# บันทึกข้อความ

**ส่วนราชการ** ศูนย์เทคโนโลยีสารสนเทศ กลุ่มระบบเครือข่ายคอมพิวเตอร์ โทร. ๒๓๒๔

**ที่** กษ ๐๔๐๓/ว ๓๐ **วันที่** ๗ พฤษภาคม ๒๕๕๗

**เรื่อง** แจ้งเวียนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมตรวจบัญชีสหกรณ์ พ.ศ. ๒๕๕๗

เรียน ทุกหน่วยงานในสังกัดกรมตรวจบัญชีสหกรณ์

ตามหนังสือที่ กษ ๐๔๐๓.๔/๓๕ ลงวันที่ ๑๑ เมษายน ๒๕๕๗ เรื่อง ขอประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมตรวจบัญชีสหกรณ์ พ.ศ.๒๕๕๗ โดยท่านอธิบดีฯ อนุญาตให้เผยแพร่แก่บุคลากรในสังกัดกรมตรวจบัญชีสหกรณ์ทราบและถือปฏิบัติโดยทั่วกัน นั้น

ศูนย์เทคโนโลยีสารสนเทศ ขอแจ้งเวียนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมตรวจบัญชีสหกรณ์ พ.ศ. ๒๕๕๗ เพื่อเผยแพร่ให้บุคลากรในสังกัดกรมตรวจบัญชีสหกรณ์ทราบและถือปฏิบัติโดยทั่วกัน ซึ่งจะนำเผยแพร่ผ่านทางเว็บไซต์กรมฯ อีกช่องทางหนึ่ง

จึงเรียนมาเพื่อโปรดทราบ

(นางกฤษณา กฤษณวรรณ)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

อธิบดีกรมตรวจบัญชีสหกรณ์
รับที่ ๙๗๐
วันที่ ๑๑ เม.ย. ๒๕๕๗
เวลา ๑๖.๒๙ น.

ศูนย์เทคโนโลยีสารสนเทศ
รับที่ ๑๓๑๑ 1647
วันที่ ๑๑ เม.ย. ๒๕๕๗
เวลา ๐๙.๑๐

# บันทึกข้อความ

**ส่วนราชการ** กลุ่มระบบเครือข่ายคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศ โทร.๒๓๒๔
**ที่** กษ ๐๔๐๓.๔/๓๕ **วันที่** ๑๑ เมษายน ๒๕๕๗
**เรื่อง** ขอประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมตรวจบัญชีสหกรณ์ พ.ศ. ๒๕๕๗

รตส.1
รับที่ ๔๔๘
วันที่ ๑๑ เม.ย. ๕๗
เวลา

เรียน อธิบดีกรมตรวจบัญชีสหกรณ์

ตามหนังสือกลุ่มนิติการที่ กษ ๐๔๐๑.๕/- ลงวันที่ ๓๑ มีนาคม ๒๕๕๗ เรื่อง ขอประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมตรวจบัญชีสหกรณ์ พ.ศ.๒๕๕๖ กลุ่มนิติการมีข้อพิจารณาในการประกาศใช้นโยบายและแนวปฏิบัติดังกล่าวคือ ร่างประกาศฉบับนี้ยังไม่มีผลตามมาตรา ๗ เป็นเพียงการเผยแพร่ประชาสัมพันธ์ให้ทราบและถือปฏิบัติเป็นการภายใน หากต่อไปภายหลังเมื่อคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ให้ความเห็นชอบ กรมตรวจบัญชีสหกรณ์ต้องออกประกาศฉบับใหม่ในเรื่องนี้อีกครั้งหนึ่งเพื่อให้มีผลบังคับใช้ตามมาตรา ๗ และหากกรมฯ ออกเป็นประกาศไปพลางก่อนเห็นสมควรแก้ไขปี พ.ศ. ๒๕๕๖ เป็น พ.ศ. ๒๕๕๗ (ตามเอกสารแนบ ๑) นั้น

ศูนย์เทคโนโลยีสารสนเทศ โดยกลุ่มระบบเครือข่ายคอมพิวเตอร์ ได้ประสานไปยังสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อหารือในการขอปรับเปลี่ยนปี พ.ศ. ๒๕๕๖ เป็น พ.ศ. ๒๕๕๗ ซึ่งเจ้าหน้าที่ให้ความเห็นว่าสามารถปรับเปลี่ยนได้ และขอให้กรมฯ ส่งร่างประกาศฯ ฉบับที่มีการปรับแก้ไข เพื่อนำเสนอให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์พิจารณาให้ความเห็นชอบต่อไป (ตามเอกสารแนบ ๒)

จึงเรียนมา

๑. เพื่อโปรดพิจารณาลงนามหนังสือถึงปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๒. เพื่อโปรดพิจารณาลงนามประกาศกรมตรวจบัญชีสหกรณ์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๗
๓. เพื่อขออนุญาตเผยแพร่ให้บุคลากรในสังกัดกรมตรวจบัญชีสหกรณ์ทราบโดยทั่วกัน

(3)
- ลงนามแล้ว ๓๐ เม.ย. ๕๗
- อนุญาต ๓๐ เม.ย. ๕๗

(นายวิณะโรจน์ ทรัพย์สังสุข)
อธิบดีกรมตรวจบัญชีสหกรณ์

(นางสาวอิสรีย์ ตันติพิพัฒน์)
นักวิชาการคอมพิวเตอร์ชำนาญการ

(นางสาวกนกพรรณ ชำนาญกิจ)
ผู้อำนวยการกลุ่มระบบเครือข่ายคอมพิวเตอร์

(4) ทราบ / กรุณาดำเนินการต่อไป

(นางกฤษณา กฤษณวรรณ)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(2)
(นางกฤษณา กฤษณวรรณ)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(นางนฤมล พนาวงศ์)
รองอธิบดีกรมตรวจบัญชีสหกรณ์

**ประกาศกรมตรวจบัญชีสหกรณ์**
**เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**
**พ.ศ. ๒๕๕๗**

---

ด้วยกรมตรวจบัญชีสหกรณ์ตระหนักถึงปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศ และเพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมตรวจบัญชีสหกรณ์เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหาย จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้มีมาตรฐาน แนวปฏิบัติ และขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

"กรมฯ" หมายความว่า กรมตรวจบัญชีสหกรณ์

"หน่วยงาน" หมายความว่า ศูนย์ สำนัก กอง หรือที่เรียกชื่อเป็นอย่างอื่นในสังกัดกรมตรวจบัญชีสหกรณ์

"ผู้บริหารระดับสูงสุด" หมายความว่า อธิบดีกรมตรวจบัญชีสหกรณ์

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจในการตัดสินใจทางด้านเทคโนโลยีสารสนเทศในส่วนกลางและส่วนภูมิภาค

- 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 ที่สามารถนำมาใช้ประกอบการตัดสินใจหรือใช้ประโยชน์ต่างๆ ตามภารกิจของกรมฯ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (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) การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ 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 ๒๙ เมษายน พ.ศ. ๒๕๕๗

(นายวิณะโรจน์ ทรัพย์ส่งสุข)
อธิบดีกรมตรวจบัญชีสหกรณ์