ประกาศกรมทรัพยากรน้ำ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมทรัพยากรน้ำ พ.ศ.๒๕๖๕

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ กอปรกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ กำหนดให้หน่วยงานของรัฐมีหน้าที่ดำเนินการเกี่ยวกับมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ กรมทรัพยากรน้ำจึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน แนวปฏิบัติขั้นตอนปฏิบัติให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ ตามประกาศ ดังต่อไปนี้

ข้อ ๑ ให้ยกเลิกประกาศกรมทรัพยากรน้ำ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมทรัพยากรน้ำ พ.ศ.๒๕๕๙ ลงวันที่ ๑๗ กุมภาพันธ์ ๒๕๕๙ และให้ใช้ประกาศนี้แทน

ข้อ ๒ วัตถุประสงค์

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรมทรัพยากรน้ำ

๒.๒ เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๒.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมทรัพยากรน้ำได้รับทราบ และเจ้าหน้าที่ทุกคนต้องยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

ข้อ ๓ ขอบเขตการดำเนินงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำ มีขอบเขตครอบคลุม ดังนี้

๓.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๓.๑.๑ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๓.๑.๒ การควบคุมการเข้าถึงสารสนเทศ

๓.๑.๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

๓.๑.๔ การกำหนดหน้าที่รับผิดชอบของผู้ใช้งาน

๓.๑.๕ การควบคุมการเข้าถึงระบบเครือข่ายและคอมพิวเตอร์

๓.๑.๖ การเข้าถึงระบบปฏิบัติการ

๓.๑.๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

๓.๑.๘ การควบคุมการเข้าถึงระบบเครือข่ายชนิดไร้สาย

๓.๑.๙ การใช้งาน...

๓.๑.๙ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๓.๑.๑๐ การใช้งานอินเทอร์เน็ต

๓.๑.๑๑ การใช้งานจดหมายอิเล็กทรอนิกส์

๓.๑.๑๒ การป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี

๓.๒ การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๔ การกำหนดความรับผิดชอบ

๔.๑ ระดับนโยบาย

๔.๑.๑ กำหนดให้ผู้บริหารระดับสูงสุดของกรมทรัพยากรน้ำ (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่กรมทรัพยากรน้ำ หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำ

๔.๑.๒ กำหนดให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรมของกรมทรัพยากรน้ำ (DCIO) เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำ

๔.๑.๓ กำหนดให้ผู้อำนวยการศูนย์สารสนเทศของกรมทรัพยากรน้ำเป็นผู้รับผิดชอบติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษากับเจ้าหน้าที่ในการปฏิบัติงาน

๔.๒ ระดับปฏิบัติ

๔.๒.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ผู้รับผิดชอบ ได้แก่

๔.๒.๑.๑ ศูนย์สารสนเทศของกรมทรัพยากรน้ำ

๔.๒.๑.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๑.๓ เจ้าหน้าที่ที่ได้รับมอบหมาย

๔.๒.๑.๔ ผู้ใช้งาน

๔.๒.๒ การสำรองและกู้คืนข้อมูลและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ผู้รับผิดชอบ ได้แก่

๔.๒.๒.๑ ศูนย์สารสนเทศของกรมทรัพยากรน้ำ

๔.๒.๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๒.๓ เจ้าหน้าที่ที่ได้รับมอบหมาย

๔.๒.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

๔.๒.๓.๑ ศูนย์สารสนเทศของกรมทรัพยากรน้ำ

๔.๒.๓.๒ ผู้ตรวจสอบภายในของกรมทรัพยากรน้ำหรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก

๔.๒.๓.๓ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๓.๔ เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อ ๕ ต้องมี...

ข้อ ๕ ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมถึงทบทวนปรับปรุงนโยบายและข้อปฏิบัติอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖ องค์ประกอบของนโยบายจัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรน้ำ โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ เรื่อง “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมทรัพยากรน้ำ พ.ศ.๒๕๖๕” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของกรมทรัพยากรน้ำและหน่วยงานภายนอก ต้องถือปฏิบัติตามอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๙ พฤษภาคม พ.ศ.๒๕๖๕

(นายภาดล ถาวรกฤชรัตน์)
อธิบดีกรมทรัพยากรน้ำ

เอกสารแนบท้ายประกาศ

กรมทรัพยากรน้ำ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมทรัพยากรน้ำ พ.ศ.๒๕๖๕

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมทรัพยากรน้ำ พ.ศ.๒๕๖๕

คำนำ

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร กอปรกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ กำหนดให้หน่วยงานของรัฐมีหน้าที่ดำเนินการเกี่ยวกับมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้

ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรมทรัพยากรน้ำมีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ กรมทรัพยากรน้ำจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมทรัพยากรน้ำ พ.ศ.๒๕๖๕ โดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ และขั้นตอนวิธีปฏิบัติ ที่ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสอดคล้องตามพระราชกฤษฎีกาและประกาศดังกล่าว เพื่อให้เจ้าหน้าที่และผู้เกี่ยวข้องรับทราบและนำไปปฏิบัติต่อไป

กรมทรัพยากรน้ำ

พฤษภาคม ๒๕๖๕

สารบัญ

	หน้า
วัตถุประสงค์	๑
องค์ประกอบของนโยบาย	๒
คำนิยาม	๓
ส่วนที่ ๑ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical Security)	๖
ส่วนที่ ๒ การควบคุมการเข้าถึงสารสนเทศ (Access Control)	๘
ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)	๑๑
ส่วนที่ ๔ การกำหนดหน้าที่รับผิดชอบของผู้ใช้งาน (User Responsibilities)	๑๓
ส่วนที่ ๕ การควบคุมการเข้าถึงระบบเครือข่ายและคอมพิวเตอร์ (Network Access Control)	๑๗
ส่วนที่ ๖ การเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	๒๑
ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control)	๒๔
ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายชนิดไร้สาย (Wireless Access Control)	๒๙
ส่วนที่ ๙ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)	๓๑
ส่วนที่ ๑๐ การใช้งานอินเทอร์เน็ต (Internet Usage)	๓๓
ส่วนที่ ๑๑ การใช้งานจดหมายอิเล็กทรอนิกส์ (Email Usage)	๓๕
ส่วนที่ ๑๒ การป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี (Malicious Code Protection)	๓๗
ส่วนที่ ๑๓ การสำรองและกู้คืนข้อมูลและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (Backup and Recovery Policy and IT Contingency Plan)	๓๙
ส่วนที่ ๑๔ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Monitoring and Risk Assessment Information)	๔๕

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมทรัพยากรน้ำ พ.ศ. ๒๕๖๕

๑. วัตถุประสงค์

๑.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรมทรัพยากรน้ำ

๑.๒ เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศโดยอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๑.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมทรัพยากรน้ำได้รับทราบ ยอมรับ และปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒. องค์ประกอบของนโยบาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำ พ.ศ. ๒๕๖๕ ฉบับนี้ ประกอบด้วยส่วนต่าง ๆ ทั้งสิ้น ๑๔ ส่วน ดังนี้

- ส่วนที่ ๑ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
- ส่วนที่ ๒ การควบคุมการเข้าถึงสารสนเทศ (Access Control)
- ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
- ส่วนที่ ๔ การกำหนดหน้าที่รับผิดชอบของผู้ใช้งาน (User Responsibilities)
- ส่วนที่ ๕ การควบคุมการเข้าถึงระบบเครือข่ายและคอมพิวเตอร์ (Network Access Control)
- ส่วนที่ ๖ การเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
- ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control)
- ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายชนิดไร้สาย (Wireless Access Control)
- ส่วนที่ ๙ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)
- ส่วนที่ ๑๐ การใช้งานอินเทอร์เน็ต (Internet Usage)
- ส่วนที่ ๑๑ การใช้งานจดหมายอิเล็กทรอนิกส์ (Email Usage)
- ส่วนที่ ๑๒ การป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี (Malicious Code Protection)
- ส่วนที่ ๑๓ การสำรองและกู้คืนข้อมูลและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (Backup and Recovery Policy and Contingency Plan)
- ส่วนที่ ๑๔ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Monitoring and Risk Assessment Information)

๓. คำนิยาม

คำนิยามที่ใช้ในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำ พ.ศ. ๒๕๖๕ ประกอบด้วย

๓.๑ **กรมทรัพยากรน้ำ** หมายถึง กรมทรัพยากรน้ำ กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

๓.๒ **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถใช้งานบริหารจัดการหรือดูแลรักษาระบบสารสนเทศของกรมทรัพยากรน้ำ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role)

๓.๓ **เจ้าหน้าที่** หมายถึง บุคคลที่กรมทรัพยากรน้ำจ้างไว้ทำงานในลักษณะประจำ หรือบุคคลที่กรมทรัพยากรน้ำจ้างไว้ทำงานโดยมีวัตถุประสงค์เฉพาะ มุ่งผลสำเร็จของงานหรือโครงการ และมีกำหนดระยะเวลาการจ้างแน่นอน เป็นรายเดือน รายวัน และรายชั่วโมง

๓.๔ **ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าสายงานให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ สามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อดูแลและจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

๓.๕ **ผู้บริหารระดับสูงสุดของกรมทรัพยากรน้ำ (CEO)** หมายถึง อธิบดีกรมทรัพยากรน้ำ

๓.๖ **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรมของกรมทรัพยากรน้ำ (DCIO)** หมายถึง ผู้ที่ได้รับการแต่งตั้งให้ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรมประจำกรมทรัพยากรน้ำ

๓.๗ **ผู้อำนวยการศูนย์สารสนเทศของกรมทรัพยากรน้ำ** หมายถึง ผู้อำนวยการศูนย์สารสนเทศทรัพยากรน้ำ

๓.๘ **หน่วยงานภายนอก** หมายถึง หน่วยงานภายนอกที่กรมทรัพยากรน้ำอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของกรมทรัพยากรน้ำ โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๓.๙ **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บริหารให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย หรือถูกเปลี่ยนแปลง

๓.๑๐ **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดของผู้ใช้งานที่เกี่ยวข้องกับระบบสารสนเทศของกรมทรัพยากรน้ำ

๓.๑๑ **สินทรัพย์** หมายถึง ข้อมูลระบบ ข้อมูลทรัพย์สินด้านระบบสารสนเทศหรือสิ่งใดก็ตามที่มีคุณค่าของกรมทรัพยากรน้ำ

๓.๑๒ **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนการกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

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

๓.๑๔ **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่ให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

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

๓.๑๖ **ระบบปฏิบัติการ (Operating system)** หมายถึง โปรแกรมที่ทำหน้าที่เป็นตัวกลางเชื่อมต่อระหว่างฮาร์ดแวร์กับซอฟต์แวร์ โดยจะทำหน้าที่ควบคุมการแสดงผลการทำงานของฮาร์ดแวร์ ในการรับ-ส่ง และจัดเก็บข้อมูลกับฮาร์ดแวร์ และจัดสรรการใช้ทรัพยากรระบบ (Resources)

๓.๑๗ **ซอฟต์แวร์ (Software)** หมายถึง ซอฟต์แวร์แอปพลิเคชั่น (Application Software) ซอฟต์แวร์ระบบปฏิบัติการคอมพิวเตอร์ (Operating System Software) เครื่องมือในการพัฒนาระบบงาน (Development Tool) และโปรแกรมอรรถประโยชน์ (Utility)

๓.๑๘ **ฮาร์ดแวร์ (Hardware)** หมายถึง เครื่องคอมพิวเตอร์และอุปกรณ์รอบข้างที่สามารถสัมผัสได้ ประกอบด้วย อุปกรณ์ทางด้านอิเล็กทรอนิกส์ที่ควบคุมการประมวลผลข้อมูล การรับข้อมูล การแสดงผลข้อมูลของเครื่องคอมพิวเตอร์ มีทั้งที่ติดตั้งภายในเครื่องคอมพิวเตอร์และเชื่อมต่อภายนอกกับเครื่องคอมพิวเตอร์

๓.๑๙ **จดหมายอิเล็กทรอนิกส์ (E-mail)** หมายถึง ระบบที่ผู้ใช้งานใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน

๓.๒๐ **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๓.๒๑ **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

๓.๒๒ **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๓.๒๓ **ศูนย์คอมพิวเตอร์** หมายถึง ห้องที่ติดตั้งและจัดวางระบบ Server อุปกรณ์เชื่อมต่อและอุปกรณ์เครือข่าย

๓.๒๔ **ระบบสารสนเทศ** หมายถึง ระบบงานของกรมทรัพยากรน้ำที่นำเอาข้อมูลคอมพิวเตอร์ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่กรมทรัพยากรน้ำสามารถนำมาใช้ประโยชน์ในการวางแผนการบริหารการสนับสนุนการให้บริการการพัฒนาและควบคุมการติดต่อสื่อสาร

๓.๒๕ **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของกรมทรัพยากรน้ำได้

๓.๒๖ ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในกรมทรัพยากรน้ำเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในกรมทรัพยากรน้ำ

๓.๒๗ ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๓.๒๘ อุปกรณ์สนับสนุน หมายถึง อุปกรณ์ที่ทำงานร่วม หรือต่อพ่วงกับระบบคอมพิวเตอร์ระบบเครือข่าย

๓.๒๙ การเข้าถึง หมายถึง การอนุญาต การกำหนดสิทธิ ให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

ส่วนที่ ๑
การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical Security)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยของการเข้าใช้งานหรือการเข้าอาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ

๒. การรักษาความปลอดภัยทางกายภาพ

๒.๑ ความปลอดภัยพื้นที่

๒.๑.๑ กรมทรัพยากรน้ำต้องกำหนดขอบเขตพื้นที่รักษาความปลอดภัย เพื่อป้องกันการเข้าไปในศูนย์คอมพิวเตอร์หรือบริเวณที่มีระบบ อุปกรณ์ประมวลผล และสารสนเทศของกรมทรัพยากรน้ำ โดยต้องจัดให้มีการควบคุมการเข้าถึงทางกายภาพอย่างเหมาะสม ได้แก่ จัดทำประตูเข้า-ออก ติดตั้งอุปกรณ์ตรวจสอบการเข้า-ออก (Access Control)

๒.๑.๒ กรมทรัพยากรน้ำต้องกำหนดบุคคลที่ได้รับอนุญาตในการเข้าถึงพื้นที่ปลอดภัยไว้เป็นลายลักษณ์อักษร โดยรายชื่อดังกล่าวต้องได้รับการอนุมัติจากผู้บริหารหรือบุคคลที่ได้รับมอบหมาย รวมทั้งต้องทำการปรับปรุงรายชื่อและทำการอนุมัติใหม่ทุกครั้งที่มีการเปลี่ยนแปลง

๒.๑.๓ กรมทรัพยากรน้ำต้องดำเนินการป้องกันความเสียหายทางกายภาพที่อาจเกิดขึ้นจากสภาพแวดล้อมทั้งโดยทางธรรมชาติและความเสียหายที่เกิดขึ้นจากมนุษย์

๒.๑.๔ ระบบและอุปกรณ์สนับสนุนการทำงานที่อยู่ในสภาพแวดล้อมที่ใช้งานจริง ซึ่งรวมถึงเครื่องแม่ข่าย ไฟร์วอลล์ ฮับ (Firewall Hub) เราเตอร์ (Router) ระบบจดหมายอิเล็กทรอนิกส์ และอื่นๆ ต้องถูกจัดวางภายในศูนย์คอมพิวเตอร์ที่มีการรักษาความปลอดภัย

๒.๑.๕ กรมทรัพยากรน้ำต้องจัดให้มีการจัดเก็บข้อมูลการเข้า-ออก ศูนย์คอมพิวเตอร์สำหรับผู้ใช้งาน โดยต้องทำการบันทึกข้อมูลเวลาเข้า-ออก เหตุผลการเข้าศูนย์คอมพิวเตอร์ลงในสมุดบันทึกการเข้า-ออก ศูนย์คอมพิวเตอร์ (Visitor Log Book) ทุกครั้ง

๒.๒ ความปลอดภัยอุปกรณ์

๒.๒.๑ ระบบสารสนเทศและอุปกรณ์สนับสนุนที่ใช้ในการประมวลผลต้องมีการจัดวางอย่างเหมาะสม และต้องมีการจัดแบ่งพื้นที่อย่างชัดเจน ได้แก่ ส่วนระบบเครือข่าย ส่วนเครื่องแม่ข่าย และส่วนงานพิมพ์

๒.๒.๒ ระบบสารสนเทศและอุปกรณ์สนับสนุนต้องได้รับการป้องกันความเสียหายที่เกิดจากความล้มเหลวของระบบไฟฟ้า หรือความหยุดชะงักของพลังงานที่มีสาเหตุมาจากอุปกรณ์สนับสนุนอื่นๆ

๒.๒.๓ ระบบสารสนเทศและอุปกรณ์สนับสนุนต้องได้รับการบำรุงรักษาอย่างถูกต้องเป็นประจำ ทุก ๓ เดือน

๒.๒.๔ ระบบสารสนเทศและอุปกรณ์สนับสนุนที่ถูกติดตั้งอยู่ภายนอกสำนักงานใหญ่ต้องได้รับการรักษาความปลอดภัยเช่นเดียวกัน

๒.๒.๕ โปรแกรมลิขสิทธิ์ต้องได้รับการลบหรือย้ายออกจากระบบสารสนเทศและอุปกรณ์สนับสนุนให้หมดสิ้นก่อนนำไปใช้ใหม่หรือจำหน่ายทิ้ง

๒.๒.๖ ระบบสารสนเทศและอุปกรณ์สนับสนุนไม่อนุญาตให้เคลื่อนย้ายออกนอกกรมทรัพยากรน้ำโดยไม่ได้รับอนุญาต

๒.๒.๗ ระบบสารสนเทศและอุปกรณ์สนับสนุนจากภายนอกที่นำมาใช้งานภายนอกกรมทรัพยากรน้ำในกรณีที่ต้องการเชื่อมต่อไปยังระบบสารสนเทศต่างๆ ภายในกรมทรัพยากรน้ำจะต้องมีการขออนุญาตในการเชื่อมต่อทุกครั้ง

๓. การป้องกันความเสียหาย

๓.๑ ระบบไฟฟ้า

๓.๑.๑ กรมทรัพยากรน้ำต้องจัดให้มีเครื่องสำรองไฟ เพื่อให้การดำเนินงานของระบบสารสนเทศของกรมทรัพยากรน้ำมีความต่อเนื่อง ได้แก่ ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบไฟฟ้าสำรอง

๓.๑.๒ กรมทรัพยากรน้ำต้องจัดให้มีระบบป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศของกรมทรัพยากรน้ำที่ติดตั้งภายในศูนย์คอมพิวเตอร์ในกรณีที่กระแสไฟไม่คงที่

๓.๑.๓ กรมทรัพยากรน้ำต้องจัดให้มีการตรวจตาระบบไฟฟ้าภายในห้องปฏิบัติการเครือข่ายเป็นประจำอย่างน้อยเดือนละ ๑ ครั้ง เพื่อตรวจสอบความพร้อมในการใช้งานของระบบไฟฟ้า

๓.๒ ระบบป้องกันไฟไหม้

๓.๒.๑ กรมทรัพยากรน้ำต้องติดตั้งอุปกรณ์เตือนภัยภายในศูนย์คอมพิวเตอร์และบริเวณตึกสำนักงานของกรมทรัพยากรน้ำ เพื่อใช้เตือนภัยในกรณีที่เกิดไฟไหม้ ได้แก่ เครื่องดักจับควัน เครื่องตรวจจับความร้อนและสัญญาณเตือนภัย

๓.๒.๒ กรมทรัพยากรน้ำต้องทำการติดตั้งอุปกรณ์ดับเพลิงอัตโนมัติภายในศูนย์คอมพิวเตอร์อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น โดยถังดับเพลิงจะต้องเป็นสารดับเพลิงที่ใช้สำหรับอุปกรณ์อิเล็กทรอนิกส์โดยเฉพาะ

๓.๒.๓ ในกรณีที่กรมทรัพยากรน้ำมีระบบป้องกันไฟไหม้อยู่แล้วควรทำการตรวจสอบความพร้อมในการใช้งานระบบป้องกันไฟไหม้เป็นประจำอย่างน้อยเดือนละ ๑ ครั้ง เพื่อตรวจสอบความพร้อมในการใช้งานของระบบป้องกันไฟไหม้

๓.๓ ระบบควบคุมอุณหภูมิ

๓.๓.๑ กรมทรัพยากรน้ำต้องทำการติดตั้งระบบควบคุมอุณหภูมิและความชื้นให้เหมาะสมกับระบบสารสนเทศของกรมทรัพยากรน้ำและอุปกรณ์คอมพิวเตอร์

๓.๓.๒ กรมทรัพยากรน้ำควรตรวจสอบอุณหภูมิและความชื้นในศูนย์คอมพิวเตอร์อย่างสม่ำเสมอ

๓.๓.๓ กรมทรัพยากรน้ำต้องกำหนดอุณหภูมิในศูนย์คอมพิวเตอร์ให้เหมาะสม ซึ่งอุณหภูมิที่เหมาะสมจะต้องอยู่ระหว่าง ๑๙-๒๓ องศาเซลเซียส เพื่อควบคุมไม่ให้อุปกรณ์คอมพิวเตอร์ต่างๆ ร้อนเกินไป เพราะอุณหภูมิที่สูงเกินไปอาจทำให้อุปกรณ์ได้รับความเสียหาย

๓.๓.๔ กรมทรัพยากรน้ำต้องกำหนดค่าความชื้นภายในศูนย์คอมพิวเตอร์ให้เหมาะสม ซึ่งค่าความชื้นที่เหมาะสมจะต้องอยู่ระหว่าง ๔๕%-๕๕% เพื่อป้องกันไฟฟ้าสถิตและการกลั่นตัวของหยดน้ำ

๓.๓.๕ กรมทรัพยากรน้ำจะต้องศึกษาแนวทางในการนำระบบรายงานการบริหารเครือข่ายมาช่วยตรวจสอบอุณหภูมิและความชื้นในศูนย์คอมพิวเตอร์ผ่านทาง SNMP Protocol

ส่วนที่ ๒
การควบคุมการเข้าถึงสารสนเทศ
(Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมผู้ใช้งานที่ไม่ได้รับอนุญาตให้เข้าถึงสารสนเทศของกรมทรัพยากรน้ำและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากชุดคำสั่งประสงค์ร้าย ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของกรมทรัพยากรน้ำได้อย่างถูกต้อง

๒. การบริหารจัดการข้อมูล

๒.๑ กรมทรัพยากรน้ำต้องจัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สินการจำแนกกลุ่มทรัพยากรของระบบสารสนเทศหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒.๒ กรมทรัพยากรน้ำต้องกำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้ระบบสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

๒.๒.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิดำเนินการ

๒.๒.๒ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของกรมทรัพยากรน้ำจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาตามลำดับขั้น หรือผู้ดูแลระบบที่ได้รับมอบหมาย และผู้ใช้งานไม่สามารถยกสิทธิให้กับผู้อื่นใช้งานได้ โดยยังไม่ได้รับอนุญาตจากผู้บังคับบัญชาตามลำดับขั้นหรือผู้ดูแลระบบที่ได้รับมอบหมาย โดยห้ามไม่ให้ผู้ใช้งานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

๒.๒.๓ ผู้ดูแลระบบต้องกำหนดเกณฑ์การระงับสิทธิมอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

๒.๓ กรมทรัพยากรน้ำจัดแบ่งประเภทของข้อมูลออกเป็น

๒.๓.๑ ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี

๒.๓.๒ ข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน ได้แก่ ข้อมูลเกี่ยวกับระบบเครือข่ายระบบคอมพิวเตอร์ และระบบสารสนเทศ ข้อมูลรายงานผลการปฏิบัติงาน

๒.๓.๓ ข้อมูลทั่วไป ได้แก่ ข้อมูลที่สามารถเผยแพร่ให้กับประชาชน ข้อมูลเกี่ยวกับการบริหารจัดการน้ำ ข้อมูลเกี่ยวกับกรมทรัพยากรน้ำ โดยข้อมูลเผยแพร่บางประเภทอาจยังต้องจำกัดในการสำเนาข้อมูลดังกล่าวออกไปเผยแพร่ เพื่อป้องกันการดัดแปลงข้อมูลอันก่อให้เกิดความเสียหายต่อหน่วยงานได้

๒.๔ กรมทรัพยากรน้ำมีการจัดแบ่งระดับความสำคัญของข้อมูลออกเป็น ๓ ระดับ ได้แก่

๒.๔.๑ ข้อมูลที่มีระดับความสำคัญมากที่สุด

๒.๔.๒ ข้อมูลที่มีระดับความสำคัญปานกลาง

๒.๔.๓ ข้อมูลที่มีระดับความสำคัญน้อย

๒.๕ กรมทรัพยากรน้ำได้กำหนดชั้นความลับของข้อมูลออกเป็น ๔ ระดับ ได้แก่

๒.๕.๑ ข้อมูลลับที่สุด คือ ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุดต่อกรมทรัพยากรน้ำได้

๒.๕.๒ ข้อมูลลับมาก คือ ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงต่อกรมทรัพยากรน้ำได้

๒.๕.๓ ข้อมูลลับ คือ ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อกรมทรัพยากรน้ำได้

๒.๕.๔ ข้อมูลทั่วไป คือ ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้ แต่ยังคงต้องระมัดระวังในการนำข้อมูลไปดัดแปลง เพราะอาจจะก่อให้เกิดความเสียหายต่อหน่วยงานได้

๒.๖ กรมทรัพยากรน้ำได้จัดแบ่งระดับชั้นการเข้าถึงออกเป็น ๔ ระดับ ได้แก่

๒.๖.๑ ระดับชั้นสำหรับผู้บริหาร ผู้บริหารสามารถเข้าถึงข้อมูลลับถึงลับที่สุดได้

๒.๖.๒ ระดับชั้นสำหรับผู้ใช้งานทั่วไป ผู้ใช้งานทั่วไปสามารถเข้าถึงข้อมูลทั่วไปได้เท่านั้น

๒.๖.๓ ระดับชั้นสำหรับผู้ดูแลระบบ ผู้ดูแลระบบสามารถเข้าถึงข้อมูลทั่วไปและข้อมูลลับได้

๒.๖.๔ ระดับชั้นสำหรับผู้ที่ได้รับมอบหมาย ได้แก่ เจ้าหน้าที่จากหน่วยงานภายนอก ซึ่งจะสามารถเข้าถึงข้อมูลทั่วไปได้เท่านั้น

๒.๗ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๒.๗.๑ ผู้ดูแลระบบและผู้เป็นเจ้าของข้อมูล ทำหน้าที่กำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทด้วย

๒.๗.๒ ผู้ดูแลระบบและผู้เป็นเจ้าของข้อมูล ต้องทำการสอบทานสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถมั่นใจได้ว่าสิทธิต่างๆ ที่ได้กำหนดไว้ยังคงมีความเหมาะสม

๒.๗.๓ กรมทรัพยากรน้ำต้องทำการควบคุมเพื่อให้เกิดความเชื่อมั่นว่าข้อมูลที่จัดเก็บ นำเข้า ประมวลผล และแสดงผล มีความถูกต้อง ครบถ้วน และปลอดภัยจากการรั่วไหล ถูกทำลาย หรือแก้ไขโดยผู้ที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้อง

๒.๘ การกำหนดเวลาที่ได้เข้าถึง

๒.๘.๑ การเข้าถึงสารสนเทศในเวลาราชการ (๐๘.๓๐ น.-๑๖.๓๐ น.)

๒.๘.๒ การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ น.-๑๖.๓๐ น.)

๒.๘.๓ การเข้าถึงในช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

๒.๘.๔ การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงการเข้าถึงและจำนวนระยะเวลาการเข้าถึง)

๒.๙ การกำหนดจำนวนช่องทางที่สามารถเข้าถึงได้

๒.๙.๑ ระบบแลน (LAN)

๒.๙.๒ ระบบอินทราเน็ต (Intranet)

๒.๙.๓ ระบบอินเทอร์เน็ต (Internet)

๒.๙.๔ ระบบควบคุมเสมือน (VPN หรือ Team Viewer)

๓. กระบวนการหลักในการเข้าถึงระบบสารสนเทศ

๓.๑ ผู้ดูแลระบบและผู้เป็นเจ้าของข้อมูลและระบบงานต้องร่วมกันจัดทำตารางสิทธิเพื่อควบคุมการเข้าถึง โดยแบ่งออกเป็น กลุ่มของผู้ใช้งานต่างๆ และระดับสิทธิ พร้อมทั้งรายละเอียดสิทธิที่สามารถเข้าถึงระบบและข้อมูลในแต่ละระดับได้ เพื่อใช้เป็นมาตรฐานในการกำหนดสิทธิในการเข้าถึงข้อมูลและระบบงานของระบบนั้นๆ

๓.๒ ผู้ดูแลระบบและผู้เป็นเจ้าของข้อมูลต้องทำการกำหนดสิทธิ เพิ่มสิทธิ ยกเลิกสิทธิ และเปลี่ยนแปลงสิทธิ การเข้าถึงข้อมูลและระบบงานต้องมีความเหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานตามที่ได้กำหนดไว้

๓.๓ ผู้ดูแลระบบและผู้เป็นเจ้าของข้อมูลต้องทำการทบทวนสิทธิการเข้าถึงข้อมูลและระบบงานอย่างสม่ำเสมอ อย่างน้อยทุก ๖ เดือน หรือเมื่อมีเหตุการณ์ใดที่มีผลต่อการเข้าถึงข้อมูลและระบบงาน เพื่อให้การเข้าถึงข้อมูลและระบบงานเป็นไปอย่างเหมาะสม

๓.๔ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบงานได้

๓.๕ ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรน้ำและหมั่นตรวจสอบการละเมิดความปลอดภัยที่มีผลต่อข้อมูลและระบบงานที่สำคัญ

๓.๖ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ อย่างต่อเนื่อง พร้อมทั้งตรวจสอบอย่างสม่ำเสมอ

๓.๗ ผู้ดูแลระบบต้องจัดทำขั้นตอนการปฏิบัติงานเพื่อบริหารจัดการสิทธิในการเข้าถึงข้อมูลและระบบสารสนเทศของกรมทรัพยากรน้ำ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๘ ผู้ดูแลระบบจะต้องทำการประสานเพื่อขอความร่วมมือบุคลากรภายในกรมทรัพยากรน้ำให้ตระหนักถึงความปลอดภัยในการเข้าถึงข้อมูลและระบบสารสนเทศของกรมทรัพยากรน้ำ ด้วยการติดตั้งระบบรักษาความปลอดภัย เช่น ระบบป้องกันไวรัสบนทุกอุปกรณ์ที่ต้องการเข้าถึงข้อมูลและระบบสารสนเทศของกรมทรัพยากรน้ำ และควรทำการอัพเดทให้เป็นปัจจุบันอยู่เสมอ

ส่วนที่ ๓

การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

๑. วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๒. การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน

กรมทรัพยากรน้ำต้องจัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น รวมถึงการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อลดภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

๓. การลงทะเบียนผู้ใช้งาน (User Registration)

๓.๑ ผู้ดูแลระบบต้องจัดทำแบบฟอร์มการขอเข้าใช้งานระบบสารสนเทศของกรมทรัพยากรน้ำ และให้ผู้ใช้งานกรอกข้อมูลในแบบฟอร์ม เพื่อดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๓.๒ ผู้ดูแลระบบต้องกำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศของกรมทรัพยากรน้ำ โดยต้องได้รับอนุญาตจากหัวหน้างานตามลำดับขั้นหรือผู้ที่เป็นเจ้าของระบบหรือข้อมูล

๓.๓ ผู้ดูแลระบบต้องจัดทำหลักเกณฑ์ในการยกเลิกการอนุญาตในการเข้าถึงระบบสารสนเทศ หรือปรับเปลี่ยนสิทธิของผู้ใช้งาน เมื่อผู้ใช้งานลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้างงาน โดยจะต้องทำการจัดการลบบัญชีผู้ใช้งานเดิมที่ไม่มีการใช้งานแล้วออกไปจากระบบก่อน แต่หากมีคำขอใช้งานเนื่องจากการเปลี่ยนตำแหน่ง โอน ย้าย ควรจะมีการเริ่มดำเนินการลงทะเบียนใหม่ตั้งแต่ขั้นตอนแรกสุดเพื่อความปลอดภัยในการใช้งานระบบสารสนเทศนั้นๆ

๓.๔ ผู้ดูแลระบบต้องทำการระบุบัญชีชื่อผู้ใช้งาน โดยต้องแยกกันเป็นรายบุคคลและไม่ซ้ำซ้อนกัน และกำหนดให้มีรูปแบบเดียวกันทั้งกรมทรัพยากรน้ำ ได้แก่ ชื่อ_ นามสกุลตัวแรก หรือ ชื่อ.นามสกุลตัวแรก หรือ ชื่อ. นามสกุล

๓.๕ ผู้ดูแลระบบต้องทำบันทึกและจัดเก็บข้อมูลการขออนุมัติการเข้าใช้ระบบสารสนเทศ

๓.๖ ผู้ดูแลระบบต้องเก็บบันทึกการปฏิบัติงานของผู้ใช้งาน ได้แก่ บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกอย่างน้อย ๙๐ วัน

๓.๗ ผู้ดูแลระบบต้องมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอทุก ๓ เดือน

๓.๘ ผู้ดูแลระบบต้องป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิในการเข้าถึงบันทึกเหล่านั้นได้เฉพาะผู้ดูแลระบบเท่านั้น

๔. การบริหารจัดการสิทธิของผู้ใช้งาน (User management)

โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๔.๑ ผู้ดูแลระบบและผู้เป็นเจ้าของข้อมูลต้องมีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

๔.๒ ผู้ดูแลระบบต้องทบทวนบัญชีและสิทธิการใช้งาน อย่างน้อยปีละ ๑ ครั้ง โดยปฏิบัติ ดังนี้

๔.๒.๑ รวบรวมรายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน

๔.๒.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

๔.๒.๓ ดำเนินการแก้ไขข้อมูลสิทธิต่างๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

๔.๒.๔ ดำเนินการลบรายชื่อบัญชี และสิทธิผู้ใช้งานที่ไม่ได้ใช้งานระบบสารสนเทศนั้นๆ แล้วออกไปทุกครั้ง

๕. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๕.๑ รหัสผ่านต้องมีความยาวอย่างน้อย ๖ ตัวอักษรสำหรับผู้ใช้งานที่ได้รับสิทธิปกติ (Regular Users)

๕.๒ รหัสผ่านต้องมีความยาวอย่างน้อย ๑๐ ตัวอักษรสำหรับผู้ใช้งานที่ได้รับสิทธิพิเศษ (Privileged Users)

๕.๓ รหัสผ่านต้องประกอบด้วยตัวอักษร (a-z) หรือตัวเลข (๐-๙)

๕.๔ รหัสผ่านต้องไม่ซ้ำกับบัญชีรายชื่อผู้ใช้ระบบงาน (User ID)

๕.๕ เมื่อมีการเปลี่ยนแปลงรหัสผ่านต้องไม่ทำการเปลี่ยนรหัสผ่านโดยการใช้รหัสเดิม (Recycle Password)

๕.๖ ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านทุก ๙๐ วัน

๕.๗ ไฟล์ที่เก็บรหัสผ่านต้องทำการเข้ารหัส

๕.๘ ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้ยากต่อการคาดเดา และผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ในการเข้าใช้งานระบบในครั้งแรก

๕.๙ ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้แก่ผู้ใช้งาน โดยใช้การส่งรหัสผ่านผ่านทางอีเมล และกำหนดให้ผู้ใช้งานทำการตอบกลับว่าได้รับรหัสผ่านแล้ว

๖. ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

กรมทรัพยากรน้ำต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

ส่วนที่ ๔
การกำหนดหน้าที่รับผิดชอบของผู้ใช้งาน
(User Responsibilities)

๑. วัตถุประสงค์

เพื่อกำหนดระเบียบและวิธีปฏิบัติสำหรับการใช้งานทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของกรมทรัพยากรน้ำ เพื่อป้องกันการเข้าถึงระบบสารสนเทศของกรมทรัพยากรน้ำโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ

๒. **การกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password use) สำหรับผู้ใช้งาน**

เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่านและการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

๒.๑ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวทันที เมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

๒.๒ ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา

๒.๓ ผู้ใช้งานต้องกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๖ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติและตัวเลขเข้าด้วยกัน

๒.๔ ผู้ใช้งานต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๒.๕ ผู้ใช้งานต้องไม่ตั้งรหัสผ่านจากอักขระที่เรียงกันหรือกลุ่มเหมือนกัน

๒.๖ ผู้ใช้งานต้องเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

๒.๗ ผู้ใช้งานต้องไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

๒.๘ ผู้ใช้งานต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

๒.๙ ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ดำเนินการเรียบร้อยแล้ว ในกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน

๒.๑๐ ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๒.๑๑ ผู้ใช้งานต้องหลีกเลี่ยงการใช้รหัสผ่านเดียวกัน สำหรับระบบงานต่างๆ ที่ตนใช้งาน

๒.๑๒ ผู้ใช้งานต้องหลีกเลี่ยงการใช้รหัสผ่านเดิม

๒.๑๓ ผู้ใช้งานจะต้องไม่เปิดเผยรหัสผ่านส่วนตัวให้ผู้อื่นทราบหรือนำไปใช้งานแทน

๓. **การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์**

๓.๑ กรมทรัพยากรน้ำต้องสร้างความตระหนักให้แก่ผู้ใช้งาน เพื่อความเข้าใจในมาตรการป้องกันสำหรับอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

๓.๒ กรมทรัพยากรน้ำต้องกำหนดไม่ให้ผู้ช้งานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

๓.๓ กรมทรัพยากรน้ำต้องกำหนดไม่ให้ผู้ใช้งานเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๓.๔ กรมทรัพยากรน้ำต้องกำหนดไม่ให้ผู้ใช้งานกระทำการใดๆ อันส่งผลให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

๓.๕ กรมทรัพยากรน้ำต้องกำหนดไม่ให้ผู้ใช้งานกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศชาติ ความปลอดภัยสาธารณะความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะหรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๓.๖ กรมทรัพยากรน้ำต้องกำหนดไม่ให้ผู้ใช้งานทำการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงของชาติเข้าสู่ระบบคอมพิวเตอร์ ซึ่งอาจเป็นผลกระทบกับความมั่นคงแห่งราชอาณาจักรหรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๓.๗ กรมทรัพยากรน้ำต้องกำหนดไม่ให้ผู้ใช้งานทำการเผยแพร่ข้อมูลที่เท็จเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ปลอมหรือเป็นเท็จไม่ว่าทั้งหมดหรือบางส่วนโดยที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๓.๘ กรมทรัพยากรน้ำต้องกำหนดไม่ให้ผู้ใช้งานทำการนำเข้าหรือเผยแพร่เนื้อหาอันไม่เหมาะสม เป็นเท็จโดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

๓.๙ กรมทรัพยากรน้ำต้องกำหนดไม่ให้ผู้ใช้งานทำการเผยแพร่ข้อมูลความผิดที่เกี่ยวกับการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

๓.๑๐ กรมทรัพยากรน้ำต้องกำหนดไม่ให้ผู้ใช้งานทำการเผยแพร่ข้อมูลที่มีลักษณะลามกลงบนระบบคอมพิวเตอร์

๓.๑๑ กรมทรัพยากรน้ำต้องกำหนดไม่ให้ผู้ใช้งานทำการเผยแพร่ภาพตัดต่อที่เป็นการหมิ่นหรือส่งต่อสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูล คอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการใดๆ

๓.๑๒ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๓.๑๓ ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๐ นาที หรือต่ำกว่านั้น และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๓.๑๔ ผู้ใช้งานต้องล็อคอุปกรณ์เครื่องคอมพิวเตอร์ที่สำคัญหรือติดตั้งอยู่ในบริเวณที่เข้าถึงได้ยากเมื่อไม่ได้ถูกใช้งาน

๔. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy)

กรมทรัพยากรน้ำต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

๔.๑ กรมทรัพยากรน้ำต้องมีการกำหนดมาตรการป้องกันทรัพย์สินของกรมทรัพยากรน้ำและควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยให้ครอบคลุมถึงเรื่องต่างๆ ได้แก่

๔.๑.๑ ผู้ใช้งานต้องเก็บเอกสาร ข้อมูลการทำงาน หรือสื่อบันทึกข้อมูล ไว้ในที่ปลอดภัย ได้แก่ ใส่ตู้หรือโต๊ะที่สามารถล็อคกุญแจได้

๔.๑.๒ ผู้ใช้งานต้องช่วยกันดูแลคอมพิวเตอร์ส่วนกลางที่ใช้ร่วมกัน ถ้าพบเห็นเหตุการณ์ผิดปกติให้แจ้งผู้ดูแลระบบทันที

๔.๑.๓ ผู้ใช้งานต้องไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญ ได้แก่ เอกสาร สื่อบันทึกข้อมูล ให้อยู่ในสถานที่ที่ไม่ปลอดภัย หรือสถานที่ที่เข้าถึงได้ง่ายทางกายภาพ

๔.๑.๔ ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นเข้าใช้งานอุปกรณ์สารสนเทศต่างๆ โดยไม่ได้รับอนุญาต

๔.๑.๕ ผู้ดูแลระบบต้องตรวจสอบการทำงานของระบบป้องกันไวรัส ระบบป้องกันแก้ไขช่องโหว่บนเครื่องคอมพิวเตอร์ให้ทำงานตามปกติ

๔.๑.๖ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลของตนเอง และต้องเก็บรักษาไว้ในที่ปลอดภัย

๔.๑.๗ ผู้ดูแลระบบต้องมีการทำลายข้อมูลและสื่อบันทึกข้อมูลที่ไม่ได้ใช้แล้ว เพื่อป้องกันการนำกลับมาใช้ใหม่ ดังนี้

- ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในเทป ใช้วิธีการลบข้อมูลในเทป ผ่าน Tape Device และทำลายเทป
- ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในแผ่น CD/DVD ใช้วิธีการทำลายแผ่น CD/DVD
- ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บใน Hard Disk หรือ Memory Devices ใช้วิธีการทำลายตามมาตรฐาน DoD ๕๒๒๐-๒๒M ของกระทรวงกลาโหม สหรัฐอเมริกา

๔.๒ กรมทรัพยากรน้ำอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

๔.๒.๑ กรมทรัพยากรน้ำต้องจัดให้มีการประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นป้องกัน

๔.๒.๒ กรมทรัพยากรน้ำต้องกำหนดมาตรฐานการเข้ารหัสข้อมูลที่ควรนำมาใช้

๔.๒.๓ กรมทรัพยากรน้ำต้องกำหนดช่องทางการรับ-ส่งข้อมูลสำคัญ หรือข้อมูลลับที่เหมาะสม ได้แก่ ระบบ LAN ระบบ Internet และระบบเครือข่ายไร้สาย

๔.๒.๔ ผู้ใช้งานต้องไม่ทำการ Share ไฟล์ข้อมูลลับบนเครือข่ายของกรมทรัพยากรน้ำ เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้โดยไม่มีการป้องกัน

๔.๓ ผู้ใช้งานต้องตระหนักไว้เสมอว่าจะต้องทำการดูแลทรัพย์สินของกรมทรัพยากรน้ำที่อยู่ภายใต้การใช้งานของตนเองให้เปรียบเสมือนทรัพย์สินของตนเอง หากมีการสูญหายหรือเสียหายจากความประมาทเลินเล่อ ผู้ใช้งานอาจจะต้องรับผิดชอบต่อความสูญหายและเสียหายที่เกิดขึ้น

๔.๔ ผู้ใช้งานต้องไม่เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

๔.๕ ผู้ใช้งานต้องไม่เข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๔.๖ ผู้ใช้งานต้องไม่กระทำการใดๆ อันส่งผลให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

๔.๗ ผู้ใช้งานต้องไม่กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศชาติ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะหรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๔.๘ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่กระทบต่อความมั่นคงของชาติเข้าสู่ระบบคอมพิวเตอร์ ซึ่งอาจเป็นผลกระทบกับความมั่นคงแห่งราชอาณาจักรหรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๔.๙ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เท็จเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมหรือเป็นเท็จไม่ว่าทั้งหมดหรือบางส่วนโดยที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๔.๑๐ ผู้ใช้งานต้องไม่นำเข้าหรือเผยแพร่เนื้อหาอันไม่เหมาะสมเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

๔.๑๑ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลความผิดที่เกี่ยวกับการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

๔.๑๒ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่มีลักษณะลามกลงบนระบบคอมพิวเตอร์

๔.๑๓ ผู้ใช้งานต้องไม่เผยแพร่ภาพตัดต่อที่เป็นการหมิ่น หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการใดๆ

ส่วนที่ ๕
การควบคุมการเข้าถึงระบบเครือข่ายและคอมพิวเตอร์
(Network Access Control)

๑. วัตถุประสงค์

เพื่อป้องกันการเข้าถึงระบบเครือข่ายและคอมพิวเตอร์โดยไม่ได้รับอนุญาต และทำให้ระบบเครือข่ายและคอมพิวเตอร์มีความปลอดภัย เชื่อถือได้ และมีประสิทธิภาพในการให้บริการ

๒. กระบวนการควบคุมการเข้าถึงระบบเครือข่าย

๒.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศ ที่รวมถึงระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงตามที่ระบุใน ส่วนที่ ๗ ข้อ ๔.๑ ได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงตามที่ศูนย์สารสนเทศของกรมทรัพยากรน้ำกำหนดเท่านั้น

๒.๒ การใช้งานบริการเครือข่าย

๒.๒.๑ ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรมทรัพยากรน้ำ

๒.๒.๒ กรมทรัพยากรน้ำไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไร ผ่านเครื่องคอมพิวเตอร์และเครือข่าย ได้แก่ การประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปหรือแสวงหาผลกำไร

๒.๒.๓ ผู้ใช้งานต้องไม่ละเมิดสิทธิต่อผู้อื่น คือผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนเองโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายและสร้างความเสื่อมเสียให้แก่ผู้อื่น การใช้ภาษาไม่สุภาพ หรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว กรมทรัพยากรน้ำไม่มีส่วนร่วมในการรับผิดชอบความเสียหายดังกล่าว

๒.๒.๔ สำหรับผู้ใช้งานที่อยู่ภายในกรมทรัพยากรน้ำ การเชื่อมต่อเครือข่ายภายในกรมทรัพยากรน้ำต้องเชื่อมต่อผ่านทางช่องทางที่ผู้ดูแลระบบของกรมทรัพยากรน้ำจัดหาให้เท่านั้น

๒.๒.๕ ผู้ใช้งานต้องไม่กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ผ่านทางระบบเครือข่ายสารสนเทศของกรมทรัพยากรน้ำ

๒.๒.๖ ผู้ดูแลระบบต้องกำหนดบัญชีผู้ใช้งาน (User Account) ที่เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน จ่าย แจกสิทธิ หรือใช้งานบัญชีผู้ใช้งานร่วมกับผู้อื่นไม่ได้

๒.๒.๗ บัญชีผู้ใช้งาน (User Account) ที่ผู้ดูแลระบบจัดสรรให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น

๒.๓ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกกรมทรัพยากรน้ำ (User Authentication for External Connections)

๒.๓.๑ ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกกรมทรัพยากรน้ำ โดยต้องแสดงตัวตนด้วยชื่อผู้ใช้ พิสูจน์และยืนยันตัวตนด้วยการใช้รหัสผ่านในการเข้าสู่ระบบเครือข่ายของกรมทรัพยากรน้ำ

๒.๓.๒ กรมทรัพยากรน้ำได้กำหนดให้การเข้าถึง หรือเชื่อมต่อระบบเครือข่ายของกรมทรัพยากรน้ำจากบริเวณที่อนุญาตให้สามารถมีการเข้าถึงได้จากระยะไกล (Remote Access) แต่ต้องต่อผ่านอุปกรณ์ Firewall เท่านั้น และการเชื่อมต่อนั้น จะต้องมีการเข้ารหัสตามมาตรฐาน SSL หรือมาตรฐาน IPSec VPN หรือมาตรฐานอื่นที่เทียบเท่า และต้องจัดให้มีการจัดเก็บข้อมูลการใช้งานทุกครั้ง

๒.๓.๓ ก่อนจะมีการเชื่อมต่อเข้าใช้งานระบบเครือข่ายของกรมทรัพยากรน้ำจากภายนอก ผู้ใช้งานจะต้องขออนุญาตเป็นลายลักษณ์อักษรหรือจัดส่งสำเนาเอกสารหลักฐานที่สามารถพิสูจน์ตัวตนได้ตามระเบียบของราชการมาเพื่อขออนุญาตในการเชื่อมต่อในแต่ละครั้ง

๒.๔ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks)

๒.๔.๑ ผู้ดูแลระบบต้องจัดทำบัญชีการขอเชื่อมต่อระบบเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง เพื่อสามารถตรวจสอบได้ในภายหลัง

๒.๔.๒ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ผู้ดูแลระบบต้องกำหนดให้มีการระบุหมายเลข IP Address ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่

๒.๔.๓ ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์เครือข่าย สามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๒.๔.๔ ผู้ดูแลระบบต้องจัดทำขั้นตอนในการขอเชื่อมต่อระบบเครือข่าย และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๔.๕ ผู้ดูแลระบบควรกำหนดบทลงโทษให้กับผู้ใช้งานที่ลักลอบกำหนดระบุหมายเลข IP Address เอง ซึ่งการกระทำดังกล่าวนี้ อาจจะทำให้เกิดความเสียหายบนระบบเครือข่ายสารสนเทศได้

๒.๕ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

๒.๕.๑ ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยผู้ดูแลระบบต้องกำหนดให้มีการปิดพอร์ตที่เสี่ยง และอาจก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๒.๕.๒ ผู้ดูแลระบบต้องทำการยกเลิกหรือปิดพอร์ตและบริการต่างๆ บนอุปกรณ์ที่ไม่มีความจำเป็นในการใช้งาน

๒.๕.๓ เจ้าหน้าที่จากหน่วยงานภายนอกที่จะเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบก่อน

๒.๖ การแบ่งแยกเครือข่าย (Segregation in networks) มีการระบุเกี่ยวกับการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งานต่างๆ โดยพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคง และระดับความสำคัญของข้อมูลบนเครือข่าย ดังนี้

๒.๖.๑ กลุ่มผู้ใช้งานพนักงานทั่วไป

๒.๖.๒ กลุ่มผู้ใช้งานของระบบสารสนเทศ หรือกลุ่มผู้ใช้งานระดับผู้ดูแลระบบ

๒.๖.๓ กลุ่มผู้ใช้งานของเจ้าหน้าที่จากหน่วยงานภายนอก

๒.๗ การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

๒.๗.๑ ผู้ดูแลระบบต้องจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบเครือข่ายและคอมพิวเตอร์ และต้องทำการติดตั้ง Firewall เพื่อป้องกันการเข้าถึงเครือข่ายจากผู้ไม่ประสงค์ดี

๒.๗.๒ ผู้ดูแลระบบต้องกำหนดให้มีการควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) โดยมีข้อปฏิบัติ ดังนี้

- ไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)
- กำหนดให้มีการบังคับการใช้เส้นทางเครือข่าย ให้สามารถเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้เท่านั้น พร้อมทั้งจำกัดสิทธิในการเข้าใช้บริการเครือข่าย ควบคุมให้ผู้ใช้งานสามารถใช้งานได้เฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
- กำหนดเส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย และอนุญาตให้ผู้ใช้งานสามารถใช้เส้นทางที่ได้กำหนดไว้เท่านั้น

๒.๗.๓ ผู้ดูแลระบบต้องจัดทำแผนผังการเชื่อมต่อระบบเครือข่าย (Network Diagram) ซึ่งระบุถึงรายละเอียดของเครือข่ายภายในกรมทรัพยากรน้ำและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๗.๔ ผู้ใช้งานต้องไม่ทำการเปิดเผยข้อมูลเกี่ยวกับการตั้งค่าติดตั้งหรือช่องโหว่ของระบบเครือข่าย รวมถึงข้อมูลที่มีความสำคัญของระบบเครือข่าย แก่บุคคลที่ไม่เกี่ยวข้องกับกรมทรัพยากรน้ำ

๒.๗.๕ ผู้ดูแลระบบต้องระงับหรือปิดการใช้งานการเชื่อมต่อใดๆ ที่ไม่ได้ใช้งานหรือไม่มีความจำเป็น

๒.๗.๖ ผู้ดูแลระบบต้องควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) ที่มีการใช้งานอยู่ภายในระบบเครือข่าย

๒.๗.๗ เมื่อผู้ดูแลระบบตรวจพบว่ามีผู้ใช้งานลักลอบกำหนดหมายเลขเครือข่าย (IP Address) เอง ให้รีบดำเนินการแจ้งไปยังผู้บังคับบัญชา เพื่อประสานต่อไปยังผู้บังคับบัญชาของผู้ใช้งานรายนั้น ให้ทำการตักเตือนและยุติการใช้งานหมายเลขเครือข่าย (IP Address) ที่ลักลอบกำหนดขึ้นมา หากตักเตือนแล้วยังมีการกระทำซ้ำอีก ควรดำเนินการแจ้งไปยังผู้บริหาร เพื่อลงโทษตามระเบียบต่อไป

๒.๗.๘ เครื่องคอมพิวเตอร์หรือระบบสารสนเทศใด ที่มีการใช้งานหมายเลขเครือข่าย (IP Address) ที่เป็นหมายเลขเครือข่ายแบบภายนอก (WAN) หรือหมายเลขเครือข่าย (IP Address Version ๖) ผู้ดูแลระบบควรติดตั้งระบบรักษาความปลอดภัย เช่น ระบบป้องกันไวรัส หรือทำการอัปเดต Patch Version ของ Application Software ให้ทันสมัยตลอดเวลา ทั้งนี้ เพื่อเป็นการลดช่องโหว่ในการลักลอบเข้าโจมตีระบบเครือข่ายผ่านทางหมายเลขเครือข่าย (IP Address) ดังกล่าว

๒.๘ กรมทรัพยากรน้ำได้กำหนดให้การส่ง-รับข้อมูลที่มีความสำคัญหรือเป็นความลับ ผ่านระบบเครือข่ายและคอมพิวเตอร์ต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล

๒.๙ กรมทรัพยากรน้ำต้องจัดเก็บข้อมูลจราจรของอุปกรณ์ที่ใช้งานบนระบบเครือข่ายและคอมพิวเตอร์อย่างต่อเนื่อง ไม่น้อยกว่า ๙๐ วัน

๒.๑๐ กรมทรัพยากรน้ำได้กำหนดให้การเข้าถึงระบบจัดเก็บข้อมูลจราจรบนระบบเครือข่าย ต้องเป็นไปอย่างรัดกุม ปลอดภัยและเข้าถึงได้เฉพาะผู้มีสิทธิเท่านั้น

๒.๑๑ การใช้เครื่องมือในการดักจับข้อมูลบนระบบเครือข่ายและคอมพิวเตอร์ และ/หรือ เครื่องมือเพื่อประเมินช่องโหว่และตรวจสอบระบบเครือข่าย ต้องได้รับความเห็นชอบอย่างเป็นทางการจากผู้ดูแลระบบเท่านั้น

๒.๑๒ กรมทรัพยากรน้ำมีข้อบังคับในการติดตั้งระบบรักษาความปลอดภัยบนอุปกรณ์คอมพิวเตอร์ทุกเครื่อง ที่มีความต้องการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ภายในกรมทรัพยากรน้ำ และไม่อนุญาตให้อุปกรณ์คอมพิวเตอร์ที่ไม่มีระบบรักษาความปลอดภัยเข้าถึงระบบเครือข่ายคอมพิวเตอร์อย่างเด็ดขาด โดยนำเทคโนโลยีต่างๆ เช่น ระบบ Network Access Control มาช่วยตรวจสอบอุปกรณ์ต่างๆ ที่เชื่อมต่ออยู่ภายในระบบเครือข่ายคอมพิวเตอร์ของกรมทรัพยากรน้ำว่ามีอุปกรณ์ใดบ้างที่ละเมิดข้อบังคับดังกล่าว

ส่วนที่ ๖
การเข้าถึงระบบปฏิบัติการ
(Operating Systems Access Control)

๑. วัตถุประสงค์

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต และเพื่อให้ระบบปฏิบัติการมีความปลอดภัย เชื่อถือได้ และมีประสิทธิภาพในการให้บริการ

๒. การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๒.๑ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒.๒ ผู้ดูแลระบบต้องจำกัดสิทธิในการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน ให้มีความเหมาะสมและเพียงพอต่อการใช้งาน โดยให้ยืนยันตัวตนในการเข้าใช้งาน

๒.๓ ผู้ดูแลระบบต้องติดตั้งโปรแกรมช่วยบริหารจัดการ หรือ Domain controller หรือระบบที่มีความเทียบเท่า เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของกรมทรัพยากรน้ำ และกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน สำหรับเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของกรมทรัพยากรน้ำ

๒.๔ ผู้ดูแลระบบต้องเป็นผู้กำหนดมาตรฐานของระบบปฏิบัติการ ที่อนุญาตให้ใช้งานภายในกรมทรัพยากรน้ำ หากมีการร้องขอเพื่อใช้ระบบปฏิบัติการที่กรมทรัพยากรน้ำไม่อนุญาต ต้องทำหนังสือเพื่อขออนุญาตผู้บังคับบัญชาตามลำดับขั้น อย่างเป็นลายลักษณ์อักษร

๒.๕ ผู้ดูแลระบบต้องกำหนดมาตรฐานชื่อผู้ใช้งาน (Username) สำหรับผู้ใช้งานทั่วไป ให้มีรูปแบบเดียวกันทั้งกรมทรัพยากรน้ำ เพื่อให้ง่ายต่อการบริหารจัดการ

๒.๖ เมื่อผู้ดูแลระบบได้จัดสรรบัญชีผู้ใช้งานและรหัสผ่านครั้งแรกให้กับผู้ใช้งาน ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ตนรับผิดชอบ

๒.๗ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องทำการใส่รหัสผ่าน (Password) เพื่อเข้าใช้งานทุกครั้ง

๒.๘ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ของกรมทรัพยากรน้ำร่วมกัน

๒.๙ เมื่อมีการนำเครื่องคอมพิวเตอร์จากภายนอกเข้ามาใช้งานภายในกรมทรัพยากรน้ำ หรือเมื่อมีการติดตั้งเครื่องคอมพิวเตอร์ชุดใหม่ภายในกรมทรัพยากรน้ำ ผู้ดูแลระบบควรตรวจสอบว่าระบบปฏิบัติการที่ติดตั้งใช้งานบนเครื่องคอมพิวเตอร์เหล่านั้น มีลิขสิทธิ์ถูกต้องตามกฎหมายหรือไม่ เนื่องจากระบบปฏิบัติการที่ละเมิดลิขสิทธิ์นั้น โดยมากมักจะมีช่องโหว่ที่แฝงมากับ Key Generator ที่ผิดกฎหมาย โดยพร้อมจะเป็นช่องทางให้เข้ามาโจมตีระบบเครือข่ายสารสนเทศได้ตลอดเวลา

๒.๑๐ กรมทรัพยากรน้ำคำนึงถึงการใช้งานระบบปฏิบัติการที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย และควรจัดเตรียมบุคลากรเพื่อทำการศึกษาเกี่ยวกับการนำระบบปฏิบัติการแบบ Open Source มาใช้งานภายในกรมทรัพยากรน้ำ

๓. **การระบุและยืนยันตัวตนของผู้ใช้งาน**

๓.๑ ผู้ใช้งานต้องทำการระบุชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ทุกครั้ง ก่อนการเข้าถึงระบบปฏิบัติการ

๓.๒ ผู้ใช้งานทุกคนต้องมีชื่อผู้ใช้งาน (Username) แยกจากกันของแต่ละบุคคล เพื่อใช้ในการพิสูจน์ตัวตน โดยไม่อนุญาตให้มีการใช้ชื่อผู้ใช้งานระบบ (Username) และรหัสผ่าน (Password) ร่วมกัน

๓.๓ ผู้ใช้งานต้องทำการเก็บรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับการเข้าถึงระบบไว้เป็นความลับ ไม่เผยแพร่ให้กับบุคคลอื่นให้รับทราบ

๓.๔ ผู้ใช้งานต้องลงบันทึกออก (Logout) ออกจากระบบปฏิบัติการทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือไม่ได้อยู่หน้าจอเป็นเวลานาน

๔. **การบริหารจัดการรหัสผ่านสำหรับการเข้าถึงระบบปฏิบัติการ**

๔.๑ กรมทรัพยากรน้ำต้องจัดให้มีระบบบริหารจัดการรหัสผ่าน ที่สามารถทำงานเชิงโต้ตอบ

๔.๒ ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย

๔.๓ วิธีการบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัยสำหรับการเข้าถึงระบบปฏิบัติการต้องเป็นไปตามการบริหารจัดการรหัสผ่าน ภายใต้นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้งาน

๔.๔ ผู้ดูแลระบบต้องกำหนดให้มีการจำกัดระยะเวลาในการป้อนรหัสผ่าน เพื่อให้กระบวนการในการเข้าสู่ระบบสารสนเทศเป็นไปอย่างมั่นคงปลอดภัย ได้แก่ เมื่อผู้ใช้งานป้อนรหัสผ่านผิดเกิน ๕ ครั้ง ระบบจะทำการล็อคสิทธิในการเข้าถึงระบบของผู้ใช้งาน

๔.๕ ผู้ดูแลระบบต้องกำหนดให้มีการเปลี่ยนรหัสผ่านสำหรับเข้าถึงระบบปฏิบัติการของผู้ใช้งานให้เป็นไปตามนโยบายการบริหารจัดการรหัสผ่าน ภายใต้นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้งาน

๔.๖ ผู้ดูแลระบบต้องกำหนดวิธีในการส่งรหัสผ่านให้กับผู้ใช้งานอย่างปลอดภัย โดยที่ผู้ใช้งานไม่ต้องใช้โปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Saved password)

๔.๗ ผู้ใช้งานต้องไม่จดหรือบันทึกรหัสผ่านส่วนบุคคล ไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น ต้องให้ผู้ใช้ลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดาและการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

๔.๘ ผู้ใช้งานต้องไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านทางเครือข่ายคอมพิวเตอร์

๔.๙ ผู้ใช้งานต้องติดต่อผู้ดูแลระบบเท่านั้น ในการขอรหัสผ่านใหม่ และในกรณีที่รหัสผ่านเดิมของผู้ใช้งานไม่สามารถใช้งานได้

๔.๑๐ เมื่อมีการเปลี่ยนแปลงผู้ใช้งานเครื่องคอมพิวเตอร์ ผู้ดูแลระบบจะต้องทำการ Format และติดตั้งระบบปฏิบัติการบนเครื่องคอมพิวเตอร์เหล่านั้นเสียใหม่ เพื่อเพิ่มความปลอดภัยให้แก่เครื่องคอมพิวเตอร์ดังกล่าว และเป็นการช่วยป้องกันมิให้มีการนำข้อมูลของผู้ใช้งานเดิมไปทำให้เกิดความเสียหายต่อกรมทรัพยากรน้ำหรือผู้ใช้งานระบบเอง

๕. การใช้งานโปรแกรมอรรถประโยชน์

การควบคุมการใช้งานโปรแกรมอรรถประโยชน์ ผู้ดูแลระบบต้องมีการกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์สำหรับการเข้าระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

๕.๑ ผู้ดูแลระบบต้องจัดทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานได้ภายในกรมทรัพยากรน้ำ

๕.๒ ผู้ดูแลระบบต้องจำกัดสิทธิในการเข้าถึงโปรแกรมอรรถประโยชน์สำหรับผู้ใช้งาน โดยให้ยืนยันตัวตนในการเข้าถึงโปรแกรมอรรถประโยชน์ดังกล่าว

๕.๓ กรมทรัพยากรน้ำต้องไม่อนุญาตให้มีการใช้งานโปรแกรมอรรถประโยชน์ที่ไม่มีลิขสิทธิ์ถูกต้องภายในกรมทรัพยากรน้ำ และหากมีการตรวจพบความผิดฐานละเมิดลิขสิทธิ์ ให้ถือเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๕.๔ ผู้ใช้งานต้องทำการยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์ที่ไม่มีความจำเป็นในการใช้งานแล้ว

๕.๕ มีการบันทึกข้อมูล Log แสดงการใช้งานโปรแกรมอรรถประโยชน์

๕.๖ ต้องทำการตรวจสอบบันทึกการเรียกใช้งานอย่างสม่ำเสมอ

๕.๗ ผู้ใช้งานห้ามทำการจำหน่ายหรือเผยแพร่ชุดคำสั่งหรือโปรแกรมอรรถประโยชน์เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐

๖. แนวปฏิบัติการหมดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

๖.๑ ผู้ดูแลระบบต้องกำหนดให้ระบบปฏิบัติการและรวมไปถึงระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรน้ำ เช่น ระบบเครือข่าย ให้มีการตัดและหมดเวลาการใช้งาน โดยกำหนดเวลาในการใช้งาน รวมทั้งตั้งปิดการใช้งาน เมื่อไม่มีกิจกรรมการใช้งานใดๆ ในช่วงระยะเวลา ๑๐ นาที

๖.๒ ผู้ดูแลระบบต้องกำหนดให้เครื่องลูกข่ายของผู้ใช้งานทำการล็อคหน้าจอ เมื่อเครื่องลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลา ๑๐ นาที

๖.๓ ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันและพิสูจน์ตัวตนสำหรับผู้ใช้งาน เมื่อเข้าใช้งานระบบปฏิบัติการหลังจากที่มีการยุติการเชื่อมต่อไปแล้ว

๗. การจำกัดระยะเวลาในการเชื่อมต่อกับระบบสารสนเทศ (Limitation of connection time)

๗.๑ ผู้ดูแลระบบต้องทำการกำหนดให้ระบบสารสนเทศ ได้แก่ ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกกรมทรัพยากรน้ำ) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๗.๒ ผู้ดูแลระบบต้องทำการกำหนดให้ระบบสารสนเทศจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น ได้แก่ กำหนดให้ใช้งานได้ ๒ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติ

ส่วนที่ ๗
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่นและสารสนเทศ
(Application Information Access Control)

๑. วัตถุประสงค์

เพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือชุดคำสั่งไม่พึงประสงค์ ซึ่งอาจจะทำให้ข้อมูลหรือระบบสารสนเทศได้รับความเสียหาย หยุดชะงัก ไม่สามารถให้บริการได้ และรวมถึงความสามารถในการตรวจสอบและติดตามการเข้าใช้งานระบบสารสนเทศของเจ้าหน้าที่ได้อย่างถูกต้อง

๒. แนวปฏิบัติการจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

๒.๑ กรมทรัพยากรน้ำต้องกำหนดผู้เป็นเจ้าของระบบสารสนเทศที่กรมทรัพยากรน้ำใช้งานอยู่อย่างชัดเจน

๒.๒ กรมทรัพยากรน้ำมีแนวทางและนโยบายในการกำหนดมาตรฐานอุปกรณ์เครือข่ายไร้สายที่อนุญาตให้ใช้ได้ภายในกรมทรัพยากรน้ำ โดยอุปกรณ์เครือข่ายไร้สายต้องผ่านมาตรฐาน IEEE (IEEE๘๐๒.๑๑ a/b/g/n/ac/ax) หรือมาตรฐานอื่นที่เทียบเท่า และผ่านการรับรองจาก Wi-Fi (Wi-Fi Alliance) รวมถึงได้รับอนุญาตจากหน่วยงานควบคุมความถี่ในประเทศไทย

๒.๓ ผู้เป็นเจ้าของระบบสารสนเทศและผู้ดูแลระบบต้องเป็นผู้กำหนดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญของกรมทรัพยากรน้ำ ได้แก่ จดหมายอิเล็กทรอนิกส์ ระบบอินเทอร์เน็ต ระบบเครือข่ายไร้สาย รวมถึงระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงตามที่ระบุในส่วนที่ ๗ ข้อ ๔.๑ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานตามหน้าที่ที่ควรจะได้รับเท่านั้น และต้องมีการทบทวนสิทธิอย่างสม่ำเสมอ

๒.๔ ผู้ดูแลระบบหรือผู้ที่เป็นเจ้าของระบบสารสนเทศต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศอย่างเหมาะสม ได้แก่ หากไม่มีการใช้ระบบงานสารสนเทศเกินกว่า ๑๐ นาที ระบบจะยุติการใช้งาน และผู้ใช้งานจำเป็นต้องทำการ Login เข้าสู่ระบบสารสนเทศใหม่อีกครั้ง

๒.๕ การบริหารจัดการรหัสผ่านและการลงทะเบียนผู้ใช้งาน สำหรับการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่นและสารสนเทศ ให้ปฏิบัติตามการบริหารจัดการรหัสผ่าน ภายใต้นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้งาน

๒.๖ ผู้ดูแลระบบต้องกำหนดให้มีการเข้ารหัสที่เป็นมาตรฐานในการเชื่อมต่อ เพื่อเข้าถึงระบบสารสนเทศที่มีข้อมูลที่มีความสำคัญมากของกรมทรัพยากรน้ำ

๓. การบริหารจัดการการเข้าถึงระบบสารสนเทศ

๓.๑ ผู้ดูแลระบบต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน สำหรับการเข้าถึงระบบสารสนเทศของกรมทรัพยากรน้ำ โดยต้องกำหนดให้มีขั้นตอนในการปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน ได้แก่ การลาออกหรือการเปลี่ยนตำแหน่งงานภายในกรมทรัพยากรน้ำ

๓.๒ ผู้ดูแลระบบต้องกำหนดให้มีการทบทวนสิทธิสำหรับการเข้าถึงระบบสารสนเทศของกรมทรัพยากรน้ำ

๓.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานและรหัสผ่านของผู้ใช้งาน ดังนี้

๓.๓.๑ รหัสผู้ใช้งานต้องไม่ซ้ำกันและสามารถตรวจสอบได้ว่าใครเป็นเจ้าของรหัสผ่าน

๓.๓.๒ การส่งมอบรหัสผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งาน ต้องกระทำด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีกลไกในการป้องกันข้อมูลในการนำส่งรหัสผู้ใช้งานและรหัสผ่าน

๓.๓.๓ กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผู้ใช้งานและรหัสผ่าน

๓.๓.๔ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓.๓.๕ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผู้ใช้งานและรหัสผ่านทันที เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๓.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าสามารถเข้าถึงระบบได้ถึงระดับใดบ้าง และต้องกำหนดให้รหัสผ่านของผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมทั้งวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

๓.๔.๑ ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๓.๔.๒ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓.๔.๓ การรับ- ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL VPN หรือ XML Encryption หรือมาตรฐานอื่นที่เทียบเท่า

๓.๔.๔ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรมทรัพยากรน้ำ ได้แก่ ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๔. ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงต่อกรมทรัพยากรน้ำดำเนินการ ดังนี้

๔.๑ ผู้ดูแลระบบและผู้เป็นเจ้าของข้อมูลต้องมีการระบุความสำคัญของระบบงาน ซึ่งไวต่อการรบกวนหรือมีผลกระทบสูงต่อกรมทรัพยากรน้ำ ซึ่งรายชื่อของระบบซึ่งไวต่อการรบกวน มีดังนี้

๔.๑.๑ DHCP Server

๔.๑.๒ Antivirus Server

๔.๑.๓ What up Gold Server

๔.๑.๔ NEWS Division Server

๔.๑.๕ GF-MIS Server

๔.๑.๖ Backup Server

๔.๑.๗ Web Regional Server

๔.๑.๘ Plan Server

๔.๑.๙ Data DWR Server

๔.๑.๑๐ WebServer

๔.๑.๑๑ DBSERVER

๔.๑.๑๒ Intranet Server

๔.๑.๑๓ IPV๖ & DNS Server

๔.๑.๑๔ DPIS Server

๔.๑.๑๕ e-library Server

๔.๑.๑๖ system Server

๔.๑.๑๗ mobile app Server

๔.๑.๑๘ Helpdesk Server

๔.๑.๑๙ VM SERVER

๔.๑.๒๐ ระบบจัดเก็บไฟล์ Server

๔.๒ ระบบงานซึ่งไวต่อการรบกวนหรือมีผลกระทบสูงต่อกรมทรัพยากรน้ำ ต้องติดตั้งไว้ในเครื่องคอมพิวเตอร์เฉพาะแยกจากระบบงานอื่น และไม่อนุญาตให้มีการใช้งานทรัพยากรร่วมกับระบบงานอื่น

๔.๓ หากมีความจำเป็นต้องติดตั้งระบบงานที่ไวต่อการรบกวนหรือมีผลกระทบสูงต่อกรมทรัพยากรน้ำร่วมกับระบบงานอื่น ผู้ดูแลระบบและผู้เป็นเจ้าของข้อมูลต้องจัดให้มีการประเมินความเสี่ยง ก่อนที่จะเริ่มดำเนินการให้มีการใช้งานทรัพยากรร่วมกัน

๔.๔ ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายสำหรับระบบที่ไวต่อการรบกวนหรือมีผลกระทบต่อกรมทรัพยากรน้ำสูง ออกจากระบบอื่น

๔.๕ ผู้ดูแลระบบต้องจัดหามาตรการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตสำหรับระบบที่ไวต่อการรบกวนหรือมีผลกระทบต่อกรมทรัพยากรน้ำสูง รวมถึงจัดหาอุปกรณ์สำหรับการตรวจสอบสภาพการให้บริการในแบบ Real Time เพื่อสามารถแก้ไขปัญหาได้ทันท่วงที

๔.๖ ผู้ดูแลระบบต้องจำกัดการเข้าถึงระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงต่อกรมทรัพยากรน้ำ สำหรับบุคลากรฝ่ายสนับสนุนการเข้าใช้งาน

๔.๗ มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารประเภทพกพา และการปฏิบัติงานจากภายนอกที่เกี่ยวข้องกับระบบดังกล่าว

๕. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอก

การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพาของผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Notebook Palmtops Laptop) กรณีเมื่อปฏิบัติงานอยู่นอกสถานที่

๕.๑ กรมทรัพยากรน้ำต้องสร้างความตระหนักให้กับผู้ใช้งานในการใช้งานอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอก เพื่อผู้ใช้งานระมัดระวังและป้องกันการใช้งานและการเข้าถึงระบบเครือข่ายของกรมทรัพยากรน้ำอย่างปลอดภัย

๕.๒ ผู้ใช้งานต้องไม่วางอุปกรณ์สื่อสารประเภทพกพาไว้ในที่ไม่ปลอดภัยหรือไม่สามารถดูแลได้

๕.๓ การใช้งานอุปกรณ์สื่อสารประเภทพกพาและรวมไปถึงการปฏิบัติงานจากภายนอกต้องผ่านขั้นตอนการระบุและพิสูจน์ตัวตนทุกครั้ง

๕.๔ ผู้ใช้งานต้องทำการเข้ารหัสข้อมูลที่สำคัญไว้

๕.๕ ผู้ดูแลระบบต้องตรวจสอบอย่างเคร่งครัดในการขออนุญาต สำหรับกรณีผู้ใช้งานที่มีความจำเป็นจะต้องนำอุปกรณ์สื่อสารประเภทพกพาเข้ามาใช้งานระบบเครือข่ายสารสนเทศ หรือระบบสารสนเทศภายในกรมทรัพยากรน้ำ โดยต้องกำหนดให้ผู้ใช้งานทำการขออนุญาตใช้งานแบบเป็นลายลักษณ์อักษรก่อน จึงจะอนุญาตให้สามารถใช้งานได้

๖. การปฏิบัติงานจากภายนอกสำนักงาน

๖.๑ การเข้าสู่ระบบเครือข่ายของกรมทรัพยากรน้ำจากระยะไกล (Remote Access) ผู้ดูแลระบบต้องกำหนดมาตรการในการรักษาความปลอดภัยที่เพิ่มขึ้น เพื่อให้การเข้าใช้งานระบบมีความปลอดภัยสูงสุด

๖.๒ วิธีการใดๆ ที่สามารถเข้าถึงข้อมูลหรือระบบสารสนเทศจากระยะไกล จะต้องได้รับการอนุมัติจากผู้ดูแลระบบและมีการควบคุมอย่างเข้มงวดก่อนที่จะนำมาใช้งานภายในกรมทรัพยากรน้ำ

๖.๓ ผู้ดูแลระบบต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล

๖.๔ กรมทรัพยากรน้ำไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัว เพื่อเข้าถึงระบบเครือข่ายของกรมทรัพยากรน้ำจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยกรมทรัพยากรน้ำ

๖.๕ การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ต้องดำเนินไปตามหลักเกณฑ์ที่ผู้ดูแลระบบกำหนดไว้และต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับขั้น

๖.๖ ผู้ดูแลระบบควรทำการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบข้อมูลจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ไม่ควรเปิด Port ทิ้งไว้โดยไม่มีความจำเป็น และต้องตัดการเชื่อมต่อเมื่อไม่มีการใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๖.๗ ผู้ดูแลระบบต้องกำหนดให้มีการเก็บบันทึกการเข้าถึงระบบจากระยะไกล โดยในการบันทึกจะต้องประกอบด้วยข้อมูลที่สำคัญที่จำเป็นต้องทราบ เช่น ชื่อสกุลของผู้ที่ต้องการเข้าถึงระบบจากระยะไกล เลขประจำตัวประชาชน ระยะเวลาในการเข้าถึง และสาเหตุที่ต้องการเข้าถึง โดยจะต้องหมั่นตรวจสอบข้อมูลที่มีการบันทึกไว้อย่างสม่ำเสมอ

๖.๘ ผู้ดูแลระบบจะต้องทำการสรุปรายละเอียดการเข้าถึงระบบจากระยะไกลให้กับผู้บังคับบัญชาทราบอย่างน้อยเดือนละ ๑ ครั้ง

๗. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๗.๑ ต้องพิจารณาระบุสิทธิในซอร์สโค้ด (Source code) ของการพัฒนาซอฟต์แวร์ โดยผู้รับจ้างที่ให้บริการจากภายนอก

๗.๒ สงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้รับจ้างที่ให้บริการจากภายนอก

๗.๓ หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่างๆ โดยเร็วที่สุดเพื่อความปลอดภัยของระบบ

๗.๔ ในกรณีผู้รับจ้างที่ให้บริการจากภายนอกมีการเข้าใช้ระบบคอมพิวเตอร์ภายในกรมทรัพยากรน้ำต้องมีการดำเนินการ ดังนี้

๗.๔.๑ ผู้รับจ้างที่ให้บริการจากภายนอกจะต้องแจ้งรายชื่อผู้ที่จะเข้ามาใช้ระบบคอมพิวเตอร์ล่วงหน้า และต้องมีการลงชื่อเข้าใช้งานห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ทุกครั้งที่มีการเข้าใช้งาน นอกจากนี้ หากผู้รับจ้างที่ให้บริการจากภายนอกต้องใช้งานห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ในวันหยุดหรือนอกเวลาราชการ จะต้องขออนุญาตจากผู้รับผิดชอบหรือผู้ดูแลระบบล่วงหน้า

๗.๔.๒ หน่วยงานภายนอกต้องทำการบันทึกค่า Config และ/หรือซอร์สโค้ดเดิม ทุกครั้งที่จะมีการแก้ไขค่า Config ซอร์สโค้ดระบบงานสารสนเทศบนระบบ Production หากการแก้ไขมีปัญหาเกิดขึ้น ผู้รับจ้างที่ให้บริการจากภายนอกจะสามารถใช้ค่าและ/หรือซอร์สโค้ดเดิม เพื่อให้ระบบสามารถกลับมาใช้งานได้

๗.๕ ซอฟต์แวร์ที่ถูกพัฒนาจากหน่วยงานภายนอก หากมีการติดตั้งบริการผ่านระบบเครือข่ายคอมพิวเตอร์ภายในกรมทรัพยากรน้ำ จะมีการจัดให้ทำ Penetration Test อย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นการตรวจสอบหาช่องโหว่บนระบบซอฟต์แวร์ดังกล่าว เพื่อนำข้อมูลที่ได้มาปรับปรุงการรักษาความปลอดภัยให้กับระบบซอฟต์แวร์ดังกล่าว เพื่อลดความเสี่ยงในการถูกโจมตีจากผู้ไม่ประสงค์ดีจากภายนอก

ส่วนที่ ๘
การควบคุมการเข้าถึงระบบเครือข่ายชนิดไร้สาย
(Wireless Access Control)

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยและกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สายของกรมทรัพยากรน้ำ โดยการกำหนดสิทธิของผู้ใช้งานให้เหมาะสม และเพื่อให้มีการควบคุมและป้องกันทางกายภาพสำหรับอุปกรณ์ระบบเครือข่ายไร้สาย

๒. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๒.๑ กรมทรัพยากรน้ำต้องกำหนดให้ศูนย์สารสนเทศของกรมทรัพยากรน้ำเป็นหน่วยงานที่ดูแล ควบคุมการติดตั้ง ใช้งาน และกำหนดสิทธิการเข้าถึงระบบเครือข่ายไร้สายของกรมทรัพยากรน้ำเท่านั้น

๒.๒ กรมทรัพยากรน้ำต้องเป็นผู้กำหนดมาตรฐานอุปกรณ์เครือข่ายไร้สายที่อนุญาตให้ใช้ได้ภายในกรมทรัพยากรน้ำ โดยอุปกรณ์เครือข่ายไร้สายต้องผ่านมาตรฐาน IEEE (IEEE ๘๐๒.๑๑b, g, n และ ac) หรือมาตรฐานอื่นที่เทียบเท่า และผ่านการรับรองจาก Wi-Fi (Wi-Fi Alliance) รวมถึงได้รับอนุญาตจากหน่วยงานควบคุมความถี่ในประเทศไทย

๒.๓ กรมทรัพยากรน้ำไม่อนุญาตให้มีการติดตั้งเครือข่ายไร้สายเพื่อใช้งานในหน่วยงานเอง โดยไม่ได้รับการอนุมัติหรือเห็นชอบจากศูนย์สารสนเทศของกรมทรัพยากรน้ำอย่างเป็นลายลักษณ์อักษร

๒.๔ กรมทรัพยากรน้ำต้องติดตั้งระบบเพื่อควบคุมการใช้งานระบบเครือข่ายไร้สาย ให้มีความปลอดภัยระหว่างระบบไร้สายกับเครือข่ายภายในกรมทรัพยากรน้ำ

๒.๕ ผู้ดูแลระบบต้องควบคุมตำแหน่งการวางอุปกรณ์ Access Point (AP) ทางกายภาพให้เหมาะสม เพื่อควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลไปนอกบริเวณพื้นที่ใช้งานของกรมทรัพยากรน้ำ และเพื่อป้องกันผู้ไม่ประสงค์ดีจากการเข้าถึงอุปกรณ์เครือข่ายไร้สายของกรมทรัพยากรน้ำได้ รวมไปถึงการโจรกรรมอุปกรณ์เครือข่ายไร้สายอีกด้วย

๒.๖ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ Access Point มาติดตั้งเพื่อใช้งานในกรมทรัพยากรน้ำ

๒.๗ ผู้ดูแลระบบต้องทำการเปลี่ยนค่ารหัสผู้ใช้งาน หรือชื่อ Login และรหัสผ่าน สำหรับการติดตั้งค่าการทำงานของอุปกรณ์ไร้สาย โดยตั้งค่า Login ให้ยากต่อการคาดเดา และติดตั้งรหัสผ่านให้เป็นไปตามนโยบายการบริหารจัดการรหัสผ่าน

๒.๘ ผู้ดูแลระบบต้องกำหนดให้มีการเก็บบันทึกเหตุการณ์หรือข้อมูลจราจรคอมพิวเตอร์ที่เกิดขึ้นของระบบเครือข่ายไร้สาย

๒.๙ ผู้ดูแลระบบต้องกำหนดขั้นตอนในการขอเข้าใช้งานเครือข่ายระบบไร้สายสำหรับผู้ใช้งาน

๒.๑๐ ผู้ใช้งานจะต้องมีบัญชีผู้ใช้งานระบบเครือข่ายไร้สายของกรมทรัพยากรน้ำ จึงจะสามารถใช้งานระบบเครือข่ายไร้สายได้

๒.๑๑ ผู้ดูแลระบบต้องทำการกำหนดขั้นตอนการปฏิบัติเพื่อลงทะเบียนผู้ใช้งาน สำหรับการใช้งานระบบเครือข่ายไร้สายของกรมทรัพยากรน้ำ

๒.๑๒ กรมทรัพยากรน้ำต้องใช้งานระบบเครือข่ายไร้สายที่มีระบบบริหารจัดการจากส่วนกลาง (Wireless Controller) เพื่อที่จะช่วยให้สามารถบริหารจัดการระบบเครือข่ายไร้สายได้อย่างมีประสิทธิภาพและถูกต้องตามมาตรฐานการใช้งานระบบเครือข่ายไร้สายภายในกรมทรัพยากรน้ำ

๒.๑๓ ผู้ดูแลระบบต้องทำการบริหารจัดการกำหนดปริมาณ Bandwidth ในการใช้งานระบบเครือข่ายไร้สายตามความเหมาะสมในการใช้งานของแต่ละกลุ่มงาน เพื่อเป็นการป้องกันปัญหาระบบเครือข่ายสารสนเทศให้บริการได้ช้าเนื่องจากปัญหาการใช้งานระบบเครือข่ายไร้สายมากเกินความจำเป็น

๒.๑๔ ในกรณีที่มีการขออนุญาตใช้งานระบบเครือข่ายไร้สายจากบุคคลภายนอก ผู้ดูแลระบบต้องทำการบันทึกข้อมูลของบุคคลภายนอกดังกล่าวไว้ทุกครั้ง โดยข้อมูลจะต้องประกอบด้วย ชื่อ-สกุล เลขบัตรประจำตัวประชาชน หน่วยงานที่สังกัด MAC ADDRESS ของอุปกรณ์ที่ต้องการทำการเชื่อมต่อ เป็นอย่างน้อย

๒.๑๕ การสร้างบัญชีการใช้งานระบบเครือข่ายไร้สายให้กับบุคคลภายนอกนั้น จะต้องทำการกำหนดให้ ๑ บัญชี ไม่สามารถใช้ได้เกินกว่า ๑-๒ อุปกรณ์เท่านั้น เพื่อเป็นการป้องกันการนำบัญชีดังกล่าวไปแจกจ่ายยังบุคคลภายนอกอื่นๆ ที่ไม่ได้ทำการขออนุญาต

๒.๑๖ ผู้ดูแลระบบต้องทำการกำหนดช่วงระยะเวลาการหมดอายุ (Session Timeout) ในการใช้งานระบบเครือข่ายไร้สายของบุคคลภายนอกทุกครั้งโดยไม่มีข้อยกเว้น ในกรณีที่บุคคลภายนอกดังกล่าวมีความต้องการใช้งานเพิ่มเติมให้ทำการแจ้งความประสงค์ในการใช้งานมายังผู้ดูแลระบบเพื่อทำการขยายเพิ่มเติมระยะเวลาในการใช้งาน

ส่วนที่ ๙
การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
(Personal Computer)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานในกรมทรัพยากรน้ำรับทราบกฎเกณฑ์ในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลอย่างปลอดภัยและป้องกันการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลผิดวัตถุประสงค์

๒. แนวปฏิบัติการใช้งานทั่วไปของเครื่องคอมพิวเตอร์ส่วนบุคคล

๒.๑ ผู้ใช้งานต้องใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่เกี่ยวข้อง รวมถึงระบบติดต่อสื่อสารของกรมทรัพยากรน้ำ ในเรื่องที่เกี่ยวข้องกับการดำเนินงานของกรมทรัพยากรน้ำเท่านั้น

๒.๒ ผู้ใช้งานต้องรับผิดชอบในการเก็บและดูแลรักษาความปลอดภัยเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อเชื่อมต่างๆ (Computer Peripherals) ที่อยู่ในความรับผิดชอบของตน

๒.๓ ผู้ใช้งานต้องทำการใส่ข้อมูลบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อทำการพิสูจน์ตัวตนก่อนเข้าถึงคอมพิวเตอร์ส่วนบุคคล

๒.๔ ห้ามผู้ใช้งานเปิดเผยบัญชีรายชื่อผู้ใช้งานหรือรหัสผ่านให้บุคคลอื่นรับทราบ หรืออนุญาตให้บุคคลอื่นใช้บัญชีรายชื่อผู้ใช้ระบบงานของตนในการปฏิบัติงาน

๒.๕ ชุดโปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ต้องเป็นโปรแกรมที่มีลิขสิทธิ์อย่างถูกต้องตามกฎหมาย

๒.๖ การติดตั้งชุดโปรแกรมที่เป็นฟรีแวร์หรือแชร์แวร์ ต้องดำเนินการตามข้อกำหนดทางกฎหมายของชุดโปรแกรมนั้นๆ

๒.๗ ผู้ใช้งานต้องทำการล็อคหน้าจอทุกครั้ง ในกรณีที่ผู้ใช้งานไม่ได้ปฏิบัติงานอยู่หน้าเครื่องคอมพิวเตอร์และต้องมีการใส่รหัสผ่านทุกครั้งเมื่อต้องการกลับเข้าสู่หน้าจอ

๒.๘ ผู้ใช้งานต้องทำการสำรองข้อมูลของตนเองอย่างสม่ำเสมอ

๒.๙ กรมทรัพยากรน้ำไม่อนุญาตให้ผู้ใช้งานนำเครื่องคอมพิวเตอร์และอุปกรณ์อื่นที่เป็นของส่วนตัวเข้ามาใช้งานร่วมกับระบบสารสนเทศ ถ้าอุปกรณ์ดังกล่าวยังไม่อยู่ภายใต้การดูแลควบคุมตามนโยบายของกรมทรัพยากรน้ำ

๒.๑๐ ผู้ใช้งานต้องทำการเก็บรักษาสื่อบันทึกข้อมูลต่างๆ ได้แก่ Diskette CD Thumb drive โดยเฉพาะอุปกรณ์ที่ใช้ในการบันทึกข้อมูลต่างๆ ของกรมทรัพยากรน้ำอย่างปลอดภัย

๒.๑๑ ห้ามผู้ใช้งานทำการโพสต์หรือนำส่งข้อมูลที่เป็นความลับของกรมทรัพยากรน้ำผ่านช่องทางส่วนตัว ได้แก่ Social Media ส่วนตัวต่างๆ

๒.๑๒ ห้ามผู้ใช้งานใช้ทรัพย์สินทางด้านคอมพิวเตอร์ของกรมทรัพยากรน้ำ ทำการส่งข้อมูลอันใดที่มีเนื้อหาเกี่ยวข้องกับการคุกคามทางเพศหรือมีเจตนาต่อต้านข้อกฎหมายต่างๆ

๒.๑๓ ห้ามผู้ใช้งานทำการละเมิดกรรมสิทธิ์ สิทธิบัตร ลิขสิทธิ์ หรือทรัพย์สินทางปัญญาของบุคคลหรือกรมทรัพยากรน้ำ รวมถึงห้ามทำการติดตั้ง แจกจ่าย ทำซ้ำ โปรแกรม เนื้อหา ภาพถ่าย หนังสือ เพลง และอื่นๆ ที่กรมทรัพยากรน้ำไม่ได้รับลิขสิทธิ์ให้บุคคลใดๆ ดำเนินการดังกล่าว

๒.๑๔ ห้ามผู้ใช้งานทำกิจกรรมใดที่ก่อให้เกิดความเสียหายต่อการรักษาความปลอดภัยสารสนเทศหรือการหยุดชะงักของการให้บริการของระบบ ได้แก่ การเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาตหรือการทำ Network Sniffing Pinged Floods Packet Spoofing Denial of Service Port Scan

๒.๑๕ ห้ามผู้ใช้งานเข้าเว็บไซต์ที่ไม่เหมาะสมและไม่เกี่ยวข้องกับการปฏิบัติงาน

๒.๑๖ ห้ามผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ส่วนบุคคล

๒.๑๗ กรณีที่ผู้ใช้งานต้องการนำอุปกรณ์คอมพิวเตอร์หรือทรัพย์สินของกรมทรัพยากรน้ำออกนอกสถานที่ ต้องได้รับอนุญาตจากกรมทรัพยากรน้ำหรือผู้มีอำนาจก่อนเท่านั้น

๒.๑๘ กรมทรัพยากรน้ำจะต้องแจ้งให้ผู้ใช้งานตระหนักถึงกฎหมายในส่วนของการละเมิดลิขสิทธิ์การใช้งานซอฟต์แวร์ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ จากการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลอย่างเคร่งครัด

๒.๑๙ กรณีที่ผู้ใช้งานต้องการนำอุปกรณ์คอมพิวเตอร์หรือทรัพย์สินจากภายนอกมาใช้งานร่วมกับระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศภายในกรมทรัพยากรน้ำ ผู้ใช้งานจะต้องแจ้งขออนุญาตจากกรมทรัพยากรน้ำหรือผู้มีอำนาจก่อนเท่านั้น และจะต้องนำอุปกรณ์คอมพิวเตอร์หรือทรัพย์สินมาให้ตรวจสอบความปลอดภัยก่อนทุกครั้ง พร้อมทั้งยินยอมให้กรมทรัพยากรน้ำติดตั้งระบบรักษาความปลอดภัยบนอุปกรณ์คอมพิวเตอร์หรือทรัพย์สินที่นำมาใช้งานเพื่อเป็นการปฏิบัติตามข้อกำหนด หรือข้อบังคับในการรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศของกรมทรัพยากรน้ำ

ส่วนที่ ๑๐
การใช้งานอินเทอร์เน็ต
(Internet Usage)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานระบบในกรมทรัพยากรน้ำรับทราบกฎเกณฑ์ในการใช้งานเครือข่ายอินเทอร์เน็ตอย่างปลอดภัยและป้องกันการใช้งานระบบอินเทอร์เน็ตผิดวัตถุประสงค์ รวมไปถึงเพื่อให้มีการบริหารจัดการระบบเครือข่ายอินเทอร์เน็ตอย่างมั่นคงปลอดภัย

๒. กระบวนการควบคุมสำหรับการใช้งานอินเทอร์เน็ต

๒.๑ ผู้ใช้งานต้องเข้าถึงอินเทอร์เน็ตผ่านช่องทางที่กรมทรัพยากรน้ำกำหนดเท่านั้น

๒.๒ ผู้ใช้งานระบบอินเทอร์เน็ตของกรมทรัพยากรน้ำ ต้องใช้อินเทอร์เน็ตเพื่อวัตถุประสงค์ทางการดำเนินธุรกรรมที่เกี่ยวข้องกับกรมทรัพยากรน้ำเท่านั้น

๒.๓ ผู้ใช้งานเครื่องคอมพิวเตอร์เพื่อเชื่อมต่อกับระบบอินเทอร์เน็ตจะต้องมีเปิดใช้โปรแกรมป้องกันไวรัสก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์ของระบบปฏิบัติการ

๒.๔ ผู้ใช้งานต้องทำการตรวจสอบไวรัสก่อนทำการดาวน์โหลดไฟล์ หรือรับ-ส่งไฟล์หรือข้อมูลจากระบบเครือข่ายอินเทอร์เน็ต

๒.๕ ผู้ใช้งานต้องไม่ใช้ เข้าถึง ดาวน์โหลด พิมพ์ เก็บ หรือส่งต่อข้อมูลใดๆ ที่ผิดกฎหมาย หรือข้อมูลที่อาจก่อให้เกิดปัญหาทางศีลธรรม โดยใช้เครือข่ายอินเทอร์เน็ตของกรมทรัพยากรน้ำ

๒.๖ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๒.๗ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมทรัพยากรน้ำที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒.๘ ห้ามผู้ใช้งานใช้เครือข่ายอินเทอร์เน็ตของกรมทรัพยากรน้ำ เพื่อการแพร่กระจายโปรแกรมไม่ประสงค์ดีทุกประเภท

๒.๙ ห้ามผู้ใช้งานใช้เครือข่ายอินเทอร์เน็ตของกรมทรัพยากรน้ำ เพื่อทำกิจกรรมที่ไม่เหมาะสม ได้แก่ กิจกรรมที่ขัดต่อศีลธรรม ข่มขู่ หรือคุกคามผู้อื่น เกี่ยวข้องกับความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เป็นภัยต่อสังคม ผิดกฎหมาย หรือก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงของกรมทรัพยากรน้ำ

๒.๑๐ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ Blog หรือ Social Media ต่างๆ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของกรมทรัพยากรน้ำ ไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรมทรัพยากรน้ำ การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๒.๑๑ กรมทรัพยากรน้ำต้องแจ้งให้ผู้ใช้งานตระหนักถึงกฎหมายในส่วนของการดาวน์โหลดและติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ และรวมถึงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ จากการใช้งานอินทอร์เน็ตของกรมทรัพยากรน้ำอย่างเคร่งครัด

๒.๑๒ ห้ามผู้ใช้งานทำการดาวน์โหลดซอฟต์แวร์ละเมิดลิขสิทธิ์ โปรแกรมในการสร้าง Licenses ปลอม หรือ Script ในการปลดลิขสิทธิ์การใช้งานซอฟต์แวร์ต่างๆ ด้วยอินเทอร์เน็ตของกรมทรัพยากรน้ำ

๒.๑๓ ห้ามผู้ใช้งานเปิดใช้งานโปรแกรมประเภท Peer-to-Peer (P๒P) เพื่อทำการดาวน์โหลด หรืออัพโหลดไฟล์ต่างๆ ผ่านทางอินเทอร์เน็ตของกรมทรัพยากรน้ำ

๒.๑๔ ห้ามผู้ใช้งานนำอินเทอร์เน็ตของกรมทรัพยากรน้ำไปใช้งานเพื่อประโยชน์เชิงพาณิชย์ส่วนตัว

๒.๑๕ ห้ามผู้ใช้งานนำอินเทอร์เน็ตของกรมทรัพยากรน้ำไปใช้งานเพื่อแสวงหาผลประโยชน์ให้กับตนเองผ่านระบบเครือข่ายบล็อกเชนในการขุด Bit Coin เป็นอันขาด

ส่วนที่ ๑๑
การใช้งานจดหมายอิเล็กทรอนิกส์
(Email Usage)

๑. วัตถุประสงค์

เพื่อทำให้การใช้งานจดหมายอิเล็กทรอนิกส์เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ ลดความเสี่ยงการนำภัยคุกคามจากภายนอกผ่านทางระบบจดหมายอิเล็กทรอนิกส์ และป้องกันการใช้งานจดหมายอิเล็กทรอนิกส์อย่างผิดวัตถุประสงค์

๒. กระบวนการควบคุมสำหรับการใช้งานจดหมายอิเล็กทรอนิกส์

๒.๑ ห้ามใช้บัญชีจดหมายอิเล็กทรอนิกส์และรหัสผ่านร่วมกัน

๒.๒ ผู้ใช้งานต้องไม่ทำการส่งจดหมายอิเล็กทรอนิกส์หรือเอกสารแนบที่มีข้อมูลที่เป็นความลับของกรมทรัพยากรน้ำ ไปยังบัญชีจดหมายอิเล็กทรอนิกส์ส่วนบุคคลที่บริหารจัดการโดยหน่วยงานภายนอก

๒.๓ ห้ามผู้ใช้งานทำการส่งจดหมายอิเล็กทรอนิกส์ให้กับหน่วยงานภายนอกหรือบุคคลภายนอกกรมทรัพยากรน้ำที่ไม่ได้ทำการตกลงในการรับข้อมูลผ่านทางจดหมายอิเล็กทรอนิกส์กับกรมทรัพยากรน้ำหรือถ้ามีความจำเป็น ต้องมีการพิจารณาถึงความเหมาะสม เพื่อป้องกันการรบกวนผู้รับจดหมายอิเล็กทรอนิกส์

๒.๔ ห้ามผู้ใช้งานทำการเปลี่ยนแปลงเนื้อหาของจดหมายอิเล็กทรอนิกส์ที่ทำการส่งต่อ ยกเว้นเมื่อได้รับอนุญาตจากเจ้าของจดหมายอิเล็กทรอนิกส์ต้นฉบับหรือมีการแสดงข้อมูลที่ทำการแก้ไขอย่างชัดเจน

๒.๕ ในกรณีที่ข้อมูลเป็นความลับ ผู้ใช้งานต้องมีทำการเข้ารหัสข้อมูลทุกครั้งก่อนส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต

๒.๖ ห้ามผู้ใช้งานทำการส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาที่ไม่เหมาะสม ได้แก่ ลามก หยาบคาย รุกราน ต่อต้าน ปลุกระดม ดูแคลน

๒.๗ การส่งจดหมายอิเล็กทรอนิกส์ทุกครั้ง ผู้ใช้งานควรมีการระบุรายละเอียดของผู้ใช้งานที่ทำการส่ง (Signature Block) โดยให้เป็นไปตามมาตรฐานของกรมทรัพยากรน้ำ โดยรายละเอียดดังกล่าวต้องระบุถึงชื่อและนามสกุลของผู้ส่งจดหมายอิเล็กทรอนิกส์ ตำแหน่งงานและต้นสังกัดของผู้ส่งจดหมายอิเล็กทรอนิกส์ รวมไปถึงหมายเลขโทรศัพท์ที่ใช้ในการติดต่อ

๒.๘ ผู้ใช้งานต้องจำกัดการใช้งานจดหมายอิเล็กทรอนิกส์ โดยใช้งานเฉพาะงานที่เกี่ยวข้องกับการดำเนินธุรกิจของกรมทรัพยากรน้ำเท่านั้น เพื่อลดความสิ้นเปลืองของทรัพยากรทางด้านเครือข่าย

๒.๙ ห้ามผู้ใช้งานใช้งานจดหมายอิเล็กทรอนิกส์ในลักษณะ ดังนี้

- ทำการส่ง Executable File หรือไฟล์ที่มีความเสี่ยงต่อการทำงานของระบบจดหมายอิเล็กทรอนิกส์
- ทำการให้ข้อมูลเกี่ยวกับบุคคลอื่นใดแก่ผู้ไม่ได้รับอนุญาต
- ทำการส่งจดหมายอิเล็กทรอนิกส์ที่ส่งผลรบกวนการให้บริการของระบบ
- ทำการส่งจดหมายอิเล็กทรอนิกส์ลูกโซ่ จดหมายอิเล็กทรอนิกส์ขยะ จดหมายอิเล็กทรอนิกส์ที่มีไวรัสหรือโปรแกรมที่ละเมิดลิขสิทธิ์

๒.๑๐ การเข้าถึงเนื้อหาของจดหมายอิเล็กทรอนิกส์ที่ทำการเก็บในระบบหรือทำการส่งผ่านระบบต้องถูกจำกัดให้สามารถเข้าถึงได้เฉพาะผู้ทำการส่งจดหมายอิเล็กทรอนิกส์ ผู้รับจดหมายอิเล็กทรอนิกส์ หรือผู้ที่ได้รับอนุญาตจากผู้ส่งเท่านั้น สำหรับการเข้าถึงรูปแบบอื่นๆ ต้องมีเหตุผลสำหรับการเข้าถึง ดังนี้

๒.๑๐.๑ เพื่อทำการตรวจสอบตามข้อบังคับหรือกฎหมายที่เกี่ยวข้อง

๒.๑๐.๒ เพื่อวัตถุประสงค์ในการสืบสวนในการรักษาความปลอดภัยของระบบ

๒.๑๑ ผู้ดูแลระบบต้องแจ้งให้ผู้ใช้งานทราบว่ากรมทรัพยากรน้ำมีการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านการให้บริการของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งจะมีการเก็บ Log การใช้งานบัญชีจดหมายอิเล็กทรอนิกส์ทุกบัญชี ดังนั้น การใช้งานจดหมายอิเล็กทรอนิกส์ของหน่วยงานจะใช้เพื่ออำนวยความสะดวกในการปฏิบัติงานเท่านั้น และระวังการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๒.๑๒ ห้ามผู้ใช้บัญชีจดหมายอิเล็กทรอนิกส์เปิดเผยรหัสผ่านของตนเองแก่ผู้ใช้งานท่านอื่น หรือผู้ใช้งานภายนอกกรมทรัพยากรน้ำ

๒.๑๓ ห้ามผู้ใช้บัญชีจดหมายอิเล็กทรอนิกส์นำบัญชีการใช้งานของตนเองเพื่อไปทำธุรกรรมในการซื้อขายแบบออนไลน์หรือนำไปสร้างเป็นบัญชีเพื่อประโยชน์ในทางการค้าเชิงพาณิชย์

๒.๑๔ ผู้ใช้บัญชีจดหมายอิเล็กทรอนิกส์ไม่ควรนำบัญชีการใช้งานของหน่วยงานไปทำการสมัครใช้งานสื่อสังคมออนไลน์ต่างๆ เพื่อความปลอดภัยในข้อมูลจดหมายอิเล็กทรอนิกส์ของผู้ใช้งานเอง

ส่วนที่ ๑๒
การป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี
(Malicious Code Protection)

๑. วัตถุประสงค์

เพื่อให้กรมทรัพยากรน้ำมีการควบคุมและป้องกันการแพร่ระบาดของไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี รวมไปถึงป้องกันการสูญเสียข้อมูลหรือเปิดเผยข้อมูลที่เป็นความลับ อันเนื่องมาจากไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี

๒. กระบวนการควบคุมสำหรับการป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี

๒.๑ ผู้ดูแลระบบต้องจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัสเวอร์ชั่นล่าสุด บนระบบปฏิบัติการทุกเครื่องในกรมทรัพยากรน้ำ ทั้งเครื่องแม่ข่ายและเครื่องลูกข่าย

๒.๒ กรมทรัพยากรน้ำต้องกำหนดให้ระบบป้องกันไวรัส มีการบริหารจัดการจากส่วนกลาง (Centralized Management)

๒.๓ ผู้ดูแลระบบต้องจัดให้มีการปรับปรุงโปรแกรมป้องกันไวรัส รวมไปถึงฐานข้อมูลโปรแกรมป้องกันไวรัสให้เป็นรุ่นล่าสุดอยู่เสมอ

๒.๔ ผู้ดูแลระบบต้องกำหนดให้โปรแกรมป้องกันไวรัสทำงานพร้อมกับการเริ่มทำงานของระบบประมวลผลหรือระบบปฏิบัติการทุกครั้ง

๒.๕ ผู้ดูแลระบบต้องกำหนดให้โปรแกรมป้องกันไวรัส มีการสแกนสื่อบันทึกข้อมูลของเครื่องคอมพิวเตอร์ (Hard disk) อยู่เป็นประจำ เพื่อทำการค้นหาและจัดการกับชุดคำสั่งประสงค์ร้ายที่อยู่ในสื่อบันทึกข้อมูลนั้นๆ

๒.๖ กรมทรัพยากรน้ำไม่อนุญาตให้มีการถอดถอน (Remove/Uninstall) หรือปิดบริการ (Disable services) ระบบป้องกันไวรัส หรือระบบป้องกันชุดคำสั่งประสงค์ร้าย โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๒.๗ ผู้ดูแลระบบต้องกำหนดแนวทางในการเฝ้าระวังเครือข่ายและเครื่องคอมพิวเตอร์ เพื่อติดตาม วิเคราะห์และหาแนวทางป้องกันปัญหาที่อาจจะเกิดขึ้นจากการแพร่ระบาดของไวรัสภายในกรมทรัพยากรน้ำ

๒.๘ ผู้ดูแลระบบจะต้องให้คำแนะนำในการใช้งานโปรแกรมป้องกันไวรัสแก่ผู้ใช้งาน และแจ้งให้ผู้ใช้งานหมั่นทำการ Update Signature ของโปรแกรมป้องกันไวรัส รวมทั้งทำการตรวจสอบไวรัสบนเครื่องคอมพิวเตอร์ภายใต้การดูแลเป็นประจำอย่างน้อยเดือนละ ๑ ครั้ง

๒.๙ ผู้ใช้งานต้องทำการตรวจหาไวรัสของไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต รวมไปถึงไฟล์ที่มาจากสื่อบันทึกข้อมูลต่างๆ ได้แก่ Thumb Drive, CD หรือ Diskette ก่อนนำไปใช้งาน

๒.๑๐ ผู้ใช้งานห้ามรับหรือทำการติดตั้งโปรแกรมที่ไม่ทราบแหล่งที่มาหรือมีแหล่งที่มาไม่น่าเชื่อถือ

๒.๑๑ ห้ามผู้ใช้งานทำการพัฒนาชุดคำสั่งประสงค์ร้ายหรือนำชุดคำสั่งประสงค์ร้ายมาใช้ภายในกรมทรัพยากรน้ำ หรือเผยแพร่สู่ภายนอกด้วยเครือข่ายหรือทรัพยากรที่เป็นของกรมทรัพยากรน้ำ

๒.๑๒ หากผู้ใช้งานที่ใช้งานเครื่องคอมพิวเตอร์พบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัส ให้รีบแจ้งผู้ดูแลระบบเพื่อทำการตรวจสอบและแก้ไขในทันที

๒.๑๓ กรมทรัพยากรน้ำต้องมีการตรวจสอบเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารของกรมทรัพยากรน้ำเพื่อให้มั่นใจว่าได้ปฏิบัติตามนโยบายการป้องกันชุดคำสั่งประสงค์ร้ายอย่างสม่ำเสมอ

๒.๑๔ เมื่อมีผู้ใช้งานจากภายนอกนำเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารมาขออนุญาตใช้งานระบบเครือข่ายสารสนเทศภายในกรมทรัพยากรน้ำ ผู้ดูแลระบบจะต้องทำการตรวจสอบก่อนว่ามีระบบรักษาความปลอดภัย หรือมีการติดตั้งใช้งานโปรแกรมป้องกันไวรัสบนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารหรือไม่ หากพบว่าไม่มีระบบรักษาความปลอดภัยหรือติดตั้งใช้งานโปรแกรมป้องกันไวรัส ผู้ดูแลระบบไม่ควรอนุญาตให้ทำการใช้งานระบบเครือข่ายสารสนเทศภายในกรมทรัพยากรน้ำเป็นอันขาด

๒.๑๕ ผู้บริหารควรมีความตระหนักในภัยโจมตีทางไซเบอร์ในรูปแบบใหม่ๆ พร้อมแนะนำและกำหนดแนวทางในการวางแผนเพื่อบริหารจัดการสำหรับการป้องกัน และแก้ไขสำหรับวิกฤติภัยโจมตีประเภทต่างๆ ทั้งปัจจุบัน และอนาคต

ส่วนที่ ๑๓

การสำรองและกู้คืนข้อมูลและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน
(Backup and Restore Policy and Contingency Plan)

๑. วัตถุประสงค์

เพื่อจัดทำมาตรฐานในการสำรองข้อมูลและการกู้คืนข้อมูลเมื่อเกิดเหตุใดๆ ที่ไม่สามารถเข้าถึงข้อมูลของกรมทรัพยากรน้ำได้ด้วยวิธีการปกติ และให้แน่ใจว่าระบบสารสนเทศและข้อมูลของกรมทรัพยากรน้ำสามารถกู้คืนกลับมาใช้งานได้ในช่วงเวลาที่กำหนด รวมถึงมีการจัดเก็บการสำรองข้อมูลในสภาพแวดล้อมที่มีการควบคุมอย่างเหมาะสม และทำการจัดเก็บการสำรองข้อมูลอย่างสม่ำเสมอ รวมทั้งมีการจัดทำการทดสอบการกู้คืนข้อมูลเพื่อให้สามารถแน่ใจในกระบวนการสำรองข้อมูล

๒. การสำรองข้อมูล

๒.๑ กรมทรัพยากรน้ำต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของกรมทรัพยากรน้ำ พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรองตามลำดับความสำคัญ และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง โดยรายชื่อระบบสารสนเทศที่มีความสำคัญของกรมทรัพยากรน้ำซึ่งไวต่อการรบกวน มีดังนี้

๒.๑.๑ DHCP Server
๒.๑.๒ Antivirus Server
๒.๑.๓ What up Gold Server
๒.๑.๔ NEWS Division Server
๒.๑.๕ GF-MIS Server
๒.๑.๖ Backup Server
๒.๑.๗ Web Regional Server
๒.๑.๘ Plan Server
๒.๑.๙ Data DWR Server
๒.๑.๑๐ WebServer
๒.๑.๑๑ DBSERVER
๒.๑.๑๒ Intranet Server
๒.๑.๑๓ IPV๖ & DNS Server
๒.๑.๑๔ DPIS Server
๒.๑.๑๕ e-library Server
๒.๑.๑๖ system Server
๒.๑.๑๗ mobile app Server
๒.๑.๑๘ Helpdesk Server
๒.๑.๑๙ VM SERVER
๒.๑.๒๐ ระบบจัดเก็บไฟล์ Server

๒.๒ ผู้ดูแลระบบและผู้ที่มีส่วนเกี่ยวข้องในการสำรองข้อมูลของระบบเครือข่ายและสารสนเทศของกรมทรัพยากรน้ำ ต้องปฏิบัติเกี่ยวกับนโยบายการสำรองข้อมูลและขั้นตอนปฏิบัติที่เกี่ยวข้องกับการสำรองข้อมูลอย่างเคร่งครัด

๒.๓ กรมทรัพยากรน้ำต้องจัดทำขั้นตอนการปฏิบัติงานสำหรับการสำรองข้อมูลอย่างเป็นลายลักษณ์อักษร เพื่อรองรับการปฏิบัติงานของผู้ดูแลระบบที่ได้รับมอบหมาย และกำหนดให้มีเอกสารคู่มือวิธีการสำรองข้อมูลแยกตามแต่ละระบบงาน โดยขั้นตอนการปฏิบัติงานสำหรับการสำรองข้อมูลต้องประกอบด้วยข้อมูลอย่างน้อย ดังนี้

๒.๓.๑ รายละเอียดข้อมูลที่ทำการสำรอง

๒.๓.๒ ความถี่ในการสำรองข้อมูล

๒.๓.๓ ประเภทของสื่อบันทึก (Backup Media)

๒.๓.๔ จำนวนที่ต้องทำการสำรอง

๒.๓.๕ ขั้นตอนและวิธีการสำรองโดยละเอียด

๒.๓.๖ สถานที่และวิธีการเก็บรักษาสื่อบันทึก

๒.๓.๗ ระยะเวลาในการจัดเก็บตามประเภทของข้อมูล (เนื่องด้วยข้อมูลบางประเภทต้องจัดเก็บเป็นระยะเวลาตามที่กฎหมายกำหนด)

๒.๔ กรมทรัพยากรน้ำต้องทำการสำรองข้อมูลเป็นระยะ (Periodic Backup) โดยมีช่วงเวลาความถี่ที่เหมาะสมต่อการใช้งานข้อมูลที่ทำการสำรอง โดยสามารถพิจารณาได้ ดังนี้

๒.๔.๑ สำหรับข้อมูลของระบบงานสารสนเทศ หรือข้อมูลที่เก็บในฐานข้อมูลของระบบงานสารสนเทศนั้นๆ ที่มีการเปลี่ยนแปลงรายวัน ต้องทำการสำรองข้อมูลรายวัน (Daily Backup)

๒.๔.๒ สำหรับ Configurations Source Code หรือ ระบบปฏิบัติการ (Operating System) ต่าง ๆ ที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศ ต้องทำการสำรองข้อมูลทุกครั้งที่มีการเปลี่ยนแปลง

๒.๔.๓ สำหรับข้อมูลระบบเครือข่ายที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของกรมทรัพยากรน้ำต้องทำการสำรองข้อมูลทุกครั้งที่มีการเปลี่ยนแปลง

๒.๔.๔ สำหรับข้อมูลของระบบงานสารสนเทศ หรือข้อมูลที่เก็บในฐานข้อมูลของระบบงานสารสนเทศนั้นๆ ที่มีการเปลี่ยนแปลงตลอดเวลา (Real-time System) สามารถทำการสำรองข้อมูลรายวัน (Daily Backup) หรือจัดทำ Replication System โดยขึ้นอยู่กับความต้องการในการสำรองข้อมูลในการดำเนินงานของกรมทรัพยากรน้ำ

๒.๔.๕ สำหรับข้อมูลส่วนประกอบอื่นๆ ของระบบ ที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศของกรมทรัพยากรน้ำ ซึ่งนอกเหนือจากที่กล่าวมาข้างต้น ให้พิจารณาความถี่ในการสำรองข้อมูลให้สอดคล้องกับการใช้งานจริงของข้อมูลนั้น ได้แก่

แผนการสำรองข้อมูล

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑. Firewall Server	ค่า Configuration	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูล Rule ของ Firewall	๑ ครั้ง ต่อเดือน
๒. DHCP Server	ค่า Configuration	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลใน DHCP	๑ ครั้ง ต่อเดือน
๓. DNS Server	ค่า Configuration	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลใน DNS	๑ ครั้ง ต่อเดือน
๔. Web Server	ค่า Configuration	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลเผยแพร่บน Website	๑ ครั้ง ต่อเดือน
๕. Application Server	ค่า Configuration	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลเผยแพร่บน Application	๑ ครั้ง ต่อเดือน
๖. Database Server	ค่า Configuration	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลเผยแพร่บน Database	๑ ครั้ง ต่อเดือน

๒.๕ กรมทรัพยากรน้ำต้องกำหนดให้มีการเข้ารหัสข้อมูลที่สำคัญในการสำรองข้อมูล (Encrypted Backup) โดยใช้เทคโนโลยีการเข้ารหัสที่มีความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำรองเหล่านั้น

๒.๖ กรมทรัพยากรน้ำต้องกำหนดรูปแบบการสำรองข้อมูล (Backup Schemes) ให้เหมาะสมกับการทำงานของแต่ละระบบสารสนเทศของกรมทรัพยากรน้ำ และสอดคล้องกับความสามารถของระบบสำรองข้อมูลของกรมทรัพยากรน้ำ ซึ่งการสำรองข้อมูลสามารถแบ่งได้ ๒ รูปแบบหลัก ดังนี้

- Full Backups: ใช้สำหรับการจัดทำการสำรองข้อมูลทั้งหมด
- Partial Backups หรือ Incremental Backups: เป็นรูปแบบการสำรองข้อมูลในส่วนที่เพิ่มเติมจากการทำ Full Backups

๒.๗ ผู้ดูแลระบบที่รับผิดชอบในการสำรองข้อมูลต้องทำการตรวจทานความสมบูรณ์ถูกต้องของการสำรองข้อมูลทุกครั้ง พร้อมทั้งจัดทำสรุปผลการตรวจทาน ที่ใช้ในการสำรองข้อมูลในแต่ละประเภทของการสำรองข้อมูล

๒.๘ ผู้ดูแลระบบที่รับผิดชอบในการสำรองข้อมูลต้องทำการบันทึกรายละเอียดของปัญหาที่พบระหว่างการสำรองข้อมูลและรายละเอียดวิธีการแก้ปัญหาและรายงานแก่ผู้บังคับบัญชาตามลำดับขั้นที่เกี่ยวข้องทราบ

๒.๙ ผู้ดูแลระบบที่รับผิดชอบในการสำรองข้อมูลต้องจัดทำบันทึกข้อมูลการปฏิบัติงานสำหรับการสำรองข้อมูล (Backup Operation Log) เพื่อรายงานให้ผู้บังคับบัญชาตามลำดับขั้นที่เกี่ยวข้องทำการตรวจทานและรับทราบการทำงานการสำรองข้อมูล โดยมีรายละเอียด ดังนี้

- วันและเวลาเริ่มต้นและสิ้นสุดในการสำรองข้อมูล
- ชื่อพร้อมลายเซ็นของผู้ปฏิบัติงานสำรองข้อมูล
- ชนิดของข้อมูลที่ทำการสำรอง
- วิธีการสำรองข้อมูล
- ปัญหาที่พบระหว่างการสำรองข้อมูล
- รายละเอียดวิธีการแก้ปัญหา

๒.๑๐ ผู้ดูแลระบบต้องมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรอง กรณีที่ผู้ดูแลระบบ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

๒.๑๑ กรมทรัพยากรน้ำต้องมีสถานที่ภายนอกสำหรับจัดเก็บสื่อบันทึกข้อมูลสำรอง และสำเนาขั้นตอนหรือวิธีการปฏิบัติงาน เพื่อใช้ในกรณีที่เกิดเหตุภัยพิบัติฉุกเฉินต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงาน

๒.๑๒ การสำรองข้อมูลภายนอกสำนักงาน (Off-site Backup) ผู้ดูแลระบบจัดให้มีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมของกรมทรัพยากรน้ำ เพื่อให้สามารถกู้ระบบกลับคืนได้อย่างรวดเร็วและเพื่อป้องกันระบบจากการถูกโจมตีหรือความหายนะที่อาจเกิดขึ้น

๒.๑๓ กรมทรัพยากรน้ำต้องกำหนดให้มีการควบคุมสถานที่สำรองข้อมูลอย่างเหมาะสม โดยมีรายละเอียดดังนี้

- การเข้าถึงสถานที่สำรองข้อมูลนั้น กำหนดให้เข้าถึงได้เฉพาะเจ้าหน้าที่ปฏิบัติงานที่เกี่ยวข้องและบุคคลผู้ซึ่งได้รับอนุญาตจากทางกรมทรัพยากรน้ำเท่านั้น
- สถานที่สำรองข้อมูลจะมีความปลอดภัยจากความเสี่ยงจากภัยธรรมชาติและมีสภาพที่เหมาะสมต่อการเก็บสื่อบันทึกข้อมูลสำรอง
- การเคลื่อนย้าย การจัดเก็บ การเข้าถึง สื่อบันทึกข้อมูล หรือเอกสารที่เกี่ยวข้องกับการปฏิบัติงานสำหรับการกู้คืนข้อมูล ต้องมีการบันทึกรายละเอียดและเวลาการนำเข้า-ออก ชื่อผู้ปฏิบัติงาน ชนิดของสื่อบันทึกข้อมูลหรือเอกสารที่เกี่ยวข้อง เพื่อรายงานให้ผู้บริหารที่เกี่ยวข้องทำการตรวจทานและรับทราบการทำงาน
- ไม่ควรเปิดเผยที่อยู่ของสถานที่สำรองข้อมูล รวมถึงรายละเอียดที่เกี่ยวข้องในการสำรองข้อมูลให้แก่บุคคลภายนอกและบุคคลที่ไม่เกี่ยวข้องรับทราบ เพื่อป้องกันความตั้งใจในการเข้าถึงสถานที่สำรองข้อมูลโดยไม่ได้รับอนุญาต

๒.๑๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๓. การกู้คืนข้อมูล

๓.๑ หากความเสียหายที่เกิดขึ้นกับระบบเครือข่ายและสารสนเทศ กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้งาน ผู้ดูแลระบบจำเป็นต้องแจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๓.๒ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบดำเนินการแก้ไข รายงานผลการแก้ไข พร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงานต่อผู้บังคับบัญชาตามลำดับขั้น หรือผู้ที่ได้รับมอบหมายให้ทราบ

๓.๓ ผู้ดูแลระบบต้องจัดทำขั้นตอนการปฏิบัติงานสำหรับการกู้คืนข้อมูล เพื่อรองรับกรณีที่เกิดเหตุภัยพิบัติฉุกเฉิน (Disaster) ต่อระบบเครือข่ายและสารสนเทศของกรมทรัพยากรน้ำ และกำหนดให้มีเอกสารคู่มือการกู้คืนข้อมูลแยกตามแต่ละระบบงาน

๓.๔ ข้อมูลที่นำมาใช้ในการกู้คืนระบบ ควรใช้ข้อมูลที่ทันสมัยที่สุดที่ได้มีการสำรองไว้หรือตามความเหมาะสมของระบบงานนั้นๆ เพื่อกู้คืนระบบให้สามารถให้บริการได้

๓.๕ ผู้ดูแลระบบต้องทำการปรับปรุงขั้นตอนการปฏิบัติงานสำหรับการกู้คืนข้อมูลให้เป็นปัจจุบัน รวมถึงสามารถรองรับการทำงานในปัจจุบันได้

๓.๖ กรมทรัพยากรน้ำต้องกำหนดอำนาจอนุมัติในการกู้คืนข้อมูลอย่างเป็นลายลักษณ์อักษรและในการกู้คืนข้อมูลทุกครั้ง ต้องได้รับการอนุมัติจากผู้มีอำนาจที่ได้มีการกำหนดไว้เท่านั้น

๓.๗ กรมทรัพยากรน้ำต้องกำหนดข้อตกลงระดับการให้บริการ (Service Level Agreement-SLA) สำหรับการกู้คืนข้อมูลของแต่ละระบบสารสนเทศของกรมทรัพยากรน้ำ ซึ่งระยะเวลาในการกู้คืนควรสอดคล้องกับความสำคัญ และความสามารถของระบบสารสนเทศที่มีอยู่

๔. การทดสอบกู้คืนข้อมูล

๔.๑ กรมทรัพยากรน้ำต้องจัดให้มีการทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ ๑ ครั้ง

๔.๒ กรมทรัพยากรน้ำต้องจัดทำรายละเอียดการทดสอบกู้คืนข้อมูล สำหรับแต่ละระบบสารสนเทศของกรมทรัพยากรน้ำ โดยให้ครอบคลุมเนื้อหา ดังนี้

- ความถี่ในการทดสอบ
- รูปแบบการทดสอบ
- ระยะเวลาในการทดสอบและการตรวจทานผลการทดสอบ
- รายชื่อ รายละเอียดบทบาท และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ปฏิบัติงานที่เกี่ยวข้อง
- รายละเอียดเอกสารที่เกี่ยวข้องกับการทดสอบ
- การประเมินผลการทดสอบ เพื่อรายงานผู้บริหารของกรมทรัพยากรน้ำได้รับทราบ

๔.๓ ผู้ดูแลระบบที่รับผิดชอบต้องทำการตรวจสอบความพร้อมในการใช้งานของสื่อบันทึกข้อมูลอย่างสม่ำเสมอ ตามที่กำหนดในรายละเอียดการทดสอบกู้คืนข้อมูล เพื่อให้แน่ใจได้ว่าสื่อบันทึกข้อมูลอยู่ในสถานะพร้อมใช้งาน

๕. แผนเตรียมความพร้อมกรณีฉุกเฉิน

กรมทรัพยากรน้ำต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง มีประสิทธิภาพ ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ ตามรายละเอียด ดังนี้

๕.๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินของระบบเทคโนโลยีสารสนเทศ เพื่อรองรับสถานการณ์ฉุกเฉิน

๕.๒ กำหนดผู้รับผิดชอบและหน้าที่ความรับผิดชอบ รับผิดชอบตามแผนเตรียมความพร้อมกรณีฉุกเฉิน ได้แก่

๕.๒.๑ กรณีภัยที่เกิดจากภายนอก

- กำหนดให้ผู้ที่อยู่เวรรักษาการณ์หรือเจ้าหน้าที่พบเหตุดำเนินการตามแผนเตรียมความพร้อมกรณีฉุกเฉิน และแจ้งผู้รับผิดชอบทราบและสั่งการตามลำดับ ได้แก่ เจ้าหน้าที่ส่วนระบบคอมพิวเตอร์ที่ดูแลห้องปฏิบัติการแม่ข่าย และ/หรือเจ้าหน้าที่กลุ่มงานพาหนะและอาคารสถานที่ ผู้อำนวยการส่วนระบบคอมพิวเตอร์ และผู้อำนวยการศูนย์สารสนเทศของกรมทรัพยากรน้ำ

๕.๒.๒ กรณีภัยที่เกิดจากภายใน

- กำหนดให้ผู้ที่อยู่เวรรักษาการณ์หรือเจ้าหน้าที่พบเหตุดำเนินการตามแผนเตรียมความพร้อมกรณีฉุกเฉิน และแจ้งผู้รับผิดชอบทราบและสั่งการตามลำดับ ได้แก่ เจ้าหน้าที่ส่วนระบบคอมพิวเตอร์ที่ดูแลห้องปฏิบัติการแม่ข่าย ผู้อำนวยการส่วนระบบคอมพิวเตอร์ และผู้อำนวยการศูนย์สารสนเทศของกรมทรัพยากรน้ำ

๕.๓ เจ้าหน้าที่รับผิดชอบและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหาย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์สารสนเทศของกรมทรัพยากรน้ำทราบ

๕.๔ เจ้าหน้าที่รับผิดชอบต้องทดสอบ ประเมิน และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้ หากเกิดเหตุการณ์ขึ้นจริง

ส่วนที่ ๑๔

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Monitoring and Risk Assessment Information)

๑. วัตถุประสงค์

๑.๑ เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๑.๒ เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

๒. นโยบายและแนวปฏิบัติ

๒.๑ กรมทรัพยากรน้ำต้องกำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

๒.๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒.๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบจากภายนอก (External Auditor) เพื่อให้กรมทรัพยากรน้ำได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒.๒ กรมทรัพยากรน้ำต้องกำหนดให้มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึงอย่างน้อย ดังนี้

๒.๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๒.๒.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๒.๒.๓ รายการที่สอบทาน

- การป้องกันการบุกรุก
- การสำรองข้อมูล
- การควบคุมการเข้าถึงห้องควบคุมระบบเครือข่าย
- การซ้อมรับสถานการณ์ฉุกเฉิน

๓. การกำหนดความรับผิดชอบ

๓.๑ ระดับนโยบาย

๓.๑.๑ กำหนดให้ผู้บริหารระดับสูงสุดของกรมทรัพยากรน้ำ (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่กรมทรัพยากรน้ำ หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำ

๓.๑.๒ กำหนดให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรมของกรมทรัพยากรน้ำ (DCIO) เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำ

๓.๑.๓ กำหนดให้ผู้อำนวยการศูนย์สารสนเทศของกรมทรัพยากรน้ำ เป็นผู้รับผิดชอบติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษากับเจ้าหน้าที่ในการปฏิบัติงาน

๓.๒ ระดับปฏิบัติ

๓.๒.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ผู้รับผิดชอบ ได้แก่

- ศูนย์สารสนเทศของกรมทรัพยากรน้ำ
- ผู้ดูแลระบบที่ได้รับมอบหมาย
- เจ้าหน้าที่ที่ได้รับมอบหมาย
- ผู้ใช้งาน

๓.๒.๒ การสำรองและกู้คืนข้อมูลและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ผู้รับผิดชอบ ได้แก่

- ศูนย์สารสนเทศของกรมทรัพยากรน้ำ
- ผู้ดูแลระบบที่ได้รับมอบหมาย
- เจ้าหน้าที่ที่ได้รับมอบหมาย

๓.๒.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

- ศูนย์สารสนเทศของกรมทรัพยากรน้ำ
- ผู้ตรวจสอบภายในของกรมทรัพยากรน้ำหรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก
- ผู้ดูแลระบบที่ได้รับมอบหมาย
- เจ้าหน้าที่ที่ได้รับมอบหมาย