ระเบียบองค์การจัดการน้ำเสีย
ว่าด้วย แนวนโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
องค์การจัดการน้ำเสีย พ.ศ. ๒๕๖๓

เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์การจัดการน้ำเสีย เป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๔ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙

อาศัยอำนาจตามความในมาตรา ๒๓ แห่งพระราชกฤษฎีกาจัดตั้งองค์การจัดการน้ำเสีย พ.ศ.๒๕๓๘ จึงออกระเบียบองค์การจัดการน้ำเสีย ว่าด้วย แนวนโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ องค์การจัดการน้ำเสีย พ.ศ. ๒๕๖๓ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบองค์การจัดการน้ำเสีย ว่าด้วย แนวนโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศองค์การจัดการน้ำเสีย พ.ศ. ๒๕๖๓”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับนับแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ให้ยกเลิกระเบียบองค์การจัดการน้ำเสีย ว่าด้วย นโยบายและทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ องค์การจัดการน้ำเสีย พ.ศ. ๒๕๖๑

ข้อ ๔ ในระเบียบนี้

“ผู้บริหารสารสนเทศ” หมายความว่า พนักงานระดับสูงขององค์การจัดการน้ำเสียที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับการดำเนินการทั้งหมดขององค์การจัดการน้ำเสีย

“หัวหน้างานสารสนเทศ” หมายความว่า พนักงานที่มีหน้าที่ควบคุมดูแลการทำงานของผู้ดูแลระบบ พร้อมทั้งมีอำนาจสั่งการผู้ดูแลระบบเครือข่ายและสารสนเทศขององค์การจัดการน้ำเสีย และรายงานต่อผู้บริหารสารสนเทศ

“ผู้ดูแลระบบ” หมายความว่า พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือ บัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

/“ผู้ใช้งาน”...

"ผู้ใช้งาน" หมายความว่า บุคลากร พนักงานและลูกจ้างขององค์การจัดการน้ำเสีย รวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้ระบบเครือข่ายคอมพิวเตอร์ขององค์การจัดการน้ำเสียได้

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิเฉพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศขององค์การจัดการน้ำเสีย

"ทรัพยากร" หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศขององค์การจัดการน้ำเสีย

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

"ความมั่นคงปลอดภัยด้านสารสนเทศ (information security)" หมายความว่า การธำรงไว้ ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิด (nonrepudiation) และความน่าเชื่อถือ (reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)" หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident)" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์การจัดการน้ำเสียถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๕ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) ในการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) มีวัตถุประสงค์เพื่อให้องค์การจัดการน้ำเสีย มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างครบถ้วน และควบคุมดูแลทรัพย์สินด้านเทคโนโลยีสารสนเทศให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

/๕.๑ กำหนด ...

๕.๑ กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน

๕.๒ ให้ปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ และบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมทั้งวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support) จากผู้ผลิตได้อย่างเหมาะสมทันการณ์

๕.๓ มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT inventory list) ของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่รองรับระบบเทคโนโลยีสารสนเทศขององค์การจัดการน้ำเสียอย่างครบถ้วนและเป็นลายลักษณ์อักษร โดยครอบคลุมอย่างน้อยดังนี้

- ชื่อเครื่องแม่ข่าย
- ชื่อระบบปฏิบัติการ (Operating System) และเวอร์ชั่น
- ชื่อระบบงาน (application) และเวอร์ชั่น
- เจ้าของทรัพย์สิน (Owner)
- ประเภทของอุปกรณ์ ยี่ห้อ รายละเอียดทางเทคนิค (specification)
- หมายเลขอ้างอิงของฮาร์ดแวร์ (serial number) และหมายเลขอ้างอิงของซอฟต์แวร์ (Software license)
- สถานที่ตั้ง
- วันที่เริ่มติดตั้ง
- ประเภทการครอบครอง (ซื้อหรือเช่า)
- รายละเอียดผู้ให้บริการหรือผู้บำรุงรักษา
- วันที่บำรุงรักษาล่าสุด
- วันสิ้นสุดการใช้งานตามสัญญา (warranty) และวันสิ้นสุดการรับประกันการใช้งาน (Support Contract)
- วันสิ้นสุดการให้บริการจากผู้ผลิต (end of support)

๕.๔ มีการปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับทะเบียนรายการอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๕.๕ มีกระบวนการในการยกเลิกและเรียกคืนทรัพย์สิน (return asset) เมื่อสิ้นสุดการใช้งานครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายในองค์การจัดการน้ำเสีย และกรณีที่ผู้ให้บริการภายนอกมีการใช้งานทรัพย์สินขององค์การจัดการน้ำเสียทันทีที่มีการยกเลิกสัญญาจ้างด้วย

/ข้อ ๖. การรักษา ...

ข้อ ๖. การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information Security) โดยองค์การจัดการน้ำเสีย ต้องมีกระบวนการในการรักษาความปลอดภัยของข้อมูลที่เพียงพอแก่การป้องกันไม่ให้บุคคลที่ไม่มีอำนาจเกี่ยวข้องเข้าถึง หรือสามารถเปลี่ยนแปลงแก้ไขข้อมูล หรือนำข้อมูลไปใช้ประโยชน์ในทางที่ผิดกฎหมาย โดยแนวทางการรักษาความปลอดภัยของข้อมูลอย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๖.๑ ผู้ดูแลระบบ ต้องกำหนดวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ โดยแบ่งชั้นความลับของข้อมูล เป็น ๓ ระดับ ดังนี้

(๑) ลับที่สุด หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์ขององค์การจัดการน้ำเสียอย่างร้ายแรงที่สุด

(๒) ลับมาก หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์ขององค์การจัดการน้ำเสียอย่างร้ายแรง

(๓) ลับ หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์ขององค์การจัดการน้ำเสีย

๖.๒ การจัดลำดับชั้นความลับและการบริหารจัดการกับข้อมูลตามข้อ ๖.๑ ให้ใช้หลักเกณฑ์ตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ โดยแสดงระดับชั้นความลับของเอกสารข้อมูลลับอย่างชัดเจนในเอกสารที่เกี่ยวข้องทุกหน้า

๖.๓ การจัดลำดับชั้นความลับและการบริหารจัดการกับข้อมูลตามข้อ ๖.๒ ให้อยู่ในดุลพินิจของผู้บริหาร

๖.๔ การบริหารจัดการกับข้อมูลตามข้อ ๖.๓ ต้องมีการตรวจสอบความถูกต้องเหมาะสมของข้อมูลที่จะเผยแพร่ออกสู่สาธารณะผ่านทางเว็บไซต์ ข้อมูลดังกล่าวจะต้องไม่ขัดต่อกฎหมาย และมีกลไกป้องกันการเข้าไปแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

๖.๕ ประเภทของข้อมูลแบ่งออกเป็น ๓ ประเภท ดังนี้

(๑) ข้อมูลที่ใช้ในการบริหารจัดการ ได้แก่ ข้อมูล นโยบาย ยุทธศาสตร์ บุคลากร งบประมาณ คำรับรองการปฏิบัติราชการ การเงินและบัญชี

(๒) ข้อมูลที่ใช้ในการดำเนินงาน ได้แก่ ข้อมูล กฎหมาย ระเบียบ ข้อมูลที่เกี่ยวกับภารกิจ หน้าที่ขององค์การจัดการน้ำเสีย

(๓) ข้อมูลเพื่อการบริการ ได้แก่ รายงานทางวิชาการ แผนที่ภาพถ่ายดาวเทียม องค์ความรู้

/๖.๖ ลำดับ ...

๖.๖ ลำดับความสำคัญของข้อมูล แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ข้อมูลที่มีความสำคัญมากที่สุด

(๒) ข้อมูลที่มีความสำคัญปานกลาง

(๓) ข้อมูลที่มีความสำคัญน้อย ได้แก่ ข้อมูลตามภารกิจขององค์การจัดการน้ำเสียที่ไม่อยู่ใน (๑) และ (๒)

๖.๗ ระดับการเข้าถึงข้อมูล แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ข้อมูลที่เข้าถึงได้เฉพาะผู้มีสิทธิสูงสุด เพื่อเข้าไปบริหารจัดการระบบสารสนเทศ ได้แก่ ผู้ดูแลระบบ

(๒) ข้อมูลที่เข้าถึงได้เฉพาะผู้ได้รับอนุมัติสิทธิ หมายถึง ข้อมูลที่ผู้ใช้งานต้องได้รับการอนุญาตจากผู้รับผิดชอบระบบสารสนเทศหรือผู้ดูแลระบบตามภาระหน้าที่และความจำเป็น

(๓) ข้อมูลที่เข้าถึงได้ทุกกลุ่มผู้ใช้งาน หมายถึง ข้อมูลพื้นฐานที่ได้รับอนุญาตจากผู้รับผิดชอบระบบสารสนเทศหรือผู้ดูแลระบบ พิจารณาแล้วว่าสามารถเข้าถึงได้

๖.๘ การกำหนดช่องทางการเข้าถึงระบบสารสนเทศขององค์การจัดการน้ำเสียต้องกำหนด ดังนี้

(๑) ต้องให้ผู้รับบริการสามารถเข้าถึงได้ทั้งจากภายในและภายนอกองค์การจัดการน้ำเสีย

(๒) ผู้รับบริการสามารถรับบริการข้อมูลข่าวสารผ่านเว็บไซต์ขององค์การจัดการน้ำเสียโดยไม่ต้องลงทะเบียน

(๓) ผู้รับบริการสามารถใช้บริการศูนย์บริการข่าวสารองค์การจัดการน้ำเสียเพื่อเข้าถึงข้อมูลข่าวสารได้

๖.๙ การรับ ส่ง และจัดเก็บข้อมูลอิเล็กทรอสิกส์ที่ประสงค์จะให้เป็นความลับได้อย่างปลอดภัย สามารถขอคำปรึกษาหรือการสนับสนุนในการเข้ารหัสจากผู้ดูแลระบบได้โดยปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๗. การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control) มีวัตถุประสงค์เพื่อกำหนดการควบคุมการเข้าถึงข้อมูลสารสนเทศ โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยด้านสารสนเทศและเพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ และการมอบอำนาจขององค์การจัดการน้ำเสีย ทั้งนี้เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึง เพื่อให้การตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศได้อย่างถูกต้อง

/๗.๑ การควบคุม ...

๗.๑ การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

(๑) ผู้ดูแลระบบต้องดำเนินการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่ผู้ใช้งานได้รับอนุญาต หรือได้รับการมอบอำนาจ

(๒) ผู้ดูแลระบบมีการกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้ อ่านข้อมูล สร้างข้อมูล นำเข้าข้อมูล แก้ไขข้อมูล อนุมัติ และ ไม่มีสิทธิ

(๓) ผู้ดูแลระบบดำเนินการควบคุมการเข้าถึงที่เหมาะสมต่อหมวดหมู่ของสารสนเทศที่จัดไว้ตามระดับชั้นความลับ

(๔) ผู้ดูแลระบบมีการถอดสิทธิการเข้าถึงการใช้งานสารสนเทศ

(๕) ผู้ดูแลระบบเป็นผู้ควบคุมการเข้าถึงจากประเภทของการเชื่อมต่อทั้งหมด

(๖) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์การจัดการน้ำเสีย จะต้องได้รับการพิจารณาจากผู้บริหารขององค์การจัดการน้ำเสียต้นสังกัดเป็นลายลักษณ์อักษร

(๗) ผู้ดูแลระบบกำหนดประเภทของข้อมูล ได้แก่ ข้อมูลภายนอกสามารถเปิดเผยได้ ข้อมูลภายใน เป็นไปตามลำดับขั้นความลับของข้อมูล

(๘) ผู้ดูแลระบบกำหนดเวลาและช่องทางที่เข้าถึงได้ ให้เหมาะสมตามแต่ละระบบงาน

๗.๒ การควบคุมการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

(๑) ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บริหาร และผู้ดูแลระบบเพื่อเข้าใช้งานระบบสารสนเทศเป็นลายลักษณ์อักษร ตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยต้องคำนึงถึงประเภทข้อมูลและชั้นความลับ

(๓) เจ้าของข้อมูลและหรือเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ ตามหน้าที่งานหรือตามความจำเป็นขั้นต่ำเท่านั้น โดยไม่อนุญาตให้กำหนดสิทธิเกินความจำเป็นในการใช้งาน

๗.๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๑) การลงทะเบียนผู้ใช้งานใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานใหม่ เพื่อให้มีสิทธิต่างๆในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกไปหรือเมื่อเปลี่ยนตำแหน่งงาน ภายใน ๑๕ วันทำการนับจากวันที่ผู้มีอำนาจลงนามในคำสั่ง

/(๒) ผู้ดูแล ...

(๒) ผู้ดูแลระบบกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบสารสนเทศ โปรแกรมประยุกต์ (Application) ภายในสำนักงาน จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบอินเทอร์เน็ต ระบบเครือข่ายไร้สาย (Wireless LAN) โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บริหาร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๗.๔ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของผู้ใช้งาน

(๑) ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

(๒) กรณีผู้ดูแลระบบมีความจำเป็นต้องให้สิทธิเพิ่มเป็นกรณีพิเศษแก่ผู้ใช้งานที่มีสิทธิพื้นฐานต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าองค์การจัดการน้ำเสีย และต้องมีการควบคุมผู้ใช้งานที่มีสิทธิพิเศษนั้นอย่างรัดกุม เพียงพอ โดยต้องดำเนินการควบคุมการใช้งานอย่างเข้มงวดและอนุญาตให้เข้าใช้งานเฉพาะกรณีที่จำเป็นเท่านั้นรวมถึงกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓) กำหนดขั้นตอนในการลงทะเบียนผู้ใช้งาน (user registration) ดังนี้

- มีการระบุชื่อบัญชีผู้ใช้งานแยกเป็นรายบุคคล

- มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากหัวหน้า

- มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดสัญญาจ้าง เป็นต้น

๗.๕ วิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

(๑) ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลาย ข้อมูลแต่ละประเภทชั้นความลับ หากข้อมูลมีความลับ

(๒) เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๓) ผู้ดูแลระบบควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงข้อมูลโดยตรง และการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับข้อมูล

/(๔) การรับส่ง ...

(๔) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL หรือ VPN

(๕) มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๗.๖ การควบคุมการเข้าใช้งานระบบจากภายนอก

(๑) ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์การจัดการน้ำเสียอย่างเพียงพอ เพื่อขอใช้สิทธิในการเข้าถึงระบบจากระยะไกล และต้องได้รับอนุมัติจากองค์การจัดการน้ำเสีย

(๒) กำหนดผู้ควบคุมการเข้าถึงระบบจากระยะไกล (Remote access)

(๓) ผู้ใช้งานที่มีความจำเป็นต้องเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับอนุมัติจากผู้ควบคุม และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบและข้อมูลอย่างเคร่งครัด

(๔) ผู้ดูแลระบบต้องควบคุมพอร์ต (Port) ที่ระบบสารสนเทศให้บริการใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

(๕) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ผู้ดูแลระบบต้องอนุญาตตามพื้นฐานของความจำเป็นเท่านั้น และให้ปิด Port และ Modem เมื่อผู้ใช้งานได้ใช้งานเสร็จสิ้นแล้วทันที

๗.๗ การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก

ผู้ใช้งานระบบทุกคนเมื่อจะเข้าใช้งานระบบขององค์การจัดการน้ำเสียต้องผ่านการพิสูจน์ตัวตนจากระบบ โดยมีแนวทางปฏิบัติดังนี้

(๑) การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username)

(๒) การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)

(๓) การเข้าสู่ระบบสารสนเทศขององค์การจัดการน้ำเสียจากอินเทอร์เน็ตนั้นจะต้องมีการตรวจสอบผู้ใช้งาน

(๔) การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน โดยใช้รหัสผ่าน หรือวิธีการเข้ารหัส

/ข้อ ๘ การรักษา ...

ข้อ ๘ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security) มีวัตถุประสงค์เพื่อให้องค์การจัดการน้ำเสียมีการรักษาความมั่นคงปลอดภัยและความพร้อมใช้งานของระบบสารสนเทศและพื้นที่สำคัญที่เกี่ยวข้องเพียงพอรองรับการทำงานอย่างต่อเนื่อง

๘.๑ การบริหารจัดการทางกายภาพ (Physical security management)

(๑) กำหนดระดับความสำคัญของพื้นที่ห้องแม่ข่ายและศูนย์ติดตามและรายงานสถานการณ์น้ำเสียประเทศไทย

(๒) มีระบบป้องกัน เมื่อมีการบุกรุกให้ครอบคลุมพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน (Data Center) หรือบริเวณที่มีความสำคัญ

(๓) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพ อย่างน้อยปีละ ๒ ครั้งเพื่อให้ระบบป้องกันพร้อมใช้งานได้เสมอ

(๔) ผู้ดูแลระบบ ต้องปิดประตูห้องแม่ข่ายให้ล็อคอยู่เสมอ

๘.๒ การควบคุมการเข้า-ออก (Physical entry Controls)

(๑) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

(๒) ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๓) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๔) สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๕) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๖) มีการพิสูจน์ตัวตนโดยการอ่านบัตรหรือการใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

(๗) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

/๘.๓ การจัด ...

๘.๓ การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)

(๑) จำกัดพื้นที่หรือบริเวณสำหรับการเข้าถึงเพื่อการส่งมอบหรือขนถ่ายผลิตภัณฑ์โดยบุคคลภายนอก

(๒) ดูแลบุคลากรซึ่งสามารถเข้าถึงพื้นที่บริเวณส่งมอบหรือขนถ่ายผลิตภัณฑ์

(๓) ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ และระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐

๘.๔ การจัดวางและการป้องกันอุปกรณ์ (Equipment setting and protection)

(๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานใน ห้อง Data Center ให้น้อยที่สุด

(๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัย

(๓) ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน (Data Center)

(๔) ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณ

๘.๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศขององค์การจัดการน้ำเสียที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบสำรองกระแสไฟฟ้า (UPS) และระบบปรับอากาศและควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนตาม ข้อ ๘.๕(๑) อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๘.๖ การนำสินทรัพย์ขององค์การจัดการน้ำเสียออกไปภายนอกสถานที่ (Removal of property)

(๑) ผู้ใช้งานต้องขออนุญาตหัวหน้าหน่วยงานก่อนนำอุปกรณ์หรือสินทรัพย์ออกนอกองค์การจัดการน้ำเสีย

/(๒) ผู้ใช้งาน ...

(๒) ผู้ใช้งานต้องบันทึกข้อมูลการนำอุปกรณ์ ออกไปภายนอกสถานที่ เพื่อเก็บไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๘.๗ การป้องกันสินทรัพย์ที่ใช้งานภายนอกองค์การจัดการน้ำเสีย (Security of equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยของสินทรัพย์ เพื่อป้องกันความเสี่ยงจากการนำสินทรัพย์ขององค์การจัดการน้ำเสียออกไปใช้งานภายนอก

(๒) ไม่ทิ้งสินทรัพย์ขององค์การจัดการน้ำเสียไว้ในที่สาธารณะโดยไม่มีผู้ดูแลรับผิดชอบ

(๓) ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบดูแลสินทรัพย์ขององค์การจัดการน้ำเสียเสมือนเป็นสินทรัพย์ของตนเอง

๘.๘ การกำจัดสินทรัพย์หรือการนำสินทรัพย์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use equipment)

(๑) ให้ทำลายข้อมูลสำคัญในสินทรัพย์ก่อนที่จะกำจัดสินทรัพย์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในสินทรัพย์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำสินทรัพย์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ข้อ ๙ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communication Security) มีวัตถุประสงค์เพื่อให้องค์การจัดการน้ำเสีย มีโครงสร้างของระบบเครือข่ายสื่อสารที่มั่นคงปลอดภัย มีการออกแบบเครือข่ายสื่อสารที่เหมาะสมตามมาตรฐานสากล และมีการป้องกันหรือเฝ้าระวังการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้นได้

๙.๑ มาตรการทางเครือข่ายสื่อสารข้อมูล (Network controls)

(๑) มีการกำหนดหน้าที่ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล และกำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

(๒) กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ

(๓) กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่างๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

(๔) มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

/๙.๒ การควบคุม ...

๙.๒ การควบคุมการเข้าถึงระบบเครือข่าย

(๑) ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ และการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ ได้แก่ โซนภายใน (Internal Zone) โซนภายนอก (External Zone) และ โซนพิเศษ (DMZ Zone) เป็นต้น เพื่อเป็นการควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ และให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การเข้าสู่ระบบเครือข่ายภายในขององค์การจัดการน้ำเสีย โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติก่อนที่จะสามารถใช้งานได้ในทุกกรณี

(๓) ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๔) ผู้ดูแลระบบ ต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

(๕) ผู้ดูแลระบบ จัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย

(๖) กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆของระบบเครือข่ายและอุปกรณ์ต่างๆที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า parameter ต่างๆอย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไข หรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๗) ระบบเครือข่ายทั้งหมดขององค์การจัดการน้ำเสียที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอก ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering

(๘) มีการจำกัดการเชื่อมต่อทางเครือข่ายโดยมีการติดตั้ง Firewall เป็นเกตเวย์สำหรับเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ เพื่อทำการกรองข้อมูลจราจรในเครือข่ายให้เป็นไปตามความเหมาะสมกับการใช้งานระบบเครือข่ายได้อย่างปลอดภัย

(๙) มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์การจัดการน้ำเสียในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๑๐) การเข้าสู่ระบบงานเครือข่ายภายในองค์การจัดการน้ำเสียผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

/(๑๑) IP address ...

(๑๑) IP address ภายในของระบบงานเครือข่ายภายในขององค์การจัดการน้ำเสียจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบได้โดยง่าย

(๑๒) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ ตามกลุ่มของเครือข่ายที่แยกตามกลุ่มเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๑๓) การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากองค์การจัดการน้ำเสียและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๑๔) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

(๑๖) การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๖ เดือน

(๑๗) มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๙.๓ การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์

(๑) ต้องลงทะเบียน Mac Address ประจำเครื่องเพื่อระบุอุปกรณ์บนเครือข่ายและต้องใช้หมายเลข IP Address ที่กำหนดให้โดยผู้ดูแลระบบสารสนเทศขององค์การจัดการน้ำเสียเท่านั้น

(๒) เครื่องคอมพิวเตอร์ทุกเครื่องต้องตั้งอยู่หลัง Firewall เพื่อป้องกันการละเมิดความมั่นคงปลอดภัยจากเครือข่ายภายนอก

(๓) ห้ามผู้ใช้งานที่ใช้งานอยู่ภายในเครือข่ายคอมพิวเตอร์ขององค์การจัดการน้ำเสียใช้ Modem หรืออุปกรณ์อื่นใดในการเชื่อมต่อระบบเครือข่ายภายนอกในขณะเดียวกัน

(๔) ห้ามผู้ใช้งานทำการต่อขยายหรือเชื่อมการบริการเครือข่าย (Switch Hub) โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ และห้ามผู้ใช้งานเปลี่ยนแปลงหรือแก้ไข (configuration) อุปกรณ์ใดๆ ในระบบเครือข่ายคอมพิวเตอร์

(๕) ห้ามติดตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ หรือ Software ที่ให้บริการเครือข่ายคอมพิวเตอร์ โดยไม่ได้รับการอนุญาตจากผู้ดูแลระบบ

/(๖) ห้ามผู้ใช้ ...

(๖) ห้ามผู้ใช้งานทำการ Download ติดตั้ง หรือทำการใช้โปรแกรมตรวจสอบทางด้านความมั่นคงปลอดภัยในเครือข่ายคอมพิวเตอร์ขององค์การจัดการน้ำเสียโดยไม่ได้รับอนุญาต

ข้อ ๑๐ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security) เป็นการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย ในประเด็นดังต่อไปนี้

๑๐.๑ การบริหารจัดการขีดความสามารถของระบบ (Capacity Management) มีวัตถุประสงค์เพื่อให้องค์การจัดการน้ำเสียสามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอรองรับต่อการทำงาน และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

(๑) กำหนดมาตรฐานและระเบียบวิธีปฏิบัติเรื่องการบริหารจัดการขีดความสามารถของระบบ เพื่อประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึงระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ

(๒) มีการประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศเพื่อวางแผนรองรับการใช้งานในอนาคต (Capacity planning) โดยครอบคลุมทั้งระบบหลักและระบบสำรอง

(๓) จัดทำรายงานความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศนำเสนอต่อคณะทำงานดิจิทัล องค์การจัดการน้ำเสีย หรือรองผู้อำนวยการวิชาการและแผน รับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อม และความเพียงพอของระบบในการรองรับการทำงานได้อย่างต่อเนื่อง รวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการณ์

๑๐.๒ การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security) มีวัตถุประสงค์เพื่อให้อุปกรณ์ที่ใช้ปฏิบัติงานมีความปลอดภัยและไม่เป็นช่องทางที่ทำให้ข้อมูลสำคัญขององค์การจัดการน้ำเสียรั่วไหลหรือมีการเข้าใช้งานโดยไม่ได้รับอนุญาต โดยให้กำหนด Security Baseline สำหรับอุปกรณ์ที่ใช้ปฏิบัติงานเพื่อป้องกันความเสี่ยงที่อุปกรณ์ขององค์การจัดการน้ำเสียและอุปกรณ์ส่วนตัว (Bring Your Own Device : BYOD) เช่น personal computer, notebook, tablet, smartphone, removable media อาจเป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญตามระดับความเสี่ยงที่เหมาะสม โดยอย่างน้อยครอบคลุมดังนี้

(๑) ติดตั้งระบบปฏิบัติการและโปรแกรมพื้นฐานที่ใช้ในการปฏิบัติงานบนเครื่องคอมพิวเตอร์ โดยมีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้ผู้ใช้งานสามารถติดตั้งโปรแกรมอื่นๆ นอกเหนือจากองค์การจัดการน้ำเสียกำหนด

/(๒) ติดตั้ง ...

(๒) ติดตั้งโปรแกรมรักษาความปลอดภัย

(๓) ควบคุมไม่ให้มีการจัดเก็บข้อมูลที่มีระดับชั้นความลับสูงสุดในเครื่องคอมพิวเตอร์ของผู้ใช้งาน แต่หากมีความจำเป็นต้องจัดเก็บ ต้องมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ เช่น มีการเข้ารหัส เป็นต้น

(๔) จำกัดการเข้าถึง shared drive หรือ shared folder ตามความจำเป็นในการใช้งานเท่านั้น

(๕) การควบคุมการใช้งานอินเทอร์เน็ต ซึ่งควรมีเครื่องมือในการควบคุมให้อุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตเข้าถึงเฉพาะเว็บไซต์ที่ได้รับอนุญาตเท่านั้น รวมถึงมีการจำกัดการดาวน์โหลดหรืออัพโหลดข้อมูลจากอินเทอร์เน็ต

๑๐.๓ การสำรองข้อมูล (Data Backup) มีวัตถุประสงค์เพื่อให้มั่นใจว่ามีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหายจนไม่สามารถใช้งานได้ตามปกติ

(๑) มีกระบวนการสำรองทั้งระบบ (full back up) ทุกครั้งภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการและระบบงาน เพื่อให้ระบบสำรองมีความเป็นปัจจุบัน

(๒) มีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกสถานที่ปฏิบัติงานหลักโดยมีการรักษาสภาพแวดล้อมและการควบคุมความปลอดภัยในการเข้าถึงข้อมูลที่จัดเก็บไว้เทียบเคียงกับศูนย์คอมพิวเตอร์หลัก

(๓) จัดให้มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้องพร้อมใช้งานและปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติขององค์การจัดการน้ำเสีย

๑๐.๔ การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging) มีวัตถุประสงค์ เพื่อให้องค์การจัดการน้ำเสียมีข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัย สามารถใช้ติดตามตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน โดยมีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่ายระบบงาน อุปกรณ์เครือข่ายสื่อสารที่สำคัญด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดที่ครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย ๙๐ วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด

๑๐.๕ การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring) มีวัตถุประสงค์ เพื่อให้องค์การจัดการน้ำเสียสามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงที โดยมีกระบวนการติดตามดูแลความมั่นคงปลอดภัยของระบบ รวมถึงเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง

/(๑) มีกระบวน ...

(๑) มีกระบวนการหรือเครื่องมือในการรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ มีการวิเคราะห์และจัดการข้อมูลภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุม ลักษณะการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้น เพื่อนำมาใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์

(๒) ในกรณีที่พบภัยคุกคามที่ส่งผลกระทบอย่างมีนัยสำคัญ องค์การจัดการน้ำเสียควรจัดให้มีการรายงานต่อคณะทำงานดิจิทัล องค์การจัดการน้ำเสีย รวมทั้งมีการรายงานหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมทั้งจัดให้มีกระบวนการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล โดยผู้ที่มีความเชี่ยวชาญเพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่และป้องกันความเสี่ยงที่อาจเกิดขึ้นอีก

๑๐.๖ การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Test) มีวัตถุประสงค์ เพื่อให้องค์การจัดการน้ำเสียได้รับทราบถึงช่องโหว่ด้านการรักษาความปลอดภัยของระบบ และสามารถดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามใหม่ๆ ที่อาจเกิดขึ้นได้อย่างทันการณ์

(๑) มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment) โดยองค์การจัดการน้ำเสียควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ให้ครอบคลุมทุกระบบงานอย่างสม่ำเสมอตามระดับความเสี่ยงสำหรับระบบงานสำคัญควรจัดทำอย่างน้อยปีละ ๑ ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๒) มีการรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะทำงานดิจิทัลองค์การจัดการน้ำเสีย หรือผู้บริหารที่ได้รับมอบหมายการทดสอบเจาะระบบ

๑๐.๗ การบริหารจัดการการเปลี่ยนแปลง (Change Management) มีวัตถุประสงค์ เพื่อให้มีการบริหารจัดการการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศสอดคล้องตามมาตรฐานสากล โดยมีการควบคุมที่รัดกุมปลอดภัยเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างครบถ้วนถูกต้อง

(๑) ให้ผู้ดูแลระบบ ประเมินความเสี่ยงและผลกระทบของการเปลี่ยนแปลงโดยองค์การจัดการน้ำเสียและผู้มีหน้าที่เกี่ยวข้องทำการประเมินองค์ประกอบที่เกี่ยวข้อง ได้แก่ ระบบโครงสร้างพื้นฐาน เครือข่าย สื่อสาร และการเชื่อมต่อกับระบบอื่น เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้น ไม่กระทบต่อการรักษา ความปลอดภัย ความถูกต้องเชื่อถือได้ ความพร้อมใช้ของระบบผลการทดสอบ เพื่อให้มั่นใจว่าระบบได้ผ่านการทดสอบอย่างครบถ้วนเหมาะสมตามมาตรฐาน

(๒) คำขอการเปลี่ยนแปลง (Change request) ควรได้รับการอนุมัติจากองค์การจัดการน้ำเสีย (System Owner) เพื่อให้มั่นใจได้ว่าการขอเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมจากองค์การจัดการน้ำเสีย

/๑๐.๘ การบริหาร ...

๑๐.๘ การบริหารจัดการการตั้งค่าระบบ (System configuration management) มีวัตถุประสงค์เพื่อให้องค์การจัดการน้ำเสียมีกระบวนการควบคุมการเปลี่ยนแปลงการตั้งค่าระบบที่มีความรัดกุม ปลอดภัย และเป็นไปตามมาตรฐาน

(๑) กำหนด minimum baseline standard เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ

(๒) มีการจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบของทุกอุปกรณ์ และระบบงาน (System Configuration Version Control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

(๓) กรณีมีความจำเป็นต้องตั้งค่าที่ไม่เป็นไปตามเอกสาร minimum baseline standard ควรผ่านกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

๑๐.๙ การบริหารจัดการ patch (patch management) มีวัตถุประสงค์เพื่อให้องค์การจัดการน้ำเสียมีการบริหารจัดการ patch โดยมีการควบคุมที่รัดกุมปลอดภัย และติดตั้งได้อย่างเหมาะสมทันการณ์

(๑) กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในกระบวนการบริหารจัดการ patch ที่ครอบคลุม การตรวจสอบความถูกต้องของ patch และการประเมินความเสี่ยงและความจำเป็นในการติดตั้ง patch ใหม่จากผู้ผลิตอย่างเหมาะสมทันการณ์

(๒) มีการจัดเก็บการเปลี่ยนแปลงการติดตั้งของทุกอุปกรณ์ และระบบงาน (patch version Control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

ข้อ ๑๑ การจัดหาและการพัฒนาระบบ (System Acquisition and Development) มีวัตถุประสงค์เพื่อให้มั่นใจได้ว่ากระบวนการจัดหาและการพัฒนาระบบ มีการควบคุมการรักษาความปลอดภัยอย่างรัดกุมและสอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล

๑๑.๑ การจัดหาระบบ (System Acquisition)

(๑) ให้มีหลักเกณฑ์การพิจารณาคัดเลือกระบบและผู้ให้บริการ เพื่อใช้เป็นแนวทางในการปฏิบัติงานซึ่งควรครอบคลุมอย่างน้อย ดังนี้

- รายละเอียดทั่วไป เช่น หมายเลขอ้างอิงของซอฟต์แวร์ (Software license) ฟังก์ชั่นการทำงาน ประสิทธิภาพของระบบ เป็นต้น
- ความมั่นคงปลอดภัยของระบบ
- ฐานะการเงิน ชื่อเสียง และความสามารถด้านเทคนิค
- การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate)
- การสนับสนุนและการบำรุงรักษาระบบ
- ความน่าเชื่อถือของระบบและผู้ให้บริการ

/(๒) องค์การ ...

(๒) องค์การจัดการน้ำเสียควรควบคุมดูแลผู้ให้บริการปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติการออกแบบและพัฒนาระบบ

(๓) องค์การจัดการน้ำเสียกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการตรวจสอบและส่งมอบระบบเทคโนโลยีสารสนเทศ

๑๑.๒ การพัฒนาระบบเทคโนโลยีสารสนเทศ (System Development)

(๑) ให้กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างเป็นลายลักษณ์อักษรโดยคำนึงถึงการรักษาความมั่นคงปลอดภัยครอบคลุมกระบวนการตั้งแต่จัดทำความต้องการ (requirement) การออกแบบ การพัฒนา และการทดสอบระบบก่อนใช้งานจริง

(๒) กำหนดให้องค์การจัดการน้ำเสียที่เกี่ยวข้องสอบทานความถูกต้องครบถ้วนตามความต้องการขององค์การจัดการน้ำเสีย (Business requirement)

(๓) จัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมการรักษาความมั่นคงปลอดภัยที่ได้มาตรฐาน

(๔) จัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชั่นและเงื่อนไขต่างๆ ด้านประสิทธิภาพ ตามความต้องการขององค์การจัดการน้ำเสีย (Business requirement) รวมถึงการควบคุมความมั่นคงปลอดภัย เพื่อเป็นแนวทางการพัฒนาระบบและสอบทานผลการทดสอบก่อนที่จะออกใช้งานจริง

(๕) ในการพัฒนาระบบ ให้มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) การทดสอบ (testing) และระบบที่ให้บริการจริง (production) ออกจากกัน เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นจากการนำระบบขึ้นใช้งานจริง

(๖) มีกระบวนการหรือเครื่องมือในการควบคุมเวอร์ชั่นของคำสั่งในการเขียนโปรแกรม (Source code version Control)

(๗) มีการทดสอบบนสภาพแวดล้อมใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงของการเปลี่ยนแปลงบนระบบที่ให้บริการจริง

(๘) การทดสอบระบบที่ได้รับการพัฒนาหรือเปลี่ยนแปลง ควรครอบคลุม

- unit test
- system and integration test
- user acceptance test performance test
- Security test ตาม security Specification

(๙) มีกระบวนการสอบทาน test Scenario หรือ test case เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอ

/(๑๐) มีกระบวน ...

(๑๐) มีกระบวนการในการจัดการข้อผิดพลาดหรือข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ เพื่อพิจารณาแนวทางปรับปรุงหรือลดความเสี่ยงหรือผลกระทบของข้อผิดพลาดหรือข้อบกพร่องที่มีต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ

(๑๑) มีการจัดทำคู่มือและอบรมผู้ใช้งานระบบ เพื่อให้มีความเข้าใจฟังก์ชั่นการทำงานและมีการใช้งานระบบอย่างปลอดภัย รวมถึงจัดให้มีคู่มือการดูแลระบบและอบรมผู้ดูแลระบบ เพื่อสามารถตรวจสอบและจัดการแก้ไขปัญหาได้

(๑๒) หลังจากนำระบบขึ้นใช้งานจริงองค์การจัดการน้ำเสียควรพิจารณาจัดให้มีการทดสอบจริงในวงจำกัด (pilot test) สำหรับฟังก์ชั่นการทำงานที่สำคัญ รวมทั้งจัดให้มีการติดตามการใช้งานระบบหลังจากให้บริการจริงอย่างใกล้ชิดตามระยะเวลาที่เหมาะสม เพื่อให้มั่นใจต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ การนำระบบขึ้นใช้งานจริง (System deployment)

(๑๓) ระบบงานสำรองควรปรับปรุงให้มีความเป็นปัจจุบัน เพื่อให้มีความพร้อมใช้งานเมื่อเกิดเหตุฉุกเฉิน

ข้อ ๑๒ การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management)

๑๒.๑ การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident Management) มีวัตถุประสงค์เพื่อให้ องค์การจัดการน้ำเสีย มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์อย่างเหมาะสมทันการณ์ ให้สามารถจัดการแก้ไขปัญหาให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อภารกิจขององค์การจัดการน้ำเสีย

(๑) กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศควรครอบคลุมตั้งแต่กระบวนการหรือเครื่องมือในการบันทึกเหตุการณ์ผิดปกติ การกำหนดประเภท การจัดระดับความรุนแรง การวิเคราะห์หาสาเหตุ การดำเนินการแก้ไข การติดตามแก้ไข การรายงานเหตุการณ์ผิดปกติ

(๒) กำหนดหลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติ และรายงานความคืบหน้าเหตุการณ์ผิดปกติให้ผู้เกี่ยวข้อง ผู้บริหารระดับสูง คณะกรรมการที่เกี่ยวข้องได้รับทราบให้สอดคล้องกับระดับความรุนแรงของเหตุการณ์ผิดปกติ

/(๓) การจัด ...

(๓) การจัดระดับความรุนแรงของปัญหา ควรพิจารณาอย่างน้อยให้ครอบคลุมผลกระทบต่อการให้บริการ ผลกระทบต่อผู้ใช้งาน โดยกรอบระยะเวลาในการแก้ไขเหตุการณ์ผิดปกติควรคำนึงถึงเป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้หยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD) เพื่อที่จะสามารถตัดสินใจใช้แผนสำรองอย่างเหมาะสมทันการณ์

(๔) จัดทำแผนการรับมือกับเหตุการณ์ผิดปกติ (incident response plan) ตามความสำคัญของเหตุการณ์เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์ โดยอย่างน้อยแผนควรระบุกระบวนการรับมือและช่องทางประสานงานจากผู้เชี่ยวชาญทั้งภายในและภายนอก และมีแนวทางการตรวจสอบวิเคราะห์หาสาเหตุ และประเมินผลกระทบ

(๕) จัดทำรายงานเหตุการณ์ผิดปกติ เสนอต่อผู้บริหารระดับสูงที่ได้รับมอบหมาย โดยครอบคลุม วัน เวลา เหตุการณ์ ความเสียหาย การวิเคราะห์ สาเหตุที่แท้จริง การวิเคราะห์ผลกระทบ การแก้ไขปัญหาและแนวทางหรือแผนดำเนินการเพื่อป้องกันเหตุการณ์ผิดปกติในอนาคต และในกรณีที่เป็นความเสียหายส่งผลกระทบต่อชื่อเสียงและการดำเนินงาน

(๖) ในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการระบบงาน หรือชื่อเสียงขององค์การจัดการน้ำเสีย รวมถึงกรณีเทคโนโลยีสารสนเทศที่สำคัญขององค์การจัดการน้ำเสียถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่องค์การจัดการน้ำเสียต้องรายงานต่อผู้อำนวยการองค์การจัดการน้ำเสียทราบ

๑๒.๒ การบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ (IT Problem Management) มีวัตถุประสงค์เพื่อให้องค์การจัดการน้ำเสียมีกระบวนการติดตามหาสาเหตุที่แท้จริงให้มีแนวทางป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

(๑) มีมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ เพื่อให้มีการนำเหตุการณ์ผิดปกติที่ยังไม่ทราบสาเหตุที่แท้จริง (unknown root cause) เหตุการณ์ผิดปกติที่เกิดขึ้นซ้ำ (repeated incident) มาวิเคราะห์และพิจารณาแนวทางแก้ไขปัญหาจากสาเหตุที่แท้จริง (root cause)

(๒) มีกระบวนการหรือเครื่องมือในการบันทึกปัญหา หลักเกณฑ์ในการจัดประเภทปัญหา การจัดลำดับความสำคัญ วิเคราะห์ และจัดให้มีการติดตามการแก้ไขปัญหาเพื่อให้ปัญหาได้รับการแก้ไข

(๓) มีกระบวนการหรือเครื่องมือบันทึกปัญหาที่เคยเกิดขึ้น เพื่อให้เป็นแหล่งข้อมูลความรู้ให้สามารถสืบค้น เหตุการณ์ปัญหาและแนวทางการแก้ไขปัญหาได้ในภายหลังอย่างรวดเร็วและมีประสิทธิภาพ

/ข้อ ๑๓ ....

ข้อ ๑๓. นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยครอบคลุมอย่างน้อย

• โครงสร้างองค์กร บทบาทหน้าที่ของผู้เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

• จัดทำหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

๑๓.๑ การประเมินความเสี่ยง (risk assessment)

(๑) การระบุความเสี่ยง (risk identification)

องค์การจัดการน้ำเสียควรจัดให้มีการระบุเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้น หรือที่เกิดขึ้นจริง รวมถึงภัยคุกคามทางไซเบอร์และช่องโหว่ต่างๆ ที่ส่งผลกระทบต่อการดำเนินงานขององค์การจัดการน้ำเสีย โดยเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรระบุอย่างน้อยครอบคลุม

• ผู้กระทำให้เกิดความเสี่ยงและเหตุการณ์ความเสี่ยง เช่น ผู้ไม่ประสงค์ดี ภัยคุกคาม หรือช่องโหว่ เป็นต้น

• ประเภทของความเสี่ยง เช่น ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ ความเสี่ยงด้านโปรแกรม ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงด้านการบริหารโครงการ เป็นต้น

• วัน เวลา สถานที่ ช่วงเวลาหรือระยะเวลาที่เกิดเหตุการณ์ผิดปกติหรือความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ถ้ามี)

• สาเหตุของการเกิดเหตุการณ์ เช่น กระบวนการปฏิบัติงาน ระบบงาน บุคลากร ปัจจัยภายนอก เป็นต้น

• ผลกระทบต่อทรัพย์สิน ทรัพยากร การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และการดำเนินธุรกิจขององค์กร

ทั้งนี้ ผู้ที่มีส่วนร่วมในการระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศควรมีความรู้และความเข้าใจถึงเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ได้ระบุไว้เป็นอย่างดี

(๒) การวิเคราะห์ความเสี่ยง (risk analysis)

องค์การจัดการน้ำเสีย ควรจัดให้มีการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม โดยควรดำเนินการ ดังนี้

• กำหนดเจ้าของความเสี่ยงด้านเทคโนโลยีสารสนเทศ (risk owner)

• ระบุการควบคุมที่มีอยู่ในปัจจุบัน (existing Control)

/พิจารณา ...

• พิจารณาและค้นหาสาเหตุและสถานการณ์ที่เป็นไปได้

• วิเคราะห์ผลกระทบที่เกิดขึ้นจากเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(๓) การประเมินค่าความเสี่ยง (risk evaluation)

องค์การจัดการน้ำเสีย ควรประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ เพื่อจัดลำดับในการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ โดยควรดำเนินการ ดังนี้

• กำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบ เช่น ด้านการเงิน ด้านปฏิบัติการ เป็นต้น

• กำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)

• ประเมินค่าโอกาสและผลกระทบของเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

• จัดลำดับความเสี่ยงด้านเทคโนโลยีสารสนเทศแสดงในแผนภาพความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑๓.๒ การจัดการความเสี่ยง (risk treatment)

องค์การจัดการน้ำเสีย ควรจัดให้มีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรครอบคลุมอย่างน้อย ดังนี้

• กำหนดแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการเลือกแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมสำหรับองค์การจัดการน้ำเสีย เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง การลดหรือบรรเทาโอกาสเกิดความเสี่ยง การลดหรือบรรเทาผลกระทบที่เกิดขึ้น การแบ่ง หรือโอนความเสี่ยงให้หน่วยงานอื่น การยอมรับความเสี่ยงไว้โดยแจ้งเหตุผลให้ผู้บริหารทราบ เพื่อตัดสินใจในการยอมรับความเสี่ยง เป็นต้น

• ระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ ระยะเวลาที่ใช้ในการดำเนินการ

• ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้

• จัดทำแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดลำดับความสำคัญในการดำเนินการ

/นำเสนอ ...

• นำเสนอและขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

• ดำเนินการสื่อสารแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

นอกจากนี้ องค์การจัดการน้ำเสีย ควรจัดให้มีการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ให้สอดคล้องกับความสำคัญของงานเทคโนโลยีสารสนเทศแต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

๑๓.๓ การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

องค์การจัดการน้ำเสีย ควรกำหนดผู้รับผิดชอบและจัดให้มีกระบวนการในการติดตามดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ตามที่กำหนดและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรจัดให้มีการจัดเก็บและบันทึกข้อมูลอย่างเป็นระบบ เพื่อใช้ติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพ ครอบคลุม

• การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

• ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อจำกัดที่เกิดขึ้น

• ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น

• รายงานความคืบหน้าของแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามรอบที่กำหนด

๑๓.๔ การรายงานความเสี่ยง (risk reporting)

องค์การจัดการน้ำเสีย ควรจัดให้มีกระบวนการนำเสนอผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ พร้อมทั้งรายงานผลการประเมินและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร รวมทั้งรายงานแนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นต่อคณะกรรมการองค์การจัดการน้ำเสีย หรือคณะกรรมการที่ได้รับมอบหมาย อย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าองค์การจัดการน้ำเสียมีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและต่อเนื่อง โดยการรายงานควรครอบคลุมอย่างน้อย

• สถานะและผลลัพธ์การดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศประจำปี

/ผลการ ...

• ผลการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร

• รายงานดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ และรายงานสรุปเหตุการณ์ผิดปกติ

• แนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นกับองค์การจัดการน้ำเสีย

• ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง ทั้งนี้ องค์การจัดการน้ำเสีย ควรจัดให้มีการทบทวนหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ ๑ ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ข้อ ๑๔. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้องค์การจัดการน้ำเสีย มีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเกิดหยุดชะงักหรือเกิดความเสียหายโดยที่ภารกิจดำเนินการต่อไปได้อย่างต่อเนื่องและสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๑๔.๑ กำหนดนโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศโดยคำนึงความสอดคล้องกับนโยบายการบริหารความต่อเนื่องของธุรกิจและนโยบายการบริหารความเสี่ยงขององค์การจัดการน้ำเสีย

๑๔.๒ นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการองค์การจัดการน้ำเสียและได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนฉุกเฉินด้านสารสนเทศ เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบายการบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการดำเนินธุรกิจหรือทรัพยากรหรือโครงสร้างระบบ IT เป็นต้น

๑๔.๓ นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมอย่างน้อย

• บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการองค์การจัดการน้ำเสีย ผู้บริหารระดับสูง และผู้เกี่ยวข้อง

• การประเมินความเสี่ยง

• การวิเคราะห์ผลกระทบทางธุรกิจและกำหนดเป้าหมายในการกู้คืนระบบเทคโนโลยีสารสนเทศ

/การจัด ...

• การจัดระดับความสำคัญของระบบงาน

• การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

• การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

• การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

• การทดสอบ การปรับปรุง และการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๑๔.๔ มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยต้องได้รับการอนุมัติจากคณะกรรมการองค์การจัดการน้ำเสีย โดยจัดให้มีการทบทวนอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๑๔.๕ จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศไว้อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและบุคลากรขององค์การจัดการน้ำเสียด้านต่างๆที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น

๑๔.๖ การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรคำนึงถึงลักษณะการดำเนินธุรกิจ เหตุการณ์ความเสียหายต่างๆ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจขององค์การจัดการน้ำเสีย เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการดำเนินธุรกิจ (interdependency risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (Concentration risk) และความเสี่ยงที่มีผลกระทบต่อองค์การจัดการน้ำเสีย ผู้ใช้บริการ ผู้มีส่วนได้เสียและระบบสารสนเทศ (Systemic risk)

๑๔.๗ กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมการดำเนินการ ดังนี้

(๑) การประเมินความเสี่ยง (risk analysis) เพื่อให้องค์การจัดการน้ำเสียสามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการ อย่างเหมาะสมเพียงพอดังนี้

• ระบุเหตุการณ์ความเสี่ยง (risk scenarios) ที่อาจทำให้กระบวนการและระบบเทคโนโลยีสารสนเทศหยุดชะงักทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์

• ประเมินความเสี่ยงโดยพิจารณาการควบคุมที่มีอยู่ รวมถึงผลกระทบและโอกาสที่จะเกิดขึ้น พร้อมทั้งกำหนดกระบวนการและทรัพยากรที่จะใช้ในการควบคุมความเสี่ยง

/จัดทำ ...

• จัดทำแผนในการจัดการความเสี่ยง เพื่อปรับปรุงกระบวนการและจัดเตรียมทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

(๒) การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) เพื่อให้ทราบถึงความสำคัญของระบบเทคโนโลยีสารสนเทศที่มีผลต่อการดำเนินธุรกิจขององค์การจัดการน้ำเสีย รวมถึงผลกระทบจากการหยุดชะงักและความเชื่อมโยงของการดำเนินธุรกิจกับระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการดังนี้

• ระบุระบบเทคโนโลยีสารสนเทศทั้งหมดขององค์การจัดการน้ำเสียและทรัพยากรที่มีการเชื่อมโยงพึ่งพาระหว่างกัน (dependency)

• วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของเทคโนโลยีสารสนเทศ โดยคำนึงถึงเป้าหมาย ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD)

• กำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO)

(๓) การจัดลำดับความสำคัญของระบบงาน โดยคำนึงถึงทรัพยากร ระยะเวลาในการกู้คืนระบบ เป้าหมายของระบบงานและข้อมูลที่ควรกู้ได้ภายหลังเกิดการหยุดชะงัก และทรัพยากรทางเทคโนโลยี สารสนเทศขั้นต่ำที่จำเป็นต้องใช้ในการกู้คืนระบบ

(๔) การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ องค์การจัดการน้ำเสียต้องมีการกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและแนวทางจัดเตรียมทรัพยากรระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามการจัดลำดับความสำคัญของระบบงาน โดยพิจารณาอย่างน้อยครอบคลุม

• เป้าหมายระยะเวลาที่ได้จากการวิเคราะห์ผลกระทบทางธุรกิจ เช่น RTO, RPO เป็นต้น

• ปัจจัยสำคัญที่สนับสนุนให้แผนเป็นไปตามกลยุทธ์ เช่น เทคโนโลยีในการสำรองและกู้คืนข้อมูลความพร้อมใช้ของสถานที่ปฏิบัติงานสำรอง เป็นต้น เพื่อให้ องค์การจัดการน้ำเสียมีทิศทางในการพัฒนาแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่บรรลุเป้าหมายที่กำหนดไว้

• ทรัพยากรและงบประมาณ เพื่อจัดเตรียมระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามแผนกลยุทธ์และกิจกรรมที่ต้องดำเนินการทั้งหมด

/(๕) การจัดทำ ...

(๕) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรมีการระบุ กระบวนการและขั้นตอนสนับสนุนการปฏิบัติที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ รวมทั้งมีความยืดหยุ่นในการตอบสนองต่อเหตุการณ์ต่างๆที่อาจเกิดขึ้นอย่างน้อย ครอบคลุม

• ชื่อแผน วัตถุประสงค์ ขอบเขต และความสัมพันธ์กับแผนอื่นๆที่เกี่ยวข้อง

• ผังโครงสร้างของการบังคับบัญชาในการดำเนินงานตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบและผู้ปฏิบัติที่ทำหน้าที่แทนในกรณีที่ผู้ปฏิบัติหน้าที่ไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึกการเปลี่ยนแปลงของแผน

• รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม แผนภาพระบบ เครือข่ายสื่อสาร เป็นต้น

• ขั้นตอนในการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศการตอบสนองต่อเหตุการณ์ฉุกเฉินและแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบขั้นตอนในการดำเนินการกู้คืนระบบ โดยควรระบุรายละเอียดอย่างชัดเจนและเพียงพอ เพื่อให้สามารถใช้เป็น checklist ควบคุมไม่ให้มีการข้ามหรือละเลยขั้นตอนที่กำหนดไว้ ทั้งนี้ องค์การจัดการน้ำเสียควรจัดทำเอกสารหรือคู่มือประกอบการกู้คืนในแต่ละระบบ ในกรณีที่มีการปรับปรุง หรือเพิ่มเติมขั้นตอนนอกเหนือจากที่ระบุในแผนขณะปฏิบัติงานจริง องค์การจัดการน้ำเสียควรมีกระบวนการรายงานและขออนุมัติจากผู้บริหารตามที่กำหนดในโครงสร้างการบังคับบัญชา พร้อมทั้งนำขั้นตอนดังกล่าวมาปรับปรุงแผนให้เป็นปัจจุบัน

• ขั้นตอนในการกลับคืนสู่ภาวะปกติ (return to normal) และการประกาศยกเลิกแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศพร้อมเอกสารประกอบการทำงานภายใต้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรจัดเก็บไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้ในสถานที่ปฏิบัติงานหลักและสำรอง

(๖) การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ องค์การจัดการน้ำเสียต้องจัดให้มีการสื่อสารแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและจัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้อง

• ในการสื่อสารแผนฉุกเฉินด้านสารสนเทศต้องมีการระบุแนวทางสื่อสารที่ชัดเจนให้บุคลากรทุกคนที่มีส่วนเกี่ยวข้องได้รับทราบถึงรายละเอียดในการจัดทำแผน ขั้นตอนการดำเนินงานตามแผน

/จัดให้ ...

• จัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างน้อยปีละ ๑ ครั้ง โดยอย่างน้อยควรครอบคลุมวัตถุประสงค์ของแผน ขั้นตอนการปฏิบัติงานตามแผน การประสานงาน และการสื่อสารกันระหว่างกลุ่ม ขั้นตอนในการรายงาน ระบบรักษาความปลอดภัย กระบวนการเฉพาะของแต่ละกลุ่มดำเนินงาน และความรับผิดชอบของแต่ละบุคคล เป็นต้น

(๗) การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

• จัดให้มีแผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปี โดยมีรายละเอียดอย่างน้อยครอบคลุมสถานการณ์จำลอง รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบบทบาทหน้าที่ของผู้ที่เกี่ยวข้อง ทั้งนี้แผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปีในภาพรวมควรได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย จัดให้มีการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศทั้งในระดับหน่วยงานและระดับองค์กรอย่างน้อยปีละ ๑ ครั้ง

• มีการรายงานผลการทดสอบต่อคณะกรรมการองค์การจัดการน้ำเสีย โดยมีรายละเอียดอย่างน้อยครอบคลุม วัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ระยะเวลาที่ใช้ในการกู้คืนระบบเทียบกับเป้าหมายที่กำหนด ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบพร้อมทั้งแนวทางปรับปรุงแก้ไข องค์การจัดการน้ำเสียควรจัดให้มีการทบทวนและปรับปรุงแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อย ปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงบุคลากรที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผนการเปลี่ยนสภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศ เป็นต้น เพื่อให้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นปัจจุบัน องค์การจัดการน้ำเสียอาจจัดให้มีการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศโดยหน่วยงานภายนอกหรือภายในที่มีความเป็นอิสระ เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่างๆ ในการจัดทำแผนให้สามารถใช้งานได้จริง

ข้อ ๑๕ การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management) มีวัตถุประสงค์เพื่อให้องค์การจัดการน้ำเสียมีการบริหารจัดการความเสี่ยงของการดำเนินโครงการด้านเทคโนโลยีสารสนเทศ อย่างมีประสิทธิภาพและไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนกลยุทธ์ทางธุรกิจ

๑๕.๑ กำหนดกรอบการบริหารจัดการโครงการ (project management framework) ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางดำเนินโครงการจัดหาหรือพัฒนาระบบเทคโนโลยีสารสนเทศ โดยควรครอบคลุมดังนี้

/(๑) โครงสร้าง ...

(๑) โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจนเพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด

• คณะกรรมการกำกับดูแลโครงการ มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลให้โครงการสำเร็จเป็นไปตามเป้าหมายที่กำหนด มีการติดตามความคืบหน้า ปัญหาและอุปสรรคของโครงการ เพื่อให้คำแนะนำและพิจารณาตัดสินใจการดำเนินงานที่สำคัญ โดยควรประกอบด้วยผู้บริหารจากหน่วยงานต่างๆที่เกี่ยวข้องและเจ้าของโครงการหรือ ผู้สนับสนุนโครงการ (project owner/ project sponsor) มีส่วนร่วมในการตัดสินใจ รวมทั้งคณะกรรมการกำกับดูแลโครงการควรมีการประชุมอย่างสม่ำเสมอ เพื่อควบคุมดูแลโครงการที่สำคัญให้เป็นไปตามแผนงานที่กำหนด

• องค์การจัดการน้ำเสียหรือทีมงานดูแลภาพรวมโครงการ มีบทบาทหน้าที่และความรับผิดชอบในการกำหนดรูปแบบ กระบวนการและเครื่องมือ ที่เป็นมาตรฐานในการบริหารจัดการและติดตามโครงการ รวมทั้งติดตาม รายงานภาพรวม โครงการสำคัญขององค์การจัดการน้ำเสียให้กับคณะกรรมการองค์การจัดการน้ำเสียและผู้บริหารระดับสูงที่เกี่ยวข้องได้รับทราบเพื่อติดตามและสนับสนุนให้บริหารจัดการโครงการสำเร็จลุล่วงสอดคล้องกับเป้าหมายในระดับกลยุทธ์ขององค์การจัดการน้ำเสียตามแผนงานที่กำหนด

• ประธานคณะทำงาน มีบทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการโครงการ ครอบคลุม กำหนดแผนงานโครงการ วิเคราะห์ผลกระทบ และจัดให้มีแนวทางรองรับหรือแผนสำรองกรณีโครงการประสบปัญหาหรือล่าช้า รวมทั้งรายงานให้คณะกรรมการกำกับดูแลโครงการพิจารณาตัดสินใจแก้ไขปัญหาได้ทันการณ์ เพื่อให้โครงการสามารถส่งมอบได้อย่างถูกต้องครบถ้วนสำเร็จตามแผนงานที่กำหนด โดยประธานคณะทำงานต้องมีความรู้ความสามารถและประสบการณ์ในการบริหารโครงการที่เพียงพอ

(๒) แนวทางการบริหารจัดการโครงการ ควรกำหนดครอบคลุมอย่างน้อย ดังนี้

• ระเบียบขั้นตอนการบริหารจัดการโครงการ ครอบคลุมตั้งแต่ก่อนเริ่มโครงการ การดำเนินการและควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ

• ปัจจัยและเกณฑ์ในการประเมินหรือจัดระดับความสำคัญของโครงการที่ชัดเจน รวมถึงขอบเขตอำนาจหน้าที่ในการอนุมัติและกำกับดูแลโครงการตามระดับความสำคัญของโครงการ

/รูปแบบ ...

• รูปแบบของเอกสารหรือผลลัพธ์ที่เป็นมาตรฐาน ที่ต้องส่งมอบในแต่ละขั้นตอนอย่างชัดเจน เช่น แผนการดำเนินโครงการ รายงานความคืบหน้า รายงานการปิดโครงการ เป็นต้น

๑๕.๒ การเริ่มโครงการ ให้มีการประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งเลือกใช้เทคโนโลยีที่เหมาะสม ทั้งนี้โครงการต้องมีเป้าหมายที่ชัดเจน (project objective) สอดคล้องกับกลยุทธ์ขององค์กรและคำนึงถึงการรักษาความมั่นคงปลอดภัย

๑๕.๓ มีแผนการดำเนินโครงการ ที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการ อย่างน้อยครอบคลุม

• เป้าหมายโครงการ

• ทรัพยากร (resources) ที่ใช้

• บทบาทหน้าที่ ความรับผิดชอบของคณะทำงานในการดำเนินโครงการ โดยคณะทำงานจะต้องมีประสิทธิภาพและมีความรู้ความเชี่ยวชาญเพียงพอในการดำเนินโครงการ

• ขอบเขตและระยะเวลาของการดำเนินโครงการในแต่ละขั้นตอน

• ผลงานที่จะส่งมอบในแต่ละขั้นตอน

• ข้อกำหนดเงื่อนไขที่เกี่ยวข้องกับโครงการ เช่น ข้อกำหนดของผู้ว่าจ้าง ภาระผูกพัน ข้อจำกัด เป็นต้น

๑๕.๔ มีการนำเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อคณะกรรมการองค์การจัดการน้ำเสีย คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงตามขอบเขตในการอนุมัติที่กำหนดไว้

๑๕.๕ มีการบันทึกและจัดเก็บข้อมูลโครงการของแต่ละโครงการอย่างเพียงพอ เพื่อใช้ติดตามดูแลและสามารถตรวจสอบย้อนหลังได้

๑๕.๖ มีการประเมินและติดตามการดำเนินโครงการอย่างต่อเนื่องและครอบคลุมขอบเขต ระยะเวลา และทรัพยากร ที่วางแผนไว้ในกรณีที่มีการเปลี่ยนแปลงขอบเขต ระยะเวลาและ/หรือทรัพยากร หรือยกเลิกโครงการ ควรมีการนำเสนอเพื่อขออนุมัติการเปลี่ยนแปลงหรือยกเลิกโครงการ

/๑๕.๗ มีการ ...

๑๕.๗ มีการรายงานความคืบหน้า ปัญหา อุปสรรคและข้อจำกัดในการดำเนินโครงการ ต่อคณะกรรมการกำกับดูแลโครงการหรือผู้บริหารที่ได้รับมอบหมายอย่างเป็นประจำ เพื่อสามารถให้คำแนะนำและแนวทางในการแก้ไขปัญหาที่จะลดความเสี่ยงที่อาจเกิดขึ้นอย่างทันท่วงที โดยโครงการที่ส่งผลกระทบต่อภารกิจขององค์การจัดการน้ำเสียอย่างมีนัยสำคัญ ควรนำเสนอแก่คณะกรรมการองค์การจัดการน้ำเสีย ด้วย

๑๕.๘ การสรุปประโยชน์ที่ได้รับจากโครงการเทียบกับเป้าหมายที่กำหนด

๑๕.๙ มีการรวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นสิ่งที่ได้เรียนรู้ (Lesson learned) ใช้สำหรับวิเคราะห์ ปรับปรุง และพัฒนากระบวนการหรือเครื่องมือในการบริหารจัดการโครงการต่อไปให้มีประสิทธิภาพมากขึ้น

๑๕.๑๐ มีการสอบทานโครงการที่สำคัญโดยหน่วยงานอิสระ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของโครงการ นโยบาย มาตรฐาน ระเบียบและวิธีปฏิบัติขององค์การจัดการน้ำเสีย รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

ข้อ ๑๖ เพื่อให้การบริหารงานและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน ให้องค์การจัดการน้ำเสียมีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล โดยมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยมุ่งหมายในการเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการและการเข้าถึงของประชาชน และในการเปิดเผยข้อมูลภาครัฐต่อสาธารณะและสร้างการมีส่วนร่วมของทุกภาคส่วน อย่างน้อยดังนี้

๑๖.๑ การนำระบบดิจิทัลที่เหมาะสมมาใช้ในการบริหารและการให้บริการเพื่อเพิ่มประสิทธิภาพและให้มีการใช้ระบบดิจิทัลอย่างคุ้มค่าและเต็มศักยภาพ

๑๖.๒ การพัฒนามาตรฐาน หลักเกณฑ์ และวิธีการเกี่ยวกับระบบดิจิทัลและพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่จำเป็นให้เป็นไปตามมาตรฐานสากล เพื่อสร้างและพัฒนากระบวนการทำงานขององค์การจัดการน้ำเสียให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐ รวมทั้ง มีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยมีการบูรณาการและสามารถทำงานร่วมกันอย่างเป็นเอกภาพ เกิดการพัฒนาการบริการภาครัฐ ที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชนแบบบูรณาการ รวมทั้งให้ประชาชนเข้าถึงได้โดยสะดวก

๑๖.๓ การสร้างและพัฒนาระบบความมั่นคงปลอดภัยในการใช้ระบบดิจิทัลและมาตรการปกป้อง คุ้มครองข้อมูลที่อาจกระทบถึงความมั่นคงหรือความเป็นส่วนตัวของประชาชนที่มีความพร้อมใช้และน่าเชื่อถือ

/๑๖.๔ การเปิด ...

๑๖.๔ การเปิดเผยข้อมูลหรือข่าวสารสาธารณะที่องค์การจัดการน้ำเสียจัดทำและครอบครองในรูปแบบและช่องทางดิจิทัล เพื่อให้ประชาชนเข้าถึงได้โดยสะดวก มีส่วนร่วมและตรวจสอบการดำเนินงานขององค์การจัดการน้ำเสีย และสามารถนำข้อมูลไปพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อองค์การจัดการน้ำเสียในด้านต่าง ๆ

๑๖.๕ การรักษาวินัยและเพิ่มประสิทธิภาพในการใช้จ่ายงบประมาณ ให้เกิดความคุ้มค่าและเป็นไปตามเป้าหมาย โดยมีการติดตาม ตรวจสอบ และประเมินความคุ้มค่าในการดำเนินงานเพื่อให้เป็นไปตามการบริหารงานขององค์การจัดการน้ำเสีย และการจัดทำบริการสาธารณะผ่านระบบดิจิทัล รวมทั้งพัฒนาให้มีกลไกการใช้ข้อมูลเพื่อลดความซ้ำซ้อนและเกิดความสอดคล้องกับแผนงานและโครงการต่างๆขององค์การจัดการน้ำเสีย

ข้อ ๑๗ การฝ่าฝืนและบทลงโทษ

(๑) องค์การจัดการน้ำเสีย จะไม่รับผิดชอบต่อผลของการกระทำความผิดใดๆ ที่เกิดขึ้นกับผู้ใช้งาน หรือบัญชีผู้ใช้งานที่มีการนำเอาไปใช้งานที่ขัดต่อข้อกฎหมาย และนโยบายขององค์การจัดการน้ำเสีย

(๒) ผู้ใช้งานที่ไม่ปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์องค์การจัดการน้ำเสีย จะถูกพิจารณาถอดถอนสิทธิในการใช้งานชั่วคราวหรือถาวร แล้วแต่กรณี

(๓) ผู้ใช้งานต้องรับผิดชอบเป็นการส่วนตัวต่อผลการกระทำความผิดใดๆ ที่ขัดต่อพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

การฝ่าฝืน หรือไม่ปฏิบัติตามระเบียบนี้ อันก่อให้เกิดความเสียหายแก่บุคคลอื่นหรือองค์การจัดการน้ำเสีย ให้ดำเนินการทางวินัย

ข้อ ๑๘ กรณีมีปัญหาการปฏิบัติตามระเบียบนี้ ให้ผู้อำนวยการองค์การจัดการน้ำเสียเป็นผู้วินิจฉัยและคำวินิจฉัยให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๗ กันยายน ๒๕๖๓

(นายชีระ วงศบูรณะ)
ผู้อำนวยการองค์การจัดการน้ำเสีย

ฝ่ายพัฒนาองค์กร
กองสารสนเทศและประเมินผล

/สำเนาเรียน...

สำเนาเรียน ผอ.อจน.

รผอ.อจน.(บร.) รผอ.อจน.(วผ.) รผอ.อจน.(ปก.)

- เพื่อโปรดทราบ

ผชช. สผอ. สตน. ฝอก. ฝบง. ฝพอ. ฝวศ. ฝบจ. ฝจส.๑ ฝจส.๒
กกม. กคพ. กพบ. กทบ. กปส. กบช. กกง. กงป. กนผ. กบค.
กสป. กมว. กพค. กปง.๑ กปง.๒ สจส. กจร. กวพ.

- เพื่อทราบ

(นางดวงแข ยงสุวรรณ)
ห.กกล.
๑๑ ก.ย.๖๓