องค์การจัดการน้ำเสีย
WASTEWATER MANAGEMENT AUTHORITY
MINISTRY OF INTERIOR, THAILAND

ประกาศองค์การจัดการน้ำเสีย

ที่ ๒๗/๒๕๖๓

เรื่อง นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี ขององค์การจัดการน้ำเสีย

๑. หลักการและเหตุผล

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology : IT) ได้เข้ามามีบทบาทสำคัญต่อ การดำเนินงานตามภารกิจมากขึ้น โดยองค์การจัดการน้ำเสียได้นำเทคโนโลยีสารสนเทศมาใช้เป็นโครงสร้างพื้นฐานที่สำคัญที่ช่วยเพิ่มประสิทธิภาพในการดำเนินงาน และลดต้นทุนในการดำเนินงาน อย่างไรก็ดี แม้ว่าการใช้เทคโนโลยีสารสนเทศจะช่วยให้การดำเนินงานมีประสิทธิภาพมากขึ้น แต่หากองค์การจัดการน้ำเสียขาดการบริหารความเสี่ยงที่ดี การใช้เทคโนโลยีสารสนเทศดังกล่าวก็อาจก่อให้เกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) และภัยคุกคามทางไซเบอร์ (Cyber Threat) ที่ส่งผลกระทบต่อการดำเนินงานขององค์การจัดการน้ำเสีย

ดังนั้น องค์การจัดการน้ำเสียจึงกำหนดหลักเกณฑ์กำกับดูแลให้องค์กรมีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และมีการบริหารความเสี่ยงดังกล่าวอย่างเหมาะสม โดยเน้นที่องค์ประกอบและบทบาทหน้าที่ของ คณะทำงานดิจิทัลองค์การจัดการน้ำเสีย โครงสร้างองค์กร และการบริหารจัดการบุคลากร โดยคณะทำงานดิจิทัลองค์การจัดการน้ำเสียและผู้บริหารระดับสูงขององค์การจัดการน้ำเสีย ต้องมีความรู้ความเข้าใจอย่างเพียงพอในการกำหนดทิศทางการใช้เทคโนโลยีให้สอดรับกับกลยุทธ์ในการดำเนินงานตามภารกิจของหน่วยงาน มีความเท่าทันความเสี่ยงที่มีมากขึ้นอันเนื่องมาจากการนำเทคโนโลยีมาใช้อย่างแพร่หลาย ให้ความสำคัญกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ และมีการกำหนดและสื่อสารนโยบายที่เกี่ยวข้องไปยังบุคลากรทุกระดับในองค์กรเพื่อให้เกิดความตระหนักและความเข้าใจ ตลอดจนมีการนำนโยบายไปปฏิบัติด้วยกระบวนการที่เหมาะสม รวมถึงต้องดูแลให้มีการวางแผนและบริหารจัดการด้านบุคลากร โดยเฉพาะที่ทำหน้าที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศให้มีคุณสมบัติและความรู้ที่เหมาะสมกับหน้าที่ที่ได้รับมอบหมาย และมีปริมาณที่เพียงพอที่จะรองรับการดำเนินงานขององค์การจัดการน้ำเสียทั้งในปัจจุบันและในอนาคต

/นอกจากนี้ ...

๓๓๓ อาคารเล้าเป๋งง้วน ๑ ชั้น ๒๓ ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กทม. ๑๐๙๐๐ โทรศัพท์ ๐ ๒๒๗๓ ๘๕๓๐-๙ โทรสาร ๐ ๒๒๗๓ ๘๕๗๗-๙
333 LAO PENG NGUAN TOWER 1 FL 23rd VIBHAVADI-RANGSIT Rd., JOMPHON, CHATUJAK, BANGKOK 10900 Tel. 0 2273 8530-9 FAX 0 2273 8577-9
URL : http://www.wma.or.th e-mail : wastewtr@wma.or.th

นอกจากนี้ องค์การจัดการน้ำเสียยังเน้นให้องค์กรมีการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ การตรวจสอบด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและรัดกุม โดยอยู่ภายใต้กรอบหลักการ ที่สำคัญ ๓ ประการ คือ (๑) การรักษาความลับของระบบและข้อมูล (Confidentiality) (๒) ความถูกต้อง เชื่อถือได้ของระบบและข้อมูล (Integrity) และ (๓) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability) รวมถึงอยู่บนพื้นฐานของการคุ้มครองข้อมูล ซึ่งองค์การจัดการน้ำเสียต้องมีการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการดำเนินงาน และความเสี่ยงที่เกี่ยวข้อง เช่น ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านชื่อเสียง และความเสี่ยงด้านกฎหมาย

ทั้งนี้ ในกรณีที่องค์การจัดการน้ำเสียเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศ ซึ่งส่งผลกระทบต่อการให้บริการระบบหรือชื่อเสียงของหน่วยงาน โดยรวมถึงกรณีที่เทคโนโลยีสารสนเทศที่สำคัญของหน่วยงานถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่หน่วยงานต้องรายงานให้ผู้บริหารในตำแหน่งสูงสุดขององค์การจัดการน้ำเสียทราบ ให้หน่วยงานที่ได้รับมอบหมายต้องรายงานตามสายงานทันทีเมื่อเกิดหรือรับรู้เหตุการณ์นั้น หรือมีการเปลี่ยนแปลงการใช้เทคโนโลยี ที่มีผลกระทบหรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินงาน

๒. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับองค์การจัดการน้ำเสีย และสำนักงานจัดการน้ำเสียทุกสาขา

/๓. คำจำกัด ...

๓. คำจำกัดความ

"ความเสี่ยงด้านเทคโนโลยีสารสนเทศ" หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินภารกิจ ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานขององค์การจัดการน้ำเสีย รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (Cyber Threat)

"เทคโนโลยีสารสนเทศ (Information Technology - IT)" หมายความว่า เทคโนโลยีสารสนเทศที่นำมาใช้ในการดำเนินงาน ซึ่งครอบคลุมถึง ข้อมูล ระบบปฏิบัติการ (Operating System) ระบบงาน (Application System) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร (Communication) เป็นต้น

"คณะทำงานดิจิทัล องค์การจัดการน้ำเสีย" หมายถึง คณะทำงานดิจิทัล องค์การจัดการน้ำเสีย ตามคำสั่งองค์การจัดการน้ำเสีย ที่ ๖/๒๕๖๒ ลงวันที่ ๑๐ มกราคม พ.ศ. ๒๕๖๒

๔. หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๔.๑ ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance)

๔.๑.๑ บทบาทหน้าที่และความรับผิดชอบของคณะทำงานดิจิทัล องค์การจัดการน้ำเสีย

คณะทำงานดิจิทัล องค์การจัดการน้ำเสีย ควรมีกรรมการที่มีความรู้ หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศอย่างน้อย ๑ ท่าน เพื่อให้สามารถกำหนดทิศทางและกำกับดูแลให้หน่วยงานมีการใช้เทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์ในการดำเนินงานขององค์การจัดการน้ำเสีย มีความรู้เท่าทันความเสี่ยงและพัฒนาการด้านเทคโนโลยีที่เปลี่ยนแปลงไป ซึ่งจะช่วยให้สามารถกำกับดูแลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

นอกจากนี้ คณะทำงานดิจิทัล องค์การจัดการน้ำเสีย ต้องได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศและความเสี่ยงที่เกี่ยวข้องอย่างเพียงพอตามระยะเวลาที่เหมาะสมเพื่อให้คณะทำงานดิจิทัลองค์การจัดการน้ำเสีย มีความรู้ความเข้าใจเกี่ยวกับเทคโนโลยีสารสนเทศและความเสี่ยงที่เกี่ยวข้องเพื่อประโยชน์ในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์การจัดการน้ำเสีย คณะทำงานดิจิทัลองค์การจัดการน้ำเสีย มีบทบาทหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยดังต่อไปนี้

/(๑) ดูแลให้ ...

(๑) ดูแลให้มีการใช้เทคโนโลยีที่สอดรับกับกลยุทธ์ในการดำเนินงาน และดูแลให้การใช้เทคโนโลยีขององค์กรมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและการเปลี่ยนแปลงการดำเนินงานในอนาคต

(๒) ดูแลให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(๓) ดูแลให้มีการกำหนด (๑) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งรวมถึงนโยบายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และ (๒) นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Policy) โดยนโยบายดังกล่าวต้องสอดคล้องกับลักษณะการดำเนินงานตามภารกิจ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งทำหน้าที่ในการอนุมัตินโยบายดังกล่าว

(๔) ดูแลให้มีการนำ (๑) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) และ (๒) นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Policy) ที่ได้อนุมัติ มาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและประเมินประสิทธิภาพของนโยบายดังกล่าวอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๕) ดูแลให้มีการติดตาม ตรวจสอบ และรายงานต่อผู้บริหารที่ได้รับมอบหมายอย่างเหมาะสม ในเรื่องที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น ผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมขององค์กร ข้อมูลเกี่ยวกับปัญหา หรือเหตุการณ์ทางด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงขององค์กร

(๖) ดูแลและสนับสนุนให้มีการสื่อสารกับบุคลากรของหน่วยงาน เพื่อให้ตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศ และให้เข้าใจถึงการใช้เทคโนโลยีสารสนเทศที่ถูกต้อง เพื่อช่วยลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ

/๔.๑.๒ โครงสร้าง ...

๔.๑.๒ โครงสร้างการกำกับดูแล

(๑) โครงสร้างองค์กร

องค์การจัดการน้ำเสียต้องจัดให้มีโครงสร้างองค์กรที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ ๓ ระดับ (Three Lines of Defence) โดยมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนระหว่างการทำหน้าที่ (๑) ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (๒) บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และ (๓) ตรวจสอบด้านเทคโนโลยีสารสนเทศ นอกจากนี้ องค์การจัดการน้ำเสียต้องจัดให้มีการถ่วงดุลอำนาจกันอย่างอิสระ โดยเฉพาะการทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศต้องมีความเป็นอิสระจากการทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(๒) คณะทำงานดิจิทัล องค์การจัดการน้ำเสีย ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(๒.๑) คณะทำงานดิจิทัล องค์การจัดการน้ำเสีย ทำหน้าที่บริหารจัดการรวมถึงกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

(๒.๒) คณะทำงานดิจิทัล องค์การจัดการน้ำเสีย ที่ทำหน้าที่ กำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้เป็นไปตามนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กำหนดไว้

(๒.๓) คณะทำงานดิจิทัล องค์การจัดการน้ำเสีย ที่ทำหน้าที่ กำกับดูแลให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งการตรวจสอบครอบคลุมถึงการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งกำกับดูแลให้มีการสอบทานการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

/๔.๑.๓ การบริหาร ...

๔.๑.๓ การบริหารจัดการบุคลากร

องค์การจัดการน้ำเสีย ต้องมีการบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงาน ด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานประจำวัน (user) อย่างเหมาะสม โดยต้องคำนึงถึงความรู้ความสามารถของบุคลากร ปริมาณงาน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยองค์การจัดการน้ำเสีย ต้องจัดให้มีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(๑) การบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ จะต้องครอบคลุมในเรื่องดังต่อไปนี้

(๑.๑) กระบวนการคัดเลือกบุคลากร เพื่อให้ได้บุคลากรที่มีคุณสมบัติเหมาะสม มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย โดยอาจพิจารณาการได้รับการรับรองความรู้ความสามารถตามมาตรฐานที่รับรองทั่วไป (certificate) เฉพาะด้านที่เกี่ยวข้องกับงานด้านเทคโนโลยีสนเทศที่ได้รับมอบหมายนั้น

(๑.๒) ความเพียงพอของบุคลากร เพื่อให้มีปริมาณบุคลากรที่เพียงพอกับปริมาณการใช้เทคโนโลยีสารสนเทศขององค์การจัดการน้ำเสีย

(๑.๓) มาตรการในการสร้างและส่งเสริมความตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้บุคลากรมีการตระหนักถึงบทบาทหน้าที่และความรับผิดชอบของตน และมาตรการดูแลให้บุคลากรปฏิบัติตามหน้าที่และรับผิดชอบตามที่กำหนดไว้

(๒) การอบรมให้ความรู้แก่คณะทำงานดิจิทัล องค์การจัดการน้ำเสีย ผู้บริหารระดับสูง และบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ อย่างเพียงพอตามระยะเวลาที่เหมาะสม โดยครอบคลุมเนื้อหาต่างๆที่เกี่ยวข้อง เช่น พัฒนาการด้านเทคโนโลยี ภัยคุกคามทางไซเบอร์ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

/เพื่อให้ ...

เพื่อให้คณะทำงานดิจิทัล องค์การจัดการน้ำเสีย ผู้บริหารระดับสูง และบุคลากรมีความรู้และทักษะที่เพียงพอต่อการกำกับดูแลหรือปฏิบัติงานในส่วนที่เกี่ยวข้อง

(๓) การบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยต้องมีการปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน เช่น ทบทวนสิทธิในการเข้าถึงข้อมูล รวมทั้งต้องมีการสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงสิทธิหน้าที่ และความรับผิดชอบดังกล่าว

๔.๑.๔ การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Awareness)

องค์การจัดการน้ำเสียต้องจัดให้มีการสื่อสารและให้ความรู้แก่บุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานประจำวันอย่างเพียงพอและเหมาะสม เพื่อให้บุคลากรมีความเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เช่น การจัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์ที่มีการเชื่อมต่อกับอินเทอร์เน็ตที่ถูกต้อง และการซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์

๔.๑.๕ นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(๑) องค์การจัดการน้ำเสียต้องจัดให้มี (๑) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) และ (๒) นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) ที่เป็นลายลักษณ์อักษร และอยู่ภายใต้กรอบหลักการที่สำคัญ ๓ ประการ คือ (๑) การรักษาความลับของระบบและข้อมูล (Confidentiality) (๒) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และ (๓) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability) โดยนโยบายดังกล่าวต้องสอดคล้องกับกลยุทธ์ขององค์กรในการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานตามภารกิจและนโยบายการบริหารความเสี่ยงขององค์การจัดการน้ำเสีย รวมทั้งสอดคล้องกับแนวทางการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

/(๒) องค์การ ...

(๒) องค์การจัดการน้ำเสียต้องจัดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๔.๒ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

เพื่อให้องค์การจัดการน้ำเสียมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่มีประสิทธิภาพ องค์การจัดการน้ำเสียต้องนำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์การจัดการน้ำเสีย โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

๔.๒.๑ การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

องค์การจัดการน้ำเสียต้องจัดให้มีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องมีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้ในการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม รวมถึงต้องจัดให้มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง

๔.๒.๒ การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

องค์การจัดการน้ำเสียต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสารและการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่างๆ มีการจัดชั้นความลับของข้อมูล (Information Classification) มีการเก็บรักษาและทำลายข้อมูลให้เหมาะสมกับชั้นความลับ และมีการบริหารจัดการการเข้ารหัสข้อมูล (Cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากล เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

/๔.๒.๓ การควบคุม ...

๔.๒.๓ การควบคุมการเข้าถึง (Access Control)

องค์การจัดการน้ำเสียต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต

๔.๒.๔ การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

องค์การจัดการน้ำเสียต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และระบบสาธารณูปโภค (facility) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้งานสามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง

๔.๒.๕ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

องค์การจัดการน้ำเสียต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบ เครือข่ายสื่อสารของหน่วยงานเพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่มีการรับส่งผ่านเครือข่ายสื่อสาร มีความมั่นคงปลอดภัย และสามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น

๔.๒.๖ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

องค์การจัดการน้ำเสียต้องจัดให้มีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย โดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

/(๑) การบริหาร ...

(๑) การบริหารจัดการขีดความสามารถของระบบ และระบบสาธารณูปโภค (capacity management) เช่น การประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอต่อการรองรับการดำเนินงานและสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

(๒) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และ อุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint) เช่น การติดตั้งโปรแกรมป้องกันไวรัส หรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่ประสงค์ดี (malware) หรือการโจมตีด้วยรูปแบบต่างๆ เพื่อป้องกันการรั่วไหลของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต

(๓) การสำรองข้อมูล (Data Backup) ด้วยวิธีการและระยะเวลาที่เหมาะสม เช่น การสำรองข้อมูลประจำวัน เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบ และข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย

(๔) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญ เช่น การจัดเก็บและสอบทานบันทึกการเข้าถึงระบบ (Access Log) และบันทึกการดำเนินงาน (Activity Log) เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการใช้งานระบบหรือข้อมูล

(๕) การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring) โดยมีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เช่น เครื่องมือในการติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่องเพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

(๖) การบริหารจัดการช่องโหว่ (Vulnerability Management) ของระบบที่เหมาะสมตามระดับความเสี่ยง เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์ โดยองค์การจัดการน้ำเสียต้องมีการประเมินช่องโหว่ของระบบงานสำคัญทุกระบบอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

/(๗) การทดสอบ ...

(๗) การทดสอบเจาะระบบ (Penetration Test) โดยจัดให้มีผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระทำหน้าที่ทดสอบเจาะระบบ โดยเฉพาะระบบงาน (Application) และระบบเครือข่าย (Network) ที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ สม่ำเสมออย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้ทราบถึงช่องโหว่ และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

(๘) การบริหารจัดการการเปลี่ยนแปลง (Change Management) โดยจัดให้มีกระบวนการในการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงอย่างรัดกุมและเพียงพอ เช่น การนำระบบขึ้นใช้งานจริง (System Deployment) การตั้งค่าระบบ (System Configuration) การติดตั้ง patch เพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต

(๙) การบริหารจัดการการตั้งค่าระบบ (System Configuration Management) โดยจัดให้มีกระบวนการในการควบคุมการตั้งค่าของระบบที่ใช้งานจริง และมีการสอบทานการตั้งค่าอย่างสม่ำเสมอ เพื่อป้องกันข้อผิดพลาดในการปฏิบัติงาน

(๑๐) การบริหารจัดการ Patch (Patch Management) โดยจัดให้มีกระบวนการในการควบคุมการติดตั้ง patch ของระบบที่ใช้งานจริง เพื่อให้สามารถติดตั้ง Patch ที่สำคัญในการรักษาความมั่นคงปลอดภัยได้อย่างทันการณ์

๔.๒.๗ การจัดหาและการพัฒนาระบบ (System Acquisition and Development)

(๑) การจัดหาระบบ (System Acquisition)

องค์การจัดการน้ำเสียต้องกำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและผู้ให้บริการ เช่น ความน่าเชื่อถือของระบบและผู้ให้บริการ การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate) ความมั่นคงปลอดภัยของระบบ การสนับสนุนและการบำรุงรักษาระบบ เพื่อให้มั่นใจว่าระบบและผู้ให้บริการ สามารถตอบสนองต่อความต้องการในการดำเนินธุรกิจของสถาบันการเงินได้ รวมถึงต้องคำนึงถึงความยืดหยุ่น ในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี หรือการเปลี่ยนแปลงกลยุทธ์ในการดำเนินธุรกิจในอนาคต

/ (๒) การพัฒนา ...

(๒) การพัฒนาระบบ (System Development)

องค์การจัดการน้ำเสียต้องจัดให้มีการออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต โดยองค์การจัดกาน้ำเสียต้องจัดให้มีอย่างน้อย ในเรื่องดังต่อไปนี้

- เอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการในการทดสอบ การดูแล และการติดตามความมั่นคงปลอดภัยในการใช้งาน

- กระบวนการหรือเครื่องมือในการควบคุมเวอร์ชั่นของคำสั่ง ในการเขียนโปรแกรม (Source Code version Control)

- การแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (Development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (Production)

- การทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ (Unit Test) ทดสอบการทำงานร่วมกันของระบบต่าง ๆ (System Integration Test) ทดสอบความพร้อมใช้งานตามกระบวนการและความต้องการของผู้ใช้งาน (User Acceptance Test) และ ทดสอบความปลอดภัยของระบบ (Security Test) ตามกระบวนการในการรักษาความมั่นคงปลอดภัยที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification)

- การพัฒนาหรือการเปลี่ยนแปลงระบบสารสนเทศ จะต้องจัดให้มีการทดสอบประสิทธิภาพ (Performance Test)

- แนวทางในการควบคุมการรักษาความมั่นคงปลอดภัยและ ความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ

- การจัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

/๔.๒.๘ การบริหาร ...

๔.๒.๘ การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT Incident and Problem Management)

องค์การจัดการน้ำเสียต้องจัดให้มีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยมีการบันทึก วิเคราะห์ และรายงาน เหตุการณ์ผิดปกติและปัญหา และการแก้ไขให้ผู้บริหารระดับสูงที่ได้รับมอบหมาย ทราบในระยะเวลาที่เหมาะสม นอกจากนี้ หน่วยงานต้องมีการวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหาเพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติในอนาคต

๔.๒.๙ การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

(๑) องค์การจัดกาน้ำเสียต้องจัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรให้เป็นไปตามนโยบายที่กำหนดไว้และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศดังกล่าวต้องได้รับอนุมัติโดยผู้บริหารที่ได้รับมอบหมาย

(๒) ในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศองค์การจัดการน้ำเสียต้องคำนึงถึงลักษณะการดำเนินงานและความเสี่ยงที่เกี่ยวข้อง รวมทั้งการบริหารความเสี่ยงที่อาจเกิดจากเหตุการณ์ ความเสียหายต่างๆ และความเสี่ยงทั่วไป เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) เป็นต้น

(๓) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต้องมีความเป็นไปได้ในทางปฏิบัติ สามารถนำมาใช้รองรับความเสียหายที่เกิดขึ้นได้จริง และสอดคล้องกับแนวปฏิบัติขององค์การจัดการน้ำเสียเรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) โดยแผนฉุกเฉินดังกล่าวควรครอบคลุมถึงการกำหนดระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) ที่สอดคล้องกับความสำคัญ

/ของระบบ ...

ของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้การดำเนินงานหยุดชะงัก (maximum tolerance period of disruption : MTPD) เพื่อรองรับการดำเนินงานอย่างต่อเนื่อง และรองรับการเกิดเหตุการณ์ผิดปกติต่างๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามทางไซเบอร์ ภัยธรรมชาติ เพื่อให้องค์การจัดการน้ำเสียดำเนินการกู้ระบบและกลับสู่การทำงานได้ตามปกติให้เร็วที่สุด

(๔) องค์การจัดการน้ำเสียต้องจัดทำคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์แผนและฝึกอบรมเพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนได้

(๕) องค์การจัดการน้ำเสียต้องจัดให้มีการทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๖) องค์การจัดการน้ำเสียควรจัดให้มีศูนย์คอมพิวเตอร์สำรอง (disaster recovery site) ที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลัก (primary Site) หยุดชะงัก โดยองค์การจัดการน้ำเสียควรพิจารณาให้ศูนย์คอมพิวเตอร์สำรองอยู่ห่างจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะมิให้เกิดปัญหาหรือได้รับผลกระทบในลักษณะเดียวกันในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง และภัยธรรมชาติ

๔.๒.๑๐ การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

ในกรณีที่องค์การจัดการน้ำเสียมีการจัดจ้างผู้ให้บริการภายนอก องค์การจัดการน้ำเสียต้องมีการจัดทำสัญญาหรือข้อตกลง การให้บริการโดยระบุหน้าที่ ความรับผิดชอบ และเงื่อนไขในการให้บริการอย่างชัดเจน

๔.๓ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

เพื่อให้องค์การจัดการน้ำเสียสามารถบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ได้อย่างมีประสิทธิภาพ องค์การจัดการน้ำเสียต้องกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีด้านเทคโนโลยีสารสนเทศ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติแลกระบวนการในการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

/๔.๓.๑ การประเมิน ...

๔.๓.๑ การประเมินความเสี่ยง (Risk Assessment)

(๑) การระบุความเสี่ยง (Risk Identification)

องค์การจัดการน้ำเสียต้องระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงภัยคุกคามทางไซเบอร์ และช่องโหว่ต่างๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงานระบบงานบุคลากร หรือปัจจัยภายนอก

(๒) การวิเคราะห์ความเสี่ยง (Risk Analysis)

องค์การจัดการน้ำเสียต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(๓) การประเมินค่าความเสี่ยง (Risk Evaluation)

องค์การจัดการน้ำเสียต้องประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินงาน รวมถึงกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT Risk Appetite)

๔.๓.๒ การจัดการความเสี่ยง (Risk Treatment)

องค์การจัดการน้ำเสียต้องมีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

๔.๓.๓ การติดตามและทบทวน (Risk Monitoring and Review)

องค์การจัดการน้ำเสียต้องจัดให้มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้

๔.๓.๔ การรายงานความเสี่ยง (Risk Reporting)

องค์การจัดการน้ำเสียต้องมีการรายงานผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและแนวโน้มของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นต่อผู้บริหารที่ได้รับมอบหมายในระยะเวลาที่เหมาะสม

/ทั้งนี้ ...

ทั้งนี้ องค์การจัดการน้ำเสียต้องจัดให้มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๔.๔ การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Compliance)

องค์การจัดการน้ำเสียต้องจัดให้มีการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Compliance) เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

๔.๕ การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit)

๔.๕.๑ องค์การจัดการน้ำเสียต้องจัดให้มีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ ที่มีความรู้ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก หรือผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๔.๕.๒ องค์การจัดการน้ำเสียต้องจัดให้มีแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำคัญและความเสี่ยงของการใช้เทคโนโลยีสารสนเทศขององค์การจัดการน้ำเสียและนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยแผนงานและขอบเขตการตรวจสอบดังกล่าวต้องได้รับความเห็นชอบจากผู้บริหารที่ได้รับมอบหมายและต้องครอบคลุมถึงเทคโนโลยีสารสนเทศที่สำคัญขององค์การจัดการน้ำเสีย ทั้งนี้ องค์การจัดการน้ำเสียต้องจัดให้มีการทบทวนแผนงานและขอบเขตการตรวจสอบดังกล่าวอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

/๔.๕.๓ องค์การ ...

๔.๕.๓ องค์การจัดการน้ำเสียต้องต้องจัดให้มีผู้เชี่ยวชาญภายนอกที่เป็นอิสระทำหน้าที่ประเมินระบบหรือเทคโนโลยีที่มีความสำคัญ

๔.๕.๔ องค์การจัดการน้ำเสียต้องจัดทำรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและเสนอต่อผู้บริหารที่ได้รับมอบหมาย

๔.๕.๕ องค์การจัดการน้ำเสียต้องจัดให้มีการติดตามประเด็นจากการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรายงานประเด็นสำคัญให้กับผู้บริหารที่ได้รับมอบหมายและฝ่ายงานที่เกี่ยวข้องทราบ

๔.๖ การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management)

๔.๖.๑ องค์การจัดการน้ำเสียต้องจัดให้มีการศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับของโครงการที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานก่อนเริ่มโครงการ โดยต้องมีการพิจารณาเลือกใช้เทคโนโลยีอย่างเหมาะสม และมีการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับสายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งต้องมีการจัดลำดับความสำคัญของโครงการและนำเสนอขออนุมัติโครงการต่อคณะทำงานดิจิทัล องค์การจัดการน้ำเสีย หรือผู้บริหารระดับสูงตามขอบเขตอำนาจในการอนุมัติที่กำหนดไว้

๔.๖.๒ องค์การจัดการน้ำเสียต้องมีการกำหนดกรอบการบริหารจัดการโครงการ (project management framework) ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางในการบริหารจัดการโครงการ (project management) โดยครอบคลุมขั้นตอนตั้งแต่การเริ่มโครงการ การดำเนินการและการควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ รวมทั้งต้องมีการกำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการที่ชัดเจน (project governance) โดยหน่วยงานต้องจัดให้มีอย่างน้อยในเรื่องต่อไปนี้

(๑) คณะกรรมการโครงการ เพื่อทำหน้าที่ในการกำกับดูแลความคืบหน้าให้คำแนะนำและพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้การดำเนินงานของโครงการเป็นไปตามแผนงานที่กำหนด ทั้งนี้ คณะกรรมการกำกับดูแลโครงการควรประกอบด้วยผู้บริหารหรือผู้แทน

/จากสาย ...

จากสายงานต่าง ๆ ที่เกี่ยวข้อง

(๒) หัวหน้าโครงการ (project manager) เพื่อทำหน้าที่ในการบริหารจัดการโครงการแต่ละโครงการตามขั้นตอนการบริหารจัดการโครงการและส่งมอบงานในแต่ละขั้นตอนตามรูปแบบ กระบวนการ และเครื่องมือ ตามที่หน่วยงานหรือทีมงานดูแลภาพรวมของโครงการกำหนด เพื่อให้สามารถส่งมอบโครงการได้อย่างถูกต้องครบถ้วนตามแผนงานที่กำหนด

ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันที่ ๗๐ กันยายน ๒๕๖๓ เป็นต้นไป

ประกาศ ณ วันที่ ๗๐ กันยายน ๒๕๖๓

(นายชีระ วงศบูรณะ)

ผู้อำนวยการองค์การจัดการน้ำเสีย

ฝ่ายพัฒนาองค์กร
กองสารสนเทศและประเมินผล

/สำเนาเรียน...