ระเบียบกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ว่าด้วยการปฏิบัติด้านระบบสารสนเทศ พ.ศ. ๒๕๕๖

เพื่อให้ระบบสารสนเทศของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานมีความมั่นคงปลอดภัย และมิให้มีผู้กระทำด้วยประการใดๆ ให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อเผยแพร่ข้อมูลอันเป็นเท็จ หรือมีลักษณะอันลามกอนาจาร ซึ่งอาจก่อให้เกิดความเสียหายแก่กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน รวมทั้งเพื่อเป็นการปฏิบัติตามระเบียบและนโยบายด้านสารสนเทศของกระทรวงพลังงาน และให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

หมวดที่ ๑
คำนิยาม

ข้อ ๑ ระเบียบนี้เรียกว่า "ระเบียบกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานว่าด้วยการปฏิบัติด้านระบบสารสนเทศ พ.ศ. ๒๕๕๖"

ข้อ ๒ ระเบียบนี้ให้บังคับใช้นับแต่วันถัดจากวันประกาศใช้ระเบียบนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิก "ระเบียบกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานว่าด้วยการปฏิบัติด้านระบบสารสนเทศ พ.ศ. ๒๕๕๓" และให้ใช้ระเบียบนี้แทน

ข้อ ๔ ในระเบียบนี้

"**กรม**" หมายถึง กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"**อธิบดี**" หมายถึง อธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"**ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง**" หมายถึง รองอธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานที่ได้รับการแต่งตั้งจากอธิบดีให้ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

"**คณะกรรมการ**" หมายถึง คณะกรรมการเทคโนโลยีสารสนเทศที่ได้รับการแต่งตั้งจากอธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน เพื่อทำหน้าที่ กำกับ ดูแลการใช้งานระบบสารสนเทศของกรม

"**ศูนย์**" หมายถึง ศูนย์สารสนเทศข้อมูลพลังงานทดแทนและอนุรักษ์พลังงาน

"ผู้อำนวยการศูนย์" หมายถึง ผู้อำนวยการศูนย์สารสนเทศข้อมูลพลังงานทดแทนและอนุรักษ์พลังงาน

"ผู้บังคับบัญชา" หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของกรม

"ผู้ดูแลระบบสารสนเทศ" หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแล บำรุงรักษาระบบงานสารสนเทศของกรม และสามารถเข้าถึงระบบสารสนเทศของกรมเพื่อการบริหารจัดการ

"ผู้ใช้งาน" หมายถึง ข้าราชการ พนักงานราชการ หรือลูกจ้างของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ผู้รับจ้างทำของและบริวารที่รับทำการงานให้กับกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน และผู้ใช้บริการที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"สิทธิของผู้ใช้งาน" หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของกรม

"สินทรัพย์" หมายถึง ระบบเครือข่ายสารสนเทศ ระบบงานสารสนเทศ ระบบคอมพิวเตอร์ และข้อมูลของกรม

"ระบบสารสนเทศ" หมายถึง ระบบเครือข่ายสารสนเทศ ระบบงานสารสนเทศ และระบบคอมพิวเตอร์

"ระบบเครือข่ายสารสนเทศ" หมายถึง เครือข่ายคอมพิวเตอร์ เครือข่ายการสื่อสารข้อมูล

"ระบบงานสารสนเทศ" หมายถึง ระบบงาน ระบบฐานข้อมูล และโปรแกรมต่างๆ ที่ใช้งานภายในและให้บริการแก่บุคลากรภายนอก

"ระบบคอมพิวเตอร์" หมายถึง เครื่องคอมพิวเตอร์ เครื่องพิมพ์ เครื่องสแกนเนอร์ เครื่องสำรองไฟฟ้า และอุปกรณ์ประกอบอื่นๆ ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์

"ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของกรมถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๕ ให้อธิบดีเป็นผู้รักษาการตามระเบียบนี้

หมวดที่ ๒
อำนาจหน้าที่

ให้อธิบดี ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้อำนวยการศูนย์ และผู้ดูแลระบบสารสนเทศ มีอำนาจหน้าที่ในการรักษาความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ดังนี้

ข้อ ๖ อธิบดี มีหน้าที่รับผิดชอบกำกับ ดูแลการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรม และรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นอันเนื่องมาจากความบกพร่อง หรือไม่ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศแล้วแต่กรณี

ข้อ ๗ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง[๑] มีอำนาจหน้าที่ดังต่อไปนี้

(๑) รับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรม

(๒) จัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร

(๓) มีอำนาจในการจัดสรรทรัพยากรในการดำเนินโครงการเทคโนโลยีสารสนเทศของกรม

(๔) ดำเนินการเรื่องอื่นตามที่อธิบดีมอบหมาย

ข้อ ๘ ผู้อำนวยการศูนย์ มีหน้าที่ดังต่อไปนี้

(๑) ให้คำแนะนำ และข้อเสนอแนะต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง/หรือคณะกรรมการในการกำหนดนโยบายและมาตรการด้านเทคโนโลยีสารสนเทศ

(๒) กำกับ ดูแล และควบคุมการให้บริการด้านระบบสารสนเทศ และการปฏิบัติตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ข้อ ๙ ผู้ดูแลระบบสารสนเทศ มีหน้าที่ดังต่อไปนี้

(๑) ดูแลรักษา และปรับปรุงระบบสารสนเทศให้สามารถใช้งานได้ดีอยู่เสมอ

(๒) ควบคุม ดูแลผู้ใช้บริการให้ปฏิบัติตามกฎระเบียบการใช้งานระบบสารสนเทศของกรม

(๓) กรณีพบว่าผู้ใช้บริการไม่ปฏิบัติตามระเบียบการใช้งานระบบสารสนเทศของกรม ผู้ดูแลระบบสารสนเทศจะต้องรายงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงทราบโดยเร็วที่สุด และในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น ผู้ดูแลระบบสารสนเทศมีอำนาจในการระงับการใช้งานของผู้ใช้บริการดังกล่าวได้ทันที

(๔) ผู้ดูแลระบบสารสนเทศมีหน้าที่ในการเสนอความเห็นต่อผู้อำนวยการศูนย์ เพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารจัดการระบบสารสนเทศ

---

[๑] ตามมติคณะรัฐมนตรีเมื่อวันที่ ๙ มิถุนายน ๒๕๔๑ เรื่องการแต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

(๕) ผู้ดูแลระบบสารสนเทศมีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัสข้อมูลอัตโนมัติ (Encryption) หรือระบบอื่นใดที่เกี่ยวข้องกับระบบเครือข่ายสารสนเทศ และอุปกรณ์คอมพิวเตอร์ตลอดจนบำรุงรักษาสิ่งต่างๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

(๖) ผู้ดูแลระบบสารสนเทศมีหน้าที่ในการกำกับดูแลรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของกรม และมีหน้าที่รับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนการสำรองข้อมูล แผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และมีหน้าที่ในการทดสอบสภาพพร้อมใช้งาน การทำสำรองข้อมูล และการทดสอบการกู้คืนข้อมูลตามระยะเวลาที่เหมาะสม

หมวดที่ ๓

ระเบียบการใช้งานระบบเครือข่ายสารสนเทศของกรม

ข้อ ๑๐ ระบบเครือข่ายสารสนเทศของกรมเป็นสมบัติของทางราชการ ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต

ข้อ ๑๑ ผู้ใช้บริการต้องยอมรับอย่างไม่มีเงื่อนไขในการรับทราบกฎระเบียบหรือนโยบายต่างๆ ที่กรมกำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบายของกรม มิได้

ข้อ ๑๒ ผู้ใช้บริการต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือกฎหมายอื่นที่เกี่ยวข้องกับระบบสารสนเทศ

ข้อ ๑๓ ผู้ใช้บริการพึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพและไม่ผิดไปจากนโยบายด้านความมั่นคงปลอดภัย

ข้อ ๑๔ ผู้ใช้บริการต้องไม่ส่ง Mail แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น

ข้อ ๑๕ ห้ามผู้ใช้บริการ โอน จำหน่าย หรือจ่ายแจกบัญชีผู้ใช้งาน (User Account) นี้ให้กับผู้อื่น

ข้อ ๑๖ การใช้งานระบบเครือข่ายสารสนเทศที่กรมให้บริการ ผู้ใช้บริการต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดจากการใช้งานนั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

ข้อ ๑๗ ห้ามผู้ใช้บริการปฏิบัติการใดๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของผู้ดูแลระบบเครือข่ายสารสนเทศ และ/หรือกรม

ข้อ ๑๘ ห้ามผู้ใช้บริการทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านระบบเครือข่ายสารสนเทศของกรม เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

ข้อ ๑๙ ผู้ใช้บริการจะต้องไม่ละเมิดต่อผู้อื่นกล่าวคือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ของส่วนราชการ หรือหน่วยงานอื่นๆ การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้บริการจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว ผู้ดูแลระบบสารสนเทศ และ/หรือกรม ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

ข้อ ๒๐ กรมจะไม่รับประกันในคุณภาพของการเก็บ การรับ-ส่งข้อมูลข่าวสาร และการไม่สามารถใช้งานได้ของระบบบางส่วนหรือทั้งหมด และจะไม่รับผิดชอบในความเสียหายของการใช้งานอันเนื่องมาจากวงจรสื่อสารชำรุด จานแม่เหล็กชำรุด ความล่าช้า แฟ้มข้อมูลหรือจดหมายส่งไปไม่ถึงปลายทางหรือส่งผิดสถานที่ และความผิดพลาดในข้อมูลหรือความเสียหายอันเกิดจากการล่วงละเมิดโดยผู้ใช้งานอื่นๆ

ข้อ ๒๑ ผู้ใช้บริการสัญญาว่าจะปฏิบัติตามเงื่อนไข/กฎ/ระเบียบ/คำแนะนำที่กรม กำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม ซึ่งจะมีผลบังคับใช้โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

ข้อ ๒๒ ผู้ดูแลระบบสารสนเทศ และ/หรือผู้บังคับบัญชา ทรงสิทธิที่จะปฏิเสธการเชื่อมต่อและ/หรือการใช้งาน ยกเลิก หรือระงับการเชื่อมต่อ และ/หรือการใช้งานใดๆ ของผู้ใช้บริการที่ล่วงละเมิดกฎระเบียบนี้

หมวดที่ ๔

ระเบียบการเชื่อมต่อระบบคอมพิวเตอร์และระบบเครือข่ายสารสนเทศ

ข้อ ๒๓ การขออนุญาตใช้งานระบบสารสนเทศหรือการนำอุปกรณ์คอมพิวเตอร์มาเชื่อมต่อกับระบบเครือข่ายสารสนเทศของกรม ผู้ขอใช้บริการจะต้องทำหนังสือขอใช้พร้อมแนบแบบฟอร์มการขอใช้งานส่งผ่านหน่วยงานต้นสังกัดมายังศูนย์ เพื่อพิจารณาดำเนินการลงทะเบียนในระบบ และกำหนดหมายเลข IP Address ของอุปกรณ์ดังกล่าว เพื่อให้สามารถระบุอุปกรณ์บนระบบเครือข่ายได้ และให้การเชื่อมต่ออุปกรณ์ต่างๆ เป็นไปตามมาตรฐานสากล และไม่เกิดผลกระทบกับระบบเครือข่ายสารสนเทศโดยรวมของกรม และหากมีค่าใช้จ่ายในการเชื่อมต่อเกิดขึ้นผู้ขอใช้บริการจะต้องรับผิดชอบค่าใช้จ่ายดังกล่าว

ข้อ ๒๔ การนำเครื่องคอมพิวเตอร์เชื่อมต่อกับระบบเครือข่ายสารสนเทศของกรม เครื่องคอมพิวเตอร์ดังกล่าวต้องมีการติดตั้งโปรแกรมป้องกันไวรัสไว้แล้ว และให้หน่วยงาน และ/หรือผู้รับผิดชอบเครื่องคอมพิวเตอร์ดังกล่าว มีหน้าที่รับผิดชอบในการดำเนินการตรวจสอบกำจัดไวรัส และหรือโปรแกรมคอมพิวเตอร์อื่นที่ก่อให้เกิด หรืออาจจะก่อให้เกิดความเสียหายแก่ระบบเครือข่ายสารสนเทศโดยรวม

ข้อ ๒๕ ห้ามกระทำการติดตั้ง เปลี่ยนแปลงการติดตั้ง หรือเปลี่ยนแปลงค่าที่กำหนด หรือทำการใดๆ ต่ออุปกรณ์ส่วนกลางโดยพลการ อันก่อให้เกิดความเสียหายแก่อุปกรณ์ส่วนกลางและระบบเครือข่ายสารสนเทศของกรมได้

ข้อ ๒๖ ในกรณีที่ผู้ดูแลระบบสารสนเทศ ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ และหรืออุปกรณ์ใดๆ ก่อให้เกิดความผิดปกติต่อระบบเครือข่ายสารสนเทศของกรม ผู้ดูแลระบบสารสนเทศจะดำเนินการหยุดให้บริการโดยไม่มีการแจ้งให้ทราบล่วงหน้าจนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติ

ข้อ ๒๗ เพื่อให้บริการการใช้งานระบบเครือข่ายสารสนเทศผ่านเครือข่ายระยะไกล หรือระบบโมเด็ม (Remote Access) ของกรม เป็นไปได้อย่างทั่วถึง ผู้ดูแลระบบสารสนเทศกำหนดให้ผู้ใช้งานสามารถเชื่อมต่อกับระบบโมเด็มได้เพียงหนึ่งการเชื่อมต่อในขณะเวลาเดียวกัน หากฝ่าฝืนจะงดการให้บริการแก่ผู้ใช้บริการนั้น

ข้อ ๒๘ การควบคุมการเข้าใช้งานระบบจากภายนอกกรม มีแนวทางปฏิบัติ ดังนี้

(๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องมีการใช้มาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน เช่น การใช้ VPN, SSL เป็นต้น

(๒) การเข้าสู่ระบบเครือข่ายหรือระบบข้อมูล จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์ก่อน และผู้ดูแลระบบต้องมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

(๓) ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับกรมอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

(๔) ผู้ดูแลระบบสารสนเทศ ต้องกำหนดให้ผู้ใช้งานสามารถเชื่อมต่อกับระบบโมเด็มได้เพียงหนึ่งการเชื่อมต่อในขณะเวลาเดียวกัน

(๕) ผู้ดูแลระบบจะต้องกำหนด Port ที่ใช้ในการเข้าสู่ระบบ และจะต้องตรวจสอบและติดตามการใช้งานเป็นประจำอย่างน้อยเดือนละ ๑ ครั้ง

(๖) การเข้าสู่ระบบจากระยะไกล ต้องไม่เปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น และช่องทางดังกล่าวจะต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วโดยอัตโนมัติ และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

ข้อ ๒๙ การควบคุมการเข้าใช้งานระบบจากภายนอกและการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบของกรม โดยจะแบ่งออกเป็น ๒ ขั้นตอน คือ

(๑) การแสดงตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้ (Username)

(๒) การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ด หรือการใช้ USB token ที่มีความสามารถ PKI หรือการใช้ Captcha เป็นต้น

ข้อ ๓๐ การแบ่งแยกเครือข่าย (Zone) กรม กำหนดให้มีการแบ่งแยกเครือข่าย (Zone) ออกเป็น ๓ โซน คือ

(๑) โซนสาธารณะ (Public Zone) สำหรับผู้ใช้งานภายนอก สามารถเข้าถึงและใช้งานสารสนเทศภายในกรม ผ่านอุปกรณ์ระบบรักษาความปลอดภัย เช่น Firewall หรือ IPS

(๒) โซนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) เป็นโซนที่มีการจัดเตรียมอุปกรณ์และระบบเพื่อการป้องกันและรักษาความมั่นคงปลอดภัยในระดับสูง เช่น ระบบป้องกันผู้บุกรุก (Firewall, IPS, IDS) ระบบสำรองไฟฟ้า ระบบสำรองข้อมูล

(๓) โซนผู้ใช้งานภายใน (Intranet) เป็นโซนสำหรับผู้ใช้งานระบบที่อยู่ภายในกรม มีการติดตั้งระบบและซอฟต์แวร์เพื่อป้องกันและรักษาความปลอดภัย เช่น Antivirus หรือ Network Access Control (NAC) เป็นต้น

ข้อ ๓๑ การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)

(๑) ผู้ใช้งานต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในสำนักงานให้น้อยที่สุด

(๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่มีความมั่นคงปลอดภัย

(๓) มีการรักษาความมั่นคงปลอดภัยเพื่อลดความเสี่ยงจากการที่อุปกรณ์ถูกทำลาย ถูกทำให้เสียหายทางกายภาพ ถูกขโมย ถูกวางเพลิง ถูกทำให้เสียหายโดยวัตถุระเบิด การสั่นสะเทือน สิ่งสกปรก สารเคมีที่มีฤทธิ์ทำลายหรือกัดกร่อน รังสีแม่เหล็กไฟฟ้า การแทรกแซงโดยกระแสไฟฟ้าหรือคลื่นแม่เหล็ก น้ำ ฝุ่น ความร้อน หรือความชื้น

(๔) ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน

(๕) ผู้ใช้งานและผู้ดูแลระบบต้องดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้นให้อยู่ในระดับปกติหรือไม่

หมวดที่ ๕

ระเบียบการจัดหา การว่าจ้างพัฒนาระบบงานสารสนเทศ และการใช้งานระบบคอมพิวเตอร์

ข้อ ๓๒ หน่วยงานที่ประสงค์จะจัดหาระบบคอมพิวเตอร์ และ/หรือว่าจ้างพัฒนา ปรับปรุงระบบงานสารสนเทศ ต้องแจ้งความต้องการดังกล่าวให้ศูนย์ทราบก่อนการดำเนินการ ทั้งนี้ เพื่อที่ศูนย์จะได้ดำเนินการขอความเห็นชอบจากคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ของกระทรวงพลังงาน

ข้อ ๓๓ การกำหนดคุณสมบัติเบื้องต้นของระบบคอมพิวเตอร์ที่จะจัดหาต้องใช้เกณฑ์ราคากลาง (คุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และได้ความเห็นชอบจากคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ของกระทรวงพลังงาน ซึ่งเป็นการปฏิบัติตามมติ ครม.)

ข้อ ๓๔ หากผู้ใช้บริการจะดำเนินการแก้ไข ซ่อมแซม หรือปรับปรุงประสิทธิภาพของระบบคอมพิวเตอร์ ต้องแจ้งผู้ดูแลระบบสารสนเทศเพื่อตรวจสอบก่อน

ข้อ ๓๕ ห้ามมิให้ผู้ใช้บริการติดตั้ง (Install) ระบบงานสารสนเทศ หรือโปรแกรมใดๆ ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายบนระบบคอมพิวเตอร์ หากฝ่าฝืนและเกิดความเสียหาย ผู้ฝ่าฝืนจะต้องเป็นผู้รับผิดชอบต่อความเสียหายทุกประการ

ข้อ ๓๖ ในการจัดหาหรือการว่าจ้างพัฒนาระบบงานสารสนเทศ ต้องสอดคล้องและสามารถใช้งานร่วมกับอุปกรณ์ทั้งด้านฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่ายตามที่กรมมีอยู่ และต้องมีการตรวจสอบประสิทธิภาพ และความมั่นคงปลอดภัยสารสนเทศก่อนการตรวจรับ เช่น การทดสอบเข้ารหัสในการจัดเก็บข้อมูลที่สำคัญ การทดสอบและวิเคราะห์ช่องโหว่ของระบบ การทดสอบความมั่นคงของระบบ การทดสอบการป้องกันเปลี่ยนแปลงข้อมูลระหว่างสื่อสาร การทดสอบการป้องกันการโจมตีจากภายนอก เป็นต้น

ข้อ ๓๗ ในการจัดหาหรือการว่าจ้างพัฒนาระบบงานสารสนเทศ ต้องมีการกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กรฯ หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไปทุกครั้ง เช่น การห้ามเปิดเผยข้อมูลหรือผลการดำเนินงาน หรือผลการศึกษาวิจัย เป็นต้น

หมวดที่ ๖

การยกเลิกหรือสิ้นสุดการให้บริการระบบสารสนเทศ

ข้อ ๓๘ ศูนย์อาจเปลี่ยนแปลงบริการหรือตัดทอนลักษณะใดของบริการ ไม่ว่าเหตุผลใดก็ตามได้ตลอดเวลา และอาจยกเลิกหรือระงับการบริการผู้ใช้บริการเมื่อพบว่าละเมิดข้อตกลงการใช้งานโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

ข้อ ๓๙ กรณีผู้ใช้บริการเป็นลูกจ้าง และพนักงานราชการของกรม เมื่อพ้นสภาพการเป็นบุคลากรของกรม จะสิ้นสุดสิทธิการใช้งานระบบเครือข่ายสารสนเทศของกรม

ข้อ ๔๐ กรณีผู้ใช้บริการเป็นบุคลากรจากภายนอกที่ได้รับสิทธิเข้าใช้งานระบบเครือข่ายสารสนเทศเพื่อปฏิบัติงานใหม่ในส่วนที่รับผิดชอบ จะสิ้นสุดสิทธิการใช้งานเมื่อจบงานตามสัญญาการทำงาน

ข้อ ๔๑ กรณีผู้ใช้บริการฝ่าฝืนระเบียบนี้ การยกเลิกสิทธิผู้ใช้บริการขึ้นอยู่กับดุลยพินิจของผู้บังคับบัญชา

ข้อ ๔๒ การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

(๑) กรมกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบปฏิบัติการ ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

(๒) กรมกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงานที่มีข้อมูลสำคัญเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๔๓ การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

(๑) กรมกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบปฏิบัติการ ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๒ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของสำนักงานตามปกติเท่านั้น

(๒) กรมกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกกรม) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อโดยสามารถใช้งานได้ ๓๐ นาทีต่อการเชื่อมต่อหนึ่งครั้ง

ข้อ ๔๔ การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)

(๑) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

(๓) จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในกรม

(๔) ให้ตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

(๕) ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของกรม

ข้อ ๔๕ การเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities) ของผู้ใช้งานต้องได้รับการอนุมัติจากผู้ดูแลระบบก่อนการเข้าใช้ โดยต้องดำเนินการลงทะเบียนเข้าใช้งาน และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร

ข้อ ๔๖ การนำทรัพย์สินของกรมออกนอกสำนักงาน (Removal of property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกกรม และต้องมีการกำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกกรม

(๒) เมื่อมีการนำอุปกรณ์ส่งคืนให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และอุปกรณ์เกิดการชำรุดเสียหายอย่างไร

(๓) ให้มีการบันทึกข้อมูลการนำอุปกรณ์ของกรมออกไปใช้งานนอกกรม เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๔๗ หน่วยงานหรือบุคคลภายนอกที่ประสงค์จะขอใช้บริการสารสนเทศต่างๆ ของกรมจะต้องทำหนังสือขอใช้บริการส่งผ่านหน่วยงานต้นสังกัดมายังกรม เพื่อให้กรมพิจารณาอนุมัติและดำเนินการลงทะเบียนในระบบ และผู้ใช้บริการต้องยอมรับและปฏิบัติตามนโยบายและระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมอย่างเคร่งครัด

ข้อ ๔๘ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของกรมออกไปใช้งานนอก เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของกรมไว้โดยลำพังในที่สาธารณะ

(๓) ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

หมวดที่ ๗
การสำรองข้อมูลและระบบคอมพิวเตอร์

ข้อ ๔๙ ผู้ดูแลระบบสารสนเทศ ต้องคัดเลือกและจัดทำแผนการสำรองข้อมูล และดำเนินการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของกรม

ข้อ ๕๐ การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

ข้อ ๕๑ การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

ข้อ ๕๒ ให้ผู้ดูแลระบบสารสนเทศมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบสารสนเทศไม่สามารถปฏิบัติงานได้

ข้อ ๕๓ ให้ผู้ดูแลระบบสารสนเทศกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมี ๒ ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

ข้อ ๕๔ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

ข้อ ๕๕ ผู้ดูแลระบบสารสนเทศต้องจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด และต้องทำการทดสอบการกู้คืนข้อมูลที่สำรองไว้ พร้อมทั้งทบทวนปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕๖ ผู้ดูแลระบบสารสนเทศต้องปฏิบัติตามนโยบายที่เกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) และขั้นตอนการสำรองข้อมูล (Backup Procedure) โดยเคร่งครัด

หมวดที่ ๘
บทลงโทษ

หากผู้ใช้งานไม่ปฏิบัติตามกฎระเบียบดังกล่าว ก่อให้เกิดความเสียหายต่อบุคคลอื่น หรือต่อสมบัติของทางราชการ จะต้องรับโทษตามบทลงโทษต่อไปนี้

ข้อ ๕๗ ระงับสิทธิการใช้งานเครือข่ายสารสนเทศ และอุปกรณ์คอมพิวเตอร์ของกรมตามระยะเวลาที่เหมาะสม

ข้อ ๕๘ หากการละเมิดฝ่าฝืนก่อให้เกิดความเสียหายต่อผู้อื่น หรือต่อทรัพย์สินทั้งของทางราชการอย่างร้ายแรง จะต้องรับโทษตามระเบียบส่วนราชการ หรือรับโทษตามกฎหมายโดยลำดับต่อไป

ประกาศ ณ วันที่ ๒๐ สิงหาคม ๒๕๕๖

(นายอำนวย ทองสถิตย์)
อธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน