# นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมทรัพยากรธรณี

**พ.ศ. ๒๕๕๘**

ศูนย์สารสนเทศทรัพยากรธรณี
กรมทรัพยากรธรณี

# คำนำ

พระราชกฤษฎีการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมทรัพยากรธรณีโดยศูนย์สารสนเทศทรัพยากรธรณี (ศสท.) ได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรธรณีเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ

ศูนย์สารสนเทศทรัพยากรธรณี กรมทรัพยากรธรณีจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน ,แนวปฏิบัติ ,ขั้นตอนปฏิบัติให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยได้จัดทำแนวปฏิบัติที่มีความสอดล้องกับแนวนโยบายดังกล่าวและแนวปฏิบัติต่างๆ เหล่านี้เป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติเพื่อให้เกิดความมั่นคงปลอดภัยในการปฏิบัติงานและให้บริการต่างๆ เพื่อสร้างความเชื่อมั่นให้กับประชาชนผู้รับบริการและสร้างความน่าเชื่อถือให้กับองค์กร

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจากทุกหน่วยงานและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว ศูนย์สารสนเทศทรัพยากรธรณีจึงหวังเป็นอย่างยิ่งว่า แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ ผู้ดูแลเครือข่าย และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรธรณีทุกคน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานต่อไป

ศูนย์สารสนเทศทรัพยากรธรณี

# สารบัญ

# ประกาศกรมทรัพยากรธรณี
# เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
# พ.ศ. ๒๕๕๘

---

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ กรมทรัพยากรธรณี จึงกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนการปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการป้องกันภัยคุกคามต่างๆ ตามประกาศดังต่อไปนี้

**ข้อ ๑** ในประกาศนี้ เรียกว่า “ประกาศกรมทรัพยากรธรณี เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมทรัพยากรธรณี พ.ศ. ๒๕๕๘”

**ข้อ ๒** วัตถุประสงค์

๒.๑ กำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และผู้ดูแลเครือข่าย ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินและปฏิบัติอย่างเคร่งครัด

๒.๒ เพื่อให้เกิดความเชื่อมั่น และความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศรวมทั้งเครือข่ายคอมพิวเตอร์ของกรมทรัพยากรธรณี ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๓ เพื่อเผยแพร่ให้ผู้ใช้งาน (เจ้าหน้าที่ทุกระดับ) ในกรมทรัพยากรธรณี ได้รับทราบ และถือปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

**ข้อ ๓** แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรธรณี สามารถแบ่งออกได้ดังนี้

๓.๑ คำนิยาม

๓.๒ แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

๓.๓ แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึง

๓.๔ แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๓.๕ แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

๓.๖ แนวปฏิบัติและหน้าที่ของผู้ดูแลเครือข่าย/ผู้ดูแลระบบ

---

๓.๗ แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

๓.๘ แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๙ แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

๓.๑๐ แนวปฏิบัติในการจัดซื้อจัดจ้างระบบสารสนเทศ

๓.๑๑ แนวปฏิบัติในการแนวการคุ้มครองข้อมูลส่วนบุคคลและการเผยแพร่ข้อมูลสาธารณะ

๓.๑๒ แนวนโยบายการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยมั่นคงด้านสารสนเทศ

๓.๑๓ ภาคผนวก ก. ขั้นตอนการลงทะเบียนผู้ใช้งานกรมทรัพยากรธรณี

๓.๑๔ ภาคผนวก ข. โปรแกรมมาตรฐานในการใช้งานของกรมทรัพยากรธรณี

**ข้อ ๔** การกำหนดผู้รับผิดชอบ

๔.๑ ระดับนโยบาย

๔.๑.๑ กำหนดให้ผู้บริหารระดับสูงสุด CEO (Chief Executive Officer) ของกรมทรัพยากรธรณี เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ

๔.๑.๒ กำหนดให้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง CIO (Chief Information Officer) ของกรมทรัพยากรธรณี เป็นผู้รับผิดชอบในการสั่งการตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรธรณี

๔.๑.๓ กำหนดให้ ผู้อำนวยการศูนย์สารสนเทศทรัพยากรธรณีเป็นรับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษาแก่เจ้าหน้าที่ระดับปฏิบัติ

๔.๒ ระดับปฏิบัติ

เพื่อให้แนวปฏิบัติต่างๆ ของแนวนโยบายและแนวความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรธรณีเป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้มีผู้ปฏิบัติเป็นไปตามแนวปฏิบัติต่างๆ ตามข้อ ๓.๒ ถึง ๓.๑๒ ,แผนแก้ไขปัญหาจากความไม่แน่นอน และภัยพิบัติอันเกิดกับระบบฐานข้อมูลและสารสนเทศ พร้อมทั้งกำหนดให้มีการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นหน้าที่ความรับผิดชอบของ ส่วนประสานและสนับสนุนทางวิชาการ ศูนย์สารสนเทศทรัพยากรธรณี ,ผู้ดูและระบบ ,เจ้าหน้าที่ที่ได้รับมอบหมาย

**ข้อ ๕** ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบ การอนุญาตการเข้าถึงและควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ และแผนการแก้ไขปัญหาจากความไม่แน่นอนและภัยพิบัติอาจเกิดขึ้นกับระบบฐานข้อมูลของกรมอย่างน้อยปีละ ๑ ครั้ง โดยผู้ตรวจสอบภายในหน่วยงานเจ้าของระบบงาน และผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) และให้นำผลการตรวจประเมินมาปรับปรุงให้สอดคล้องกับนโยบาย

**ข้อ ๖** สร้างความรู้ความเข้าใจให้กับผู้ใช้งานของกรมทรัพยากรธรณี เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการ

๖.๑ เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์กรมฯ ให้แก่ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

๖.๒ จัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

**ข้อ ๗** รายละเอียดและองค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรธรณี โดยอ้างอิงจากรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรธรณี พ.ศ. ๒๕๕๘ เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยเชื่อถือได้เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้องซึ่งเจ้าหน้าที่ของกรมทรัพยากรธรณีและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๖ พฤศจิกายน พ.ศ. ๒๕๕๘

(นายสุพจน์ เจิมสวัสดิพงษ์)
อธิบดีกรมทรัพยากรธรณี

## คำนิยาม

**"กรม"** หมายถึง กรมทรัพยากรธรณี

**"ศูนย์สารสนเทศทรัพยากรธรณี"** หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร พัฒนา ปรับปรุง บำรุงรักษา ระบบสารสนเทศ ระบบคอมพิวเตอร์ และเครือข่ายภายในองค์กร รวมทั้งให้บริการแผนที่ ห้องสมุดและองค์ความรู้ด้านธรณีวิทยาและทรัพยากรธรณี

**"การรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ" (Information security)** หมายถึง การศึกษาถึงความไม่ปลอดภัยในการใช้งานสารสนเทศที่เกี่ยวข้องกับคอมพิวเตอร์ การวางแผนและการจัดระบบความปลอดภัยในคอมพิวเตอร์

**"ระบบงาน"** หมายถึง ระบบที่กรมฯ ใช้งานเพื่อบริหารจัดการกิจการภายในของกรมฯ

**"ระบบคอมพิวเตอร์"** หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่มีการเชื่อมต่อการทำงานเข้าด้วยกัน โดยมีการกำหนดชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

**"ข้อมูลคอมพิวเตอร์"** หมายถึง ข้อมูลข้อความคำสั่งชุดคำสั่งหรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

**"คอมพิวเตอร์โน้ตบุค"** หมายถึง เครื่องคอมพิวเตอร์ส่วนบุคคลที่ออกแบบให้สามารถพกพาไปใช้ในสถานที่ต่างๆ ได้โดยสะดวกซึ่งมีความหมายตรงกับคำภาษาอังกฤษว่า Notebook

**"คอมพิวเตอร์ส่วนตัว"** หมายถึง คอมพิวเตอร์ที่ไม่ใช่ทรัพย์สินของกรมทรัพยากรธรณีซึ่งเจ้าหน้าที่นำมาใช้ภายในกรมฯ

**"อุปกรณ์คอมพิวเตอร์"** หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อหรือทำงานเป็นส่วนหนึ่งของระบบคอมพิวเตอร์โดยอาจใช้ทำหน้าที่เป็นอุปกรณ์สื่อสารหรือใช้บันทึกข้อมูลเป็นต้น

**"เครือข่าย"** หมายถึง ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ตั้งแต่ ๒ เครื่องขึ้นไปเข้าด้วยกันเพื่อสะดวกต่อการร่วมใช้ข้อมูลโปรแกรมหรือเครื่องพิมพ์และอำนวยความสะดวกในการติดต่อแลกเปลี่ยนข้อมูลระหว่างเครื่องได้ตลอดเวลา

**"สื่อลามกอนาจาร"** หมายถึง สื่อประเภทอันเป็นที่น่ารังเกียจน่าอับอายนอกรีตนอกแบบผิดปกติไปจากศีลธรรมอันดีของประชาชน

**"ลิขสิทธิ์"** หมายถึง สิทธิที่ได้รับแต่เพียงผู้เดียวตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น

**"ระบบอินเตอร์เน็ต"** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของกรมฯ เข้ากับเครือข่ายอินเตอร์เน็ตสากล

**"จดหมายอิเล็กทรอนิกส์ (e-mail)"** หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับผ่านโปรโตคอลต่างๆ เช่น SMTP, POP3, IMAP ฯลฯ

**"จดหมายอิเล็กทรอนิกส์แบบขยะ"** หมายถึง จดหมายอิเล็กทรอนิกส์ที่ไม่เป็นประโยชน์หรือไม่เป็นที่ต้องการของผู้รับโดยที่ผู้ส่งปกปิดตัวตนที่แท้จริงหรืออาศัยเครื่องรับของผู้รับเป็นช่องทางในการกระจายจดหมายอิเล็กทรอนิกส์นั้นต่อไป

**"ผู้ใช้งาน"** หมายถึง ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบของกรมทรัพยากรธรณีผู้บริหารองค์กรผู้รับบริการผู้รับจ้างทำของและผู้ใช้งานที่ใช้บริการระบบเทคโนโลยีสารสนเทศของกรมฯ

**"สิทธิของผู้ใช้งาน"** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

**"สินทรัพย์"** หมายถึง ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับกรมฯ

**"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ"** หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตสาหรับบุคคลภายนอก ตลอดจนการกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

**"ความมั่นคงปลอดภัยด้านสารสนเทศ"** หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

**"เหตุการณ์ด้านความมั่นคงปลอดภัย"** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่ให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

**"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด"** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยคุกคาม

**"จดหมายอิเล็กทรอนิกส์แบบลูกโซ่"** หมายถึง จดหมายอิเล็กทรอนิกส์ที่มีข้อความในลักษณะที่ต้องการให้ผู้รับส่งต่อไปเรื่อยๆแบบไม่รู้จบโดยมีวิวัฒนาการมาจากจดหมายกระดาษลูกโซ่ที่ระบุข้อความท้ายจดหมายว่าถ้าผู้รับไม่ส่งต่อจะประสบเคราะห์ร้ายถ้าส่งต่อจะพบแต่สิ่งที่ดี

**"โปรแกรมมาตรฐาน"** หมายถึง โปรแกรมที่กรมทรัพยากรธรณีกำหนดให้เป็นโปรแกรมมาตรฐานสำหรับให้เจ้าหน้าที่ใช้งานได้ตามปกติ

**"หน่วยงาน"** หมายถึง สำนัก/ศูนย์/สำนักงานทรัพยากรธรณีเขต/กลุ่มงานขึ้นตรงหรือที่เรียกชื่อเป็นอย่างอื่นในสังกัดกรมทรัพยากรธรณี

**"หน่วยงานภายนอก"** หมายถึง องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึง และการใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของกรมทรัพยากรธรณี โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

**"เหตุฉุกเฉิน"** หมายถึง เหตุที่ก่อให้เกิดเป็นปัญหาการทำงานของระบบและนำมาซึ่งการหยุดชะงักของระบบ เช่น ไฟไหม้ การถูกปิดล้อม ไฟฟ้าดับ การก่อวินาศกรรม เป็นต้น

**"ผู้บริหารระดับสูงสุด"** CEO (Chief Executive Officer) หมายถึง อธิบดีกรมทรัพยากรธรณีเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ

**"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง** CIO (Chief Executive Officer)" หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกรมทรัพยากรธรณี (รองอธิบดี) เป็นผู้รับผิดชอบในการสั่งการตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรธรณี

**"ผู้อำนวยการศูนย์สารสนเทศทรัพยากรธรณี"** หมายถึง ผู้ที่มีอำนาจในด้านเทคโนโลยีสารสนเทศ ซึ่งมีบทบาทหน้าที่ความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

**"ชื่อผู้ใช้งาน (username)"** หมายถึง ชุดของตัวอักษร หรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์ และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

**"รหัสผ่าน (password)"** หมายถึง กลุ่มข้อความที่ประกอบด้วยตัวอักษรตัวเลขหรือเครื่องหมายที่ผู้ใช้งานระบบเทคโนโลยีสารสนเทศกำหนดขึ้นเพื่อใช้ในการระบุตัวตนและสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศซึ่งมีความหมายตรงกับคำภาษาอังกฤษว่า Password

**"บัญชีผู้ใช้งาน"** หมายถึง บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมฯ

**"ผู้ดูแลระบบสารสนเทศ"** หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่ดูแลระบบงานของกรมทรัพยากรธรณีในภาพรวม กำหนดแนวทางในการปฏิบัติงานให้มีประสิทธิภาพ

**"ผู้ดูแลเครือข่าย"** หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลเครือข่ายสารสนเทศของกรมทรัพยากรธรณี และมีหน้าที่ดูแลบำรุงรักษาระบบเครือข่าย ระบบสารสนเทศของกรมทรัพยากรธรณี หรืออาจได้รับมอบหมายให้เป็น ผู้ดูแลระบบ แทนหน่วยงานผู้เป็นเจ้าของระบบสารสนเทศ

**"ผู้ดูแลระบบ"** หมายถึง ผู้ที่ได้รับมอบหมายให้บริหารจัดการบัญชีรายชื่อผู้มีสิทธิในการเข้าถึงระบบงาน เช่น การให้สิทธิ การเพิ่มสิทธิ การลดสิทธิ การยกเลิกสิทธิ รวมทั้งการพัฒนา ปรับปรุงดูแลบำรุงรักษาระบบงาน

**"ผู้บังคับบัญชา"** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการแบ่งส่วนราชการ

**"การพิสูจน์ยืนยันตัวตน (Authentication)"** หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปและจะเป็นการพิสูจน์ โดยใช้ชื่อผู้ใช้งาน และรหัสผ่าน

**"MAC Address (media access control address)"** หมายถึง หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ติดต่อกับระบบเครือข่าย หมายเลขนี้จะมากับการ์ดแลน โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๕ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

**"VPN (virtual private network)"** หมายถึง เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเตอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

**"สื่อบันทึกพกพา (portable media)"** หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD, DVD, fash dive, external hard disk ฯลฯ

**"สินทรัพย์คอมพิวเตอร์"** หมายถึง โปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย

**"แผนผังระบบเครือข่าย (network diagram)"** หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของกรมทรัพยากรธรณี

## *ส่วนที่ ๑.*

### แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

ข้อ ๑. ผู้ดูแลเครือข่าย/ผู้ดูแลระบบของหน่วยงานภายในกรมทรัพยากรธรณี ต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงาน ดังนี้

(๑) ผู้ดูแลระบบ ต้องจัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(๒) ผู้ดูแลระบบ ต้องกำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

๒.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

๒.๒ กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่กำหนดไว้

(๓) ผู้ดูแลระบบกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๔) ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบกล่าวคือ ในการขออนุญาตเข้าระบบงานนั้นผู้ใช้จะต้องทำเป็นบันทึก และกรอกแบบเอกสารที่กรมฯ กำหนดเพื่อขออนุญาตเข้าสู่ระบบ และต้องลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐานจากนั้นผู้ดูแลระบบจะสร้างบัญชีสำหรับการเข้าถึงโดยอนุญาตเฉพาะในส่วนที่จำเป็นและโดยคำนึงถึงประเภทข้อมูลและชั้นความลับ

(๕) การเข้าถึงระบบสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมาย เพื่อดำเนินการใดๆ จะต้องได้รับสิทธิ และได้รับอนุญาตในการเข้าดำเนินการ หลังจากเสร็จสิ้นแล้วผู้ดูแลระบบจะต้องยกเลิกสิทธิให้กับหน่วยงานนั้นๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใดๆ ที่มีผลกระทบต่อระบบจะต้องเป็นผู้รับผิดชอบ

(๖) ผู้ดูแลระบบงานต้องกำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้หากผู้ใช้งานใส่รหัสผ่านเข้าระบบผิด ๓ ครั้ง จนกว่าจะยื่นเรื่องพร้อมหลักฐานแสดงความเป็นตัวตนต่อเจ้าหน้าที่ดูแลระบบเพื่อขอรหัสใหม่อีกครั้ง

ข้อ ๒. ผู้ดูแลเครือข่ายของหน่วยงานภายในกรมทรัพยากรธรณี ต้องจัดการรักษาความปลอดภัยทางกายภาพ (Physical security management) ดังนี้

(๑) กำหนดระดับความสำคัญของพื้นที่ หรือจำแนกพื้นที่ที่ใช้งานกับพื้นที่ที่มีการควบคุม

(๒) ดำเนินการควบคุมการเข้าถึงพื้นที่ทางกายภาพ

(๓) ผู้ปฏิบัติงานควรปิดประตูและหน้าต่างให้ล็อคอยู่เสมอ

ข้อ ๓. ผู้ดูแลเครือข่ายของหน่วยงานภายในกรมทรัพยากรธรณี ต้องจัดการควบคุมการเข้า - ออกพื้นที่ควบคุม เช่น ห้องแม่ข่าย ดังนี้

(๑) ต้องบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาเยือน (visitors)

(๒) ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญสำหรับจนกระทั่งเสร็จสิ้นภารกิจ และจากไปเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๓) จัดให้มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของกรมทรัพยากรธรณี โดยบุคคลภายนอกและควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๔) จัดอบรมประชาสัมพันธ์เพื่อสร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๕) ต้องควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๖) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๗) จัดเก็บบันทึกการเข้า – ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญโดยเฉพาะห้องแม่ข่าย Server Farm) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๘) บุคคลภายนอก เช่นเจ้าหน้าที่บริษัท, นักศึกษาฝึกงานหรือผู้ได้รับการว่าจ้างอื่นๆ ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

(๙) ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

(๑๐) ต้องดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๑) ต้องทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

ข้อ ๔. ผู้ดูแลเครือข่ายต้องกำหนดการจัดวางและการป้องกันฮาร์ดแวร์และอุปกรณ์ต่างๆ ดังนี้

(๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงของบุคคลภายนอก

(๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

(๓) ห้ามนำอาหารเครื่องดื่มและสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในศูนย์คอมพิวเตอร์ (data center) ของกรมทรัพยากรธรณี

(๔) ดำเนินการตรวจสอบสอดส่องและดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว

ข้อ ๕. ผู้ดูแลเครือข่ายของหน่วยงานภายในกรมทรัพยากรธรณี ต้องกำหนดระบบและอุปกรณ์สนับสนุนการทำงาน ดังนี้

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบ ดังต่อไปนี้

(๑.๑) ระบบสำรองกระแสไฟฟ้า (UPS)

(๑.๒) ระบบปรับอากาศ

(๒) ต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

ข้อ ๖. ผู้ดูแลเครือข่ายต้องกำหนดและควบคุมการเดินสายไฟสายสื่อสารและสายเคเบิ้ลอื่นๆ ดังนี้

(๑) เครือข่ายของกรมทรัพยากรธรณี ในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้นั้น ต้องให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหายและป้องกันสัตว์ต่างๆ กัดสาย

(๒) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๓) จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๔) ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิทเพื่อป้องกันการเข้าถึงของบุคคลภายนอก

ข้อ ๗. ผู้ดูแลเครือข่ายของหน่วยงานภายในกรมฯ ต้องกำหนดการบำรุงรักษาอุปกรณ์ ดังนี้

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๗) ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๗) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องควบคุมการนำอุปกรณ์คอมพิวเตอร์ของกรมฯ ออกนอกหน่วยงาน ดังนี้

(๑) ต้องขออนุญาตก่อนนำสิ่งอุปกรณ์หรือทรัพย์สินออกนอกหน่วยงาน

(๒) บันทึกข้อมูลการนำสิ่งอุปกรณ์ของกรมฯ ออกนอกหน่วยเพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องจัดการป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน

(๑) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๕ นาที

(๒) ห้ามผู้ใช้งานละทิ้งอุปกรณ์คอมพิวเตอร์ของกรมฯ ไว้โดยลำพังในที่สาธารณะ

(๓) ให้ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์คอมพิวเตอร์ของกรมฯ เสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องควบคุมการจำหน่ายอุปกรณ์คอมพิวเตอร์หรือการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

(๑) ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะแทงจำหน่ายอุปกรณ์ดังกล่าว (ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลในส่วนที่ ๓ แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ข้อ ๑ (๔)

## *ส่วนที่ ๒.*
## แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึง

ข้อ ๑. ผู้ดูแลเครือข่าย ผู้ดูแลระบบของหน่วยงานภายในกรมทรัพยากรธรณี ต้องบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน ดังนี้

(๑) ข้าราชการ เจ้าหน้าที่ ลูกจ้าง พนักงานราชการ รวมทั้งผู้ดูแลเครือข่าย ผู้ดูแลระบบเองต้องปฏิบัติตามขั้นตอนการลงทะเบียนที่กรมทรัพยากรธรณีกำหนดขึ้น เพื่อให้มีสิทธิในการใช้งานระบบสารสนเทศตามความจำเป็นรวมทั้งปฏิบัติตามขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในกรมทรัพยากรธรณี เป็นต้น

(๒) กำหนดสิทธิการใช้ระบบงานภายในที่สำคัญต่างๆ ของกรมทรัพยากรธรณี โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๓) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุดต้องพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณาเพื่อขอความเห็นชอบและอนุมัติจากผู้บังคับบัญชา

(๓.๑) ควบคุมการใช้งานอย่างเข้มงวด

(๓.๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓.๓) เปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือนเป็นต้น

ข้อ ๒. ผู้ดูแลเครือข่าย ผู้ดูแลระบบของหน่วยงานภายในกรมทรัพยากรธรณี ต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (user account) และรหัสผ่านของเจ้าหน้าที่ ดังนี้

(๑) กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคลกล่าวคือไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน

(๒) ไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้นและต้องสอดคล้องกับนโยบายควบคุมการเข้าถึงข้อมูล

(๓) จัดเก็บข้อมูลการลงทะเบียนของผู้ที่ร้องขอใช้ระบบไว้เพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบในภายหลัง

(๔) ทบทวนบัญชีผู้ใช้งานทั้งหมด อย่างสม่ำเสมอ โดยเฉพาะการทบทวนสิทธิสำหรับผู้มีสิทธิระดับสูงอย่างน้อยปีละ ๑ ครั้งเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตโดยปฏิบัติตามแนวทาง ดังนี้

(๔.๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงานภายในของกรมฯ

(๔.๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานภายในนั้นเพื่อดำเนินการทบทวนว่ามีรายชื่อที่ออกไปแล้ว หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

(๔.๓) ผู้บังคับบัญชาของหน่วยงานภายในแจ้งกลับว่ามีรายชื่อใดที่ต้องดำเนินการแก้ไขให้ถูกต้อง

(๔.๔) ดำเนินการแก้ไขข้อมูลสิทธิให้ถูกต้องตามที่ได้รับแจ้ง

ข้อ ๓. ผู้ดูแลเครือข่าย ผู้ดูแลระบบของหน่วยงานภายในกรมทรัพยากรธรณี ต้องจัดให้มีการพิสูจน์ตัวตนเพื่อเข้าใช้ระบบงานสำคัญสำหรับผู้ใช้ที่อยู่ภายนอก ดังนี้

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบของกรมทรัพยากรธรณี ต้องผ่านการพิสูจน์ตัวตนจากระบบของกรมทรัพยากรธรณี โดยมีแนวทางปฏิบัติดังนี้

(๑) การแสดงตัวตนด้วยชื่อบัญชีผู้ใช้งาน

(๒) การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน

(๓) การเข้าสู่ระบบงานสำคัญของกรมทรัพยากรธรณี ผ่านเครือข่ายอินเทอร์เน็ตนั้นจะมีการตรวจสอบผู้ใช้งาน

ข้อ ๔. ผู้ดูแลเครือข่าย ผู้ดูแลระบบของหน่วยงานภายในกรมทรัพยากรธรณี ต้องกำหนดวิธีการบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัยตามแนวทางปฏิบัติ ดังนี้

(๑) ผู้ดูแลระบบจะให้สิทธิเฉพาะผู้ที่มีสิทธิการใช้งานเท่านั้น และการให้สิทธิการใช้งานตามสิทธิของผู้ใช้งาน

(๒) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษรโดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติตัวเลขและใช้เทคนิคส่วนตัวที่ง่ายต่อการจำ หรือสัญลักษณ์ต่างๆ เข้าด้วยกันพร้อมทั้งยากต่อการเดา

(๓) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๔) ไม่อนุญาตให้เจ้าหน้าที่ ใช้รหัสผ่านร่วมกัน

(๕) กำหนดรหัสผ่านเริ่มต้นให้กับเจ้าหน้าที่ให้ยากต่อการเดา เมื่อผู้ใช้งานได้รับรหัสผ่านครั้งแรกหรือได้รับรหัสผ่านใหม่ต้องทำการเปลี่ยนแปลงรหัสผ่านนั้นโดยทันที

(๖) ผู้ดูแลระบบต้องเปลี่ยนรหัสถี่กว่าผู้ใช้งานทั่วไป และกำหนดให้เปลี่ยนรหัสตามรอบระยะเวลาและหลีกเลี่ยงการใช้รหัสผ่านเดิม

(๗) หลีกเลี่ยงการใช้ E-mail ในการจัดส่งรหัสผ่าน

(๘) เมื่อเจ้าหน้าที่ของหน่วยงานลาออกหรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งานให้หน่วยงานแจ้งผู้รับผิดชอบระบบสารสนเทศทันทีเพื่อเปลี่ยนสิทธิหรือถอดถอนสิทธิของผู้ที่ลาออก ออกจากระบบทันทีที่ได้รับแจ้ง

(๙) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๑๐) การส่งมอบรหัสผ่านสำหรับการเริ่มต้นใช้งานให้กับเจ้าหน้าที่ต้องเป็นไปอย่างปลอดภัยโดยการส่งมอบแบบลับ รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติเก็บรักษารหัสผ่านเป็นความลับพร้อมทั้งลงนามรับทราบด้วย เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน และผู้ใช้งานต้องปลี่ยนรหัสผ่านทันทีหลังจากได้รับเอกสาร

ข้อ ๕. ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนด และการใช้งานรหัสผ่าน

(๑) ผู้ใช้งานต้องเก็บรักษารหัสผ่านที่ได้รับให้เป็นความลับ และเก็บรหัสผ่านในสถานที่ปลอดภัย

(๒) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากอักขระที่เรียงกัน กลุ่มคำที่เหมือนกัน หรือชื่อนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตนหรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๓) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password)

(๔) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๕) กำหนดรหัสผ่านเริ่มต้นให้กับเจ้าหน้าที่ให้ยากต่อการเดา เมื่อผู้ใช้งานได้รับรหัสผ่านครั้งแรก หรือได้รับรหัสผ่านใหม่ต้องทำการเปลี่ยนแปลงรหัสผ่านนั้นโดยทันที

(๕) ผู้ใช้งานต้องเปลี่ยนรหัสทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๖) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น หากมีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงานหลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

## *ส่วนที่ ๓.*
## แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ข้อ ๑. ผู้บังคับบัญชาหน่วยงานภายในกรมทรัพยากรธรณี ต้องจัดให้มีวิธีการจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับซึ่งเบื้องต้นกรมฯ ใช้แนวทางตาม พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบที่เกี่ยวข้องในการกำหนดชั้นความลับของข้อมูลจึงกำหนดให้มีแนวทางปฏิบัติ ดังนี้

(๑) ผู้ใช้งานต้องจัดการกับข้อมูลตามชั้นความลับของข้อมูลกรมทรัพยากรธรณีได้กำหนดชั้นความลับของข้อมูลเป็น ๓ ระดับ ดังนี้

- ลับที่สุด (Top secret) หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งภาครัฐร้ายแรงที่สุด
- ลับมาก (Secret) หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง
- ลับ (Confidential) หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

(๒) ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติ ดังนี้

- ระมัดระวังการกระจาย หรือแจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับของกรมทรัพยากรธรณีไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น
- ผู้ที่เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ต้องตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน
- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย เมื่อมีการนำไฟล์ข้อมูลลับไปใช้งานต้องมีการเข้ารหัส โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ ๒๕๕๔
- ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายของกรมฯเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตามเนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)
- ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่
- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่
- ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น
- ต้องทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

(๓) ประเภทข้อมูล

- ข้อมูลสารสนเทศเพื่อการบริหาร หมายถึง นโยบาย ,ข้อมูลยุทธศาสตร์ , คำรับรองการปฏิบัติราชการ, ข้อมูลบุคลากร, งบประมาณ, การเงินและบัญชี
- ข้อมูลด้านการดำเนินงาน หมายถึง การดำเนินงานตามภารกิจกรมทรัพยากรธรณี, กฎหมาย ระเบียบ, การใช้จ่ายงบประมาณ, ผลการปฏิบัติงาน
- ข้อมูลสารสนเทศเพื่อการบริการ หมายถึง ข้อมูลวิชาการและองค์ความรู้

(๔) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๕) จัดแบ่งระดับชั้นการเข้าถึง

- เข้าถึงได้ทุกกลุ่มผู้ใช้งานที่กำหนดไว้ หมายถึง ข้อมูลพื้นฐานที่ผู้ใช้งานได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงาน ในการใช้งานระบบ
- เข้าถึงได้เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิ หมายถึง ข้อมูลที่ผู้ใช้งานได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตาม ความจำเป็นต่อการใช้งานระบบสารสนเทศ
- เข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ หมายถึง ผู้ดูแลระบบสารสนเทศ

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

(๗) การกำหนดเวลาที่ได้เข้าถึงสารสนเทศของกรมทรัพยากรธรณี ให้ดำเนินการดังนี้

๗.๑ ระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงสูง มีกำหนดระยะเวลาในการเข้าถึงสารสนเทศในวันเวลาราชการ (๘.๓๐- ๑๖.๓๐ น.) เท่านั้น เว้นแต่ได้ขออนุญาต

๗.๒ ระบบสารสนเทศทั่วไป ต้องกำหนดระยะเวลา ในการเข้าถึงระบบสารสนเทศได้ตลอด ๒๔ ช.ม. ไม่เว้นวันหยุดราชการ หรือวันหยุดนักขัตฤกษ์

(๘) การกำหนดจำนวนช่องทางในการเข้าถึงระบบสารสนเทศของกรมทรัพยากรธรณี ต้องกำหนดให้เข้าถึงได้ทั้งภายใน และภายนอก โดยเชื่อมต่อผ่าน WiFi ,Lan ,Internet และมีต้องติดต่อด้วยตนเอง ,โทรศัพท์หรือโทรสาร ,หนังสือหรือบันทึกข้อความ ,จดหมายอิเล็กทรอนิกส์ (E-mail)

(๙) ในการทำลายข้อมูลลับให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ ประเภทสื่อบันทึกข้อมูลและวิธีการทำลายมีดังนี้

- Flash Drive ใช้วิธีการทุบหรือบดให้เสียหาย
- กระดาษใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
- แผ่น CD/DVD ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
- เทปใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
- ฮาร์ดดิสก์ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

## *ส่วนที่ ๔.*
## แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

ข้อ ๑. การใช้คอมพิวเตอร์ของกรมทรัพยากรธรณี ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

(๑) ผู้ใช้รายใหม่ ห้ามใช้คอมพิวเตอร์จนกว่าจะได้รับการอนุมัติให้ใช้ได้โดยผ่านการลงทะเบียนตามแบบท้ายประกาศนี้ *(DMR_01)* และต้องสแกนไวรัสก่อนการใช้งานทุกครั้ง

(๒) ต้องตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติ และต้องปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ หากพบว่าโปรแกรมดังกล่าวทำงานผิดปกติให้รีบแจ้งศูนย์สารสนเทศทรัพยากรธรณีเพื่อดำเนินการแก้ไขโดยเร็ว

(๒) คอมพิวเตอร์ที่ใช้ในกรมทรัพยากรธรณี ให้ติดตั้งโปรแกรมมาตรฐานตามที่กำหนดไว้ท้ายระเบียบนี้ การเปลี่ยนแปลงหรือติดตั้งโปรแกรมเพิ่มเติมต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานภายใน หรือผู้ที่ได้รับมอบหมาย การเปลี่ยนแปลงหรือการติดตั้งโปรแกรมเพิ่มเติม เพื่อทดลองการใช้งานจะดำเนินการโดยศูนย์สารสนเทศทรัพยากรธรณี หรือผู้ที่ได้รับการว่าจ้างให้มาจัดทำหรือดูแลระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรธรณี

(๓) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์เพื่อให้บุคคลภายนอกสามารถใช้งานเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของกรมทรัพยากรธรณีได้

(๕) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกจากโปรแกรมมาตรฐานที่กำหนดไว้ท้ายประกาศนี้

(๖) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

(๗) ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟท์แวร์ที่มีลิขสิทธิถูกต้องของกรมทรัพยากรธรณี

(๘) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย

(๙) ต้องระมัดระวังการใช้งานและดูแลคอมพิวเตอร์รวมทั้งระบบเครือข่ายตามที่วิญญูชนทั่วไปจะพึงปฏิบัติ

(๑๐) เอกสาร หรือข้อมูลต่างๆ ไม่ว่าจะอยู่ในรูปแบบใดก็ตามที่ได้มีการกำหนดเงื่อนไขการใช้งานไว้ ต้องใช้งานด้วยความระมัดระวังและต้องปฏิบัติตามเงื่อนไขอย่างเคร่งครัดเพื่อป้องกันมิให้เกิดการละเมิดตามกฎหมาย

(๑๑) ต้องลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากคอมพิวเตอร์เพื่อประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

(๑๒) ต้องออกจากระบบ (Log off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์รวมทั้งปิดคอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

(๑๓) การขอยืมเครื่องคอมพิวเตอร์/อุปกรณ์ต่อพ่วง และอุปกรณ์อื่นๆ ของศูนย์สารสนเทศทรัพยากรธรณีต้องได้รับอนุญาตจากผู้มีอำนาจโดยผ่านการลงทะเบียนตามแบบท้ายประกาศนี้ *(DMR_02)*

(๑๔) การนำคอมพิวเตอร์ส่วนตัวมาใช้กับระบบเครือข่ายของกรมทรัพยกรธรณี ต้องได้รับการตรวจสอบ และอนุญาตจากศูนย์สารสนเทศทรัพยากรธรณีโดยผ่านการลงทะเบียนตามแบบท้ายประกาศนี้ *(DMR_03)* และต้องสแกนไวรัสก่อนการใช้งานทุกครั้ง

ข้อ ๒. การยืมใช้คอมพิวเตอร์แบบพกพาของกรมทรัพยากรธรณี นอกจากต้องปฏิบัติตามที่กำหนดไว้ในข้างต้นแล้วให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

(๑) ต้องตรวจสอบคอมพิวเตอร์แบบพกพาที่นำไปใช้ว่าได้ติดตั้งโปรแกรมมาตรฐานที่กำหนดไว้ท้ายระเบียบนี้แล้วหรือไม่หากพบว่ายังไม่ได้ติดตั้งให้แจ้งศูนย์สารสนเทศทรัพยากรธรณีเพื่อขอรับการติดตั้งก่อนการใช้งาน

(๒) ต้องระมัดระวังไม่ให้บุคคลภายนอกมองเห็นหรือคัดลอกข้อมูลจากคอมพิวเตอร์แบบพกพาที่นำไปใช้เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้คอมพิวเตอร์แบบพกพาแล้วให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบของหน่วยงานทันที ทั้งนี้ให้เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนตรวจสอบสภาพความพร้อมในการใช้งานของคอมพิวเตอร์ที่รับคืนไว้ดังกล่าวด้วย

ข้อ ๓. ในกรณีที่เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนคอมพิวเตอร์แบบพกพาตรวจพบความเสียหายให้แจ้งผู้ส่งคืนผู้บังคับบัญชาและศูนย์สารสนเทศทรัพยากรธรณีทราบ โดยเร็วและหากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทเลินเล่ออย่างร้ายแรงของผู้นำไปใช้ต้องให้ผู้นำไปใช้รับผิดชอบต่อความเสียหายที่เกิดขึ้นดังกล่าว

ข้อ ๔. การเข้าถึงระบบงานเจ้าหน้าที่ใช้งานต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

(๑) กรอกแบบฟอร์มเพื่อขออนุมัติใช้งานระบบงาน และนำเสนอต่อผู้บังคับบัญชาเพื่อขออนุมัติโดยผ่านการลงทะเบียนตามแบบท้ายประกาศนี้ *(DMR_03)*

(๒) ต้องไม่เข้าถึงระบบงานอื่นที่ตนไม่ได้รับอนุมัติให้ใช้งาน

(๓) ต้องออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

ข้อ ๕. การใช้งานอินเตอร์เน็ตผู้ใช้งานต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

(๑) ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

(ก) การพนัน

(ข) การประมูล

(ค) วิพากษ์วิจารณ์ที่เกี่ยวข้องกับชาติศาสนาและพระมหากษัตริย์

(ง) ลามกอนาจาร

(จ) อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมายหรือผิดศีลธรรมจริยธรรม

(๒) ห้ามเล่นหรือดาวน์โหลดเกมส์ การละเมิดลิขสิทธิของผู้เป็นเจ้าของข้อมูลนั้น

(๕) ห้ามใช้อินเตอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์หรือชื่อเสียงของกรมทรัพยากรธรณี

ข้อ ๖. การใช้งานจดหมายอิเล็กทรอนิกส์ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

(๑) ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ตามที่กรมทรัพยากรธรณีกำหนดเท่านั้น

(๒) ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ที่กรมทรัพยากรธรณีกำหนดให้ลงทะเบียนตามเว็บไซต์ที่ไม่เกี่ยวข้องกับงานของกรมทรัพยากรธรณี

(๓) ห้ามดู หรือเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาต

(๔) ห้ามปลอมแปลงรับหรือส่งจดหมายอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาต

(๕) ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้

(ก) จดหมายขยะ (Spam Mail)

(ข) จดหมายลูกโซ่ (Chain Letter)

(ค) จดหมายที่ละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

(ง) จดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

(๖) ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีขนาดใหญ่เกินกว่าที่กรมทรัพยากรธรณี กำหนด

(๗) ต้องระบุชื่อเรื่อง (Subject) และชื่อผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

(๘) ต้องใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับจดหมายอิเล็กทรอนิกส์เท่าที่มีความจำเป็นต้องรับรู้เท่านั้น

(๙) ต้องใช้คำที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์

ข้อ ๗. เอกสารที่เป็นความลับหรือมีระดับความสำคัญซึ่งพิมพ์ออกมาจากเครื่องพิมพ์เจ้าหน้าที่ต้องปฏิบัติให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการดังต่อไปนี้

(๑) จัดหมวดหมู่เอกสารที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก

(๒) จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ

(๓) การสำเนาเอกสารที่เป็นความลับหรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของ

(๔) ระมัดระวังการกระจายหรือแจกจ่ายเอกสารที่เป็นความลับของกรมทรัพยากรธรณีไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

(๕) ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน

(๖) ให้ทำลายเอกสารที่เป็นความลับหรือมีระดับความสำคัญสูงเมื่อหมดความจำเป็นในการใช้งาน

ข้อ ๘. การจัดการข้อมูลที่เป็นความลับที่อยู่ในรูปอิเล็กทรอนิกส์ผู้ใช้งานปฏิบัติตามแนวทางปฏิบัติในการจัดการกับข้อมูลลับในข้อข้างต้น

## *ส่วนที่ ๕.*

## แนวปฏิบัติและหน้าที่ของผู้ดูแลเครือข่าย/ผู้ดูแลระบบ

ข้อ ๑. ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์ระบบงานสารสนเทศและระบบเครือข่ายของกรมทรัพยากรธรณีให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพหากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไขรวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันทีและในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบ (System Administrator) พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าวได้ทันที

ข้อ ๒. ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่ายให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

ข้อ ๓ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) ระบบงานสารสนเทศและระบบเครือข่าย

ข้อ ๔. ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

ข้อ ๕. บริหารจัดการบัญชีผู้ใช้งานตามอำนาจหน้าที่ที่ตนเองรับผิดชอบเท่านั้น

ข้อ ๖ .บริหารจัดการระบบงานสารสนเทศและระบบเครือข่ายตามอำนาจหน้าที่ที่ตนเองรับผิดชอบเท่านั้น

ข้อ ๗. บริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามอำนาจหน้าที่ที่ตนเองรับผิดชอบเท่านั้น

ข้อ ๘. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์ระบบสารสนเทศและระบบเครือข่ายโดยไม่มีเหตุผลอันสมควร

ข้อ ๙. ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่ายโดยไม่มีเหตุผลอันสมควร

ข้อ ๑๐. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สามารถเปิดเผยได้ให้บุคคลอื่นทราบโดยไม่มีเหตุผลอันสมควร

ข้อ ๑๑. เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งานและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วันนับแต่การใช้บริการสิ้นสุดลง

## *ส่วนที่ ๖.*

## แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

ข้อ ๑. กำหนดมาตรการทางเครือข่ายสื่อสารข้อมูลเพื่อป้องกันข้อมูลในเครือข่าย ระบบงาน หรือบริการต่างๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

(๑) กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

(๒) กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งานที่อนุญาตให้สามารถเข้าใช้ระบบสารสนเทศจากระยะไกล

(๓) กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะเช่นเครือข่ายอินเตอร์เน็ต เครือข่ายไร้สายเป็นต้น

(๔) กำหนดมาตรการเพื่อป้องกันระบบสารสนเทศต้องเชื่อมโยงกับเครือข่ายสาธารณะ

(๕) กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบสารสนเทศต่างๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

(๖) ต้องบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

ข้อ ๒. ผู้ดูแลเครือข่ายของหน่วยงานภายในกรมทรัพยากรธรณี ผู้ดูแลต้องปฏิบัติตามข้อกำหนด ดังต่อไปนี้

(๑) ผู้ดูแลเครือข่ายต้องออกแบบแบ่งระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารต้องแบ่งกลุ่มตามกลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ

(๒) ผู้ดูแลเครือข่ายต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๓) ผู้ดูแลเครือข่ายต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน รวมทั้งตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๔) ผู้ดูแลเครือข่าย ต้องจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้ โดยการทำ VLAN

(๕) กำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและมีการทบทวนการกำหนดค่าตัวแปร (Parameter) ต่างๆอย่างน้อยปีละครั้งนอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๖) ระบบเครือข่ายทั้งหมดของหน่วยงานที่ต้องเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ต้องจัดให้มีการเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก Firewall, Proxy และจะต้องตั้งค่าอุปกรณ์ดังกล่าวเพื่อควบคุมการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน หรือจัดเส้นทางของระบบเครือข่ายของกรมฯ เพื่อเพิ่มความมั่นคงปลอดภัยของสารสนเทศ

(๗) ต้องติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติผ่านระบบเครือข่ายโดยต้องตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติ

(๙) การเข้าสู่ระบบงานเครือข่ายภายในหน่วยงานผ่านทางอินเทอร์เน็ตต้อง Login เข้าระบบและต้องพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

(๙) ข้อมูลหมายเลขชุดอินเตอร์เน็ตของคอมพิวเตอร์ (IP Address) ภายใน (Local) ของระบบงานเครือข่ายภายในของกรมทรัพยากรธรณี จำเป็นต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของกรมฯ ได้โดยง่าย

(๑๐) จัดทำแผนผังระบบเครือข่าย (Network Diagram) พร้อม IP Address และ Mac Address ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๑๑) จัดให้มีการใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๑๒) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์สารสนเทศทรัพยากรธรณีเท่านั้น

(๑๓) การบริหารจัดการการบันทึกและตรวจสอบในระบบป้องกันการบุกรุก ต้องกำหนดให้มีการบันทึกการทำงาน เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อยกว่า ๓ เดือนหรือไม่ต่ำกว่า ๙๐ วัน

(๑๔) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ผู้ดูแลเครือข่ายต้องเก็บบัญชีการขอเชื่อมต่อเครือข่าย อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้ และผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “แบบฟอร์มการขอใช้บริการ Authentication Authorization Accounting ของบุคลากร/บุคลากรภายนอกหน่วยงาน ให้ใช้แบบฟอร์ม DMR_04”

(๑๕) ต้องตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

ข้อ ๓. การเข้าถึงระบบเครือข่าย หรือระบบสารสนเทศภายในของกรมฯ ด้วยการเชื่อมต่อจากระบบเครือข่ายภายนอก ต้องถูกจำกัดให้ดำเนินการได้เฉพาะที่จำเป็นเท่านั้น โดยมีแนวทางปฏิบัติ ดังนี้

(๑) อนุญาตให้ทำการเข้าถึงระบบจากระยะไกลได้เฉพาะระบบบริการที่มีความจำเป็นเท่านั้น

(๒) การเข้าสู่ระบบเครือข่ายภายในของกรมทรัพยากรธรณี โดยผ่านทางอินเตอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาก่อนเท่านั้นที่มีสิทธิดำเนินการเข้าถึงระบบ

(๓) การเข้าถึงระบบสำคัญ หรือระบบที่เกี่ยวข้องกับสารสนเทศสำคัญจากระยะไกล ต้องได้รับการพิสูจน์ตัวตน

(๔) ห้ามใช้บริการระบบเครือข่าย หรือ Protocol ที่ไม่มั่นคงปลอดภัยในการเข้าถึงระบบสารสนเทศจากระยะไกล

(๕) การเข้าสู่ระบบจากระยะไกล (remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของกรมฯ ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของกรมทรัพยากรธรณี การควบคุมบุคคลที่เข้าสู่ระบบของกรมฯ จากระยะไกลจึงต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน ผ่านระบบ VPN จากบัญชีรายชื่อผู้ใช้งาน (Active Directory)

ข้อ ๔. ผู้ใช้งานที่ปฏิบัติงานอยู่ภายนอกสำนักงานจะต้องมีแนวปฏิบัติ ดังนี้

(๑) ผู้ใช้งานต้องแสดงตัวตนด้วยบัญชีของผู้ใช้งานและรหัสผ่านที่เป็นมาตรฐานของกรมฯ ก่อนการเข้าถึงระบบสารสนเทศของกรมฯ ทุกครั้ง

(๒) กำหนดให้ใช้งานซอฟต์แวร์ (Software) ป้องกันไวรัสที่ได้รับการอัพเดทอยู่เสมอ

(๓) กำหนดใช้งานซอฟแวร์ไฟร์วอลล์ส่วนบุคคล (Personal Fireeall)

(๔) ใช้งานซอฟต์แวร์ หรืออุปกรณ์ประเภท Virtual Private Networking หรือใช้เทคโนโลยีอื่นๆ เพื่อป้องกันการเชื่อมต่อระหว่างสถานที่ปฏิบัติงานภายนอกกับระบบเครือข่ายภายในของกรมฯ

(๕) ต้องใช้ความระมัดระวังมากเป็นพิเศษ เพื่อป้องกันอุปกรณ์คอมพิวเตอร์ รวมถึงสารสนเทศที่อยู่ในกอุปกรณ์นั้น มิให้ถูกล่วงละเมิดโดยบุคคลที่ไม่ได้รับอนุญาต

ข้อ ๕. การควบคุมการเข้าถึงระบบเครือข่ายไร้สายผู้ดูแลเครือข่ายของหน่วยงานภายในกรมทรัพยากรธรณี ผู้รับผิดชอบต้องปฏิบัติตามข้อกำหนด ดังต่อไปนี้

(๑) ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในกรมทรัพยกรธรณี จะต้องทำการลงทะเบียนกับผู้ดูแลเครือข่ายและต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน

(๒) ผู้ดูแลเครือข่ายต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งต้องทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(๓) ผู้ดูแลเครือข่ายควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

ข้อ ๖ การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) กรมทรัพยากรธรณี ไม่มีการปฏิบัติงานในเรื่องดังกล่าว

## *ส่วนที่ ๗.*
## แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

ข้อ ๑. ผู้ดูแลระบบ (system administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (domain controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

ข้อ ๒. กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

(๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การ เข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดา รหัสผ่านจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้าง ความเสียหายให้กับระบบได้

ข้อ ๓. ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค

(๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น Smart Card

ข้อ ๔. การบริหารจัดการรหัสผ่าน (password management system) มีระบบบริหารจัดการ รหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนด รหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

ข้อ ๕. การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ต้องมีการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการ ละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการ ดังนี้

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๔) กำหนดให้เก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) ซอฟต์แวร์ที่ติดตั้งต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามผู้ใช้งาน คัดลอกซอฟต์แวร์ต่างๆ และนำไปติดตั้งหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

ข้อ ๖. เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (secsion time-out)

(๑) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็น เวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

ข้อ ๗. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศ หรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งาน ได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๓ ช.ม. ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

(๒) กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) ต้องจำกัดช่วงระยะเวลาการเชื่อมต่อโดยมีการจำกัดการเข้าถึงระบบ ๕ นาที หลักจากไม่ใช้งาน

## *ส่วนที่ ๘.*

## แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

ข้อ ๑. ผู้ดูแลระบบสารสนเทศของหน่วยงานภายในกรมฯ ต้องกำหนดแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูลเมื่อมีระบบงานใหม่เกิดขึ้น หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่ควรกำหนดให้ใช้แนวทางการสำรองและกู้คืนข้อมูล ดังนี้

(๑) กำหนด คัดเลือกระบบงานที่มีความจำเป็นต้องสำรองข้อมูลไว้ให้อยู่สภาพพร้อมใช้งานที่เหมาะสม ตามเอกสารแนบ ๓

(๒) กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องซึ่งดูและรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการทางอิเล็กทรอนิกส์ได้ โดยกำหนดให้มีผู้รับผิดชอบ และให้ปฏิบัติตามแผนเอกสารแนบ ๓

(๓) กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อยต้องประกอบด้วยข้อมูลในฐานข้อมูลของระบบ ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์อื่นๆ ที่เกี่ยวข้องเป็นต้น

(๔) กำหนดความถี่ในการสำรองข้อมูลของระบบงาน

(๕) กำหนดขั้นตอนการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้องรวมทั้งซอฟต์แวร์ที่ใช้ในการสำรองข้อมูล

(๖) ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

(๗) ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้นสำเร็จครบถ้วนหรือไม่

(๘) ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่

(๙) จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนดแผนควรมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๙.๑) การกำหนดหน้าที่และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

(๙.๒) การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้นและกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น โดยมีผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) และผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor)

(๙.๓) การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน

(๙.๔) การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

(๙.๕) การกำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่ายฮาร์ดแวร์ซอฟต์แวร์เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่างๆ

(๑๐) ให้ทำการทบทวนปรับปรุงแผนดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

(๑๑) ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนรับมือฯ รวมทั้งเมื่อมีการปรับปรุงแผนใหม่จะต้องจัดประชุมใหม่และแจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

(๑๒) กำหนดให้มีการจัดทำรายงานผลการวิเคราะห์โครงสร้างพื้นฐานระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์เป็นประจำทุกปี

## *ส่วนที่ ๙.*

## แนวปฏิบัติในการจัดซื้อจัดจ้างระบบสารสนเทศ

ข้อ ๑. การจัดหาเพื่อให้ได้มาซึ่งระบบสารสนเทศ จะต้องดำเนินการตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรธรณี โดยเคร่งครัด ดังนี้

(๑) การเชื่อมโยง หรือทำงานร่วมกันกับระบบงานเดิมที่กรมทรัพยากรธรณีมีใช้งานอยู่

(๒) การจัดหาเครื่องแม่ข่าย เพื่อรองรับระบบสารสนเทศใหม่ให้รวมอยู่ในการจัดหาด้วย รวมถึงการดูแลระบบ การดูแลข้อมูล การสำรองข้อมูล และการ Update ระบบต่างๆ ให้เป็นหน้าที่ของผู้พัฒนาระบบ

(๓) การดูแลการเชื่อมต่อกับระบบเครือข่าย ของกรมทรัพยากรธรณีให้เป็นหน้าที่ของผู้ดูแลเครือข่าย

(๔) การจัดหาระบบงานจะต้องรวมถึงการอบรม หรือการแนะนำการใช้งาน

ข้อ ๒. ภายหลังจากที่ได้มีการตรวจรับระบบที่พัฒนาขึ้นใหม่แล้ว ผู้ดูแลระบบของหน่วยงานภายในกรมทรัพยากรธรณี ต้องกำหนดการควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการ

(๑) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือผู้มีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงาน และผู้ดูแลระบบงานต้องเปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟแวร์ที่ได้จัดซื้อ

(๒) ต้องขออนุมัติให้ติดตั้งก่อนดำเนินการ

(๓) กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบงาน เป็นต้น

(๔) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วนก่อนดำเนินการติดตั้งบนระบบเครื่องให้บริการระบบงาน

(๕) ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล ซอฟต์แวร์ ค่าคอนฟิกกูเรชัน หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จจะได้กลับไปใช้ระบบงานเดิมได้

(๖) ในกรณีที่มีความจำเป็นต้องเปลี่ยนแปลงข้อมูลในระบบงานเดิม ไปสู่ข้อมูลในระบบงานที่จะทำการติดตั้ง ให้กำหนดแผนการถ่ายโอน หรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ กำหนดให้มีการถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งาน เพื่อตรวจสอบว่าข้อมูลที่ถ่ายโอนข้อมูลไปนั้น มีความถูกต้องและครบถ้วนหรือไม่

(๗) กำหนดแผนการติดตั้งสำหรับระบบงาน ซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า เช่น แผนการติดตั้งฮาดร์ดแวร์ ซอฟต์แวร์ และอื่นๆ

(๘) สำหรับซอฟแวร์ที่จะทำการติดตั้ง ให้ตรวจก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

(๙) ให้อ่านและปฏิบัติตามเงื่อนไข หรือข้อตกลงการใช้งานซอฟต์แวร์ที่จะทำการติดตั้งอย่างเคร่งครัด

(๑๐) สำหรับการติดตั้งซอฟต์แวร์ยูทิลิตี้ (Utility software) ต้องตรวจสอบก่อนว่าเป็นซอฟต์แวร์ที่มีการทำงานที่ถูกต้อง และเชื่อถือได้ โดยห้ามมิให้ติดตั้งโปรแกรม (Utility software) หากไม่ได้รับอนุญาตจากผู้ดูและระบบ

(๑๑) ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่างๆ (Patch) ที่เกี่ยวข้องกับระบบงานตามความจำเป็น เช่น โปรแกรมแก้ไขช่องโหว่ สำหรับระบบปฏิบัติการ โปรแกรมแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

(๑๒) ตรวจสอบและปิดพอร์ด (Port) บนระบบงานที่ไม่มีความจำเป็นในการใช้งานก่อนเปิดระบบให้บริการ

(๑๓) กำหนดให้มีการป้องกันไวรัสคอมพิวเตอร์บนระบบงานที่ทำการติดตั้ง

(๑๔) จำกัดการเชื่อมต่อทางเครือข่ายเพื่ออนุญาตให้เฉพาะกลุ่มผู้ใช้งานที่เกี่ยวข้องเท่านั้นจึงจะสามารถเชื่อมต่อเพื่อเข้าสู่ระบบงานที่ทำการติดตั้ง

ข้อ ๓. ผู้ดูแลเครือข่ายและผู้ดูแลระบบของหน่วยงานภายในกรมทรัพยากรธรณีต้องกำหนดให้มีการทบทวนการทำงานของระบบภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes) ดังนี้

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้น มีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบ รวมทั้งการวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่กรมทรัพยากรธรณีต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

## *ส่วนที่ ๑๐.*

## แนวปฏิบัติในการแนวการคุ้มครองข้อมูลส่วนบุคคลและการเผยแพร่ข้อมูลสาธารณะ

ข้อ ๑. ข้อมูลเบื้องต้น ประกอบด้วย ข้อมูลส่วนบุคคลที่กรมทรัพยากรธรณี เก็บรวบรวมหรือได้รับมา เท่านั้น ซึ่งข้อมูลดังกล่าว รวมถึงข้อมูลที่ผู้ใช้บริการใช้บริการของกรมทรัพยากรธรณีด้วย ซึ่งข้อมูลส่วนบุคคล คือ ข้อมูลที่ระบุตัวบุคคลของผู้ใช้บริการได้เช่นเดียวกับชื่อ ที่อยู่ อีเมล์ หมายเลขโทรศัพท์ ของผู้ใช้บริการ ทั้งนี้ ข้อมูลส่วนบุคคลในที่นี้ ไม่ได้หมายรวมถึงข้อมูลที่สาธารณชนสามารถเข้าถึงได้เป็นการทั่วไป และไม่ใช้กับแนวปฏิบัติต่อข้อมูลส่วนบุคคลของหน่วยงานอื่นที่กรมทรัพยากรธรณีมิได้เกี่ยวข้อง หรือสามารถควบคุมได้ และไม่ใช้บังคับกับแนวปฏิบัติของบุคคลที่มิได้เป็นผู้ดูแลระบบสารสนเทศของกรมทรัพยากรธรณีไม่มีอำนาจควบคุมดูแล

ข้อ ๒. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

(๑) การเก็บรวบรวมข้อมูลส่วนบุคคลของกรมทรัพยากรธรณีผ่าน ทางการลงทะเบียน หรือการกรอกแบบฟอร์มนั้น ข้อมูลที่จำเป็นต้องกรอกลงไปได้แก่ ชื่อ ชื่อสกุล หมายเลขประจำตัวประชาชน ที่อยู่ อีเมล์ หมายเลขโทรศัพท์ โดยข้อมูลเหล่านี้จำเป็นต่อการประมวลผลและการดำเนินงานตามภารกิจการให้บริการของกรมทรัพยากรธรณี ส่วนข้อมูลอื่นๆ นอกจากนี้ ผู้ใช้บริการมีสิทธิเลือกที่จะให้หรือไม่ให้ก็ได้ ซึ่งข้อมูลต่างๆ เหล่านี้ กรมทรัพยากรธรณีจะใช้ เพื่อปรับปรุงการให้บริการที่ดีขึ้นต่อไป

(๒) ผู้ใช้บริการอาจได้รับการร้องขอให้แจ้งข้อมูลส่วนบุคคลในเวลาใดๆ ที่ติดต่อกรมทรัพยากรธรณีและกรมทรัพยากรธรณีอาจมีการใช้งานข้อมูลส่วนบุคคลนี้ในหน่วยงาน รวมทั้ง อาจผนวกข้อมูลส่วนบุคคลนี้เข้ากับข้อมูลอื่นๆ เพื่อการดำเนินงานของหน่วยงาน และข้อมูลที่ผนวกเข้าด้วยกันจะถือว่าเป็นข้อมูลส่วนบุคคลตราบเท่าที่ยังคงผนวกเข้าด้วยกันอยู่

(๓) กรมทรัพยากรธรณี จัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการที่ส่ง เรื่องร้องเรียน / ติดต่อทางเว็บไซต์ โดย ชื่อหน่วยงาน จะจัดเก็บรวบรวมข้อมูลดังกล่าวไว้ เช่น ชื่อผู้ร้องเรียน อีเมล์ เบอร์ติดต่อ และจัดเก็บข้อมูลหมายเลขไอพีแอดเดรส ของผู้ใช้บริการทุกท่านที่เข้าเยี่ยมชม เว็บของกรมทรัพยากรธรณีเพื่อใช้เป็นข้อมูลอ้างอิงต่อไป

(๔) กรมทรัพยากรธรณีจะใช้ข้อมูลส่วนบุคคลของผู้ใช้บริการเพียงเท่าที่ จำเป็น เช่น ชื่อ ชื่อสกุล ที่อยู่ อีเมล์ หมายเลขโทรศัพท์ เพื่อใช้ในการติดต่อการให้บริการ ประชาสัมพันธ์ หรือ ให้ข้อมูลข่าวสารกรมทรัพยากรธรณีเท่านั้น

(๕) ในกรณีที่กรมทรัพยากรธรณีว่าจ้างให้หน่วยงานอื่นดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการ เช่น การจัดทำแปลงเอกสารเป็นข้อมูลอิเล็กทรอนิกส์ การทำสำเนาเอกสาร ในกิจการหรือกิจกรรมของกรมทรัพยากรธรณีจะกำหนดให้หน่วยงานที่ได้ว่าจ้างให้ดำเนินการต่างๆ ข้างต้น เก็บรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคลของ ผู้ใช้บริการ และกำหนดข้อห้ามมิให้นำข้อมูลส่วนบุคคลไปใช้นอกเหนือจากกิจการหรือกิจกรรมของกรมทรัพยากรธรณี

ข้อ ๓. การรวมข้อมูลจากที่มาหลายๆ แห่ง ในบางกรณีกรมทรัพยากรธรณีอาจจะนำข้อมูลส่วนบุคคลที่ผู้ใช้บริการให้ข้อมูลผ่านทางเว็บไซต์รวมเข้ากับข้อมูลที่ได้มาจากแหล่งอื่น เช่น ข้อมูลที่อยู่ปัจจุบันของผู้ใช้บริการ เป็นต้น ทั้งนี้เพื่อทำให้ข้อมูลของกรมทรัพยากรธรณีมีความครบถ้วนและถูกต้อง เป็นปัจจุบัน และเพื่อทำให้กรมทรัพยากรธรณี สามารถให้บริการตามภารกิจและหน้าที่ของหน่วยงานได้อย่างดียิ่งขึ้น

ข้อ ๔. การให้บุคคลอื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลกรมทรัพยากรธรณีไม่อนุญาตให้บุคคลอื่นเข้าถึงหรือใช้ข้อมูลที่กรมทรัพยากรธรณี เก็บรวบรวมมาจากเว็บไซต์ หมายเหตุ กรณีที่มีการบังคับให้เปิดเผยข้อมูลตามกฎหมาย ตามหมายศาลหรือ ตามคำสั่งศาลนั้นกรมทรัพยากรธรณีมีหน้าที่ที่จะต้องปฏิบัติตาม

ข้อ ๕. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน ในกรณีที่ผู้ใช้บริการได้ให้ข้อมูลต่างๆ กับกรมทรัพยากรธรณีผ่านทางเว็บไซต์ของกรมทรัพยากรธรณีและประสงค์จะแก้ไขหรือปรับปรุงข้อมูลดังกล่าวให้ถูกต้องหรือ ให้เป็นปัจจุบันสามารถติดต่อกรมทรัพยากรธรณีได้ทางช่องทางที่ระบุไว้

ข้อ ๖. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล กรมทรัพยากรธรณีเสริมสร้างความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่ ข้าราชการ ลูกจ้างประจำ พนักงานราชการของกรมทรัพยากรธรณีด้วยการ เผยแพร่ข้อมูลข่าวสาร การจัดอบรม และจัดสัมมนา

ข้อ ๗. การเผยแพร่ข้อมูลสิ่งพิมพ์ออกในความรับผิดชอบของกรมทรัพยากรธรณีสู่สาธารณะ โดยผ่านระบบสารสนเทศของกรมทรัพยากรธรณี หน่วยงานเจ้าของข้อมูลจะต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำออกเผยแพร่และหากข้อมูลที่นำออกเผยแพร่เกี่ยวข้องกับเรื่องนโยบายจะต้องได้รับความเห็นชอบจากอธิบดีกรมทรัพยากรธรณีหรือผู้ซึ่งอธิบดีกรมทรัพยากรธรณีมอบหมายก่อนนำออกเผยแพร่ ในกรณีที่ข้อมูลที่นำออกเผยแพร่มีความผิดพลาดและมีความเสียหายเกิดขึ้น โดยความเสียหายนั้นเกิดจากความจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ให้เป็นความรับผิดของเจ้าหน้าที่ที่นำข้อมูลดังกล่าวออกเผยแพร่

ข้อ ๘. การเผยแพร่ข้อมูลสิ่งพิมพ์ออกสู่สาธารณะโดยผ่านระบบสารสนเทศของกรมทรัพยากรธรณีให้ดำเนินการโดยหน่วยงานเจ้าของข้อมูล เว้นแต่กรณีที่อธิบดีกรมทรัพยากรธรณีหรือผู้ซึ่งอธิบดีกรมทรัพยากรธรณีมอบหมายได้สั่งการหรือเห็นชอบไว้เป็นอย่างอื่น

## *ส่วนที่ ๑๑.*

## แนวนโยบายการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยมั่นคงด้านสารสนเทศ

ข้อ ๑. จัดอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

ข้อ ๒. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยกำหนดให้ปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๓. เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์กรมฯ ให้แก่ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

*ภาคผนวก ก.*

**ขั้นตอนการลงทะเบียนผู้ใช้งานกรมทรัพยากรธรณี**

มีขั้นตอนการปฏิบัติดังนี้

๑. การลงทะเบียนขอใช้เครื่องคอมพิวเตอร์กรมทรัพยากรธรณีให้ใช้แบบฟอร์ม DMR_01 แบบลงทะเบียนขอใช้เครื่องคอมพิวเตอร์/อุปกรณ์ต่อพ่วงและอุปกรณ์อื่นๆ กรมทรัพยากรธรณี ทั้งนี้ให้ ศสท. เป็นผู้ดำเนินการเก็บรวบรวมข้อมูลต่อไป

๒. การลงทะเบียนขอยืมเครื่องคอมพิวเตอร์/อุปกรณ์ต่อพ่วง และอุปกรณ์อื่นๆ ศูนย์สารสนเทศทรัพยากรธรณี ให้ใช้แบบฟอร์ม DMR_02 แบบลงทะเบียนขอยืมเครื่องคอมพิวเตอร์กรมทรัพยากรธรณี โดยให้ ศสท. เป็นผู้ควบคุม ในการยืม-คืน ต่อไป

๓. การลงทะเบียนขอใช้ระบบงานทรัพยากรธรณี ของผู้ใช้งานภายในหน่วยงาน ให้ใช้แบบฟอร์ม DMR_03 แบบลงทะเบียนขอใช้ระบบงานของกรมทรัพยากรธรณี โดยให้ผู้ดูแลระบบ ในแต่ละระบบเป็นผู้ดำเนินการ และเป็นผู้เก็บรวบรวมข้อมูลเอกสาร

๔. การลงทะเบียนขอใช้ ระบบคอมพิวเตอร์เครือข่ายและอินเตอร์เน็ต (Authentication Authothorization Accounting ) กรมทรัพยากรธรณี

๔.๑ กรณีของผู้ใช้งานภายในหน่วยงานให้ใช้แบบฟอร์มการขอใช้บริการ Authentication Authorization Accounting ของบุคลากร/บุคลากรภายนอกหน่วยงาน ให้ใช้แบบฟอร์ม DMR_04

๔.๒ กรณีของผู้ใช้งานภายนอกหน่วยงานให้ใช้แบบฟอร์มการขอใช้บริการ Authentication Authorization Accounting ของบุคลากร/บุคลากรภายนอกหน่วยงาน ให้ใช้แบบฟอร์ม DMR_04 แต่ต้องแนบสำเนาบัตรประชาชน

๕. การลงทะเบียนขอใช้ระบบงานกรมทรัพยากรธรณี ของผู้ใช้งานภายในหน่วยงาน ให้ใช้แบบฟอร์ม DMR_03 แบบลงทะเบียนขอใช้ระบบงานกรมทรัพยากรธรณี

๖. การลงทะเบียนขอใช้ระบบงานกรมทรัพยากรธรณี ของผู้ใช้งานภายนอกหน่วยงานให้ผู้ใช้งานภายนอกติดต่อกับผู้ดูแลระบบงานนั้น (แบบฟอร์ม DMR_03) ทำการขอใช้ระบบงานตามขั้นตอนและวิธีการที่นโยบายนี้ได้กำหนดไว้

*ภาคผนวก ข.*

**โปรแกรมมาตรฐานในการใช้งานของกรมทรัพยากรธรณี**

๑. Microsoft Windows

๒. Microsoft Office

๓. Anti-virus Symantec

๔. Adobe Acrobat

๕. WinRAR/WinZip

๖. Nero

# แบบขอยืมใช้เครื่องคอมพิวเตอร์ /อุปกรณ์ต่อพ่วง หรืออุปกรณ์อื่นๆ กรมทรัพยากรธรณี

วันที่ _____ เดือน _____ พ.ศ. _____

**เรียน อธิบดี กรมทรัพยากรธรณี**

ข้าพเจ้า นาย/นาง/นางสาว _____ ตำแหน่ง _____
สังกัดหน่วยงาน _____ หมายเลขโทรศัพท์ _____
โทรศัพท์เคลื่อนที่ _____ ใคร่ขออนุญาตยืม

- ☐ **คอมพิวเตอร์ แบบตั้งโต๊ะ** จำนวน _____ ชุด
- ☐ **คอมพิวเตอร์ Notebook** จำนวน _____ ชุด
- ☐ **อุปกรณ์ต่อพ่วง หรืออุปกรณ์อื่นๆ** จำนวน _____ เครื่อง/ชิ้น

*สำหรับผู้ขอยืมเป็นผู้กรอก*

**รายละเอียดเครื่องคอมพิวเตอร์ /อุปกรณ์ต่อพ่วง และอุปกรณ์อื่นๆ**

| หมายเลขครุภัณฑ์ | Serial Number | ชื่อบริษัทผู้ผลิต/รุ่น |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

**หมายเหตุ** .....

.....

เพื่อใช้ในการปฏิบัติงานหรือกิจกรรมพิเศษต่างๆ ที่เกี่ยวข้องกับภารกิจของกรมทรัพยากรธรณีเท่านั้น ทั้งนี้ข้าพเจ้าได้อ่านระเบียบการยืมครุภัณฑ์ เครื่องคอมพิวเตอร์/คอมพิวเตอร์แบบพกพา และข้อ แนะนำในการดูแล/ใช้งานเครื่อง (ด้านหลังแบบฟอร์มนี้) แล้ว และจะปฏิบัติตามระเบียบและข้อแนะนำ โดยเคร่งครัด

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาต

ลงชื่อผู้ขอใช้บริการ.....

วันที่...../...../.....

| เพื่อโปรดพิจารณา *(ผู้ให้บริการ)* | ความคิดเห็นของผู้อำนวยการ |
|---|---|
| ลงชื่อ..... ผู้ขอยืม<br>(.....)<br>วันที่...../...../..... | .....<br>.....<br>ลงชื่อ.....<br>(.....)<br>ผอ. สำนัก/ศูนย์/สทข./กลุ่มงานขึ้นตรง |

**โปรดศึกษารายละเอียดและแนวปฏิบัติในการดูแล/ใช้งานอุปกรณ์คอมพิวเตอร์ฯ ด้านหลังแบบฟอร์มฉบับนี้ก่อนลงนาม**

# ข้อแนะนำในการดูแล/ใช้งานเครื่องคอมพิวเตอร์/
# เครื่องคอมพิวเตอร์แบบแบบพกพา ของกรมทรัพยากรธรณี

1. ไม่ควรทิ้งเครื่องไว้ในรถยนต์ เพราะความร้อนจะทำให้เครื่องเสียได้
2. ควรหิ้วเครื่องด้วยตนเอง ไม่ควรวางบนรถลาก เพราะความสะเทือนจะทำให้เครื่องพังได้
3. ขณะใช้งานควรวางเครื่องบนพื้นแข็งและราบเรียบ หรือวางในลักษณะที่ทำให้พัดลมระบายความร้อนทำงานได้ดี
4. ไม่ควรทิ้งแผ่นซีดีไว้ในเครื่อง เพราะจะทำให้หัวอ่านเสียหายได้
5. ใช้ Shut down เครื่องทุกครั้งเมื่อเลิกใช้งาน และปิดฝาเครื่องด้วยทุกครั้ง
6. ไม่นำสิ่งของที่มีน้ำหนักมาวางทับบนฝาของเครื่อง เพราะน้ำหนักที่กดส่งผลให้จอภาพเสียหายได้ (กรณีที่เป็นคอมพิวเตอร์แบบพกพา)
7. ไม่ใช้นิ้วหรือวัสดุอื่นใดจิ้มบนจอภาพ รวมทั้งการเช็ดจอภาพต้องใช้ผ้าเช็ดจอโดยเฉพาะมิฉะนั้นจะทำให้เกิดรอยบนจอได้
8. เวลายกเครื่องให้ยกที่ฐาน ไม่ใช่จับยกที่จอภาพ (กรณีที่เป็นคอมพิวเตอร์แบบพกพา)
9. ไม่รับประทานอาหารใกล้ๆ เครื่องคอมพิวเตอร์
10. ต้องระมัดระวังการใช้งานและดูแลคอมพิวเตอร์รวมทั้งระบบเครือข่ายตามที่วิญญูชนทั่วไปจะพึงปฏิบัติ
11. หากเกษียณอายุราชการ หรือสับเปลี่ยนโอนย้ายเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นๆ ระหว่างกัน ให้ทำการแจ้งข้อมูลให้ ศสท. ทราบได้ที่ ผู้อำนวยการศูนย์สารสนเทศทรัพยากรธรณี พร้อมแนบแบบฟอร์มขอยืมใช้เครื่องคอมพิวเตอร์/อุปกรณ์ต่อพ่วง หรืออุปกรณ์อื่นๆ เดิมแนบมาด้วย

# แบบขอยืมเครื่องคอมพิวเตอร์ /อุปกรณ์ต่อพ่วง และอุปกรณ์อื่นๆ ของศูนย์สารสนเทศทรัพยากรธรณี

ส่วนเทคโนโลยีสารสนเทศฯ
รับวันที่ _____
เวลา _____ น.
ผู้รับ _____

วันที่ _____ เดือน _____ พ.ศ. _____

**เรียน ผู้อำนวยการศูนย์สารสนเทศทรัพยากรธรณี**

ข้าพเจ้า นาย / นาง / นางสาว _____ ตำแหน่ง _____
สังกัดหน่วยงาน _____ หมายเลขโทรศัพท์ _____
โทรศัพท์เคลื่อนที่ _____ ใคร่ขออนุญาตยืม

☐ **คอมพิวเตอร์ แบบตั้งโต๊ะ** จำนวน _____ เครื่อง

☐ **คอมพิวเตอร์ Notebook** จำนวน _____ เครื่อง

☐ **อุปกรณ์ต่อพ่วงคอมพิวเตอร์** ได้แก่ _____ จำนวน _____ เครื่อง
ได้แก่ _____ จำนวน _____ เครื่อง
ได้แก่ _____ จำนวน _____ เครื่อง

☐ **อื่นๆ** ได้แก่ _____
_____

เพื่อใช้ในกิจกรรม _____ ณ _____
กำหนดยืม _____ วัน ระหว่าง วันที่ ____ เดือน_____ พ.ศ. _____ ถึง วันที่ ____ เดือน_____
พ.ศ. _____ ต้องการรับมอบอุปกรณ์ใน วันที่ ____ เดือน_____ พ.ศ. _____ ทั้งนี้มอบหมายให้ นาย/นาง/
น.ส. _____หมายเลขบัตรประจำตัวประชาชน_____
เป็นผู้รับมอบอุปกรณ์ดังกล่าวแทนข้าพเจ้า

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาต

ลงนาม ..... **ผู้ขอยืม**
(.....)
วันที่ .....

ลงนาม .....**หัวหน้าหน่วยงาน**
(.....)
วันที่ .....

**หมายเหตุ**
โปรดศึกษารายละเอียดและแนวปฏิบัติในการยืมฯ ด้านหลังแบบฟอร์มฉบับนี้ก่อนลงนาม

*สำหรับเจ้าหน้าที่ศูนย์สารสนเทศทรัพยากรธรณี*

| ผลการพิจารณา | ความเห็นผู้รับผิดชอบดูแล | ความเห็นของเจ้าหน้าที่ |
|---|---|---|
| ☐ อนุญาต<br>☐ อื่นๆ .....<br><br>ลงชื่อ.....<br>(.....)<br>ผอ. ศูนย์สารสนเทศทรัพยากรธรณี<br>วันที่ ..... | ☐ แจ้งเพื่อทราบ<br>☐ แจ้งเพื่อทราบและดำเนินการต่อไป<br>☐ อื่นๆ<br><br>ลงชื่อ.....<br>(.....)<br>ผอ. ส่วนเทคโนสารสนเทศและการสื่อสาร<br>วันที่ ..... | ☐ ตรวจสอบแล้ว สามารถให้บริการได้<br>☐ ไม่สามารถให้บริการ เนื่องจาก<br>.....<br>.....<br>ลงชื่อ.....<br>(.....)<br>เจ้าหน้าที่<br>วันที่ ..... |

# ข้อกำหนดการยืมเครื่องคอมพิวเตอร์ /อุปกรณ์ต่อพ่วงและอุปกรณ์อื่นๆ ของศูนย์สารสนเทศทรัพยากรธรณี

1. เนื่องจากเครื่องคอมพิวเตอร์ / อุปกรณ์ต่อพ่วงและอุปกรณ์อื่นๆ มีจำนวนจำกัดและมีหน่วยงานยืมใช้จำนวนมากเพื่อความสะดวก โปรดตรวจสอบสถานภาพการจองใช้อุปกรณ์ที่ต้องการขอยืมได้ก่อนที่ **ส่วนเทคโนยีสารสนเทศฯ ศูนย์สารสนเทศทรัพยากรธรณี โทรศัพท์ 9686 (คุณจำลอง)**
2. **ผู้ขอยืม** ต้องเป็นข้าราชการ พนักงานราชการ ลูกจ้างประจำ สังกัด กรมทรัพยากรธรณี
3. **หัวหน้าหน่วยงาน** หมายถึง ผู้อำนวยการ สำนัก/ศูนย์/สทข./กลุ่มงานขึ้นตรง (หรือหน่วยงานเทียบเท่าที่มีชื่อเรียกอย่างอื่น) หัวหน้าส่วน หัวหน้าฝ่าย
4. เป็นการให้บริการยืมใช้เพื่องานหรือกิจกรรมพิเศษที่เกี่ยวข้องกับภารกิจของกรมทรัพยากรธรณีเท่านั้น
5. โปรดส่งแบบขอยืมฯ ล่วงหน้า <u>อย่างน้อย 3 วันทำการ</u> กรณีเร่งด่วน กรุณาส่งแบบขอยืมฯ ทางโทรสารหมายเลข 9686 เพื่อความสะดวกและรวดเร็วในการพิจารณาและจัดเตรียมความพร้อมของอุปกรณ์
6. โปรดตรวจสอบจำนวนและสภาพอุปกรณ์ทุกชิ้นที่ขอยืมก่อนการรับมอบ
7. กรณีมอบหมายให้ผู้อื่นที่ไม่ใช่ผู้ลงนามขอยืมเป็นผู้รับมอบอุปกรณ์ **โปรดแจ้งให้ผู้ที่รับมอบหมายนำบัตรประจำตัวประชาชน หรือบัตรอื่นที่สามารถระบุตัวตนได้เพื่อแสดงตนด้วย**
8. กรณีเกิดสูญหายหรือชำรุดเสียหายเนื่องจากการใช้งานผิดประเภท (ที่นอกเหนือจากการรับประกันตามสัญญา) **ผู้ขอยืมและหน่วยงานต้นสังกัดเป็นผู้รับผิดชอบค่าใช้จ่าย** ที่เกิดขึ้นจริง ตามที่จะได้รับการประเมินจากการซ่อมแซมหรือเปลี่ยนแปลงโดยบริษัทผู้ผลิต/ขายอุปกรณ์ดังกล่าว
9. กรณียืมเป็นระยะเวลานานต้องมีบันทึกจากผู้บังคับบัญชาระดับ ผู้อำนวยการ สำนัก/ศูนย์/สทข./กลุ่มงานขึ้นตรง ถึง ผอ. ศสท. พร้อมแนบแบบขอยืมเครื่องคอมพิวเตอร์/อุปกรณ์ต่อพ่วง และอุปกรณ์อื่นๆ ของ ศสท.
10. กรณีที่ไม่นำอุปกรณ์ คืนภายในเวลาที่กำหนด ศสท. จะระงับสิทธ์การใช้งานอินเตอร์เน็ตเป็นเวลา 15 วัน

*สำหรับเจ้าหน้าที่ศูนย์สารสนเทศทรัพยากรธรณี*

**รายละเอียดเครื่องคอมพิวเตอร์ /อุปกรณ์ต่อพ่วง และอุปกรณ์อื่นๆ ที่ขอยืม**

| หมายเลขครุภัณฑ์ | Serial Number | ประเภทอุปกรณ์/ชื่อบริษัทผู้ผลิต/รุ่น | สถาพของอุปกรณ์ |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**หมายเหตุ** .....

.....

ได้ตรวจสอบเครื่องมือ / อุปกรณ์ที่ขอยืมข้างต้นแล้วครบถ้วนถูกต้อง

| ลงชื่อผู้จ่าย | ลงชื่อผู้รับ | การส่งมอบ / ตรวจรับคืน |
|---|---|---|
| ..... | ..... | ☐ ได้รับคืนเมื่อวันที่ ..... ในสภาพเรียบร้อย |
| (.....) | (.....) | ☐ อื่นๆ ..... |
| วันที่ ..... | วันที่ ..... | ลงชื่อ .....ผู้รับ<br>วันที่..... |

# แบบฟอร์มการขอใช้บริการ ระบบงานคอมพิวเตอร์ สำหรับบุคลากร ทธ.

**ข้อมูลหน่วยงาน**

ชื่อหน่วยงาน สำนัก/ศูนย์/สนข./กลุ่มงานขึ้นตรง (ภาษาไทย).....

**ข้อมูลของผู้ขอใช้บริการ** *( ผู้ขอใช้บริการเป็นผู้กรอกข้อมูลส่วนนี้ )*

ชื่อ – สกุล (ภาษาไทย).....

Name (ชื่อ) ..... Surname (นามสกุล) .....

e-mail.....

เลขที่บัตรประชาชน ☐-☐☐☐☐-☐☐☐☐☐-☐☐-☐ วัน-เดือน-ปีเกิด ☐☐-☐☐-☐☐☐☐

ตำแหน่ง.....สังกัด/ส่วน/แผนก/ฝ่าย.....

หมายเลขโทรศัพท์.....หมายเลขมือถือ.....

**ประเภทของผู้รับบริกา**

☐ ข้าราชการ ☐ ลูกจ้างประจำ ☐ พนักงานราชการ

☐ พนักงานจ้างเหมาบริการ ☐ อื่นๆ (โปรดระบุ).....

ลงชื่อผู้ขอใช้บริการ.....

วันที่...../...../.....

| | | |
|---|---|---|
| **บริการที่ต้องการ** | ☐ ขอสิทธิ์การใช้งาน<br>☐ ขอเปลี่ยนแปลงสิทธิ์การใช้งาน<br>☐ การเพิ่มสิทธิ์<br>☐ ยกเลิก<br>☐ เปลี่ยนรหัสผ่าน<br>..... | ☐ ระบบ WebMail (.....@dmr.mail.go.th)<br>☐ ระบบอินทราเน็ต (intranet)<br>☐ ระบบ File Server<br>☐ ระบบบริการข้อมูลอิเล็กทรอนิกส์ (CMS)<br>☐ ระบบ ระบบสารบรรณอิเล็กทรอนิกส์<br>☐ ระบบ WebGIS<br>☐ ระบบบริหารจัดการฐานความรู้ (KM)<br>☐ ระบบบริหารจัดการการเรียนรู้ (LMS: e-learning)<br>☐ ระบบ พัสดุ ครุภัณฑ์ โครงงาน และแผนงาน<br>☐ ระบบสารสนเทศทรัพยากรบุคคล (DPIS)<br>☐ อื่นๆ..... |

| ความคิดเห็นผู้บังคับบัญชา *(ผู้ขอใช้บริการ)* | ความคิดเห็นผู้บังคับบัญชา *(ศสท.)* | ความคิดเห็นของผู้ให้บริการ |
|---|---|---|
| ..... | ..... | ..... |
| ..... | ..... | ..... |
| ลงชื่อ..... | ลงชื่อ..... | ลงชื่อ..... ผู้ให้บริการ |
| (.....) | (.....) | (.....) |
| ผอ. สำนัก/ศูนย์/สทข./กลุ่มงานขึ้นตรง | ผอ. ศูนย์สารสนเทศทรัพยากรธรณี | วันที่...../...../..... |

**** หมายเหตุ แนบสำเนาบัตรข้าราชการ หรือสำเนาบัตรประชาชนของผู้ขอใช้บริการ พร้อมสำเนาถูกต้อง**

**ผลการให้บริการ** *(เจ้าหน้าที่ ผู้ดูแลเครือข่าย/ผู้ดูแลระบบงาน เป็นผู้กรอกข้อมูลในส่วนนี้)*

**ผลการดำเนินงาน**

Username.....

Password.....

Expire Date.....

# แบบฟอร์มการขอใช้บริการ Authentication Authorization Accounting ของบุคลากร / บุคลากรภายนอกหน่วยงานภายนอก

**ข้อมูลหน่วยงาน**

ชื่อหน่วยงาน สำนัก/ศูนย์/สนข./กลุ่มงานขึ้นตรง (ภาษาไทย).....

**ข้อมูลของผู้ขอใช้บริการ** *( ผู้ขอใช้บริการเป็นผู้กรอกข้อมูลส่วนนี้ )*

ชื่อ – สกุล (ภาษาไทย).....

Name (ชื่อ) ..... Surname (นามสกุล) .....

e-mail.....

เลขที่บัตรประชาชน ☐-☐☐☐☐-☐☐☐☐☐-☐☐-☐ วัน-เดือน-ปีเกิด ☐☐-☐☐-☐☐☐☐

ตำแหน่ง.....สังกัด/ส่วน/แผนก/ฝ่าย.....

หมายเลขโทรศัพท์.....หมายเลขมือถือ.....

**ประเภทของผู้รับบริการ**

☐ ข้าราชการ ☐ ลูกจ้างประจำ ☐ พนักงานราชการ

☐ พนักงานจ้างเหมาบริการ ☐ อื่นๆ (โปรดระบุ).....

ข้าพเจ้ามีความประสงค์ ขอใช้บริการ Authentication Authorization Accounting ของบุคลากร / บุคลากรภายนอกหน่วยงาน ภายใต้เครือข่ายของกรมทรัพยากรธรณี โดยข้าพเจ้าจะปฏิบัติตาม พระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และระเบียบอื่นๆ ที่กรมทรัพยากรธรณีกำหนด อย่างเคร่งครัด

ลงชื่อผู้ขอใช้บริการ.....

วันที่...../...../.....

| ความคิดเห็นผู้บังคับบัญชา *(ผู้ขอใช้บริการ)* | เพื่อโปรดพิจารณา |
|---|---|
| ..... | ..... |
| ..... | ..... |
| ลงชื่อ..... | ลงชื่อ..... ผู้ให้บริการ |
| (.....) | (.....) |
| ผอ. สำนัก/ศูนย์/สทข./กลุ่มงานขึ้นตรง | วันที่...../...../..... |

**** หมายเหตุ แนบสำเนาบัตรข้าราชการ หรือสำบัตรประชาชนของผู้ขอใช้บริการ พร้อมสำเนาถูกต้อง**

# ระเบียบการใช้บริการระบบเครือข่ายอินเตอร์เน็ต กรมทรัพยากรธรณี

1. อินเตอร์เน็ต กรมทรัพยากรธรณีมีจุดประสงค์เพื่ออำนวยความสะดวกในการติดต่อสื่อสาร โดยข้าพเจ้าสัญญาว่าจะไม่รับส่งข่าวที่เป็นความลับของทางราชการหรือในทางที่ผิดกฎหมาย ซึ่งได้แก่ เอกสารสิทธิ์ เอกสาร ซึ่งทางการตีความว่าเป็นการข่มขู่ หรือลามกอนาจารฯลฯ ข้าพเจ้ารับรองว่าหากมีการกล่าวหาว่ากระทำ หรือถูกกระทำ สิ่งที่เข้าข่ายผิดกฎหมาย ข้าพเจ้าขอรับผิดชอบแต่เพียงผู้เดียว

2. ข้าพเจ้าสัญญาว่าจะปฏิบัติตามเงื่อนไข กฎระเบียบ มารยาท (Rules and Regulations/Etiquette) ที่อินเตอร์เน็ต กรมทรัพยากรธรณี กำหนดขึ้นและที่กำหนดต่อไปในอนาคต กรมทรัพยากรธรณี มีสิทธิ์จะระงับการใช้งานของผู้ที่ละเมิดหรือพยายามละเมิดเงื่อนไข กฎเกณฑ์และมารยาทการใช้บริการคอมพิวเตอร์ได้ โดยไม่ต้องตักเตือนล่วงหน้า

3. ไม่อนุญาตให้ทำการค้าใด ๆ ผ่านระบบเครือข่ายและระบบคอมพิวเตอร์ การแจ้งความจำหน่ายซื้อสินค้า การนำข้อมูลไปขายต่อ และการเปิดบริการอินเตอร์เน็ตแก่บุคคลทั่วไป เพื่อแสวงหาผลกำไร ถือว่าเป็นการละเมิดขอบเขตบริการอินเตอร์เน็ต

4. ข้าพเจ้าจะไม่ละเมิดความเป็นส่วนตัวของผู้อื่น กล่าวคือ ไม่อ่านข้อความส่วนตัวของผู้อื่น ไม่ว่าข้อความนั้นจะใช้ระบบความปลอดภัยของแฟ้มข้อมูลป้องกันไว้หรือไม่ก็ตาม นอกจากนั้นการเผยแพร่ข้อความส่วนตัวที่ผู้อื่นส่งมากระจายออกไปในวงกว้าง โดยไม่ได้รับอนุญาตจากผู้เขียน การใช้ภาษาไม่สุภาพ การเขียนข้อความที่ทำให้ผู้อื่นเสียหายออกไปเผยแพร่ในที่สาธารณะ เช่น world wide web (www.) หรือ mail หรือ การแพร่ข้อความ ล้วนแล้วแต่เป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น หากมีปัญหาทางด้านความประพฤติเสื่อมเสียจากข้าพเจ้า ข้าพเจ้าจะยอมรับว่าเป็นความรับผิดชอบ

5. ข้าพเจ้าจะไม่บุกรุก ระบบคอมพิวเตอร์อื่นๆ และเครือข่ายอินเตอร์เน็ตอื่นๆ ทั้งในและต่างประเทศที่ไม่อนุญาตให้บุคคลภายนอกเข้าไปใช้งาน

6. ข้าพเจ้าสัญญาว่าจะรักษาความลับ password ของตนเป็นอย่างดี ไม่ปล่อยปละละเลยให้บุคคลภายนอกใช้ password ของข้าพเจ้า

7. กรมทรัพยากรธรณี จะไม่ควบคุมเนื้อหาของข้อมูลข่าวสารที่ผ่านเข้าออกอินเตอร์เน็ต กรมทรัพยากรธรณี แต่อย่างใด และอินเตอร์เน็ต กรมทรัพยากรธรณี จะไม่รับประกันในคุณภาพของการรับ – ส่งข้อมูลข่าวสารและ down – time ของระบบบางส่วนหรือทั้งหมด และไม่รับผิดชอบในความเสียหายของข้าพเจ้าอันเนื่องมาจากวงจรสื่อสารชำรุด ความล่าช้าของการจราจรบนเครือข่าย หรือจดหมายไม่ถึงปลายทาง ส่งผิดสถานที่ เกิดความผิดพลาดในข้อมูล หรือความเสียหายอันเกิดจากการละเมิดโดยข้าพเจ้าอื่นๆ

8. ห้ามใช้อินเตอร์เน็ต กรมทรัพยากรธรณี ไปกระทำการใด ๆ ที่เข้าข่ายผิดกฎหมาย และหากมีการกระทำผิดกฎหมายดังกล่าว ข้าพเจ้าจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว โดยจะเอาผิดกับ กรมทรัพยากรธรณี ไม่ได้ทั้งสิ้น

**ข้าพเจ้าขอรับรองว่าจะปฏิบัติตามระเบียบข้อบังคับการใช้บริการที่มีอยู่แล้ว และที่จะมีต่อไปโดยเคร่งครัด ทุกประการ**

ลงชื่อ.....

(.....)

วันที่...../...../.....

**ผลการให้บริการ** *(เจ้าหน้าที่ ผู้ดูแลเครือข่าย/ผู้ดูแลระบบงาน เป็นผู้กรอกข้อมูลในส่วนนี้)*

**ผลการดำเนินงาน**

Username.....

Password.....

Expire Date.....