ประกาศกรมทรัพยากรน้ำบาดาล
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมทรัพยากรน้ำบาดาล พ.ศ.๒๕๕๘

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และเพื่อให้ระบบเทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลของกรมทรัพยากรน้ำบาดาลเป็นไปอย่างมีประสิทธิภาพ เหมาะสม มีความมั่นคงปลอดภัย และสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ กรมทรัพยากรน้ำบาดาลจึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ ตามประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศกรมทรัพยากรน้ำบาดาล เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำบาดาล พ.ศ.๒๕๕๘”

ข้อ ๒ วัตถุประสงค์

๒.๑ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมทรัพยากรน้ำบาดาล ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๒ เพื่อให้เกิดความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรมทรัพยากรน้ำบาดาล ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมทรัพยากรน้ำบาดาล ได้รับทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

ข้อ ๓ ขอบเขตการดำเนินงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำบาดาล มีขอบเขตครอบคลุม ดังนี้

๓.๑ การควบคุมการเข้าถึงและการใช้งานสารสนเทศ

๓.๑.๑ การควบคุมการเข้าถึงระบบสารสนเทศ

๓.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

๓.๑.๓ การควบคุมการเข้าถึงระบบเครือข่าย

/ ๓.๑.๔ การบริหาร...

๓.๑.๔ การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๓.๑.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๓.๒ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๔ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๔ การกำหนดความรับผิดชอบ

๔.๑ ระดับนโยบาย

กำหนดให้ผู้บริหารระดับสูงสุด (CEO) ของกรมทรัพยากรน้ำบาดาลเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) กรมทรัพยากรน้ำบาดาลเป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำบาดาล

กำหนดให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลเป็นผู้รับผิดชอบติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษากับเจ้าหน้าที่ในการปฏิบัติงาน

๔.๒ ระดับปฏิบัติการ

๔.๒.๑ นโยบายการควบคุมการเข้าถึงและการใช้งานสารสนเทศ ผู้รับผิดชอบ ได้แก่

๔.๒.๑.๑ ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๔.๒.๑.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๑.๓ เจ้าหน้าที่ที่ได้รับมอบหมาย

๔.๒.๑.๔ ผู้ใช้งาน

๔.๒.๒ นโยบายการจัดทำระบบสำรองของระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

๔.๒.๒.๑ ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๔.๒.๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๒.๓ เจ้าหน้าที่ที่ได้รับมอบหมาย

๔.๒.๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

๔.๒.๓.๑ ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๔.๒.๓.๒ ผู้ตรวจสอบภายใน

/ ๔.๒.๓.๓ ผู้ดูแล...

๔.๒.๓.๓ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๔ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

๔.๒.๔.๑ ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๔.๒.๔.๒ ส่วนบริหารทรัพยากรบุคคล สำนักบริหารกลาง

๔.๒.๔.๓ หน่วยงานที่ได้รับมอบหมายในการฝึกอบรม

๔.๒.๔.๔ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๔.๕ เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อ ๕ ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมถึงทบทวนปรับปรุงนโยบายและข้อปฏิบัติอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรน้ำบาดาล โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ เรื่อง “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำบาดาล พ.ศ.๒๕๕๘” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง การปฏิบัติตามประกาศกรมทรัพยากรน้ำบาดาลเรื่องแนวนโยบายนี้ ให้เป็นไปตามเอกสารแนบท้ายประกาศ ซึ่งเจ้าหน้าที่ของกรมทรัพยากรน้ำบาดาล และหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๐ กันยายน พ.ศ.๒๕๕๘

(นางสาวสุทธิลักษณ์ ระวิวรรณ)
อธิบดีกรมทรัพยากรน้ำบาดาล

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมทรัพยากรน้ำบาดาล (Information Security Policy)

๑. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรน้ำบาดาล หรือต่อไปนี้เรียกว่า "องค์กร" เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุมคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์กรและหน่วยงานในสังกัด อีกทั้งเป็นการดำเนินงานตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินงานใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ องค์กรจึงต้องกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุมคามต่าง ๆ โดยมีวัตถุประสงค์ ดังนี้

๑.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ เพื่อให้องค์กรมีการกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ Annex A และศึกษารายละเอียดวิธีปฏิบัติทางเทคนิคจาก ISO/IEC ๑๗๗๙๙:๒๐๐๕ รวมทั้งมีการปรับปรุงอย่างต่อเนื่อง

๑.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๕ การกำหนดความรับผิดชอบ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศขององค์กร (CIO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

๑.๖ นโยบายนี้ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลา ๑ ครั้งต่อปี

๒. องค์ประกอบของนโยบาย

๒.๑ ส่วนที่ ๑ นโยบายการควบคุมการเข้าถึงและการใช้งานสารสนเทศ

๒.๒.๑ การควบคุมการเข้าถึงระบบสารสนเทศ

๒.๒.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

๒.๒.๓ การควบคุมการเข้าถึงระบบเครือข่าย

๒.๒.๔ การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๒.๒.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ

๒.๒.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๒.๒ ส่วนที่ ๒ นโยบายการจัดทำระบบสำรองของระบบสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

๒.๒.๑ การคัดเลือกและจัดทำระบบสำรอง

๒.๒.๒ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒.๒.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

๒.๒.๔ การทดสอบสภาพพร้อมใช้งาน

๒.๒.๕ ระยะความถี่ของการปฏิบัติ

๒.๓ ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยง

๒.๔ ส่วนที่ ๔ นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๕ คำนิยาม

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำบาดาลแต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ ผู้รับผิดชอบ ข้อปฏิบัติ ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน สินทรัพย์ บุคลากรขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัด

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมทรัพยากรน้ำบาดาล พ.ศ.๒๕๕๘

ส่วนที่ ๑
นโยบายการควบคุมการเข้าถึงและการใช้งานสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างถูกต้อง

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย
๔. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เวอร์ชั่น ๒.๕

ข้อปฏิบัติ

๑. การควบคุมการเข้าถึงระบบสารสนเทศ

เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลให้มีความมั่นคงปลอดภัย มีข้อปฏิบัติ ดังนี้

๑.๑ จัดทำบัญชีสินทรัพย์หรือทะเบียนสินทรัพย์ โดยจำแนกกลุ่มทรัพยากรระบบ การทำงาน และสถานที่เก็บหรือประมวลผล และระบุสิทธิในการเข้าถึงสินทรัพย์นั้น

๑.๒ กำหนดสิทธิของผู้ใช้งาน ดังนี้

๑.๒.๑ กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งานแต่ละกลุ่ม ได้แก่

๑.๒.๑.๑ สิทธิอ่านอย่างเดียว
๑.๒.๑.๒ สิทธิการเพิ่มข้อมูล
๑.๒.๑.๓ สิทธิการแก้ไขข้อมูล
๑.๒.๑.๔ สิทธิการลบข้อมูล
๑.๒.๑.๕ สิทธิการอนุมัติ/อนุญาต
๑.๒.๑.๖ ไม่มีสิทธิ

๑.๒.๒ กำหนดการระงับสิทธิ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงข้อมูลสารสนเทศและระบบสารสนเทศของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมายตามแบบลงทะเบียนผู้ใช้งาน

๑.๓ กำหนดประเภทข้อมูล ลำดับชั้นความลับ ความสำคัญ เวลา และช่องที่เข้าถึง ดังนี้

๑.๓.๑ จัดแบ่งประเภทข้อมูลออกเป็น

๑.๓.๑.๑ ข้อมูลด้านการบริหาร ได้แก่

๑.๓.๑.๑.๑ นโยบาย

๑.๓.๑.๑.๒ ข้อมูลยุทธศาสตร์

๑.๓.๑.๑.๓ คำรับรองการปฏิบัติราชการ

๑.๓.๑.๑.๔ ข้อมูลบุคลากร

๑.๓.๑.๑.๕ งบประมาณ

๑.๓.๑.๑.๖ การเงินและบัญชี

๑.๓.๑.๒ ข้อมูลด้านการดำเนินงาน ได้แก่

๑.๓.๑.๒.๑ การดำเนินงานตามภารกิจกรมทรัพยากรน้ำบาดาล

๑.๓.๑.๒.๒ กฎหมาย ระเบียบ

๑.๓.๑.๒.๓ การใช้จ่ายงบประมาณ

๑.๓.๑.๒.๔ ผลการปฏิบัติงาน

๑.๓.๑.๓ ข้อมูลด้านการให้บริการ ได้แก่

๑.๓.๑.๓.๑ ข้อมูลสถิติกรมทรัพยากรน้ำบาดาล

๑.๓.๑.๓.๒ ข้อมูลวิชาการและองค์ความรู้ด้านทรัพยากรน้ำบาดาล

๑.๓.๑.๓.๓ ข้อมูลบ่อน้ำบาดาล

๑.๓.๒ จัดแบ่งลำดับชั้นความลับของข้อมูลแต่ละประเภทตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ.๒๕๔๔ เป็น ๓ ชั้น คือ

๑.๓.๒.๑ ลับที่สุด หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๑.๓.๒.๒ ลับมาก หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๑.๓.๒.๓ ลับ หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๑.๓.๓ จัดแบ่งระดับความสำคัญของข้อมูลแต่ละประเภท เป็น ๔ ระดับ คือ

๑.๓.๓.๑ สำคัญมากที่สุด

๑.๓.๓.๒ สำคัญมาก

๑.๓.๓.๓ สำคัญ

๑.๓.๓.๔ ทั่วไป

๑.๓.๔ จัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภท

๑.๓.๔.๑ ข้อมูลทั่วไปสามารถเข้าถึงได้ทุกกลุ่มผู้ใช้งานที่กำหนดไว้

๑.๓.๔.๒ ฐานข้อมูลทรัพยากรน้ำบาดาลสามารถเข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง

๑.๓.๔.๓ ระบบข้อมูลทรัพยากรน้ำบาดาลสามารถเข้าถึงได้เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิ

๑.๓.๔.๔ ระบบเทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลสามารถเข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ

๑.๓.๕ กำหนดช่องทางในการเข้าถึงข้อมูล

๑.๓.๕.๑ เครือข่ายภายใน (LAN)

๑.๓.๕.๒ อินทราเน็ต (Intranet)

๑.๓.๕.๓ อินเตอร์เน็ต (Internet)

๑.๓.๕.๔ จดหมายอิเล็กทรอนิกส์ (e-mail)

๑.๓.๖ กำหนดเวลาและจำนวนระยะเวลาในการเข้าถึงข้อมูล

๑.๓.๖.๑ เวลาราชการ (๐๘.๓๐-๑๖.๓๐ น.)

๑.๓.๖.๒ นอกเวลาราชการ

๑.๓.๖.๓ ช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

๑.๓.๖.๔ ช่วงเวลาพิเศษเป็นรายครั้ง

๑.๔ กำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ ดังนี้

๑.๔.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

๑.๔.๒ เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น

๑.๔.๓ ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งาน โดยต้องมีการจัดทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ

๑.๕ กำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

๑.๕.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๑.๕.๒ มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ การสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดมาตรการเชิงป้องกัน ดังนี้

๒.๑.๑ มีการเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ใช้งานได้รับทราบ

๒.๑.๒ มีการฝึกอบรมหลักสูตรเพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศให้ทราบถึงภัยและผลกระทบจากการใช้เทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

๒.๒ การลงทะเบียนผู้ใช้งาน (User Registration)

๒.๒.๑ การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๒.๑.๑ เจ้าหน้าที่ใหม่ขององค์กรกรอกข้อมูลคำขอใช้บริการลงแบบฟอร์มลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๒.๑.๒ ส่งคำแบบลงทะเบียนผู้ใช้งานเพื่อขอใช้อินเตอร์เน็ต ระบบอีเมล์ หรือระบบงานต่าง ๆ เพื่อขอใช้บริการให้กับศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๒.๒.๑.๓ ยื่นคำขอกับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล หรือเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลผู้ที่ได้รับมอบหมาย

๒.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

๒.๓.๑ การให้สิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๓.๑.๑ ผู้ดูแลระบบตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมด พร้อมทั้งต้องมีลายเซ็นของผู้ขอเข้าใช้งานระบบ ลายเซ็นของบุคคลผู้มีสิทธิอนุญาตในการลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๓.๑.๒ ผู้ดูแลระบบตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน

๒.๓.๑.๓ ผู้ดูแลระบบให้สิทธิการใช้งานระบบตามคำขอในแบบฟอร์ม

๒.๓.๒ การแจ้งยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๓.๒.๑ หัวหน้างานหรือผู้บังคับบัญชา กรอกข้อมูลลงในแบบฟอร์ม และยื่นคำขอกับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๒.๓.๒.๒ ผู้ดูแลระบบยกเลิกสิทธิการใช้งานระบบตามคำขอในแบบฟอร์ม และลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

๒.๓.๓ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบ จากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๓.๔ ผู้ใช้ ต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

๒.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๒.๔.๑ ผู้ดูแลระบบต้องกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ

๒.๔.๒ ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยพิจารณาจากลำดับชั้นความลับของข้อมูล หรือความสำคัญตามภารกิจ และรหัสผ่านที่กำหนดใหม่ ต้องไม่ซ้ำกับรหัสผ่านเดิม

๒.๔.๓ ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ต้องเปลี่ยนรหัสผ่านที่ได้รับ โดยทันที

๒.๔.๔ ผู้ใช้งานต้องกำหนดรหัสผ่านและเปลี่ยนรหัสผ่านของตนเองในการใช้งานตามหลักเกณฑ์ ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๒.๔.๕ ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ และระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใด ๆ ทั้งสิ้น เว้นแต่ กรณี

ผู้ใช้งานที่มีอำนาจอนุมัติใด ๆ ในระบบเทคโนโลยีสารสนเทศไม่สามารถปฏิบัติราชการอันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าวเพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้วให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

๒.๔.๖ กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

๒.๔.๗ ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน “abcdef” “aaaaaa” “๑๒๓๔๕”

๒.๔.๘ ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

๒.๔.๙ ไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

๒.๔.๑๐ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๓ ครั้ง

๒.๔.๑๑ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์

๒.๔.๑๒ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

๒.๔.๑๓ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๒.๔.๑๔ ในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลต้องเปลี่ยนรหัสผ่านทันที

๒.๔.๑๕ เมื่อมีปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ติดต่อผู้ดูแลระบบ เช่น ลืมชื่อผู้ใช้งานหรือรหัสผ่าน

๒.๔.๑๖ การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย โดยใส่ซองปิดผนึกและประทับตรา“ลับ” และส่งไปยังผู้ใช้งาน รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

๒.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

๒.๕.๑ สิทธิการเข้าถึงข้อมูลของผู้ใช้ต้องได้รับการพิจารณาทบทวนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดทุก ๆ ๖ เดือน และทุกครั้งที่มีการย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง

๒.๕.๒ สิทธิการเข้าถึงข้อมูลต้องได้รับการทบทวนและจัดสรรใหม่เมื่อมีการเคลื่อนย้ายบุคลากรภายในองค์กร

๒.๕.๓ การให้อำนาจสำหรับสิทธิการเข้าถึงพิเศษ ต้องมีการทบทวนทุก ๓ เดือน

๒.๕.๔ การจัดสรรสิทธิพิเศษต้องได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดเพื่อให้มั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้ที่ไม่ได้รับมอบอำนาจ

๒.๕.๕ ความเปลี่ยนแปลงของผู้ใช้ที่ได้รับสิทธิพิเศษต้องถูกบันทึกเพื่อการทบทวน

๒.๖ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยการล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๒.๖.๑ การใช้งานรหัสผ่าน

๒.๖.๑.๑ เก็บรหัสผ่านไว้เป็นความลับ

๒.๖.๑.๒ หลีกเลี่ยงการบันทึกรหัสผ่าน (เช่น บันทึกลงในกระดาษ ในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่าง ๆ) นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัยและวิธีการในการบันทึกได้รับการอนุมัติแล้ว

๒.๖.๑.๓ เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้

๒.๖.๑.๔ กำหนดรหัสผ่านที่มีคุณภาพและมีความยาวเพียงพอ สำหรับ

๒.๖.๑.๔.๑ ง่ายสำหรับจดจำ

๒.๖.๑.๔.๒ ไม่อยู่บนพื้นฐานของสิ่งที่คนอื่นสามารถคาดเดาได้ง่ายหรือสามารถหาได้จากข้อมูลเกี่ยวกับตน เช่น ชื่อ หมายเลขโทรศัพท์ และวันเกิด เป็นต้น

๒.๖.๑.๔.๓ ไม่สร้างจุดอ่อนโดยใช้คำที่อยู่ในพจนานุกรม

๒.๖.๑.๔.๔ ไม่มีคำซ้ำหรือตัวอักษรซ้ำ ไม่เป็นตัวเลขทั้งหมด หรือไม่เป็นตัวอักษรทั้งหมด

๒.๖.๑.๕ เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้ที่ได้สิทธิพิเศษต้องได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) และหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยใช้แล้ว

๒.๖.๑.๖ กำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

๒.๖.๑.๗ ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ

๒.๖.๑.๘ ไม่ใช้รหัสผ่านรวมกับผู้อื่น

๒.๖.๑.๙ ไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงานและในกรณีใช้สวนตัว

๒.๖.๑.๑๐ ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว แนะนำให้ใช้รหัสผ่านเดียวกันที่มีคุณภาพข้างต้น สำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นต้องมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

๒.๖.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๒.๖.๒.๑ ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์พกพา โดยทันทีเมื่อเสร็จสิ้นงาน

๒.๖.๒.๒ ผู้ใช้งาน ต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๒.๖.๒.๓ ผู้ดูแลระบบ ต้องกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

๒.๖.๒.๔ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล๊อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๖.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศหรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศ

๒.๖.๓.๑ การจัดการสภาพแวดล้อมทางกายภาพ

๒.๖.๓.๑.๑ จำแนกและกำหนดพื้นที่การใช้งานและระดับความสำคัญของระบบเทคโนโลยีสารสนเทศ

๒.๖.๓.๑.๒ มีระบบป้องกันการบุกรุกติดตั้งครอบคลุมพื้นที่ที่มีความสำคัญ

๒.๖.๓.๑.๓ มีระบบรักษาความปลอดภัย โดยมีพนักงานรักษาความปลอดภัยดูแลอาคาร และมีการติดตั้งกล้องวงจรปิดเพื่อบันทึกเหตุการณ์ไว้ใช้ในการตรวจสอบภายหลัง

๒.๖.๓.๑.๔ บุคลากรที่ปฏิบัติงานในพื้นที่ต้องปิดล็อกประตูและหน้าต่างทุกครั้งหลังเลิกงาน

๒.๖.๓.๑.๕ ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพว่าใช้งานได้ตามปกติอย่างสม่ำเสมอ

๒.๖.๓.๒ การควบคุมการเข้าออกพื้นที่ใช้งาน

๒.๖.๓.๒.๑ จัดทำบันทึกการเข้า-ออกพื้นที่ใช้งานสำหรับบุคคลภายนอกหรือผู้มาติดต่อ

๒.๖.๓.๒.๒ มีเจ้าหน้าที่ดูแลบุคคลภายนอกหรือผู้มาติดต่อในพื้นที่ที่มีความสำคัญทุกครั้งจนเสร็จสิ้นภารกิจ

๒.๖.๓.๒.๓ กรณีบุคคลภายนอกหรือผู้มาติดต่อต้องการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเข้ามาในบริเวณพื้นที่ใช้งาน ต้องบันทึกแบบฟอร์มการเข้า-ออกในรายการอุปกรณ์ด้วยทุกครั้ง

๒.๖.๓.๒.๔ มีการควบคุมการเข้าออกสถานที่ตั้งของระบบเทคโนโลยีสารสนเทศอย่างรัดกุม และอนุญาตให้เฉพาะผู้มีสิทธิและความจำเป็นผ่านเข้าถึงพื้นที่ได้เท่านั้น

๒.๖.๓.๒.๕ กรณีที่ต้องการนำทรัพย์สินสารสนเทศออกจากพื้นที่ใช้งานต้องขออนุมัติจากผู้บังคับบัญชาก่อนทุกครั้ง

๒.๖.๓.๒.๖ จัดให้มีการทบทวนสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๒.๖.๓.๓ การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

๒.๖.๓.๓.๑ จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๖.๓.๓.๒ จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๒.๖.๓.๓.๓ จัดพื้นที่หรือบริเวณส่งมอบไว้ต่างหาก เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายในองค์กร

๒.๖.๓.๓.๔ ต้องตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนจะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

๒.๖.๓.๓.๕ ต้องลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอก ให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินขององค์กร

๒.๖.๓.๔ การจัดวางและป้องกันอุปกรณ์

๒.๖.๓.๔.๑ ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของระบบเทคโนโลยีสารสนเทศน้อยที่สุด

๒.๖.๓.๔.๒ ต้องแยกอุปกรณ์ที่มีความสำคัญเก็บไว้ในที่ที่มีความปลอดภัย

๒.๖.๓.๔.๓ ไม่นำอาหารและเครื่องดื่มเข้ามาในบริเวณพื้นที่ของระบบเทคโนโลยีสารสนเทศ

๒.๖.๓.๔.๔ ดำเนินการตรวจสอบ ดูแลสภาพแวดล้อม อุณหภูมิความชื้นภายในบริเวณพื้นที่ของระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายต่ออุปกรณ์ภายในบริเวณพื้นที่จัดวางอุปกรณ์

๒.๖.๓.๔.๕ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศขององค์กรอย่างเพียงพอ ได้แก่กระแสไฟฟ้าสำรองและป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการเกิดกระแสไฟฟ้าผิดปกติ ระบบปรับอากาศ ระบบระบายอากาศ และระบบควบคุมความชื้น

๒.๖.๓.๔.๖ ต้องตรวจสอบหรือทดสอบการทำงานของระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ และลดความเสี่ยงจากการทำงานของระบบล้มเหลว

๒.๖.๓.๕ การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและทรัพย์สินอื่น ๆ

๒.๖.๓.๕.๑ ผู้ใช้งานต้องระมัดระวัง และดูแลทรัพย์สินขององค์กรที่ตนเองใช้งาน หรือถือครองเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหาย หรือเสียหายโดยประมาทเลินเล่อ ผู้ใช้งานต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

๒.๖.๓.๕.๒ ผู้ใช้งานต้องเก็บเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลสำคัญไว้ในที่ปลอดภัย เช่น ในตู้หรือโต๊ะที่สามารถล็อกได้ และแยกเอกสารสำคัญสำหรับทำลายไว้ เพื่อความปลอดภัยของทรัพย์สินราชการ

๒.๖.๓.๕.๓ นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๒.๖.๓.๕.๔ ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารต่าง ๆ โดยไม่ได้รับอนุญาต

๒.๖.๓.๖ มาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์

๒.๖.๓.๖.๑ ต้องทำการล้างข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนการส่งซ่อมหรือเปลี่ยนอุปกรณ์

๒.๖.๓.๖.๒ ต้องทำการลบข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนทำการทำลายหรือจำหน่าย

๒.๖.๓.๖.๓ ต้องทำการฟอร์แมตฮาร์ดดิสก์ เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์ โดยใช้วิธีแบบเขียนทับซ้ำจำนวน ๑ ครั้ง ตามมาตรฐาน NIST ๘๐๐-๘๘ สำหรับข้อมูลที่เป็นชั้นความลับที่ไม่ลับมาก เขียนทับซ้ำจำนวน ๓ ครั้ง ตามมาตรฐาน DoD ๕๒๒๐.๒๒-M สำหรับข้อมูลที่มีชั้นความลับเป็นลับมาก และเขียนทับซ้ำจำนวน ๗ ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลที่มีชั้นความลับเป็นลับมากที่สุด

๒.๖.๓.๖.๔ ลบข้อมูลการดำเนินงานที่มีอายุตั้งแต่ ๕ ปีขึ้นไปออกจากฐานข้อมูล และสำรองข้อมูลโดยการจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๒.๖.๓.๖.๕ ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาในการทำลายสื่อบันทึกข้อมูล และเจ้าของข้อมูลในการลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

๒.๖.๓.๗ การรักษาความลับข้อมูล

๒.๖.๓.๗.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและผ่านระบบงานสารสนเทศ

๒.๖.๓.๗.๒ การรับส่งข้อมูลที่เป็นความลับหรือข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption

๒.๖.๓.๗.๓ ผู้ใช้งานสามารถนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

๒.๖.๓.๗.๔ กำหนดรหัสผ่านในการเข้าถึงไฟล์ข้อมูลลับ เพื่อป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ใช้งาน

๒.๖.๓.๗.๕ ไม่แชร์ไฟล์ข้อมูลลับบนเครือข่าย เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

๒.๖.๓.๗.๖ ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัส และติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องอย่างสม่ำเสมอ

๒.๖.๔ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๒.๖.๔.๑ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ระยะเวลาในการเข้าถึง ช่องทางในการเข้าถึง รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๒.๖.๔.๑.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน

๒.๖.๔.๑.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๖.๔.๑.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๖.๔.๑.๔ การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล SSL VPN หรือ XML Encryption เป็นต้น

๒.๖.๔.๑.๕ ต้องกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๖.๔.๑.๖ ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน ต้องส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๒.๖.๔.๒ ผู้ใช้ต้องนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๒.๖.๔.๓ เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลอย่างน้อยปีละ ๔ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๓. การควบคุมการเข้าถึงระบบเครือข่าย

๓.๑ การใช้งานบริการเครือข่าย

๓.๑.๑ ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดี แห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่า อยู่นอกเหนือ ความรับผิดชอบขององค์กร

๓.๑.๒ องค์กรไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความการซื้อ หรือการจำหน่ายสินค้าการนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๓.๑.๓ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว องค์กรไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๓.๑.๔ ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

๓.๑.๕ องค์กรให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๓.๑.๖ บัญชีผู้ใช้งาน (User Account) ที่องค์กรให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๑.๗ กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓.๑.๘ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๓.๑.๙ ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง ในระหว่างปฏิบัติงาน

๓.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน

จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

๓.๒.๑ ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

๓.๒.๒ ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง การใช้รหัสผ่าน (Password) ที่ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลกำหนดขึ้นมาให้

๓.๒.๓ ต้องมีการตรวจสอบผู้ใช้งานเมื่อมีเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต

๓.๓ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่องค์กรมีแนวทางปฏิบัติดังนี้

๓.๓.๑ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิบุคคลในการเข้า-ออกห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

๓.๓.๒ สิทธิในการเข้า-ออกห้องต่าง ๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่าย เป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายห้องควบคุมระบบเครือข่าย

๓.๓.๓ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

๓.๔ ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติดังนี้

๓.๔.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร“แบบฟอร์มการเข้า-ออกพื้นที่”

๓.๔.๒ ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร มาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า-ออก ตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน

๓.๔.๓ เจ้าหน้าที่ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน

๓.๕ การระบุอุปกรณ์บนเครือข่าย

๓.๕.๑ ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

๓.๕.๒ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

๓.๕.๓ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๓.๖ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๓.๖.๑ ผู้ดูแลระบบต้องกำหนดการเปิด–ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๓.๖.๒ บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องควบคุมระบบเครือข่าย/ระบบคอมพิวเตอร์ จะต้องลงชื่อเข้า-ออกใน “แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้องและได้รับการอนุมัติจากหัวหน้ากลุ่มระบบคอมพิวเตอร์และการสื่อสารก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

๓.๖.๓ บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

๓.๖.๔ ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๓.๗ การแบ่งแยกเครือข่าย

๓.๗.๑ องค์กรต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๓ กลุ่ม คือ กลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน กลุ่มของระบบสารสนเทศ

๓.๗.๒ องค์กรแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

๓.๗.๓ องค์กรจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ

๓.๗.๔ องค์กรติดตั้ง Firewall เพื่อป้องกันทางเข้าเครือข่ายจากผู้ไม่หวังดี

๓.๘ การควบคุมการเชื่อมต่อทางเครือข่าย

ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

๓.๘.๑ มีการตรวจสอบการเชื่อมต่อเครือข่าย

๓.๘.๒ จำกัดสิทธิความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

๓.๘.๓ ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๓.๘.๔ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๓.๘.๕ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๓.๙ การควบคุมการจัดเส้นทางบนเครือข่าย

ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ ใช้งานตามภารกิจ ดังนี้

๓.๙.๑ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๓.๙.๒ กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๓.๙.๓ กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๔. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๔.๑ ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๔.๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

๔.๓ ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ Telnet Ftp หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติม

๔.๔ ต้องดำเนินการติดตั้งอัพเดตระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

๔.๕ ต้องมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๔.๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลเท่านั้น

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๕.๑ การเข้าใช้งานที่มั่นคงปลอดภัย

๕.๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๕.๑.๒ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๕.๑.๓ ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง

๕.๑.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๕.๑.๕ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๕.๑.๖ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๕.๑.๗ ซอฟต์แวร์ที่องค์กรใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

๕.๑.๘ ซอฟต์แวร์ที่องค์กรจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

๕.๑.๙ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นขององค์กรเพื่อประโยชน์ทางการค้า

๕.๑.๑๐ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๕.๑.๑๑ ห้ามผู้ใช้ระบบสารสนเทศขององค์กร เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๕.๒ การเข้าถึงระบบปฏิบัติการ ต้องแสดงวิธีการยืนยันตัวตน

๕.๒.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๕.๒.๒ ผู้ใช้ไม่ต้องอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๕.๒.๓ ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ต้อง Logout ออกจากเครื่องคอมพิวเตอร์ หรือล็อกหน้าจอด้วยโปรแกรม Screen Saver เมื่อไม่มีการใช้งานโดยตั้งเวลาประมาณ ๑๐ นาที

๕.๒.๔ มีการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศ เมื่อไม่มีการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

๕.๓ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) พิสูจน์ตัวบุคคลโดยใช้หมายเลขบัตรประชาชน ๑๓ หลัก เป็นตัวอ้างอิงในการขอใช้บริการ

๕.๓.๑ ผู้ใช้งานต้องทำการเขียนแบบฟอร์มขอใช้บริการอินเทอร์เน็ตผ่านเครือข่ายกรมทรัพยากรน้ำบาดาล และแนบสำเนาบัตรประจำตัวประชาชน เพื่อขอสิทธิการเข้าใช้บริการระบบอินเทอร์เน็ตภายในของกรมทรัพยากรน้ำบาดาล โดยใช้หมายเลขบัตรประชาชน ๑๓ หลักในการยืนยันตัวบุคคล และทางผู้ดูแลระบบจะดำเนินการแจ้ง Username และ Password เพื่อให้สามารถเข้าใช้งานระบบของกรมทรัพยากรน้ำบาดาลได้

๕.๓.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ เข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๕.๓.๓ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๕.๓.๔ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๕.๓.๕ ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชี ผู้ใช้บริการ (Account) ของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๕.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๕.๔.๑ ผู้ดูแลระบบต้องกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ

๕.๔.๒ ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยพิจารณาจากลำดับชั้นความลับของข้อมูล หรือความสำคัญตามภารกิจ และรหัสผ่านที่กำหนดใหม่ ต้องไม่ซ้ำกับรหัสผ่านเดิม

๕.๕ การใช้งานรหัสผ่าน

๕.๕.๑ ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ต้องเปลี่ยนรหัสผ่านที่ได้รับ โดยทันที

๕.๕.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านและเปลี่ยนรหัสผ่านของตนเองในการใช้งานตามหลักเกณฑ์ ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๕.๕.๓ ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ และระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใด ๆ ทั้งสิ้น เว้นแต่ กรณีผู้ใช้งานที่มีอำนาจอนุมัติใด ๆ ในระบบเทคโนโลยีสารสนเทศไม่สามารถปฏิบัติราชการอันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าวเพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้วให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

๕.๕.๔ กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

๕.๕.๕ ต้องกำหนดรหัสผ่านอย่างเป็นแบบแผน “abcdef” “aaaaaa” “๑๒๓๔๕”

๕.๕.๖ ต้องกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

๕.๕.๗ ต้องกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

๕.๕.๘ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๓ ครั้ง

๕.๕.๙ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์

๕.๕.๑๐ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

๕.๕.๑๑ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๕.๕.๑๒ ในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหล ต้องเปลี่ยนรหัสผ่านทันที

๕.๕.๑๓ เมื่อมีปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ติดต่อผู้ดูแลระบบ

๕.๕.๑๔ การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย โดยใส่ซองปิดผนึก และประทับตรา"ลับ" และส่งไปยังผู้ใช้งาน รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

๕.๖ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

๕.๖.๑ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมอรรถประโยชน์ ระดับสิทธิของผู้ขออนุมัติและการระบุและพิสูจน์ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

๕.๖.๒ ต้องจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน

๕.๖.๓ ต้องจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์

๕.๖.๔ ต้องยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงาน ที่ไม่มีความจำเป็น ในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรม อรรถประโยชน์ได้

๕.๖.๕ ตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบสารสนเทศอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบโดยไม่ได้รับอนุญาต

๕.๖.๖ ซอฟต์แวร์ที่ติดตั้งต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามผู้ใช้งาน คัดลอกซอฟต์แวร์ต่าง ๆ และนำไปติดตั้งหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๕.๗ การกำหนดเวลาเพื่อยุติการใช้งานระบบสารสนเทศ (Session Time-out)

๕.๗.๑ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการตัด และหมดเวลาการใช้งาน รวมถึงปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๐ นาที

๕.๗.๒ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรม การใช้งาน ช่วงระยะเวลา ๑๐ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

๕.๗.๓ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้น สำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๕.๘ การจำกัดเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

๕.๘.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ มีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับ การใช้งานระบบสารสนเทศแต่ละครั้งไม่เกิน ๓ ชั่วโมง โดยจะต้องระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ และหากไม่มีการใช้งานนานเกิน ๓๐ นาที ต้องยกเลิกการเชื่อมต่อระบบทันที

๕.๘.๒ กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูง และระบบงานที่มีการใช้งานในสถานที่ ที่มีความเสี่ยง ให้มีการจำกัดระยะเวลาเชื่อมต่อระบบน้อยลง

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Information Access Control)

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

๖.๑.๑ ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กร ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติ สำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน

๖.๑.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ ที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเตอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๖.๑.๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกินกว่า ๑๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Login เข้าระบบสารสนเทศอีกครั้ง

๖.๑.๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน ของบุคลากรดังต่อไปนี้

๖.๑.๔.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๖.๑.๔.๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มี การป้องกันในการส่งรหัสผ่าน (Password)

๖.๑.๔.๓ กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๖.๑.๔.๔ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๖.๑.๔.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๖.๑.๔.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๖.๑.๕ เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ องค์กรได้กำหนดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญที่องค์กรพัฒนาในรูปแบบของ Webbase Application โดยเข้าถึงได้ผ่านระบบเครือข่ายภายใน ซึ่งสามารถใช้งานได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายดังกล่าว

๖.๑.๖ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๖.๑.๖.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๖.๑.๖.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๖.๑.๖.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๖.๑.๖.๔ การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๖.๑.๖.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๖.๑.๖.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๖.๑.๖.๗ กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด

๖.๑.๗ การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (Outsourcing)

๖.๑.๗.๑ ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ โดยให้เจ้าหน้าที่ควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่กรมทรัพยากรน้ำบาดาล และให้เจ้าหน้าที่ตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ Remote Access และปิด Modem ทันทีที่การให้บริการเสร็จสิ้น

๖.๑.๗.๒ ต้องให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

๖.๑.๗.๓ ต้องกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข

๖.๑.๗.๔ ต้องมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ

๖.๑.๗.๕ ต้องให้ผู้ให้บริการลงนามรักษาความลับของกรมทรัพยากรน้ำบาดาลอย่างเคร่งครัด ผู้ให้บริการต้องไม่นำความลับทางราชการไปเผยแพร่ให้บุคคลภายนอกทราบ

๖.๒ การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

๖.๒.๑ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ ใช้งานได้ ๑ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงาน ของสำนักงานตามปกติเท่านั้น

๖.๒.๒ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกองค์กร) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๖.๒.๓ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศที่ต้องมีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุ และพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ ทุก ๆ ๑ ชั่วโมง

๖.๓ การจัดการกับระบบซึ่งไวต่อการรบกวน

๖.๓.๑ ข้อปฏิบัติ

๖.๓.๑.๑ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ได้แก่ ระบบ GFMIS หรือระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ เป็นระบบที่ใช้ในการปฏิบัติงานด้านการงบประมาณการบัญชี การจัดซื้อจัดจ้าง การเบิกจ่าย และการบริหารทรัพยากร ซึ่งดูแลรับผิดชอบโดยกรมบัญชีกลางจะได้รับการแยกออกจากระบบงานอื่นของกรมทรัพยากรน้ำบาดาล ต้องไม่สามารถเข้าถึงได้จากอุปกรณ์สื่อสารเคลื่อนที่

๖.๓.๑.๒ ระบบซึ่งไวต่อการรบกวน ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้นเข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว ต้องไม่สามารถปฏิบัติงานจากภายนอกองค์กรได้

๖.๔ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ เพื่อดูแลรักษาความปลอดภัยในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ดังนี้

๖.๔.๑ ข้อปฏิบัติ

๖.๔.๑.๑ เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ เป็นทรัพย์สินขององค์กร ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานขององค์กรเท่านั้น

๖.๔.๑.๒ โปรแกรมที่ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่องค์กรมีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้ง แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๖.๔.๑.๓ ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๖.๔.๑.๔ ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์และอุปกรณ์ และรักษาสภาพให้มีสภาพเดิมอยู่เสมอ

๖.๔.๑.๕ กรณีต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาหรืออุปกรณ์สื่อสารเคลื่อนที่ ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาหรืออุปกรณ์สื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่อาจเกิดจากการกระทบกระเทือน

๖.๔.๑.๖ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ซึ่งอาจทำให้เป็นรอยขีดข่วนหรือแตกเสียหาย

๖.๔.๑.๗ การเช็ดทำความสะอาดจอภาพ ต้องเช็ดอย่างถนอม และไปในทิศทางเดียวกัน ห้ามหมุนวน เนื่องจากจะทำให้หน้าจอเป็นรอยขีดข่วนได้

๖.๔.๑.๘ หากมีการนำเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ซึ่งไม่ใช่ทรัพย์สินขององค์กรมาใช้งานกับระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลก่อนการใช้งาน

๖.๔.๑.๙ การใช้อุปกรณ์สื่อสารเคลื่อนที่เข้าถึงระบบสารสนเทศขององค์กร ต้องผ่านการตรวจสอบสิทธิในการเข้าใช้ระบบจากศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลก่อน

๖.๕ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๖.๕.๑ ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๖.๕.๒ ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๖.๕.๓ ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร

๖.๕.๔ ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรในสถานที่ดังกล่าว

๖.๕.๕ ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร รวมทั้งมาตรการควบคุมการใช้เครือข่ายไร้สายที่บ้าน

๖.๕.๖ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่องค์กรต้องการ หากผ่านการตรวจสอบจึงจะสามารถเข้าถึงระบบสารสนเทศขององค์กรได้

๖.๕.๗ ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูลและอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

๖.๕.๘ องค์กรไม่อนุญาตให้ ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยองค์กร

๖.๕.๙ องค์กรต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกลชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

๖.๕.๑๐ องค์กรต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

๖.๖ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer Policy)

๖.๖.๑ เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้ต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร

๖.๖.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๖.๖.๓ ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคล ขององค์กร

๖.๖.๔ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ ขององค์กรเท่านั้น

๖.๖.๕ การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ ของศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลเท่านั้น

๖.๖.๖ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๖.๖.๗ ไม่เก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

๖.๖.๘ ไม่สร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์กร

๖.๖.๙ ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดยต้องปฏิบัติ ดังนี้

๖.๖.๙.๑ ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๖.๖.๙.๒ ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๖.๗ การปฏิบัติในการใช้รหัสผ่าน

๖.๗.๑ การใช้งานรหัสผ่าน

๖.๗.๑.๑ เก็บรหัสผ่านไว้เป็นความลับ

๖.๗.๑.๒ หลีกเลี่ยงการบันทึกรหัสผ่าน (เช่น บันทึกลงในกระดาษ ในแฟ้มข้อมูลหรือในอุปกรณ์พกพาต่าง ๆ) นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัยและวิธีการในการบันทึกได้รับการอนุมัติแล้ว

๖.๗.๑.๓ เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้

๖.๗.๑.๔ กำหนดรหัสผ่านที่มีคุณภาพและมีความยาวเพียงพอ สำหรับ

๖.๗.๑.๔.๑ ง่ายสำหรับจดจำ

๖.๗.๑.๔.๒ ไม่อยู่บนพื้นฐานของสิ่งที่คนอื่นสามารถคาดเดาได้ง่ายหรือสามารถหาได้จากข้อมูลเกี่ยวกับตน เช่น ชื่อ หมายเลขโทรศัพท์ และวันเกิด เป็นต้น

๖.๗.๑.๔.๓ ไม่สร้างจุดอ่อนโดยใช้คำที่อยู่ในพจนานุกรม

๖.๗.๑.๔.๔ ไม่มีคำซ้ำหรือตัวอักษรซ้ำ ไม่เป็นตัวเลขทั้งหมด หรือไม่เป็นตัวอักษรทั้งหมด

๖.๗.๑.๕ เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้ที่ได้สิทธิพิเศษต้องได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) และหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยใช้แล้ว

๖.๗.๑.๖ กำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

๖.๗.๑.๗ ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ

๖.๗.๑.๘ ไม่ใช้รหัสผ่านรวมกับผู้อื่น

๖.๗.๑.๙ ไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงานและในกรณีใช้สวนตัว

๖.๗.๑.๑๐ ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว แนะนำให้ใช้รหัสผ่านเดียวกันที่มีคุณภาพข้างต้น สำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นต้องมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

๖.๘ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๖.๘.๑ ผู้ใช้ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๖.๘.๒ ผู้ใช้มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

๖.๘.๓ ผู้ใช้ต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk Thumb Drive และ Data Storage อื่น ๆ ก่อนนามาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๖.๘.๔ ผู้ใช้ต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๖.๘.๕ ผู้ใช้ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๖.๙ การสำรองข้อมูลและการกู้คืน

๖.๙.๑ ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD DVD External Hard Disk เป็นต้น

๖.๙.๒ ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๖.๙.๓ ผู้ใช้ต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ต้องไม่เป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

๖.๑๐ การบริหารจัดการการบันทึกและตรวจสอบ

๖.๑๐.๑ ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย ๓ เดือน

๖.๑๐.๒ ต้องมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๖.๑๐.๓ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๖.๑๑ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Use of Notebook Computer Policy)

๖.๑๑.๑ เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้น ผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร

๖.๑๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพา หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๖.๑๑.๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่ ของศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลเท่านั้น

๖.๑๑.๔ การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ ของศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาลเท่านั้น

๖.๑๑.๕ ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๖.๑๑.๖ ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ ให้มีสภาพเดิม

๖.๑๑.๗ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

๖.๑๑.๘ ไม่ใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสียงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

๖.๑๑.๙ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๖.๑๑.๑๐ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๖.๑๑.๑๑ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๖.๑๑.๑๒ การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๖.๑๑.๑๓ ไม่เคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

๖.๑๑.๑๔ ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

๖.๑๑.๑๕ ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ต้องอยู่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส

๖.๑๑.๑๖ ไม่วางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๖.๑๑.๑๗ ไม่ติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

๖.๑๑.๑๘ การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๖.๑๒ การป้องกันความปลอดภัยทางด้านกายภาพ

๖.๑๒.๑ ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๖.๑๒.๒ ผู้ใช้ไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

๖.๑๒.๓ ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

ส่วนที่ ๒
นโยบายการจัดทำระบบสำรองของระบบสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหาย ถูกทำลาย หรือถูกเปลี่ยนแปลงจากไวรัสคอมพิวเตอร์ โปรแกรมชุดคำสั่งไม่พึงประสงค์ ผู้บุกรุกทำลาย โดยสามารถนำกู้ข้อมูลที่มีปัญหากลับมาใช้งานได้

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการสำรองข้อมูล เพื่อความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เวอร์ชั่น ๒.๕

ข้อปฏิบัติ

๑. การคัดเลือกและจัดทำระบบสำรอง

๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

๑.๓ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๑.๔ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูล แบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๑.๕ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๑.๖ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูล Configuration ข้อมูลในฐานข้อมูล เป็นต้น

๑.๗ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๑.๘ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

๑.๙ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๑.๑๐ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๑.๑๑ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๑.๑๒ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งาน ตามภารกิจ ตามแนวทางต่อไปนี้

๒.๑ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

๒.๑.๑ ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๑.๒ ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงของเหตุการณ์ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้

๒.๑.๓ ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๒.๑.๔ ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๒.๑.๕ ต้องกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๒.๑.๖ ต้องสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๒.๒ ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. การกำหนดหน้าที่และความรับผิดชอบของบุคลากร

๓.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๓.๑.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๓.๑.๒ หัวหน้ากลุ่มระบบคอมพิวเตอร์และการสื่อสาร

๓.๑.๓ บุคลากรกลุ่มระบบคอมพิวเตอร์และการสื่อสาร

๓.๑.๔ บุคลากรที่รับผิดชอบระบบสารสนเทศทุกระบบ

๓.๒ ระบบสำรองและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๓.๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๓.๒.๒ หัวหน้ากลุ่มระบบคอมพิวเตอร์และการสื่อสาร

๓.๒.๓ บุคลากรกลุ่มระบบคอมพิวเตอร์และการสื่อสาร

๓.๓ ควบคุม กำกับดูแลระบบสารสนเทศกรมทรัพยากรน้ำบาดาลเมื่อเกิดเหตุฉุกเฉิน

๓.๓.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

๓.๓.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๓.๓.๓ หัวหน้ากลุ่มระบบคอมพิวเตอร์และการสื่อสาร

๓.๓.๕ หัวหน้าหน่วยงานที่เกิดเหตุ (On-Site Manager)

๓.๔ กำกับดูแลให้ระบบใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan)

๓.๔.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

๓.๔.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๓.๔.๓ หัวหน้ากลุ่มระบบคอมพิวเตอร์และการสื่อสาร

๓.๔.๔ หัวหน้าหน่วยงานที่เกิดเหตุ (On-Site Manager)

๔. การทดสอบสภาพพร้อมใช้งาน

๔.๑ ทดสอบว่าการสำรองข้อมูลสำเร็จครบถ้วนอย่างน้อยสัปดาห์ละ ๑ ครั้ง

๔.๒ ทดสอบการกู้คืนข้อมูลที่สำรองไว้ว่าสามารถกู้คืนได้อย่างครบถ้วนและสามารถใช้งานได้ตามปกติอย่างน้อยเดือนละ ๑ ครั้ง

๔.๓ ทดสอบระบบแผนเตรียมความพร้อมสำหรับสถานการณ์ฉุกเฉินจากภัยพิบัติให้มีสภาพพร้อมใช้งานอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๕. ระยะความถี่ของการปฏิบัติ

๕.๑ ความถี่ในการสำรองข้อมูลของระบบสารสนเทศขึ้นอยู่กับความสำคัญของระบบสารสนเทศและสภาพการเปลี่ยนแปลงข้อมูล โดยระบบที่มีความสำคัญมาก หรือมีการเปลี่ยนแปลงข้อมูลบ่อย ต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

๕.๒ ทำการทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง

๕.๓ มีการทบทวนและปรับปรุงการบริหารจัดการความเสี่ยงด้านสารสนเทศ แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติและแผนบริหารความต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓
นโยบายการตรวจสอบและประเมินความเสี่ยง

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศขององค์กร เพื่อให้มั่นใจว่านโยบายและมาตรฐานต่าง ๆ ด้านความมั่นคงปลอดภัยสารสนเทศได้มีการปฏิบัติตามอย่างมีประสิทธิผล

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล

๒. ผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก

๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เวอร์ชั่น ๒.๕

ข้อปฏิบัติ

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๒. ตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายในขององค์กรหรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

๓. การตรวจสอบและประเมินความเสี่ยงของการรักษาความมั่นคงปลอดภัยครอบคลุมหัวข้อต่อไปนี้

๓.๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของกรมทรัพยากรน้ำบาดาล เพื่อการตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้

๓.๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการ เพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๓.๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๓.๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๓.๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด

๓.๑.๕ ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๓.๑.๖ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๓.๒ กำหนดวิธีการในการตรวจสอบและประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๓.๓ การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

๓.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๓.๓.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๓.๓.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๓.๓.๔ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในกรมทรัพยากรน้ำบาดาล เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศความเสียหายหรืออันตรายที่จะเกิดขึ้นของหน่วยงาน

ส่วนที่ ๔
นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้บุคลากรขององค์กรได้รับทราบ เข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้องเหมาะสม

ผู้รับผิดชอบ

๑. ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล
๒. ส่วนบริหารทรัพยากรบุคคล สำนักบริหารกลาง
๓. หน่วยงานที่ได้รับมอบหมายในการฝึกอบรม
๔. ผู้ดูแลระบบที่ได้รับมอบหมาย
๕. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เวอร์ชั่น ๒.๕

ข้อปฏิบัติ

๑. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรม ใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ

๒. เผยแพร่ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในลักษณะเกร็ดความรู้ผ่านทางการติดประกาศประชาสัมพันธ์ แผ่นพับ เว็บไซต์กรมทรัพยากรน้ำบาดาล

๓. จัดทำคู่มือการใช้ระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย โดยให้มีการเผยแพร่ทางหนังสือเวียนและเว็บไซต์กรมทรัพยากรน้ำบาดาล

๔. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมทรัพยากรน้ำบาดาล พ.ศ.๒๕๕๘

ว่าด้วยคำนิยาม

คำนิยามที่ใช้ในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ ประกอบด้วย

องค์กร หมายความว่า กรมทรัพยากรน้ำบาดาล

ผู้บังคับบัญชา หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมทรัพยากรน้ำบาดาล

ผู้บริหารระดับสูงสุด (Chief Executive Officer: CEO) หมายความว่า ผู้มีอำนาจสูงสุดของกรมทรัพยากรน้ำบาดาล ได้แก่ อธิบดีกรมทรัพยากรน้ำบาดาล ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย ตัดสินใจ และแนะนำแนวทางการดำเนินงานของกรมทรัพยากรน้ำบาดาล

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) หมายความว่า ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของกรมทรัพยากรน้ำบาดาล ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล หมายความว่า ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล มีหน้าที่ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในกรมทรัพยากรน้ำบาดาลส่วนกลางและส่วนภูมิภาค

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล หมายความว่า ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรน้ำบาดาล และมีอำนาจตัดสินใจเกี่ยวกับระบบเทคโนโลยีสารสนเทศภายในกรมทรัพยากรน้ำบาดาล

การรักษาความมั่นคงปลอดภัย หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรน้ำบาดาล

มาตรฐาน (Standard) หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ (Procedure) หมายความว่า รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายความว่า แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน (User) หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานราชการ พนักงานกองทุนพัฒนาน้ำบาดาล ลูกจ้างโครงการ ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป บุคคลที่ได้รับอนุญาต (Authorize User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของ

หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานภายนอกที่กรมทรัพยากรน้ำบาดาลอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของกรมทรัพยากรน้ำบาดาล

ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

สินทรัพย์ (Asset) หมายความว่า ข้อมูล ระบบฐานข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์

รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ฮาร์ดแวร์ หมายความว่า อุปกรณ์ เครื่องคอมพิวเตอร์ เครื่องมือวัด ที่จับต้องได้โดยทำงานควบคู่กับซอฟต์แวร์ระบบและซอฟต์แวร์ประยุกต์

เครื่องคอมพิวเตอร์แม่ข่าย (Server Computer) หมายความว่า เครื่องคอมพิวเตอร์ประสิทธิภาพสูงที่ต้องทำงานตลอดเวลา เพื่อให้บริการเครื่องลูกข่ายผ่านทางเครือข่าย จึงต้องมีอุปกรณ์ที่มีคุณภาพสูงทนทานต่อการใช้งานหนัก และต้องทำงานในอุณหภูมิและความชื้นที่เหมาะสมจึงจะยืดอายุการใช้งานได้เต็มประสิทธิภาพ

ซอฟต์แวร์ประยุกต์ (Application Software) หมายความว่า ชุดคำสั่งหรือโปรแกรมที่เสริมการทำงานของเครื่องคอมพิวเตอร์ เพื่อให้ผู้ใช้สามารถปฏิบัติงานได้ตามภาระหน้าที่ โปรแกรมตารางคำนวณ โปรแกรมพิมพ์เอกสาร

ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายความว่า ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ตที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กร

ระบบปฏิบัติการ (Operating System) หมายความว่า ซอฟต์แวร์หรือโปรแกรมที่จำเป็นของเครื่องคอมพิวเตอร์ เพื่อให้ผู้ใช้สามารถติดตั้งซอฟต์แวร์ประยุกต์ในการทำงาน ไมโครซอฟท์วินโดวส์เวอร์ชั่นต่าง ๆ

การกู้คืนระบบ หมายความว่า การปฏิบัติการตามแผนเพื่อทำให้ระบบสารสนเทศสามารถกลับมาทำงานได้ตามปกติ

สำนักงานเทคทรัพยากรน้ำบาดาล
๒๗๘๙
๓ ธ.ค. ๒๕๕๘
๑๐.๐๙ น.

ที่ ทก ๐๒๐๙.๔/ว๑๑๙๘๔

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ
อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

๑๐๙๔๙
๒ ธ.ค. ๒๕๕๘
๑๑.๑๐

หน้าห้อง รอง อทบ.(อรัญญา)
เลขรับ 3307
วันที่ - 3 ธ.ค. 2558
เวลา 17.50

๑๓ พฤศจิกายน ๒๕๕๘

เรื่อง การดำเนินงานภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประจำปีงบประมาณ พ.ศ. ๒๕๕๙

หน้าห้อง ผอ.สบก.
เลขรับ 20160
วันที่ - 3 ธ.ค. 2558
เวลา 17.03

เรียน อธิบดีกรมทรัพยากรน้ำบาดาล

สิ่งที่ส่งมาด้วย ๑. ประกาศสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง รายชื่อหน่วยงานที่ผ่านความเห็นชอบตามมาตรา ๗ ภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประจำปีงบประมาณ พ.ศ. ๒๕๕๘
๒. รายละเอียดเพื่อขอความร่วมมือหน่วยงานของรัฐ
๓. CD เอกสารขั้นตอนการดำเนินงาน

ด้วย พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ ทั้งนี้ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือหน่วยงานที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมายก่อน จึงมีผลใช้บังคับได้

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ในฐานะฝ่ายเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ขอนำส่งประกาศเรื่อง รายชื่อหน่วยงานที่ผ่านความเห็นชอบตามมาตรา ๗ ภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประจำปีงบประมาณ พ.ศ. ๒๕๕๘ ตามสิ่งที่ส่งมาด้วย ๑ มาเพื่อโปรดทราบ และใคร่ขอความร่วมมือท่านดำเนินการตามมาตรา ๕ มาตรา ๖ และมาตรา ๗ ภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ รายละเอียดตามสิ่งที่ส่งมาด้วย ๒ โดยมีรายละเอียดขั้นตอนการดำเนินงานปรากฏตามสิ่งที่ส่งมาด้วย ๓ และนำเสนอต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เพื่อพิจารณาให้ความเห็นชอบ ภายในวันที่ ๓๑ มีนาคม ๒๕๕๙

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไปด้วย

เรียน รอง อทบ. (อรัญญา)
เพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายวิโรจน์ เหลืองวิไลย์)
ผู้อำนวยการสำนักบริหารกลาง
3 ธ.ค. 2558

นาวาอากาศเอก
(สมศักดิ์ ขาวสุวรรณ์)
รองปลัดกระทรวง ปฏิบัติราชการแทน
ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ศักดิ์ พิจารณาดำเนินการต่อไป

(นางอรัญญา เฟื่องสวัสดิ์)
รองอธิบดีกรมทรัพยากรน้ำบาดาล
ปฏิบัติราชการแทนอธิบดีกรมทรัพยากรน้ำบาดาล
- 4 ธ.ค. 2558

สำนักงานปลัดกระทรวง
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๘๘ ๐ ๒๑๔๑ ๖๕๙๔
โทรสาร ๐ ๒๑๔๓ ๘๐๓๖ ๐ ๒๑๔๓ ๘๐๓๗

สิ่งที่ส่งมาด้วย ๑

ประกาศสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง รายชื่อหน่วยงานที่ผ่านความเห็นชอบตามมาตรา ๗ ภายใต้
พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙
ประจำปีงบประมาณ พ.ศ. ๒๕๕๘

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ทั้งนี้ ให้หน่วยงานของรัฐจัดทำเป็นประกาศและต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือหน่วยงานที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมายก่อน จึงมีผลใช้บังคับได้

สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงประกาศรายชื่อหน่วยงานที่ได้ดำเนินการตามมาตรา ๕ มาตรา ๖ และ มาตรา ๗ ซึ่งผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประจำปีงบประมาณ พ.ศ. ๒๕๕๘ ดังนี้

๑. หน่วยงานที่ได้รับความเห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ฉบับแรก จำนวน ๓๑ หน่วยงาน โดยมีรายชื่อดังต่อไปนี้

๑.๑. สำนักราชเลขาธิการ
๑.๒. สำนักงานคณะกรรมการส่งเสริมการลงทุน
๑.๓. กรมธนารักษ์
๑.๔. องค์การเภสัชกรรม
๑.๕. กรมการพัฒนาชุมชน
๑.๖. บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)
๑.๗. กองทัพเรือ
๑.๘. สำนักงานเศรษฐกิจอุตสาหกรรม
๑.๙. สำนักงานตำรวจแห่งชาติ
๑.๑๐. สำนักงานเลขาธิการสภาผู้แทนราษฎร
๑.๑๑. สำนักงานตรวจคนเข้าเมือง
๑.๑๒. สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
๑.๑๓. สำนักงานคณะกรรมการกฤษฎีกา
๑.๑๔. สำนักงานนโยบายและแผนพลังงาน
๑.๑๕. มหาวิทยาลัยสงขลานครินทร์
๑.๑๖. มหาวิทยาลัยศรีนครินทรวิโรฒ
๑.๑๗. สำนักพระราชวัง
๑.๑๘. กรมหม่อนไหม
๑.๑๙. การไฟฟ้าส่วนภูมิภาค
๑.๒๐. บริษัท วิทยุการบิน จำกัด

( ) ...ต่อ

๑.๒๑. องค์การสวนสัตว์ ในพระบรมราชูปถัมภ์
๑.๒๒. สำนักงานประกันสังคม
๑.๒๓. กรมสรรพสามิต
๑.๒๔. สำนักงานปลัดกระทรวงกลาโหม
๑.๒๕. กรมการบินพลเรือน
๑.๒๖. บรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม (บสย.)
๑.๒๗. กรมทรัพยากรน้ำบาดาล
๑.๒๘. สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)
๑.๒๙. การไฟฟ้านครหลวง
๑.๓๐. กรมอุตุนิยมวิทยา
๑.๓๑. กรมทรัพยากรธรณี

๒. หน่วยงานที่ได้รับความเห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ฉบับทบทวน จำนวน ๑๐ หน่วยงาน โดยมีรายชื่อดังต่อไปนี้

๒.๑. ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
๒.๒. สำนักงานพระพุทธศาสนาแห่งชาติ
๒.๓. สำนักงานปลัดกระทรวงพาณิชย์
๒.๔. สำนักเลขาธิการคณะรัฐมนตรี
๒.๕. การทางพิเศษแห่งประเทศไทย
๒.๖. สถาบันมาตรวิทยาแห่งชาติ
๒.๗. สถาบันพัฒนาองค์กรชุมชน
๒.๘. กรมพัฒนาธุรกิจการค้า
๒.๙. กรมบังคับคดี
๒.๑๐. การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

๓. หน่วยงานที่ได้รับความเห็นชอบต่อนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล จำนวน ๑ หน่วยงาน คือ ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

ทั้งนี้ ขอให้ทุกหน่วยงานมีการปฏิบัติตามนโยบายและแนวปฏิบัติที่ได้รับความเห็นชอบอย่างเคร่งครัดต่อไป

ประกาศ ณ วันที่ ๑๐ พฤศจิกายน พ.ศ. ๒๕๕๘

ทรงพร โกมลสุรเดช

(นางทรงพร โกมลสุรเดช)
ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร