ประกาศกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
พ.ศ. ๒๕๕๖

โดยที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ประกาศกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ เพื่อให้หน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ อธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ"

ข้อ ๒ ประกาศนี้ให้บังคับใช้นับแต่วันถัดจากวันประกาศใช้นโยบายนี้เป็นต้นไป

ข้อ ๓ ในประกาศนี้

"**กรม**" หมายถึง กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"**อธิบดี**" หมายถึง อธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"**ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง**" หมายถึง รองอธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานที่ได้รับการแต่งตั้งจากอธิบดีให้ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

"**ผู้บังคับบัญชา**" หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของกรม

"**ผู้ดูแลระบบ**" หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแล บำรุงรักษาระบบงานสารสนเทศของกรม และสามารถเข้าถึงระบบสารสนเทศของกรมเพื่อการบริหารจัดการ

"**ผู้ใช้งาน**" หมายความว่า ข้าราชการ พนักงานราชการ หรือลูกจ้างของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ผู้รับจ้างทำของและบริวารที่รับทำการงานให้กับกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน และผู้ใช้บริการที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

ข้อ ๔ การจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๔.๑ การจัดทำนโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีความสอดคล้องกับมาตรฐาน ISO/IEC๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๔.๓ นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๔.๔ ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ต้องตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๔.๕ นโยบายนี้ต้องมีการดำเนินการทบทวนตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี หรือตามที่ระบุไว้ในเอกสาร "การตรวจสอบประเมินนโยบาย"

ข้อ ๕ นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

กรมกำหนดพื้นที่ควบคุม กระบวนการควบคุมการเข้าออกเฉพาะบุคคลที่ได้รับการอนุญาตเพื่อปฏิบัติงานในพื้นที่ควบคุม การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม การบริหารจัดการระบบสารสนเทศและอุปกรณ์สนับสนุนการปฏิบัติงาน และการบำรุงรักษาอุปกรณ์

ข้อ ๖ นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๖.๑ การควบคุมการเข้าถึงระบบสารสนเทศผู้ดูแลระบบต้องตรวจสอบ อนุมัติและกำหนดรหัสผ่าน ลงทะเบียนผู้ใช้งานเพื่อให้ผู้ใช้ที่มีสิทธิ (User Authentication) เท่านั้นที่สามารถเข้าถึงระบบสารสนเทศได้ และมีการเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์

๖.๒ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงสิทธิ การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน และดำเนินการการทบทวนสิทธิการใช้งาน และตรวจสอบการละเมิดความปลอดภัย

๖.๓ การควบคุมการเข้าถึงระบบเครือข่าย ผู้ดูแลต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อใช้งานอินเทอร์เน็ต ต้องผ่านระบบรักษาความปลอดภัยที่กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานจัดสรรไว้ เช่น Firewall, IPS/IDS, Proxy, การตรวจสอบไวรัสคอมพิวเตอร์ เป็นต้น และมีการออกแบบระบบเครือข่ายแบบแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็น

ระบบ โดยแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามลักษณะของการใช้งาน จัดทำระบบป้องกันการบุกรุกระหว่างเครือข่าย มีระบบตรวจสอบการบุกรุกและการใช้งานที่ผิดปกติผ่านระบบเครือข่าย จัดทำแผนผัง (Network Diagram) และขอบเขตของระบบเครือข่าย การเชื่อมต่อเครือข่ายต้องได้รับอนุมัติจากผู้บังคับบัญชา และตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนการเชื่อมต่อ มีผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ของระบบเครือข่ายและอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย และทบทวนการกำหนดค่า Parameter อย่างน้อยปีละ ๑ ครั้ง ให้มีการติดตั้ง Software ที่ถูกต้องตามลิขสิทธิ์และติดตั้งเท่าที่จำเป็นต่อการใช้งาน ติดตั้ง Software ป้องกันไวรัสและควบคุมไม่ให้ผู้ใช้งานระงับการใช้ Software ป้องกันไวรัสที่ติดตั้งไว้

๖.๔ การควบคุมการเข้าใช้งานจากภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ผู้ดูแลระบบจะต้องกำหนดให้มีการควบคุมการใช้งานจากภายนอก (Remote Access) โดยการกำหนดสิทธิ ควบคุมพอร์ต (Port) ที่ใช้เข้าสู่ระบบอย่างรัดกุม และมีการแสดงตัวตนของผู้ใช้งาน (Identification) และการพิสูจน์ยืนยันตัวตน (Authentication) เช่น การใช้รหัสผ่าน (Password) Smart Card การใช้ USB token หรือการใช้ Captcha เป็นต้น

๖.๕ การควบคุมสิทธิการเข้าถึงและใช้งานโปรแกรมประยุกต์ ระบบปฏิบัติการหรือแอพพลิเคชั่นและสารสนเทศ ต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร

๖.๖ ผู้ดูแลระบบต้องตรวจสอบ และทบทวนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๖.๗ การบริหารจัดการข้อมูล โดยมีการกำหนดประเภทของข้อมูลโดยแบ่งเป็นข้อมูลทั่วไป ข้อมูลที่ไม่เปิดเผย ข้อมูลส่วนบุคคล และข้อมูลลับ มีการกำหนดชั้นความลับและวิธีปฏิบัติการจัดเก็บข้อมูลแต่ละประเภท มีวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลและมีการกำหนดช่องทางและระยะเวลาในการเข้าถึงข้อมูล ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ มีการกำหนดมาตรการความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) ในกรณีจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องตรงกัน รวมทั้งกำหนดมาตรการรักษาความปลอดภัยของข้อมูลกรณีนำเครื่องคอมพิวเตอร์ออกไปนอกพื้นที่หวงห้าม

๖.๘ การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege) โดยกำหนดระดับชั้นของสิทธิที่จะให้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ ควบคุมการให้สิทธิแก่ผู้ใช้งานทั้งภายในและภายนอก โดยการให้สิทธิผู้ใช้งานภายในที่สามารถเข้าถึงเปลี่ยนแปลง แก้ไขเทคโนโลยีสารสนเทศต้องควบคุมอย่างเคร่งครัดและได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร ให้มีการตรวจสอบทบทวนอำนาจหน้าที่ของผู้ใช้งานภายในอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องยกเลิกหรือเปลี่ยนแปลงสิทธิให้สอดคล้องกับอำนาจหน้าที่ของผู้ใช้งานนั้นทันที กำหนดรหัสผ่านให้ยากแก่การ

คาดเดา กำหนดมาตรการให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ข้อกำหนดในการเก็บรักษารหัสผ่าน และห้ามผู้ไม่ใช่เจ้าของรหัสผ่านใช้รหัสผ่าน การป้องกันการใช้งานในกรณีไม่ได้ปฏิบัติงานหน้าเครื่องคอมพิวเตอร์ (Log out)

ข้อ ๗ นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้

การลงทะเบียนเจ้าหน้าที่ใหม่ของกรมกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปต้องดำเนินการภายใน ๒๔ ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน ๗ วัน

๗.๑ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๗.๒ ผู้ใช้ต้องลงนามรับทราบสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๗.๓ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

๗.๓.๑ ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กรมกำหนดไว้

๗.๓.๒ การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามแนวทางปฏิบัติตามที่กรมกำหนดไว้

๗.๓.๓ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ (Super User) หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

(๑) ควรได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้นๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ

(๒) ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

(๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

ข้อ ๘ การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ

กรมมีนโยบายที่จะรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ โดยมีระบบการควบคุมและเทคโนโลยีในการจัดเก็บและการเข้ารหัสลำหรับข้อมูลที่เป็นความลับ โดยใช้โครงสร้างพื้นฐานกุญแจสาธารณะและหน่วยงานบริการพื้นฐานต่างๆ และมีระบบเทคโนโลยีสารสนเทศเพื่อการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ ที่มีมาตรฐานในการรักษาความมั่นคงปลอดภัยเป็นที่ยอมรับ

ข้อ ๙ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๙.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศของกรม

๙.๒ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๙.๓ ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและควรกำหนดรหัสผ่านที่แตกต่างกัน

๙.๔ ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่ง และควรกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

๙.๕ ผู้ดูแลระบบจะต้องจัดให้มีระบบการกู้คืนหรือกำหนดค่า Password ใหม่โดยทำงานเชิงโต้ตอบหรืออัตโนมัติ

ข้อ ๑๐ นโยบายการบริหารจัดการระบบเครือข่าย

กรมมีโนบายในการบริหารจัดการระบบเครือข่าย (Network) โดยแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามลักษณะของการใช้งาน จัดทำระบบป้องกันการบุกรุกระหว่างเครือข่าย มีระบบตรวจสอบการบุกรุกและการใช้งานที่ผิดปกติผ่านระบบเครือข่าย จัดทำแผนผัง (Network Diagram) และขอบเขตของระบบเครือข่าย การเชื่อมต่อเครือข่ายต้องได้รับอนุมัติจากผู้บังคับบัญชา และตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนการเชื่อมต่อ มีผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ของระบบเครือข่ายและอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย และทบทวนการกำหนดค่า Parameter อย่างน้อยปีละ ๑ ครั้ง ให้มีการติดตั้ง Software ที่ถูกต้องตามลิขสิทธิ์ และติดตั้งเท่าที่จำเป็นต่อการใช้งาน ติดตั้ง Software ป้องกันไวรัสและควบคุมไม่ให้ผู้ใช้งานระงับการใช้ Software ป้องกันไวรัสที่ติดตั้งไว้ รวมทั้งต้องดำเนินการลงทะเบียนอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์บนเครือข่ายได้

ข้อ ๑๑ นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพา

๑๑.๑ กำหนดให้ใช้เครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน รวมทั้งโปรแกรมใช้งานต่างๆ ควรมีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามการติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับงานที่ปฏิบัติ

๑๑.๒ กำหนดให้ใช้ Username และ Password ก่อนใช้งานเครื่อง และผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งานหรือพักการใช้เครื่องชั่วคราว อีกทั้งผู้ใช้ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๑๑.๓ ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลและกู้คืนข้อมูลบนสื่อเก็บข้อมูลที่มีความเหมาะสม และต้องเก็บรักษาไว้ในที่ปลอดภัย

ข้อ ๑๒ นโยบายการบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๑๒.๑ ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๑๒.๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

๑๒.๓ ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ Telnet ftp หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการป้องกันเพิ่มเติมด้วย

๑๒.๔ ต้องดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

๑๒.๕ ต้องมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๑๒.๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยแจ้งเจ้าหน้าที่ผู้รับผิดชอบเท่านั้น

ข้อ ๑๓ นโยบายการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

๑๓.๑ ผู้ดูแลระบบจะต้องกำหนดให้เฉพาะผู้ที่มีสิทธิ (User Authentication) จึงจะสามารถเชื่อมต่อระบบเพื่อใช้งานอินเทอร์เน็ตหรือจดหมายอิเล็กทรอนิกส์ได้

๑๓.๒ มีระบบรักษาความปลอดภัยของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานเพื่อตรวจสอบการใช้งานและภัยคุกคาม

๑๓.๓ กำหนดแนวทางปฏิบัติการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ที่ถูกต้อง โดยไม่ละเมิดสิทธิหรือการกระทำใดๆ ที่สร้างปัญหาให้แก่ระบบหรือผู้ใช้อื่น

๑๓.๔ ในการติดต่อเรื่องที่เป็นงานราชการ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน หรือจดหมายอิเล็กทรอนิกส์กลาง เพื่อการสื่อสารในภาครัฐของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

๑๓.๕ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ต้องไม่เปิดเผยข้อมูลที่เป็นความลับของทางราชการและไม่สร้างความเสียหายต่อองค์กร

ข้อ ๑๔ นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ผู้ดูแลระบบจะต้องทำการลงทะเบียนกำหนดรหัสผ่านและสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย และลงทะเบียนอุปกรณ์ไร้สายทุกเครื่อง กำหนดตำแหน่งการวางอุปกรณ์ Access Point ให้เหมาะสมไม่มีสัญญาณรั่วไหลไปนอกบริเวณที่ใช้งาน

ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรม จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

ข้อ ๑๕ นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี

ผู้ดูแลระบบต้องตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่จะนำมาต่อกับระบบเครือข่ายคอมพิวเตอร์ของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส และผู้ใช้จะต้องตรวจสอบไวรัสคอมพิวเตอร์จากสื่อเก็บข้อมูลทุกชนิดก่อนนำมาใช้งานร่วมกับคอมพิวเตอร์

ข้อ ๑๖ นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ

๑๖.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อยืนยันตัวตนในการเข้าใช้งานระบบปฏิบัติการ

๑๖.๒ ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Log out ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver

๑๖.๓ ผู้ใช้มีหน้าที่รักษารหัสผ่าน (Password) อย่างเคร่งครัด โดยไม่เปิดเผยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้บุคคลอื่นทราบหรือนำไปใช้งาน

ข้อ ๑๗ นโยบายการสร้างความรู้ความเข้าใจในการใช้งานระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งาน

กรมมีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๑๘ นโยบายการจัดระบบเทคโนโลยีสารสนเทศ ระบบสำรองเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ รวมทั้งแผนใช้งานเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ในกรณีฉุกเฉิน

กรมมีนโยบายในการบริหารจัดการเทคโนโลยีสารสนเทศที่ได้มาตรฐาน โดยมีระบบการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีการจัดทำระบบสำรองเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์สำรอง เพื่อให้สามารถทำงานได้อย่างต่อเนื่อง และมีการทบทวนแผนเป็นประจำทุกปี

ข้อ ๑๙ นโยบายการตรวจสอบ การประเมินความเสี่ยง และมาตรการในการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กรมมีนโยบายให้มีการตรวจสอบ ประเมินความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปีตามเกณฑ์คุณภาพการบริหารจัดการภาครัฐ (PMQA) ของสำนักงาน กพร. ในส่วนของหมวด ๔ การวัด วิเคราะห์ และการจัดการความรู้ รหัส IT๖ กำหนดให้ส่วนราชการต้องมีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ และกำหนดมาตรการในการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง และมีการกำหนดความรับผิดชอบของผู้ใช้งานหรือผู้บริหาร ให้ผู้ใช้งานและผู้บริหารรับผิดชอบ ในกรณีเกิดความเสียหายหรืออันตรายอันเนื่องมาจากผู้ใช้งานหรือผู้บริหารบกพร่องหรือไม่ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศแล้วแต่กรณี

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานนี้ ได้กำหนดขึ้นเพื่อที่จะทำให้กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานมีมาตรการและแนวทางในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ซึ่งเจ้าหน้าที่ของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๒๐ สิงหาคม พ.ศ. ๒๕๕๖

(นายอำนวย ทองสถิตย์)
อธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน