



มาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร  
สำหรับธุรกรรมภาษีทางอิเล็กทรอนิกส์

ว่าด้วยการเก็บรักษาข้อมูลในรูปแบบอิเล็กทรอนิกส์

RD ICT Standard for Electronic Tax Transactions  
: Data Retention

RD STD. [02-2566]



## คำนำ

ด้วยกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มีบทบัญญัติเกี่ยวกับการบังคับใช้ทางกฎหมายของข้อความที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ มีสาระสำคัญว่า ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปแบบของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ที่กำหนดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว หรือในกรณีที่กฎหมายกำหนดให้เก็บรักษาเอกสารหรือข้อความใด ถ้าได้เก็บรักษาในรูปแบบของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ที่กำหนดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ถือว่าได้มีการเก็บรักษาเอกสารหรือข้อความตามที่กฎหมายต้องการแล้ว

ดังนั้น เพื่อให้การปฏิบัติตามประมวลรัษฎากรมีความสอดคล้องกับกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าว และเพื่อให้เจ้าพนักงานสรรพากรถือเป็นแนวทางปฏิบัติในการตรวจและแนะนำเกี่ยวกับการจัดทำและการจัดเก็บเอกสารหลักฐานตามประมวลรัษฎากรที่มีข้อความอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ จึงได้กำหนดมาตรฐานในการจัดเก็บรักษาข้อมูลในรูปแบบอิเล็กทรอนิกส์ สำหรับผู้มีหน้าที่เสียภาษีหรือผู้ประกอบการจดทะเบียนอาจจัดทำเอกสารหลักฐานที่เป็นต้นฉบับในรูปแบบกระดาษและจัดเก็บสำเนาไว้ในรูปแบบกระดาษ หรืออาจจัดทำเอกสารหลักฐานที่เป็นต้นฉบับในรูปแบบกระดาษและจัดเก็บสำเนาไว้ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ หรืออาจจัดทำเอกสารหลักฐานที่เป็นต้นฉบับในรูปแบบของข้อมูลอิเล็กทรอนิกส์และจัดเก็บสำเนาไว้ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ซึ่งไม่ว่าจะดำเนินการในลักษณะใด การจัดทำและการจัดเก็บเอกสารหลักฐานตามประมวลรัษฎากรต้องมีความถูกต้องและต้องกระทำตามวิธีการแบบปลอดภัยที่เชื่อถือได้



ประวัติการปรับปรุงเอกสาร

Version	รายละเอียด	วันที่
01.00.0000	เวอร์ชันแรก	23 สิงหาคม 2566



## สารบัญ

เรื่อง	หน้าที่
1. ขอบข่าย.....	1
2. การจัดเก็บรักษาข้อมูลในรูปแบบอิเล็กทรอนิกส์.....	2
3. การรักษาความปลอดภัยและความถูกต้องครบถ้วนของข้อมูลที่จัดเก็บ.....	3
4. การควบคุมการเข้าถึงข้อมูลในรูปแบบอิเล็กทรอนิกส์.....	4
บรรณานุกรม.....	5



## 1. ขอบข่าย

มาตรฐานการเก็บรักษาข้อมูลในรูปแบบอิเล็กทรอนิกส์ ฉบับนี้ เป็นข้อกำหนดและแนวทางปฏิบัติในการจัดเก็บรักษาข้อมูลในรูปแบบอิเล็กทรอนิกส์ โดยครอบคลุมตามวัตถุประสงค์และข้อกำหนดด้านความมั่นคงปลอดภัย กรมสรรพากรจึงกำหนดมาตรฐานฯ เพื่อใช้เป็นแนวทางในการเก็บรักษาความมั่นคงปลอดภัยของข้อมูลในรูปแบบอิเล็กทรอนิกส์ให้เป็นมาตรฐานเดียวกัน โดยข้อมูลอิเล็กทรอนิกส์จะต้องมีความถูกต้องครบถ้วน พร้อมใช้งาน และน่าเชื่อถือ



## 2. การจัดเก็บรักษาข้อมูลในรูปแบบอิเล็กทรอนิกส์

การจัดเก็บเอกสารหลักฐานตามประมวลรัษฎากรที่มีข้อความอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์จะต้องเป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และสามารถแสดงข้อความนั้นในภายหลังได้

(2) ข้อความที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำกลับมาใช้ได้ โดยความหมายของข้อความไม่เปลี่ยนแปลง

(3) ได้เก็บรักษาข้อความที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์นั้น ให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้

(4) ได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทางที่สร้าง ส่ง จำนวนหน่วยของข้อมูลที่ส่ง วัน เดือน ปี และเวลาที่ส่ง รหัสหน่วยงานที่ส่ง และปลายทางของข้อมูล จำนวนข้อมูลอิเล็กทรอนิกส์ที่ปลายทางได้รับ วัน เดือน ปี และเวลาที่ได้รับข้อมูล

(5) สามารถเรียกดูหรือพิมพ์ข้อมูลของเอกสารหลักฐานที่ได้เก็บรักษา ข้อความอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ได้

(6) ต้องสามารถถ่ายโอนข้อมูล (Export File) ที่เก็บบันทึกไว้ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ โดยมีรูปแบบ (Format) ของรายการต่าง ๆ ตามที่อธิบดีกรมสรรพากรประกาศกำหนด

(7) กรณีเอกสารหลักฐานตามประมวลรัษฎากรเป็นเอกสารที่กฎหมายกำหนดให้ลงลายมือชื่อ และมีการจัดทำเอกสารหลักฐานดังกล่าวในรูปแบบของข้อมูลอิเล็กทรอนิกส์ การลงลายมือชื่อจะต้องจัดทำลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ และสามารถระบุตัวเจ้าของ ลายมือชื่อได้ ซึ่งเจ้าของลายมือชื่อจะต้องใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้องและความสมบูรณ์ของการแสดงสาระสำคัญทั้งหมดที่ได้กระทำโดยเจ้าของลายมือชื่อ



### 3. การรักษาความปลอดภัยและความถูกต้องครบถ้วนของข้อมูลที่จัดเก็บ

การรักษาความปลอดภัยของข้อมูลที่จัดเก็บในรูปแบบอิเล็กทรอนิกส์ เพื่อลดปัจจัยเสี่ยงที่จะเกิดความเสียหายกับข้อมูลที่จัดเก็บในรูปแบบอิเล็กทรอนิกส์ เนื่องจากความผิดพลาดในการทำงานของผู้ใช้ระบบ แพ้ข้อมูลเสียหาย ความผิดพลาดในการทำงานของเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ การปฏิบัติงานที่ไม่เหมาะสม และการเปิดเผยข้อมูลที่เป็นความลับ ซึ่งจะต้องคำนึงถึงการกำหนดนโยบาย (policy) ขององค์กร และระบบการรักษาความปลอดภัย ดังนี้

(1) มีการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วยกฎ ข้อบังคับ และหน้าที่ความรับผิดชอบของบุคคลากรขององค์กร พร้อมทั้งระเบียบวิธีปฏิบัติที่ใช้เป็นหลักในการทำงาน รวมทั้งการติดตามตรวจสอบให้ทุกคนปฏิบัติตามกฎ ระเบียบ มาตรฐานที่วางไว้อย่างเคร่งครัด และสม่ำเสมอ

(2) มีการกำหนดความมั่นคงปลอดภัยในการรักษาความลับและความถูกต้องครบถ้วนของข้อมูล โดยต้องมีองค์ประกอบของความมั่นคงปลอดภัยของข้อมูล ดังนี้

(2.1) การรักษาความลับ (Confidentiality) กำหนดให้บุคคลผู้มีสิทธิสามารถเข้าถึงเรียกดูข้อมูลได้ มีการควบคุมการเข้าถึงข้อมูลที่เป็นความลับ ข้อมูลต้องไม่ถูกเปิดเผยกับผู้ไม่มีสิทธิ และมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น การจัดประเภทของข้อมูล การรักษาความปลอดภัยให้กับแหล่งจัดเก็บข้อมูล เป็นต้น

(2.2) ความถูกต้องแท้จริง (Integrity) มีขั้นตอนการตรวจสอบความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล วิธีการประมวลผล การควบคุมความผิดพลาด และต้องไม่ให้ผู้ไม่มีสิทธิมาทำการเปลี่ยนแปลงแก้ไข

(2.3) ความสามารถพร้อมใช้เสมอ (Availability) ผู้มีสิทธิสามารถเข้าถึงข้อมูลได้เมื่อมีความต้องการใช้ได้อย่างราบรื่น โดยมีการควบคุมระบบให้มีความพร้อมใช้งานอย่างต่อเนื่อง

(3) มีการกำหนดระยะเวลาการเก็บรักษาข้อมูลแต่ละประเภท ตามระยะเวลาที่กฎหมายหรือระเบียบข้อบังคับที่กำหนดไว้

(4) มีขั้นตอนการปฏิบัติการสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ (Software) และข้อมูลในระบบเทคโนโลยีสารสนเทศ

(5) มีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศให้กับผู้ใช้งานระบบสารสนเทศ



#### 4. การควบคุมการเข้าถึงข้อมูลในรูปแบบอิเล็กทรอนิกส์

การจัดเก็บและเข้าถึงเอกสารที่มีข้อความให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์จะต้องมีการควบคุมการเข้าถึงข้อมูลซึ่งจะต้องดำเนินการตามวิธีการแบบปลอดภัยที่เชื่อถือได้ทั้งในส่วนของระบบฮาร์ดแวร์ (Hardware) และระบบซอฟต์แวร์ (Software) ดังต่อไปนี้

(1) มีระบบรักษาความปลอดภัยเพื่อควบคุมการเข้าถึงข้อมูลได้ โดยจะต้องมี

(ก) ภาพการทำงานโดยรวมของระบบ (System Flowchart) ได้

(ข) แสดงระดับการปฏิบัติงานของเจ้าหน้าที่ผู้ใช้ระบบ โดยระบุจำนวนและระดับเจ้าหน้าที่ที่สามารถบันทึก อ่าน หรือเข้าไปใช้ระบบงานในแต่ละระดับได้

(ค) เป็นโปรแกรมที่เมื่อบันทึกข้อมูลแล้วจะแก้ไขรายการนั้น ๆ โดยไร้ร่องรอยไม่ได้ การแก้ไขรายการไม่ให้ใช้วิธีลบทิ้ง หรือล้างรายการออก ถ้าจะแก้ไขต้องบันทึกรายการปรับปรุงเพิ่มเข้าไปเพื่อแสดงให้เห็นรายการก่อนปรับปรุงและหลังปรับปรุง และต้องมี รายงานการแก้ไขรายการเพื่อการตรวจสอบได้

(ง) มีการควบคุมการเข้าถึงข้อมูลทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ โดยการยืนยันตัวตนบนระบบได้ เช่น การกรอกรหัสผู้ใช้และรหัสผ่านผ่าน (Username และ Password), การกรอกรหัสผ่านที่ใช้ได้ครั้งเดียว (OTP), การสแกนลายนิ้วมือ (Biometric), และอื่น ๆ

(จ) มีการควบคุมสิทธิเข้าไปใช้ระบบงานทุกระดับและมีระบบงานที่บันทึกการเปลี่ยนรหัสผ่านทุกครั้งที่มีการเปลี่ยนแปลง

(ฉ) มีรายงานบันทึกการใช้ระบบงาน โดยระบุให้ทราบถึงรหัสประจำตัวของเจ้าหน้าที่ผู้ใช้ระบบ งานที่ทำ วัน เดือน ปี และเวลาที่เข้าไปใช้ระบบงาน (Access) ในกรณี ที่มีการแก้ไขรายการจะต้องระบุให้ทราบถึงรหัสประจำตัวของเจ้าหน้าที่ผู้ใช้ระบบ จำนวน และรายละเอียดของรายการที่แก้ไขปรับปรุง

(ช) มีระบบการตรวจสอบผู้เข้าใช้หรือผู้เข้าไปแก้ไขข้อมูลในระบบ และมีกระบวนการในการตรวจสอบข้อมูลที่บันทึกไว้ในระบบที่สามารถแสดงว่าข้อมูลดังกล่าวได้บันทึกไว้ครบถ้วนทุกรายการแล้ว และไม่มีการแก้ไขรายการของเอกสารที่มีข้อความอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

(2) กรณีเพิ่มข้อมูลมีการควบคุมโดยการเข้ารหัส (Encryption) เพื่อป้องกันการเข้าถึงข้อมูล ถ้ามีการถอดรหัส (Decryption) ต้องบันทึกหลักฐานไว้ทุกครั้งเพื่อการตรวจสอบ และสามารถจัดพิมพ์เป็นรายงานเพื่อการตรวจสอบได้

(3) กรณีมีการรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานการรักษาความปลอดภัยของข้อมูลที่รับส่งผ่านอินเทอร์เน็ต (Secure Sockets Layer: SSL) และเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN), XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากล ในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่าง ๆ ภายในหน่วยงาน





### บรรณานุกรม

- [1] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 (ฉบับอัปเดต)
- [2] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ [ชมธอ. 21-2562]
- [3] คำสั่งกรมสรรพากรที่ ป. 121/2545 วันที่ 26 ธันวาคม พ.ศ. 2545 เรื่อง การจัดทำและการจัดเก็บเอกสารหลักฐานตามประมวลรัษฎากร ที่มีข้อความอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์