ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๗ ให้ศูนย์เทคโนโลยีสารสนเทศ กรมตรวจบัญชีสหกรณ์ เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติอย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๓ ตุลาคม พ.ศ. ๒๕๕๗



(นายวิณะโรจน์ ทรัพย์ส่งสุข)
อธิบดีกรมตรวจบัญชีสหกรณ์