ประกาศการกีฬาแห่งประเทศไทย

เรื่อง นโยบายและแนวปฏิบัติในการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย (Information Security Management)

.....

เพื่อให้ระบบสารสนเทศของการกีฬาแห่งประเทศไทย มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างมีประสิทธิภาพ และมิให้มีผู้กระทำด้วยประการใด ๆ ให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่ง หรือผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อการเผยแพร่ข้อมูลอันเป็นเท็จ ซึ่งอาจก่อให้เกิดความเสียหายแก่การกีฬาแห่งประเทศไทย และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการถูกคุกคามจากภัยต่าง ๆ

การกีฬาแห่งประเทศไทย จึงได้จัดทำนโยบายและแนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขึ้น เพื่อเผยแพร่ให้บุคลากรทุกระดับปฏิบัติตามอย่างเคร่งครัด และกำหนดให้มีการทบทวนอย่างสม่ำเสมอ ปีละ ๑ ครั้ง

อาศัยอำนาจตามความในมาตรา ๒๓ แห่งพระราชบัญญัติการกีฬาแห่งประเทศไทย พ.ศ. ๒๕๕๘ และที่แก้ไขเพิ่มเติม การกีฬาแห่งประเทศไทย จึงออกประกาศการกีฬาแห่งประเทศไทย เรื่อง นโยบายและแนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย (Information Security Management) ดังต่อไปนี้

๑. นโยบายและแนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย (Information Security Management) มีวัตถุประสงค์ ดังนี้

๑.๑ เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของการกีฬาแห่งประเทศไทย ให้ดำเนินงานได้อย่างมีประสิทธิภาพ และประสิทธิผล

๑.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๑.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับการกีฬาแห่งประเทศไทย ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการใช้งานด้านสารสนเทศ

๒. นโยบาย ...

๒. นโยบายและแนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย สามารถแบ่งออกได้ ดังนี้

๒.๑ การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

๒.๒ การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information security)

๒.๓ การควบคุมการเข้าถึง (Access control)

๒.๔ รักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

๒.๕ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications security)

๒.๖ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

๒.๗ การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System acquisition and development)

๒.๘ การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem management)

๒.๙ การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๒.๑๐ การบริหารจัดการผู้ให้บริการภายนอก (Third party management)

๓. การกำหนดผู้รับผิดชอบ

๓.๑ ระดับนโยบาย

ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) เป็น ผู้กำหนดแผนการดำเนินงาน แนวนโยบายและแนวปฏิบัติ รวมถึงกำกับดูแล ให้เป็นไปตามนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) เป็นผู้รับผิดชอบในการสั่งการ ตามแนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย

ผู้อำนวยการฝ่ายสารสนเทศและวิชาการกีฬา เป็นผู้รับผิดชอบติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ ให้คำปรึกษา แก่เจ้าหน้าที่ระดับปฏิบัติ

๓.๒ ระดับปฏิบัติ

เพื่อให้การปฏิบัติตามแนวนโยบาย และแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย การกีฬาแห่งประเทศไทยเป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้ฝ่ายสารสนเทศและวิชาการกีฬา เป็นผู้ดูแลระบบ ผู้รับผิดชอบระบบสารสนเทศและผู้ที่ได้รับมอบหมายเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุง นโยบายและแนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง และหากมีการเปลี่ยนแปลงนโยบายและแนวปฏิบัติให้ประกาศให้เจ้าหน้าที่ทุกระดับในหน่วยงานการกีฬาแห่งประเทศไทยรับทราบทุกครั้ง

๔. ฝ่ายสารสนเทศและวิชาการกีฬา มีหน้าที่ออกระเบียบปฏิบัติในการจำกัด ระงับ หรือเพิกถอนสิทธิการใช้เครือข่ายของผู้ฝ่าฝืนระเบียบ ตลอดจนระงับหรือจำกัดการเข้าถึงคอมพิวเตอร์ที่มีข้อมูลขัดต่อระเบียบ

นโยบาย ...

นโยบายพระราชบัญญัติการกีฬาแห่งประเทศไทย พ.ศ.๒๕๕๘ และที่แก้ไขเพิ่มเติม หรือกฎหมายที่เกี่ยวข้อง ทั้งนี้ให้ฝ่ายสารสนเทศและวิชาการกีฬา รายงานการฝ่าฝืนระเบียบให้หน่วยงานต้นสังกัดหรือการกีฬาแห่งประเทศไทย เพื่อพิจารณาลงโทษ

๕. นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของการกีฬาแห่งประเทศไทย เพื่อใช้เป็นแนวทางในการดำเนินงานในระบบสารสนเทศให้มีความปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้อง จึงให้ใช้แนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทยตามเอกสารแนบท้ายประกาศนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๓ สิงหาคม พ.ศ. ๒๕๖๓

(นายก้องศักด ยอดมณี)
ผู้ว่าการการกีฬาแห่งประเทศไทย

เอกสารแนบท้ายประกาศ
แนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรของการกีฬาแห่งประเทศไทย
พ.ศ. ๒๕๖๓

ความหมายและคำจำกัดความ

๑. **“กกท.”** หมายความว่า การกีฬาแห่งประเทศไทย

๒. **หน่วยงาน** หมายความว่า ฝ่าย/สำนัก/สายงาน/ศูนย์ ที่เป็นส่วนราชการตามโครงสร้างของการกีฬาแห่งประเทศไทย

๓. **หน่วยงานภายนอก** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของการกีฬาแห่งประเทศไทย โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

๔. **ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO)** หมายความว่า ผู้ว่าการการกีฬาแห่งประเทศไทย

๕. **ผู้บริหารด้านเทคโนโลยีสารสนเทศระดับสูง (Chief Information officer : CIO)** หมายความว่า รองผู้ว่าการ ที่มีหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

๖. **ผู้บริหาร** หมายความว่า ผู้อำนวยการฝ่ายสารสนเทศและวิชาการกีฬา ผู้อำนวยการกองสารสนเทศ หัวหน้างานบริการเทคโนโลยีสารสนเทศ หัวหน้างานปฏิบัติการคอมพิวเตอร์ ที่ได้รับมอบหมายให้ดูแลด้านไอที

๗. **ผู้บังคับบัญชา** หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

๘. **ผู้ดูแลระบบ (System administrator)** หมายความว่า ผู้ซึ่งได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่ดูแลเซิร์ฟเวอร์ ระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ ให้บริการได้อย่างมีเสถียรภาพ

๙. **ผู้พัฒนาระบบ** หมายความว่า ผู้ซึ่งได้รับมอบหมายให้รับผิดชอบในการพัฒนาระบบสารสนเทศ

๑๐. **เจ้าหน้าที่** หมายความว่า บุคลากรทุกประเภทของการกีฬาแห่งประเทศไทย

๑๑. **ผู้ใช้งาน (user)** หมายความว่า บุคลากรของการกีฬาแห่งประเทศไทย บุคคลหรือหน่วยงานภายนอกที่มีบัญชีรายชื่อที่ออกโดย ฝ่ายสารสนเทศและวิชาการกีฬา และ/หรือที่ได้รับอนุญาตให้ใช้สินทรัพย์สารสนเทศของการกีฬาแห่งประเทศไทย

๑๒. **การรักษาความมั่นคงปลอดภัย** หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ และการสื่อสาร

๑๓. **มาตรฐาน (Standard)** หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

๑๔. **แนวปฏิบัติ (Guideline)** หมายความว่า แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

๑๕. **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของการกีฬาแห่งประเทศไทย

๑๖. **เจ้าของข้อมูล** หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๑๗. **สินทรัพย์** หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เซิร์ฟเวอร์ ระบบสารสนเทศ ระบบเครือข่ายอุปกรณ์เครือข่าย เลขที่อยู่ไอพี โดเมนเนม รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ หรือสิ่งใดก็ตามที่มีคุณค่าต่อหน่วยงาน

๑๘. **ห้องควบคุมระบบ** หมายความว่า ห้องที่ติดตั้งและจัดวางระบบเซิร์ฟเวอร์ อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่ายของการกีฬาแห่งประเทศไทย ภายใต้การดูแลของฝ่ายสารสนเทศและวิชาการกีฬา และ/หรือ หน่วยงานที่ให้บริการสารสนเทศ

๑๙. **ระบบอินเทอร์เน็ต (Internet)** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของการกีฬาแห่งประเทศไทยเข้ากับเครือข่ายอินเทอร์เน็ต

๒๐. **ระบบสารสนเทศ** หมายความว่า ระบบงานของการกีฬาแห่งประเทศไทย ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศในองค์กร สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุม การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ ฯลฯ

๒๑. **ระบบเครือข่ายคอมพิวเตอร์ (Computer Network System)** หมายความว่า ระบบที่เชื่อมต่อคอมพิวเตอร์ เซิร์ฟเวอร์ อุปกรณ์เครือข่ายต่าง ๆ ของการกีฬาแห่งประเทศไทย

๒๒. **จดหมายอิเล็กทรอนิกส์ (e-mail)** หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่ายภาพกราฟิกภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับผ่านโพรโทคอล ต่างๆ เช่น SMTP, POP๓, IMAP ฯลฯ

๒๓. **การควบคุมการเข้าถึง (Access control)** หมายความว่า ควบคุมการเข้าออกแบบอัตโนมัติ ถูกออกแบบขึ้นเพื่อใช้กำหนดสิทธิ์ในการเข้าออก ให้กับบุคลากรภายในที่เกี่ยวข้อง และป้องกันเหตุร้ายที่อาจเกิดจากบุคคลภายนอก

๒๔. **ชื่อผู้ใช้ (username)** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่กำหนดสิทธิการใช้งานไว้

๒๕. **รหัสผ่าน (password)** หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

๒๖. **การเข้ารหัส (encryption)** หมายความว่า การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๒๗. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน และหน่วยงานภายนอก เข้าถึงหรือใช้งานระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบเครือข่าย ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

๒๘. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายความว่า การรักษาไว้ซึ่งความลับ (confidentiality) ความครบถ้วนถูกต้อง (integrity) และความพร้อมใช้ (availability) ของสารสนเทศ และระบบเครือข่ายรวมทั้ง คุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธ ความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๒๙. **การพิสูจน์ยืนยันตัวตน (authentication)** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ยืนยันตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน

๓๐. **MAC Address (media access control address)** หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ติดต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกันตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๓๑. **WPA (Wi-Fi protected access)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

๓๒. **VPN (virtual private network)** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ - ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๓๓. **Source code** หมายความว่า ข้อความที่เป็นชุดที่ถูกเขียนขึ้น และสามารถอ่านและเข้าใจได้ ใช้สำหรับภาษาโปรแกรม ในการเขียนโปรแกรมแบบใหม่ รหัสต้นฉบับนิยมเก็บไว้ในไฟล์หลายไฟล์แยกจากกันเพื่อให้ง่ายในการเรียกใช้ส่วนย่อยของคำสั่งนั้น

๓๔. **ระบบปฏิบัติการ (operating system)** หมายความว่า ระบบซอฟต์แวร์ที่ทำหน้าที่จัดการอุปกรณ์คอมพิวเตอร์และแหล่งซอฟต์แวร์และบริการโปรแกรมคอมพิวเตอร์

สารบัญ

ส่วนที่ ๑

การบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ (Information Security Management) ขององค์กร

๑. จุดประสงค์ของการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ

จุดประสงค์ของการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ คือความลับ (confidentiality) ความสมบูรณ์ (integrity) ความพร้อมใช้ (availability) ของข้อมูลต่างๆภายในองค์กรโดยมีรายละเอียดดังนี้

๑.๑.การรักษาความลับ (confidentiality) คือการรักษาความลับ มีการเก็บข้อมูลไว้เป็นความลับให้เฉพาะผู้มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้

๑.๒.การรักษาความสมบูรณ์ (integrity) คือความครบถ้วน ความถูกต้องสมบูรณ์ ไม่มีการแก้ไขเปลี่ยนแปลงหรือทำลายจากผู้ไม่มีสิทธิไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา

๑.๓.ความพร้อมใช้ (availability) คือความพร้อมใช้งานของข้อมูลและบริการการสื่อสารต่างๆ สามารถตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ

๒. มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ

การนำมาตรฐานการรักษาความมั่นคงปลอดภัยมาประยุกต์ใช้กับระบบสารสนเทศในองค์กรเริ่มเป็นที่แพร่หลายมากขึ้นมาตรฐาน ISO/IEC ๒๗๐๐๑ เป็นมาตรฐานหนึ่งที่กำลังได้รับความนิยมอย่างแพร่หลายในปัจจุบันได้รับการยอมรับจากหลายประเทศในการนำไปใช้บริหารจัดการระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศมาตรฐาน ISO/IEC ๒๗๐๐๑ เป็นมาตรฐานที่พัฒนามาจากมาตรฐานในตระกูล ISO/IEC ๒๗๐๐๐ ซึ่งเกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security Management System: ISMS)

๓. โครงสร้างความมั่นคงปลอดภัยสารสนเทศภายในองค์กร (Internal organization)

วัตถุประสงค์ เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศภายในองค์กรนโยบาย

๓.๑ การกำหนดบทบาทและหน้าที่ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

๑) ผู้บริหารระดับสูงสุดต้องแต่งตั้งกลุ่มหรือคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ และมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

๓.๒ การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

๑) ผู้บริหารด้านไอทีต้องกำหนดตำแหน่งด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดความรับผิดชอบให้เหมาะสม พร้อมทั้งควบคุมการปฏิบัติงานเพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย

๒) ผู้บริหารด้านไอทีเป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ การกีฬาแห่งประเทศไทย

๓) ผู้บริหารต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย

๔) ผู้ใช้งาน และหน่วยงานภายนอกต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของ การกีฬาแห่งประเทศไทย ในการรักษาความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย

๔. นโยบายและแล้วปฏิบัติในการจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร

วัตถุประสงค์ เพื่อกำหนดทิศทางและสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ โดยให้สอดคล้องตามภารกิจขององค์กร และไม่ขัดต่อกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องนโยบาย

๔.๑ เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศที่เป็นลายลักษณ์อักษร (Information Security Policy Document)

๑) คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ ต้องจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นลายลักษณ์อักษรเพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายสื่อสารข้อมูล โดยนโยบายฯ ดังกล่าวจะต้องได้รับการอนุมัติจากผู้ว่าการการกีฬาแห่งประเทศไทยเพื่อการนำไปใช้

๒) คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ ต้องจัดให้เผยแพร่ เอกสารนโยบายระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ ให้กับผู้ใช้งาน หน่วยงานภายนอก และผู้ที่เกี่ยวข้องในขอบเขตรับทราบ

๔.๒ การทบทวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๑) คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการตรวจสอบ ทบทวนและประเมินนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย ๑ ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

ส่วนที่ ๒

๑. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

วัตถุประสงค์

เพื่อให้ระบุสินทรัพย์ขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันสินทรัพย์อย่างเหมาะสม

นโยบายและแนวปฏิบัติ

๑.) บัญชีสินทรัพย์ (Inventory of assets)

๑.๑) ต้องจัดทำและเก็บทะเบียนสินทรัพย์สารสนเทศ เพื่อเป็นข้อมูลสำหรับการนำไปวิเคราะห์และประเมินความเสี่ยง และบริหารจัดการความเสี่ยงได้อย่างเหมาะสม

๑.๒) ต้องตรวจสอบสินทรัพย์ตามระยะเวลาที่กำหนด เช่น ปีละ ๑ ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ

๒.) ผู้ถือครองสินทรัพย์ (Ownership of assets)

๓.) สินทรัพย์ในทะเบียนสินทรัพย์ต้องกำหนดผู้รับผิดชอบให้ชัดเจน

๔.) การใช้สินทรัพย์อย่างเหมาะสม (Acceptable use of assets)

๔.๑) การอนุญาตให้ใช้สินทรัพย์สารสนเทศให้เป็นไปตามข้อกำหนด ดังนี้

- ข้อกำหนดการใช้งานเครือข่าย
- ข้อกำหนดการใช้ไอพีแอดเดรสและชื่อโดเมนของระบบเครือข่ายคอมพิวเตอร์
- ข้อกำหนดการใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail)

๕.) การคืนสินทรัพย์ (Return of assets)

๕.๑) พนักงานที่สิ้นสุดการจ้างงาน หรือสิ้นสุดโครงการต้องคืนสินทรัพย์สารสนเทศที่รับผิดชอบทั้งหมดรวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้าออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือและอุปกรณ์ต่าง ๆ

๒. การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information security)

วัตถุประสงค์

เพื่อป้องกันข้อมูลสารสนเทศที่เกิดขึ้นจากการใช้ระบบ ควบคุมและป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต รวมถึงองค์ประกอบอื่นๆ ที่เกี่ยวข้องเช่น ระบบและฮาร์ดแวร์ที่ใช้ในการจัดเก็บและถ่ายโอนข้อมูลสารสนเทศนั้นให้รอดพ้นจากภัยคุกคามต่างๆ

นโยบายและแนวปฏิบัติ

๑. การจัดการข้อมูลสารสนเทศและการรักษาความลับ

(๑) การจำแนกประเภทของข้อมูลสารสนเทศ (information classification) เพื่อกำหนดมาตรการ รักษาความมั่นคงปลอดภัย

(๒) การสำรองข้อมูล (backup)

(๓) การควบคุมการเข้ารหัสข้อมูล (cryptographic controls)

(๔) การป้องกันข้อมูลส่วนบุคคล (privacy and protection of personally identifiable information)

(๕) มีวิธีการจัดการการเข้าถึงข้อมูล ตามระดับชั้นความลับโดยกำหนดให้มีแนวทางปฏิบัติ ดังนี้

(๑) ผู้ใช้งานต้องจัดการกับข้อมูลตามชั้นความลับของข้อมูลกรมทรัพยากรธรณีได้กำหนดชั้น ความลับของข้อมูลเป็น ๓ ระดับ ดังนี้

- ลับที่สุด (Top secret) หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งภาครัฐร้ายแรงที่สุด

- ลับมาก (Secret) หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

- ลับ (Confidential) หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๒) ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติ ดังนี้

- ระมัดระวังการกระจาย หรือแจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับของกรมทรัพยากรธรณีไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

- ผู้ที่เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ต้องตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน

- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการใช้ รหัสผ่านที่มีความมั่นคงปลอดภัย เมื่อมีการนำไฟล์ข้อมูลลับไปใช้งานต้องมีการเข้ารหัส

- ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายของกกท. เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่า บุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตามเนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

- ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

- ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

- ต้องทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

(๓) ประเภทข้อมูล

- ข้อมูลสารสนเทศเพื่อการบริหาร หมายถึง นโยบาย ข้อมูลยุทธศาสตร์, คำรับรอง การปฏิบัติราชการ, ข้อมูลบุคลากร, งบประมาณ, การเงินและบัญชี

- ข้อมูลด้านการดำเนินงาน หมายถึง การดำเนินงานตามภารกิจกกท., กฎหมายระเบียบ, การใช้จ่ายงบประมาณ, ผลการปฏิบัติงาน

- ข้อมูลสารสนเทศเพื่อการบริการ หมายถึง ข้อมูลวิชาการและองค์ความรู้

(๔) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด

- ข้อมูลที่มีระดับความสำคัญปานกลาง

- ข้อมูลที่มีระดับความสำคัญน้อย

(๕) จัดแบ่งระดับชั้นการเข้าถึง

- เข้าถึงได้ทุกกลุ่มผู้ใช้งานที่กำหนดไว้ หมายถึง ข้อมูลพื้นฐานที่ผู้ใช้งานได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงาน ในการใช้งานระบบ

- เข้าถึงได้เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิ หมายถึง ข้อมูลที่ผู้ใช้งานได้รับอนุญาตจาก เจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตาม ความจำเป็นต่อการใช้งานระบบสารสนเทศ

- เข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ หมายถึง ผู้ดูแลระบบสารสนเทศ

๒. การควบคุมรักษาความปลอดภัยโดยตัวซอฟต์แวร์ (Software Control)

(๑) การควบคุมจากระบบภายในของซอฟต์แวร์ (Internal Program Control) คือการที่โปรแกรมนั้นได้มีการควบคุมสิทธิการเข้าถึง และสิทธิในการใช้ข้อมูลภายในระบบ ซึ่งถูกจัดเก็บไว้ในระบบฐานข้อมูลภายในระบบเอง

(๒) การควบคุมความปลอดภัยโดยระบบปฏิบัติการ (Operating System Control) คือการควบคุมสิทธิการเข้าถึงและการใช้ข้อมูลในส่วนต่าง ๆ ภายในระบบคอมพิวเตอร์ของผู้ใช้คนหนึ่ง และจำแนกแตกต่างจากผู้ใช้คนอื่น ๆ

๓. การควบคุมความปลอดภัยของระบบโดยฮาร์ดแวร์ (Hardware Control)

โดยเลือกใช้เทคโนโลยีทางด้านฮาร์ดแวร์ ที่สามารถควบคุมการเข้าถึง และป้องกันการทำงานผิดพลาดด้วยอุปกรณ์ภายในตัวเอง

๔. การใช้นโยบายในการควบคุม (Policies)

โดยมีการประกาศใช้นโยบายและการปรับปรุงนโยบายให้มีการทำงานสอดคล้องกับการดำเนินธุรกิจ และสภาพแวดล้อมที่เปลี่ยนแปลง โดยมีผลบังคับใช้ทั้งองค์กร

๕. การป้องกันทางกายภาพ (Physical Control)

การมีมาตรการการเข้าถึงศูนย์คอมพิวเตอร์ และเครื่องคอมพิวเตอร์ที่สำคัญได้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น รวมทั้งมีระบบสำรองข้อมูลอย่างสม่ำเสมอ

๓. การควบคุมการเข้าถึง (Access control)

วัตถุประสงค์

เพื่อจำกัดการเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต

นโยบายและแนวปฏิบัติ

๑. นโยบายควบคุมการเข้าถึง (Access control policy)

๑) กำหนดนโยบายควบคุมการเข้าถึงเป็นการกำหนดมาตรฐานแนวทางปฏิบัติที่มีความสอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับผู้ใช้งาน เจ้าหน้าที่ รวมถึงบุคคลภายนอกเพื่อควบคุมให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต โดยมีมาตรการควบคุมการเข้าถึง ตามแนวปฏิบัติดังต่อไปนี้

๑) แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

๒) แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย

๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๔) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๕) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๒.) การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)

๑) กำหนดการป้องกันทางเครือข่ายให้มีความมั่นคงปลอดภัย ตามแนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่ายและแนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

๑. การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration)

๑) การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการเพื่อให้สามารถใช้งานระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ ในกรณีที่ผู้ใช้งานสิ้นสุดสถานภาพต้องยกเลิกออกจากระบบทันทีตาม แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

๒. การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access Provisioning)

๑) ผู้ดูแลระบบต้องมีกระบวนการกำหนดสิทธิให้ครอบคลุมผู้ใช้งานให้ครบทุกประเภทและทุกบริการ

๓. การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

๑) ผู้ดูแลระบบต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่รับผิดชอบด้วย โดยให้เป็นไปตามแนวปฏิบัติการจัดการ การเข้าถึงของผู้ใช้งาน

๔. การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of privileged access right)

๑) การส่งมอบข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ ดังนั้นต้องมีกระบวนการป้องกันและการปกปิด โดยให้เป็นไปตามแนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

๕. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

๑) ผู้ดูแลระบบต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

๖. การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)

๑) เมื่อเจ้าหน้าที่ลาออก เปลี่ยนแปลงข้อตกลงหรือหรือสัญญา ผู้ดูแลระบบต้องทำการถอดถอนหรือปรับปรุงสิทธิให้ถูกต้อง

๓. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

๑. การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of secret authentication information)

๑) ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศองค์กร การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน และการจัดการควบคุมการใช้รหัสผ่านตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย หัวข้อ การใช้งานรหัสผ่าน

๒) รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคง ปลอดภัย

๓) ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งานและรหัสผ่านของตนทั้งหมด

๔) รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้

๔. การควบคุมการเข้าถึงระบบ (System and application access control)

๑. การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

๑) ต้องควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิในการใช้งาน ได้แก่ เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้งาน ที่สามารถใช้งานได้ ตรวจสอบว่า สารสนเทศที่อนุญาตให้ใช้งานนั้นมี เฉพาะข้อมูลที่จำเป็นต้องใช้งาน โดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๒) บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น และกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

๓) บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของ การกีฬาแห่งประเทศไทย อย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบสารสนเทศของ การกีฬาแห่งประเทศไทย ตามแนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

๒. ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

๑) การเข้าถึงระบบปฏิบัติการจะต้องผ่านการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย ตาม แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๓. การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

๑) ต้องกำหนดให้ควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้

๔. การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)

๑) อนุญาตเฉพาะผู้รับผิดชอบสามารถเข้าถึงซอร์สโค้ดของโปรแกรม

๕. แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ ให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต และรวมความถึงการกำหนดหน้าที่ของผู้ใช้งาน การเข้าถึงเครือข่าย การใช้งานระบบสารสนเทศ การเฝ้าดูการใช้งานระบบสารสนเทศ และอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศของการกีฬาแห่งประเทศไทย เป็นต้น

๑. ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้

๑.๑. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

- สิทธิอ่านอย่างเดียว
- สิทธิการเพิ่มข้อมูล
- สิทธิการแก้ไขข้อมูล
- สิทธิการลบข้อมูล
- สิทธิการอนุมัติ/อนุญาต
- ไม่มีสิทธิ

๑.๒. กำหนดการระงับสิทธิ มอบอำนาจ ให้เป็นไปตามแนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน ที่ได้กำหนดไว้

๑.๓. ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๔. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการ และกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๑. จัดแบ่งประเภทข้อมูลออกเป็น

๑) ข้อมูลทั่วไปที่เปิดเผยได้

๒) ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ ได้แก่

๑) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำร้อง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

๒) ข้อมูลสารสนเทศตามพันธกิจ ได้แก่ ข้อมูลด้านการเรียนการสอน ข้อมูลด้านการวิจัย และข้อมูลด้านบริการวิชาการ เป็นต้น

๒. จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๔ ระดับ

๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด ได้แก่ ข้อมูลผลการเรียนนิสิต ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลด้านการวิจัย

๒) ข้อมูลที่มีระดับความสำคัญมาก ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลส่วนบุคคล ข้อมูลบุคลากร

๓) ข้อมูลที่มีระดับความสำคัญปานกลาง

๔) ข้อมูลที่มีระดับความสำคัญน้อย

หากข้อมูลที่นอกเหนือจากที่กำหนด การจัดระดับความสำคัญของข้อมูล ให้พิจารณาในระดับฐานข้อมูลด้วยการประเมินมูลค่าความเสียหายต่อหน่วยงานหากข้อมูลมีปัญหา ไม่สมบูรณ์ แนวปฏิบัติในการพิจารณาจัดลำดับความสำคัญของข้อมูลมีดังนี้

ระดับความสำคัญของข้อมูล	การประเมินมูลค่าความเสียหายหากข้อมูลมีปัญหา หรือไม่สมบูรณ์
ความสำคัญมากที่สุด	มีผลกระทบรุนแรงต่อการดำรงอยู่ของหน่วยงาน หรือปิดหน่วยงาน
ความสำคัญมาก	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
ความสำคัญปานกลาง	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
ความสำคัญน้อย	มีผลกระทบใดๆ ต่อการดำเนินภารกิจ

๓. จัดแบ่งลำดับชั้นความลับของข้อมูล

๑) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๒) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๓) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๔) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๔. จัดแบ่งระดับชั้นการเข้าถึง ดังนี้

๑) เข้าถึงได้ทุกกลุ่มผู้ใช้งาน ได้แก่ ข้อมูลทั่วไปที่เปิดเผยได้

๒) เข้าถึงได้เฉพาะกลุ่มผู้ใช้งานที่ได้รับสิทธิ ได้แก่ ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ ข้อมูลลับ

๓) เข้าถึงได้เฉพาะผู้มีสิทธิในการบริหารจัดการระบบสารสนเทศ ได้แก่ ข้อมูลระบบ

๕. กำหนดช่องทางในการเข้าถึงข้อมูล

๑) ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายภายใน ได้ตลอด ๒๔ ชั่วโมง

๒) ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายอินเตอร์เน็ตที่อยู่ภายนอก ผ่านระบบ VPN ได้ตลอด ๒๔ ชั่วโมง

๖. กำหนดเวลาและจำนวนระยะเวลาในการเข้าถึงข้อมูล

๑) ระบบงานบริการสำหรับผู้ใช้งานทั่วไปเข้าถึงได้ตลอดเวลา

๒) ระบบงานภายในสำหรับผู้ใช้งานสามารถเข้าถึงระบบตามช่วงเวลา ดังนี้

๑) เวลาราชการ (๘.๓๐ – ๑๖.๓๐ น.)

๒) นอกเวลาราชการ (นอกช่วงเวลา ๘.๓๐ – ๑๖.๓๐ น.)

๓) ช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)

๔) ช่วงเวลาพิเศษเป็นรายครั้ง โดยระบุช่วงเวลา ระยะเวลาการเข้าถึง

๑.๕. มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ โดยแบ่งการจัดทำข้อปฏิบัติเป็นสองส่วน คือ

๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๒) มีการปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๑.๖. ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

๑.๗. ต้องจัดให้มีการบันทึกการผ่านเข้า – ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

๖. แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและระบบเครือข่ายไร้สาย

๑. ผู้ดูแลระบบต้องออกแบบและแบ่งแยกระบบเครือข่าย ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยประกอบด้วย โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เพื่อให้การบริหารจัดการและควบคุมเป็นระบบ และป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ

๒. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกการกีฬาแห่งประเทศไทยผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตน ก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกการกีฬาแห่งประเทศไทยสามารถเข้าใช้งานเครือข่าย และระบบสารสนเทศของการกีฬาแห่งประเทศไทย ได้แก่

๑) การแสดงตัวตน ด้วยชื่อผู้ใช้งาน (Username)

๒) การพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่าน (Password)

๓) การเข้าสู่ระบบสารสนเทศของ การกีฬาแห่งประเทศไทย จะต้องมีการตรวจสอบผู้ใช้งานอีกครั้ง

๔) การเข้าสู่ระบบจากระยะไกล เพื่อเพิ่มความปลอดภัยของการรับส่งข้อมูล ต้องมีการใช้การเข้ารหัสข้อมูล ได้แก่ SSL

๓. การใช้งานเครือข่ายจากแหล่ง หรือสถานที่ที่ได้รับอนุญาต ผู้ดูแลระบบต้องจัดทำกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายของการกีฬาแห่งประเทศไทยและเครือข่ายภายนอกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตเท่านั้น

๔. ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย ผู้ดูแลระบบต้องจัดทำข้อกำหนดหรือข้อตกลงสำหรับคุณสมบัติด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่างการกีฬาแห่งประเทศไทยกับหน่วยงานภายนอก

๕. การควบคุมผู้ใช้งานในการใช้งานเครือข่าย ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น ได้แก่

๑) ใช้ Monitoring Tool เพื่อตรวจสอบการเชื่อมต่อทางระบบเครือข่าย

๒) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องแม่ข่าย

๓) ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต

๖. การจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน ผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network routing Control) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาติเท่านั้น

๗. ผู้ดูแลระบบต้องกำหนด IP Address ให้กับอุปกรณ์ที่เชื่อมต่อเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้ IP Address ระบุถึงอุปกรณ์ได้ กำหนดให้ผู้ใช้งานต้องลงทะเบียน MAC Address อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้อง

๘. ผู้ดูแลระบบจะต้องทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและผ่านทางเครือข่าย ได้แก่

๑) ต้องตรวจสอบ และปิดพอร์ตที่ไม่มีการใช้งานอยู่เสมอ

๒) ต้องควบคุมการเข้าถึงระบบผ่านอุปกรณ์ป้องกันการบุกรุก (firewall) ของระบบเครือข่าย

๓) การขอใช้งานพอร์ตดังกล่าวต้องได้รับอนุญาตจากผู้อำนวยการฝ่ายสารสนเทศและวิชาการกีฬา หรือผ่านช่องทางที่ฝ่ายสารสนเทศและวิชาการกีฬาจัดเตรียมไว้ให้

๔) ต้องเก็บอุปกรณ์ที่เชื่อมต่อเครือข่ายไว้ในห้องที่มีการควบคุมการเข้าถึง และจะเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หรือล็อกกุญแจเพื่อป้องกันการเชื่อมต่อโดยไม่ได้รับอนุญาต

๙. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๑๐. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานโดยใช้รหัสบัญชีผู้ใช้ที่ออกโดยฝ่ายสารสนเทศและวิชาการกีฬา

๑๑. ผู้ดูแลระบบต้องดำเนินการดังต่อไปนี้

๑) ต้องลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๓) เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน

๔) เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๕) ต้องกำหนดค่าใช้ WPA (Wi-Fi protected access) หรือดีกว่าในการเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจายสัญญาณ (access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

๖) เลือกใช้วิธีการควบคุม ชื่อผู้ใช้และรหัสผ่านของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สายโดยจะอนุญาตเฉพาะชื่อผู้ใช้และรหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๗) ติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

๘) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายและเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการฝ่ายสารสนเทศและวิชาการกีฬา ทราบโดยทันที

๗. แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้ และควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ ให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต

๑. กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) ครอบคลุมในเรื่องต่อไปนี้

๑.๑. จัดทำแบบฟอร์มลงทะเบียนผู้ใช้งานระบบสารสนเทศเพื่อตรวจสอบสิทธิ และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๑.๒. ต้องจัดทำเอกสารแสดงถึงสิทธิ และความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนามรับทราบด้วย

๑.๓. ต้องบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๑.๔. กำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ ได้แก่

๑) บุคลากรของการกีฬาแห่งประเทศไทย หรือบุคคลภายนอกที่มีบัญชีรายชื่อที่ออกโดยฝ่ายสารสนเทศและวิชาการกีฬา และ/หรือบุคคลภายนอกที่ได้รับอนุญาตให้ใช้สินทรัพย์สารสนเทศของการกีฬาแห่งประเทศไทย

๒) ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าของข้อมูล และได้รับมอบหมายจากผู้บังคับบัญชา

๓) ได้รับการอนุมัติจากผู้อำนวยการฝ่ายสารสนเทศและวิชาการกีฬา หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๕. กำหนดหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ ได้แก่

๑) การตัดออกจากทะเบียน การโยกย้ายหน่วยงาน การระงับการปฏิบัติงาน หรือเมื่อสิ้นสุดสถานภาพการเป็นผู้ใช้งาน

๒) การใช้งานที่ขัดต่อข้อกำหนดการใช้งานเครือข่าย

๒. การบริหารจัดการสิทธิของผู้ใช้งาน (Privileges Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึง และใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๒.๑. ต้องมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งานที่เหมาะสมต่อสถานภาพหรือหน้าที่ความรับผิดชอบ

๒.๒. ต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

๒.๓. ต้องมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

๒.๔. ต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๓. การบริหารจัดการรหัสผ่าน

๓.๑. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๓.๒. ต้องให้ผู้ใช้งานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับและไม่เปิดเผยให้ผู้อื่นทราบ

๓.๓. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา

๓.๔. ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๓.๕. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๓.๖. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

๔. การทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งาน ผู้ดูแลระบบต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อเปลี่ยนแปลงสถานภาพ

๕. ต้องกำหนดหลักสูตร และฝึกอบรมเกี่ยวกับการสร้างความรู้ความเข้าใจถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ และความตระหนักเรื่องความมั่นคงปลอดภัย และกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๘. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๑. กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยสำหรับระบบที่มีความความสำคัญสูงหรือมีความเสี่ยงสูง การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวสำหรับระบบสารสนเทศ ดังนี้

๑.๑. ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๑.๒. ต้องกำหนดระยะเวลาสำหรับการป้อนรหัสผ่าน

๑.๓. จำกัดเข้าถึงระบบปฏิบัติการเฉพาะอินทราเน็ต

๒. การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบสารสนเทศ ได้แก่

๒.๑. ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อผู้ใช้ (Username) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๒.๒. ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันเกิดจากการใช้ชื่อผู้ใช้ (Username) เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓. การบริหารจัดการรหัสผ่าน ผู้ดูแลระบบต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด ได้แก่

๓.๑. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๓.๒. ต้องให้ผู้ใช้งานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับและไม่เปิดเผยให้ผู้อื่นทราบ

๓.๓. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา

๓.๔. ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๓.๕. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๓.๖. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

๔. กระบวนการในการเข้าสู่ระบบให้บริการอย่างมั่นคงปลอดภัย ผู้ดูแลระบบต้องกำหนดกระบวนการในการเข้าสู่ระบบให้บริการเพื่อใช้งานเครื่องให้บริการที่มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการปฏิเสธการใช้งาน หากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง เป็นต้น

๕. การพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ ผู้ดูแลระบบต้องมีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบเครือข่ายคอมพิวเตอร์

๖. การตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ ผู้ดูแลระบบต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์เมื่อเครื่องคอมพิวเตอร์ นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อคหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ เป็นต้น

๗. การควบคุมการใช้งานโปรแกรมยูทิลิตี้ ผู้ดูแลระบบต้องกำหนดให้ควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

๗.๑. ก่อนใช้งานโปรแกรมยูทิลิตี้ต้องพิสูจน์ตัวตนก่อน

๗.๒. จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

๗.๓. ให้แยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน

๗.๔. ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้

๗.๕. โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ

๘. การติดตั้งระบบเตือนภัยสำหรับระบบที่มีความสำคัญสูง ผู้บริหารต้องจัดให้ติดตั้งระบบเตือนภัยให้กับผู้ใช้ที่ปฏิบัติงานกับระบบที่มีความสำคัญสูง

๙. การใช้งานระบบเทคโนโลยีสารสนเทศต้องกำหนดให้ตัด และหมดเวลาการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานเกิน ๓๐ นาที

๙. แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

การใช้บริการด้านไอซีทีจากหน่วยงานภายนอก บางครั้งหน่วยงานภายนอกอาจเข้าถึงระบบสารสนเทศ แก้ไข เปลี่ยนแปลง และประมวลผลระบบงานโดยไม่ได้รับอนุญาต ดังนั้น จึงต้องกำหนดแนวทางในการปฏิบัติงานของหน่วยงานภายนอกเพื่อความมั่นคง ปลอดภัย ของระบบสารสนเทศของการกีฬาแห่งประเทศไทย โดยนโยบายและแนวปฏิบัตินี้ต้องตรวจสอบ และประเมินตามระยะเวลา ๑ ครั้งต่อปี

๑. หน่วยงานภายนอก ที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศและการสื่อสารของการกีฬาแห่งประเทศไทย จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้บริหารของหน่วยงาน

๒. จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

๑) เหตุผลในการขอใช้งาน

๒) ระยะเวลาในการใช้งาน

๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๔) การตรวจสอบ Mac Address ของอุปกรณ์ที่เชื่อมต่อ

๕) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓. หน่วยงานภายนอกที่ทำงานให้กับการกีฬาแห่งประเทศไทยทุกหน่วยงาน จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของการกีฬาแห่งประเทศไทย โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

๔. ผู้ให้บริการจากหน่วยงานภายนอก ต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งปรับปรุงให้ทันสมัย และหากมีการปรับเปลี่ยนจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

๕. เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๖. การกีฬาแห่งประเทศไทยมีสิทธิในการตรวจสอบตามสัญญาการใช้บริการด้านไอซีทีเพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานอย่างทั่วถึงตามข้อกำหนด

๗. ในการจ้างเหมาพัฒนา บำรุงรักษาระบบผู้ดูแลระบบต้องกำหนดการเข้าถึงระบบสารสนเทศสำหรับผู้ปฏิบัติงานจากภายนอก ได้แก่

๑) ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิในการใช้งานเฉพาะที่จำเป็นขั้นต่ำ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๒) ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งานภายนอก ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศ ได้แก่ การกำหนดชื่อผู้ใช้ และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ

๓) ต้องบันทึกกิจกรรมการใช้งานข้อมูลเก็บเป็น Log File

๔) ในระบบที่มีความสำคัญสูงไม่อนุญาตให้ทดสอบบนระบบจริง (Production) แต่ต้องทดสอบบนระบบทดสอบ (Test) ให้เสร็จสิ้นก่อนจึงจะนำมาติดตั้งบนระบบจริง และก่อนการติดตั้งระบบจริงต้องได้รับอนุญาตจากผู้บริหารก่อน

๔. รักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

๔.๑ พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

นโยบายและแนวปฏิบัติ

๑. ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

๑) ต้องแบ่งพื้นที่อย่างชัดเจน และกำหนดระดับการควบคุมเพื่อป้องกันการเข้าถึงสินทรัพย์สารสนเทศที่มีความสำคัญ

๒) ต้องจัดทำแผนผังแสดงตำแหน่งและพื้นที่แต่ละชนิดและประกาศให้ผู้เกี่ยวข้องทราบ

๓) ต้องดูแลรักษาสภาพแวดล้อมของพื้นที่ให้เป็นไปตาม แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ

๒. การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

๑) ต้องควบคุมให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่ได้รับอนุญาตสามารถเข้าออกในพื้นที่

๒) ต้องกำหนดสิทธิ และช่วงเวลาในการผ่านเข้าออกพื้นที่

๓) ต้องบันทึกการผ่านเข้าออกในพื้นที่ที่สำคัญ

๔) ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

๓ การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing office, room and facilities)

๑) ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับสำนักงาน ห้องทำงานและเครื่องมือต่างๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก

๒) เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่างๆ ได้รับการปิดล็อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๓) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงานในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

๔) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม โดยให้เป็นไปตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

๕) เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่ บุคคลผู้นั้นเป็นเจ้าหน้าที่ ที่ได้รับอนุญาตให้ดำเนินการและเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

๔. การรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ

ความมั่นคงทางกายภาพถือเป็นส่วนสำคัญอันหนึ่งของระบบรักษาความปลอดภัย ความมั่นคงทางกายภาพ รวมถึงการป้องกันสถานที่และอุปกรณ์ ให้ปลอดภัยจากการปล้น การโจรกรรม อุบัติภัยทางธรรมชาติ เช่นแผ่นดินไหว น้ำท่วมเป็นต้น การป้องกันอุบัติเหตุอันก่อให้เกิดความเสียหายเนื่องจากกระแสไฟฟ้าลัดวงจร อุณหภูมิ หรือความชื้น ในห้องควบคุมที่สูงเกินขีดจำกัด หรือการกระทำโดยประมาท เช่น การทำน้ำหกรดโดนเครื่องคอมพิวเตอร์แม่ข่าย ดังนั้นจึงมีความจำเป็นในการป้องกันอาคารและอุปกรณ์โดยกำหนดเป็นนโยบายเพื่อถือปฏิบัติ ในเรื่องการสร้างห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายรวมถึงมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๑. จำแนกและกำหนดพื้นที่ห้องควบคุมระบบ เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้ โดยจัดแบ่งพื้นที่ดังนี้

๑) ห้องควบคุมระบบแบ่งเป็นสองพื้นที่ ได้แก่ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

๒) พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตการณ์ระบบ ส่วนพื้นที่จำกัดการเข้าถึงเป็นห้องที่มีเซิร์ฟเวอร์ ระบบเครือข่ายคอมพิวเตอร์ติดตั้งอยู่

๒. การเข้าไปในพื้นที่ควบคุม

๑) ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ ผู้บริหารหน่วยงานหรือบุคคลที่ผู้บริหารหน่วยงานนำเข้าเยี่ยมชม

๒) ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

๓) ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่ควบคุมเว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๔) ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อสินทรัพย์ของหน่วยงานจะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๕) บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชมในพื้นที่ควบคุมต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมายและต้องมีเจ้าหน้าที่อยู่ด้วยตลอดเวลา

๓. การเข้าไปในพื้นที่จำกัดการเข้าถึง

๑) ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบหรือในกรณีที่บุคคลอื่นที่มีความจำเป็นเข้าไปปฏิบัติงานต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมายและต้องมีผู้ดูแลระบบที่ได้รับมอบหมายอย่างน้อย ๑ คนเข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

๒) ไม่อนุญาตให้บุคคลที่มีอายุต่ำกว่า ๑๕ ปี เข้าไปในพื้นที่จำกัดการเข้าถึง

๓) ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง

๔) ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่จำกัดการเข้าถึงเว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๕) ไม่อนุญาตให้เข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง

๖) ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อสินทรัพย์จะอนุญาตให้เข้าไปในพื้นที่จำกัดการเข้าถึงได้โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๔. ด้านกายภาพของห้องควบคุมระบบ

๑) แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้เช่น router, switch, server, UPS เป็นต้น

๒) มี rack ในการจัดเก็บอุปกรณ์ต่างๆ ที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา

๓) ตำแหน่งของการวางอุปกรณ์ต่างๆ ไม่ควรวางใกล้ประตู หน้าต่างเพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น ไม่ควรวางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรงเพื่อหลีกเลี่ยงความชื้น

๔) การจัดวางสาย cable network สายไฟฟ้าควรติดป้ายชื่อสายต้นทางปลายทาง และเก็บสายให้เรียบร้อยเพื่อป้องการการเดินสะดุด

๕) ติดประกาศบันทึกการบำรุงรักษา ชื่อและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด

๖) มีระบบรักษาความปลอดภัยในห้องเช่น กล้อง CCTV ระบบการเข้าออกห้องโดยระบบ fingerprint scan หรือ RFID เป็นต้น

๗) มีระบบสังเกตการณ์อุณหภูมิภายใน rack ระบบแจ้งเตือนและป้องกันอัคคีภัย

๘) มีระบบสำรองไฟฟ้าเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติ และระบบสำรองไฟฟ้าอัตโนมัติ เป็นต้น

๙) มีระบบป้องกันกระแสไฟฟ้าจากฟ้าผ่า

๑๐) ระบบปรับอากาศแบบควบคุมอุณหภูมิ (๕๐-๘๐°F) และความชื้น (๒๐- ๘๐%)

๑๑) ติดตั้งฉนวนกันไฟไหม้ ที่ฝ้าเพดานและกำแพง

๕. การบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

๑) กรณีติดตั้งเซิร์ฟเวอร์หรืออุปกรณ์ต่างๆ ให้แกะหีบห่อและประกอบให้แล้วเสร็จจากภายนอกพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงก่อนนำไปติดตั้งเว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๒) กรณีที่จำเป็นต้องทำงานก่อสร้าง แก้ไข และติดตั้ง ในพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงต้องมีอุปกรณ์ควบคุม ฝุ่น ความร้อน เพื่อป้องกันความเสียหาย โดยผ่านความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมายก่อนการปฏิบัติงาน

๓) ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยทุก ๓ เดือน

๔) ร่างขั้นตอนแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟฟ้าลัดวงจร ไฟไหม้ แผ่นดินไหว น้ำท่วมหรือมีผู้บุกรุก เป็นต้น

๕) ซ้อมการปฏิบัติงานตามแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน ทุก ๖ เดือน

๖) มีตารางการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

๕. การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external end environmental threats)

๑) ต้องมีวิธีป้องกันจากการทำลายของธรรมชาติหรือคนที่อาจจะเกิดขึ้น

๖. การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)

๑) หากพบสิ่งผิดปกติ หรือการละเมิดความมั่นคงปลอดภัย จะต้องแจ้งให้ผู้บังคับบัญชาทราบ

๒) ในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยต้องติดประกาศแจ้งเตือน เช่น “ห้ามเข้าก่อนได้รับอนุญาต”

๗. พื้นที่สำหรับรับส่งของสิ่งของ (Delivery and loading areas)

๑) ต้องแยกจุดที่รับส่งสิ่งของ ออกจากพื้นที่ที่มีอุปกรณ์ประมวลผลสารสนเทศ และดำเนินการแกะหีบห่อหรือตรวจสอบให้เสร็จสิ้น ก่อนนำเข้าสู่พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย

๔.๒ อุปกรณ์ (Equipment)

วัตถุประสงค์

เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อสินทรัพย์และป้องกันการหยุดชะงักต่อการดำเนินงานขององค์กร

นโยบายและแนวปฏิบัติ

๑. การจัดตั้งและป้องกันอุปกรณ์ (Equipment siting and protection)

๑) การจัดตั้ง หรือการจัดวางอุปกรณ์สินทรัพย์สารสนเทศ อุปกรณ์ใดที่มีความสำคัญสูงต้องจัดวางในที่ที่เข้าถึงได้ยาก

๒. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

๑) อุปกรณ์ที่มีความสำคัญสูงควรติดตั้งระบบป้องกันความล้มเหลวของอุปกรณ์ เช่น ระบบสำรองไฟฟ้า ระบบปรับอากาศ เป็นต้น

๓. ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)

๑) การเดินสายสัญญาณต้องแยกท่อเพื่อป้องกันสัญญาณรบกวน

๒) ต้องมีการทำป้ายสายสัญญาณชัดเจน และเมื่อมีการเปลี่ยนแปลงต้องมีการปรับปรุงป้ายสายสัญญาณให้ถูกต้อง

๔. การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

๑) ต้องจัดให้มีการบำรุงรักษาอุปกรณ์เพื่อให้มีสภาพพร้อมใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือมากกว่าตามระดับความสำคัญ

๕. การนำสินทรัพย์ขององค์กรออกนอกสำนักงาน (Removal of assets)

๑) ห้ามนำสินทรัพย์สารสนเทศออกนอกพื้นที่ก่อนได้รับอนุญาตจากผู้รับผิดชอบ และต้องมีขั้นตอนในการตรวจสอบและติดตาม

๖. ความมั่นคงปลอดภัยของอุปกรณ์และสินทรัพย์ที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off- premises)

๑) สินทรัพย์ที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัยตามความเสี่ยง

๗. ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

๑) ข้อมูลที่เก็บอยู่บนสื่อบันทึกข้อมูล หากไม่มีการใช้งานแล้วต้องทำลายให้สิ้นซาก โดยให้เป็นไปตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

๘. อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment)

๑) ต้องป้องกันให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สินทรัพย์สารสนเทศที่ไม่มีผู้ดูแล

๙. การควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear desk and clear screen policy)

๑) เจ้าหน้าที่ต้องควบคุมเอกสาร ข้อมูล หรือสื่อต่างๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน โดยให้เป็นไปตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

๕. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications security)

วัตถุประสงค์

เพื่อป้องกัน ควบคุมการใช้งานระบบเครือข่ายสื่อสารที่ไม่พึงประสงค์และรักษาความปลอดภัยจากภายนอก และภัยคุกคามที่เข้ามาผ่านทางระบบเครือข่ายสื่อสาร เช่น ระบบจดหมายอิเลกทรอนิกส์ หรืออุปกรณ์สื่อสารไร้สายแบบพกพา คอมพิวเตอร์แบบพกพา รวมทั้งการปฏิบัติงานนอกหน่วยจากระยะไกล

นโยบายและแนวปฏิบัติ

๑. ระบบเครือข่ายสื่อสารและระบบเครือข่ายไร้สาย

๑. ผู้ดูแลระบบต้องออกแบบและแบ่งแยกระบบเครือข่าย ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยประกอบด้วย โซนภายใน (Internal Zone) โซนภายนอก
(External Zone) เพื่อให้การบริหารจัดการและควบคุมเป็นระบบ และป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ

๒. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกการกีฬาแห่งประเทศไทยผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตน ก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกการกีฬาแห่งประเทศไทยสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของการกีฬาแห่งประเทศไทย ได้แก่

๑) การแสดงตัวตน ด้วยชื่อผู้ใช้งาน (Username)

๒) การพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่าน (Password)

๓) การเข้าสู่ระบบสารสนเทศของ การกีฬาแห่งประเทศไทย จะต้องมีการตรวจสอบผู้ใช้งานอีกครั้ง

๔) การเข้าสู่ระบบจากระยะไกล เพื่อเพิ่มความปลอดภัยของการรับส่งข้อมูล ต้องมีการใช้การเข้ารหัสข้อมูล ได้แก่ SSL

๓. การใช้งานเครือข่ายจากแหล่ง หรือสถานที่ที่ได้รับอนุญาต ผู้ดูแลระบบต้องจัดทำกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายของการกีฬาแห่งประเทศไทยและเครือข่ายภายนอกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตเท่านั้น

๔. ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย ผู้ดูแลระบบต้องจัดทำข้อกำหนดหรือข้อตกลงสำหรับคุณสมบัติด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่างการกีฬาแห่งประเทศไทยกับหน่วยงานภายนอก

๕. การควบคุมผู้ใช้งานในการใช้งานเครือข่าย ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น ได้แก่

๑) ใช้ Monitoring Tool เพื่อตรวจสอบการเชื่อมต่อทางระบบเครือข่าย

๒) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องแม่ข่าย

๓) ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต

๖. การจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน ผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network routing Control) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาติเท่านั้น

๗. ผู้ดูแลระบบต้องกำหนด IP Address ให้กับอุปกรณ์ที่เชื่อมต่อเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้ IP Address ระบุถึงอุปกรณ์ได้ กำหนดให้ผู้ใช้งานต้องลงทะเบียน MAC Address อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้อง

๒. อุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

๑) ต้องกำหนดวิธีการป้องกันข้อมูลและสินทรัพย์สารสนเทศที่อยู่ในอุปกรณ์คอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารอื่นๆ โดยให้เป็นไปตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

๓. การปฏิบัติงานภายนอกหน่วยงาน (Teleworking)

๑) อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานโดยต้องใช้งานผ่านช่องทางที่จัดเตรียมไว้ให้ และต้องตรวจสอบตัวตนก่อนการใช้งาน โดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๒) ต้องไม่นำข้อมูลลับขององค์กรไว้บนอุปกรณ์ส่วนตัว หรือหากมีความจำเป็นต้องใช้งาน เมื่อใช้เสร็จแล้วควรลบทิ้งไป

๔. การใช้งานระบบจดหมายอิเลกทรอนิกส์

สำหรับผู้ใช้งานทั่วไป

๑) กำหนดให้มีการกรอกข้อมูลคำขอเข้าใช้งานและยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์ชื่อผู้ใช้งานรายใหม่และรหัสผ่าน (Password)

๒) เมื่อได้รับรหัสผ่าน (Password) จะต้องเปลี่ยนรหัสผ่าน(Password)โดยทันทีหลังจากการเข้าสู่ระบบเป็นครั้งแรก

๓) ควรกำหนดรหัสผ่านที่ยากต่อการคาดเดาให้มีตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติตัวเลขและสัญลักษณ์เข้าด้วยกัน

๔) ผู้ใช้งานควรเปลี่ยนรหัสผ่านทุก ๆ ๖ เดือน

๕) หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของ กกท. จะต้องใช้จดหมายอิเล็กทรอนิกส์ของ กกท. เพื่อผลประโยชน์ของทางราชการ

๖) หลังจากการใช้งาน ควรลงชื่อออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบ

๗) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๘) ห้ามส่ง E-Mail ที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น

- การส่งจดหมายจำนวนมาก (Spam Mail)
- จดหมายลูกโซ่ (Chain Letter)
- การส่งจดหมายต่อเนื่อง (Letter bomb)

- การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์
- การละเมิดต่อกฎหมาย หรือสิทธิ์ของบุคคลอื่น
- การส่งไวรัสไปให้กับบุคคลอื่นโดยเจตนา

๙) ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น.exe .com เป็นต้น

๑๐) ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๑) ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของ กกท. หรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ และข้อตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของ กกท. ได้อย่างถูกต้อง

๑๒) กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงบบริการแก่สมาชิกนั้นๆ เป็นการชั่วคราวหรือเพื่อทำการสอบสวน และตรวจสอบหาสาเหตุของมูลเหตุนั้นๆ

๑๓) การกระทำใดๆ ที่เกี่ยวกับการเผยแพร่ ทั้งในรูปแบบอีเมล์ และ/หรือโฮมเพจของผู้ใช้บริการให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการ ฝ่ายสารสนเทศและวิชาการกีฬาไม่มีส่วนเกี่ยวข้องใดๆ

๑๑) ในกรณีที่ผู้ใช้ลาออก หรือเกษียณอายุราชการผู้ใช้ยังสามารถใช้งานระบบ E-Mail ของสำนักงานต่อได้อีก ๑ ปี ก่อนที่ผู้ดูแลระบบจะทำการระงับสิทธิ์การใช้งาน

๕. แนวปฏิบัติสำหรับผู้ดูแลระบบ (System Administrator)

๑) กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของเจ้าหน้าที่ ระบบเครือข่ายและระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒) มีการทบทวนสิทธิ์การเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การลาออก โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๓) มีการควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๔) ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านทุกๆ ๓ เดือน

๕) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๖) เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน

๗) เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๘) ต้องกำหนดค่าใช้ WPA (Wi-Fi protected access) หรือดีกว่าในการเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจายสัญญาณ (access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

๙) เลือกใช้วิธีการควบคุม ชื่อผู้ใช้และรหัสผ่านของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สายโดยจะอนุญาตเฉพาะชื่อผู้ใช้และรหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๑๐) ติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

๑๑) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายและเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการฝ่ายสารสนเทศและวิชาการกีฬา ทราบโดยทันที

๖. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

๖.๑) การบริหารจัดการขีดความสามารถของระบบและระบบสาธารณูปโภค (Capacity management)

วัตถุประสงค์

เพื่อให้หน่วยงานสามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอรองรับต่อการดำเนินงานและสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

นโยบายและแนวปฏิบัติ

๑. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติเรื่องการบริหารจัดการขีดความสามารถของระบบเพื่อประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึง ระบบคอมพิวเตอร์ระบบฐานข้อมูลระบบเครือข่ายสื่อสารและระบบสาธารณูปโภคที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ

๒. มีการประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศเพื่อวางแผนรองรับการใช้งานในอนาคต (capacity planning) โดยครอบคลุมทั้งระบบหลักและระบบสำรอง

๓. มีกระบวนการหรือเครื่องมือในการติดตามประสิทธิภาพและความเพียงพอของการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศของระบบ เพื่อบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างทันท่วงทีและสามารถตอบสนองความต้องการในการดำเนินงานได้อย่างต่อเนื่อง

๔. มีการกำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (threshold และ trigger) ในระดับต่าง ๆ เพื่อให้มีการแจ้งเตือนผู้เกี่ยวข้องอย่างทันท่วงทีและสามารถวิเคราะห์ปัญหาและแนวทางการรับมือที่เหมาะสมรวมถึงการประสานงานกับหน่วยงานทั้งภายในและภายนอกกรณีเกิดเหตุขัดข้อง

๕. จัดทำรายงานความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมและความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง รวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการณ์

๖.๒ รักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint)

๑. รักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (Server)

วัตถุประสงค์

เพื่อให้อุปกรณ์ที่ใช้ปฏิบัติงานมีความปลอดภัยและไม่เป็นช่องทางที่ทำให้ข้อมูลสำคัญของหน่วยงานรั่วไหลหรือมีการเข้าใช้งานโดยไม่ได้รับอนุญาต

นโยบายนโยบายและแนวปฏิบัติ

๑. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๑) กำหนดให้มีรหัสผู้ใช้/รหัสผ่าน (Username/Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ

๒) กำหนดจำนวนครั้งที่สามารถพิมพ์รหัสผิดได้หากเกินกว่าที่กำหนดระบบต้องทำการ Lockไม่ให้ใช้งานเป็นระยะเวลาหนึ่ง

๓) ผู้ดูแลระบบควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๔) ผู้ดูแลระบบควรตั้งระบบการล็อคหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๕) ผู้ดูแลระบบต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๖) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ หรือเครื่องแม่ข่าย เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ หรือเครื่องแม่ข่าย

๗) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ หรือเครื่องแม่ข่ายของระบบงานรวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการ หรือเครื่องแม่ข่ายใหม่

๒. การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ (Control of operational software)

๑) มีการควบคุมการเปลี่ยนแปลงต่อระบบงานของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

๒) ผู้ดูแลระบบที่ได้รับการอบรมแล้วหรือมีความชำนาญเท่านั้นที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานของหน่วยงาน

๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๔) กำหนดให้มีการจัดเก็บ Source Code และ Library สำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๕) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๒. อุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint)

๑.) กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงานเป็นลายลักษณ์อักษร

๒.) กำหนด Security Baseline สำหรับอุปกรณ์ที่ใช้ปฏิบัติงานของหน่วยงานเพื่อป้องกันความเสี่ยงที่อุปกรณ์เหล่านั้นอาจเป็นช่องทางในการแพร่กระจายของโปรแกรมไม่พึงประสงค์(malware)และการรั่วไหลของข้อมูลสำคัญตามระดับความเสี่ยงที่เหมาะสมโดยอย่างน้อยครอบคลุมดังนี้

- ติดตั้งระบบปฏิบัติการและโปรแกรมพื้นฐานที่ใช้ในการปฏิบัติงานบนเครื่องคอมพิวเตอร์ (personal computer, notebook) โดยมีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้ผู้ใช้งานสามารถติดตั้งโปรแกรมอื่น ๆ นอกเหนือจากหน่วยงานกำหนด

- ติดตั้งโปรแกรมรักษาความปลอดภัยเช่น anti-Virus/anti-malware เป็นต้นโดยมีการปรับปรุงประสิทธิภาพของการป้องกันโปรแกรมไม่พึงประสงค์(malware)ให้เพียงพอและเป็นปัจจุบัน เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ ๆ

- มีกระบวนการหรือเครื่องมือในการตรวจจับ (detect) คัดกรอง (filter) สกัดกั้น (block) เพื่อป้องกันการถูกโจมตีจากภายนอก และปกป้องกันข้อมูลสำคัญรั่วไหล (Data Leakage Prevention : DLP)

- จำกัดการเข้าถึง shared drive หรือ shared folder ตามความจำเป็นในการใช้งานเท่านั้น

- การควบคุมการใช้งานอินเตอร์เน็ต โดยมีอุปกรณ์หรือซอฟท์แวร์ในการควบคุมให้อุปกรณ์ที่สามารถเชื่อมต่ออินเตอร์เน็ตเข้าถึงเฉพาะเว็บไซต์ที่ได้รับอนุญาตเท่านั้นรวมถึงมีการจำกัดการดาวน์โหลดหรืออัพโหลดข้อมูลจากอินเตอร์เน็ต

๖.๓ การสำรองข้อมูล (data backup)

วัตถุประสงค์

เพื่อป้องกันการสูญหายของข้อมูล และให้มั่นใจว่าระบบสารสนเทศอยู่ในสภาพพร้อมใช้งาน

นโยบายและแนวปฏิบัติ

๑. การสำรองและกู้คืนข้อมูล (Information backup and recovery policy)

๑) หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายให้บริการให้ดำเนินการสำรองข้อมูล ตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

๒) ต้องสำรวจข้อมูล และจัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรอง และความถี่ในการสำรองข้อมูล

๓) ข้อมูลที่มีความสำคัญสูงต้องจัดให้มีความถี่การสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกสำนักงาน

๔) ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

๕) จัดเก็บข้อมูลที่สำรองไว้ทั้งนอกหน่วยงาน และภายในหน่วยงาน โดยระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

๖) จัดทำคู่มือการปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๕) ต้องทดสอบข้อมูลที่สำรองอย่างสม่ำเสมอ

๖) ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๗) หากต้องมีการกู้คืนข้อมูลให้ดำเนินการกู้คืนข้อมูลตาม ตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

๘) การสำรองข้อมูล และการกู้ข้อมูลของทุกระบบ ต้องถูกบันทึกเป็นเอกสาร และมีการตรวจสอบความถูกต้องเป็นระยะๆ

๒. แนวปฏิบัติการสำรองและการกู้คืนข้อมูล

๑. การสำรองข้อมูล หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายให้บริการให้ดำเนินการคัดเลือกและจัดทำระบบสำรองข้อมูล ดังนี้

๑) ต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และจัดระดับความสำคัญของข้อมูล

๒) สำรวจข้อมูล และ จัดระดับความสำคัญในการสำรองข้อมูล ดังนี้

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
๐	ไม่มีผลกระทบ	ไม่มีผลกระทบใดๆ ต่อการดำเนินภารกิจ
๑	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานองค์กร
๒	กระทบค่อนข้างน้อย	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
๓	กระทบค่อนข้างรุนแรง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินภารกิจ
๔	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
๕	ปิดหน่วยงาน	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

๓) ต้องจัดให้มีความถี่ในการสำรองให้พอเพียง ในระบบที่มีความสำคัญสูง เครื่องที่มีความสำคัญสูงควรเพิ่มความถี่การสำรองให้มากขึ้น ดังนี้

ที่	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑	Mail servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในเมล์บ็อกซ์	Full ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
๒	Web servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	Full ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
๓	Database	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	Full ๒ ครั้งต่อสัปดาห์ และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
๔	Firewall	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูล Rule ของ Firewall	Full ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
๕	Server อื่นๆ เช่น...	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลบนเซิร์ฟเวอร์อื่นๆ	Full ๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่

๔) ต้องจัดทำผังหรือขั้นตอนการสำรองข้อมูล

๕) ต้องทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๖) ต้องจัดทำบันทึกการสำรองข้อมูล และตรวจสอบว่าการสำรองข้อมูลสำเร็จหรือไม่ แก้ไข และรายงานต่อผู้บังคับบัญชา

๗) ต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงานในระบบที่มีความสำคัญระดับสูง

๘) ต้องจัดให้มีการเข้ารหัสข้อมูลที่มีระดับความสำคัญสูง (Encrypted backup) โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๙) ต้องดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บังคับบัญชา หรือ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้

๑๐) เป็นผู้กำหนดชนิด เช่น Full หรือ Incremental และช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล

๑๑) ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๒. การกู้คืนข้อมูล ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ผู้ดูแลระบบมีหน้าที่ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงาน ต่อผู้บังคับบัญชา ดังนี้

๑) ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๒) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๓. สาเหตุและวิธีการกู้คืน

สาเหตุ	วิธีการ
กรณีที่ ๑ เกิดความเสียหายขึ้นกับโปรแกรมต้นฉบับ (Source code)	ดำเนินการติดตั้งโปรแกรมต้นฉบับ (Source code) ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด
กรณีที่ ๒ เกิดความเสียหายขึ้นกับฐานข้อมูล (Database)	ดำเนินการกู้คืนฐานข้อมูลที่เก็บไว้ล่าสุด เพื่อให้ใช้งานได้ต่อเนื่องโดยที่ข้อมูลสูญหายน้อยที่สุด
กรณีที่ ๓ เกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ฮาร์ดแวร์ยังคงทำงานปกติ	ดำเนินการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจากโปรแกรมต้นฉบับที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมถึงกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด
กรณีที่ ๔ เกิดความเสียหายขึ้นกับฮาร์ดแวร์	ให้บริษัทผู้ดูแลแก้ไขเบื้องต้นให้สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับระบบปฏิบัติการและระบบงานให้บริษัทหรือผู้ได้รับมอบหมายดำเนินการติดตั้งระบบปฏิบัติการและระบบงานนั้นใหม่ โดยใช้โปรแกรมต้นฉบับ ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด และกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

๖.๔ การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging)

วัตถุประสงค์

เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

นโยบายและแนวปฏิบัติ

๑. การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging)

๑) ฝ่ายสารสนเทศและวิชาการกีฬา ต้องจัดเก็บข้อมูลบันทึกกิจกรรมของผู้ใช้งาน เพื่อใช้ติดตามกรณีเกิดเหตุความมั่นคงปลอดภัย หรือบันทึกการทำงานของระบบที่ไม่เป็นไปตามปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บและทบทวนอย่างสม่ำเสมอ รวมทั้งกำหนดวิธีการและระยะเวลาในการจัดเก็บให้สอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

๒. การป้องกันข้อมูลล็อก (Protection of log information)

๑) อุปกรณ์บันทึกล็อกและข้อมูลการล็อกต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๒) ต้องมีการตรวจสอบติดตามประเมินผลระบบการป้องกันข้อมูลล็อกที่มีประสิทธิภาพ

๓. ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)

๑) ต้องมีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ และมีการทบทวนอยู่เสมอ

๔. การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

๑) เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องและระบบงานทุกระบบภายในกกท. ต้องมีการตั้งเวลาให้ตรงกันโดยเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้

๒) ต้องมีการวางแผนและตรวจสอบการตั้งนาฬิกาให้ตรงและถูกต้อง

๖.๕ การติดตามตูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring)

วัตถุประสงค์

เพื่อให้หน่วยงานสามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงทีโดยมีกระบวนการติดตามดูแลความมั่นคงปลอดภัยของระบบรวมถึงเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง

นโยบายและแนวปฏิบัติ

๑. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคามเพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง

๒. กำหนดกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยของระบบ

ที่สำคัญอย่างทันท่วงทีครอบคลุมระบบงานและระบบเครือข่ายสื่อสารทั้งในเชิง physical และ logical เช่น ห้อง DATA Center ระบบ ERP และระบบจดหมายอิเล็กทรอนิกส์ เป็นต้นเพื่อให้รับทราบความผิดปกติหรือภัยคุกคามและสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม

๓. มีกระบวนการหรือเครื่องมือในการรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ มีการวิเคราะห์และจัดการข้อมูลภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุม ลักษณะการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้นเพื่อนำมาใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์

๔. ให้กองสารสนเทศประสานงานแลกเปลี่ยนข้อมูลภัยคุกคาม ระหว่าง หน่วยงานที่เกี่ยวข้อง รวมทั้งมีกระบวนการและช่องทางในการรายงาน แลกเปลี่ยน ติดตามเพื่อป้องกันรับมือและแก้ไขภัยคุกคาม

๕. ในกรณีที่พบภัยคุกคามที่ส่งผลกระทบอย่างมีนัยสำคัญ ผู้อำนวยการกองสารสนเทศมีหน้าที่รายงานผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง รวมทั้งจัดให้มีกระบวนการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) โดยผู้ที่มีความเชี่ยวชาญ เพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบและสามารถดำเนินการปิดช่องโหว่และป้องกันความเสี่ยงที่อาจเกิดขึ้นอีก

๖.๖ การบริหารจัดการช่องโหว่ (vulnerability management)

วัตถุประสงค์

เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ และสามารถดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้อย่างทันท่วงที

นโยบายและแนวปฏิบัติ

๑. การจำกัดการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Restrictions on software installation)

๑) ระบบที่ให้บริการต้องทำการ Patch ซอฟต์แวร์อย่างสม่ำเสมอ

๒) ต้องทำการลบ User ที่ไม่จำเป็นออกจากระบบ เช่น AAA, BBB

๓) ต้องปิด Service ที่ไม่ได้ใช้งาน

๔) ซอฟต์แวร์ใดไม่ได้ใช้งานต้องลบออก

๒. การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

๑) ต้องติดตามข้อมูลทางด้านเทคนิคของช่องโหว่อย่างสม่ำเสมอ

๖.๗ การทดสอบเจาะระบบ (penetration test)

วัตถุประสงค์

เพื่อทดสอบหาช่องโหว่ที่พบจากการใช้งานระบบสารสนเทศในองค์กรเพื่อประเมินช่องโหว่และทำการปิดกั้นช่องโหว่ที่ค้นพบขึ้นเพื่อไม่เกิดปัญหาขึ้นในระยะยาว

นโยบายและแนวปฏิบัติ

๑. มีการทดสอบเจาะระบบ (penetration test) จากหน่วยงานภายนอกที่มีความเชียวชาญ โดยการทดสอบจะต้องครอบคลุมระบบงานและระบบเครือข่ายภายในกกท. หรือระบบที่มีการเชื่อมต่อกับเครือข่าย

สาธารณะ (internet facing) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๒. มีการรายงานผลการทดสอบเจาะระบบไปยังผู้บริหาร รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อผู้บริหารที่ได้รับมอบหมาย

๓. มีกระบวนการรวบรวมและวิเคราะห์ช่องโหว่ทางด้านเทคนิคที่ตรวจพบเพื่อกำหนดเป็นมาตรการรักษาความมั่นคงปลอดภัยของระบบงานที่จะมีการพัฒนาในอนาคต

๖.๘ การบริหารจัดการการเปลี่ยนแปลง (Change management)

วัตถุประสงค์

เพื่อให้มีการบริหารจัดการการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศสอดคล้องตามมาตรฐานสากล โดยมีการควบคุมที่รัดกุมปลอดภัยเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างครบถ้วนถูกต้อง

นโยบายและแนวปฏิบัติ

๑) มีการควบคุมการเปลี่ยนแปลงระบบสารสนเทศ เช่น ต้องมีการขออนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ

๒) ต้องมีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ

๓) กรณีการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน ควรมีกระบวนการในการพิจารณาความเสี่ยงและผลกระทบ รวมถึงขออนุมัติจากผู้บริหารที่ได้รับมอบหมายให้สามารถตัดสินใจได้กรณีเร่งด่วนโดยภายหลังดำเนินการให้มีการรายงานผู้บริหารที่เกี่ยวข้องได้รับทราบโดยเร็ว

๔) มีการจัดเก็บการเปลี่ยนแปลงของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (version control) เช่นการนำระบบขึ้นใช้งานจริง การตั้งค่าระบบ การติดตั้ง patch บนระบบที่ให้บริการจริง เป็นต้นเพื่อควบคุมความเสี่ยงในการเปลี่ยนแปลงและลดข้อผิดพลาดที่อาจเกิดขึ้น

๖.๙ การบริหารจัดการการตั้งค่าระบบ (system Configuration management)

วัตถุประสงค์

เพื่อให้หน่วยงานมีกระบวนการควบคุมการเปลี่ยนแปลงการตั้งค่าระบบที่มีความรัดกุมปลอดภัยและเป็นไปตามมาตรฐาน

นโยบายและแนวปฏิบัติ

๑. จัดทำเอกสาร minimum baseline standard เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ อย่างเป็นลายลักษณ์อักษรโดยมีการทบทวนปรับปรุงเอกสารให้เป็นปัจจุบันอย่างสม่ำเสมอ

๒. การเปลี่ยนแปลงการตั้งค่าบนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการเปลี่ยนแปลงที่หน่วยงานกำหนดเพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

๓ มีการจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบของทุกอุปกรณ์ ระบบและระบบงาน (system configuration version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

๔. มีการสอบทานการตั้งค่าจากหน่วยงานที่มีหน้าที่ควบคุมดูแลความปลอดภัยหรือความเสี่ยงด้านเทคโนโลยี อย่างสม่ำเสมอเพื่อให้สอดคล้องตามมาตรฐานของหน่วยงาน

๕. กรณีมีความจำเป็นต้องตั้งค่าที่ไม่เป็นไปตามเอกสารminimum baseline standard ควรผ่านกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

๖.๑๐ การบริหารจัดการ patch (patch management)

วัตถุประสงค์

เพื่อให้หน่วยงานมีการบริหารจัดการ patch โดยมีการควบคุมที่รัดกุมปลอดภัย และติดตั้งได้อย่างเหมาะสมทันการณ์

นโยบายและแนวปฏิบัติ

๑. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในกระบวนการบริหารจัดการ patch ที่ครอบคลุมการตรวจสอบความถูกต้องของ patch และการประเมินความเสี่ยงและความจำเป็นในการติดตั้ง patch ใหม่จากผู้ผลิตอย่างเหมาะสมทันการณ์

๒. จัดเก็บการเปลี่ยนแปลงการติดตั้งของทุกอุปกรณ์ระบบและระบบงาน (patch version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

๓. ทำการทดสอบ patch ที่ออกใหม่ทุกครั้งก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

๔. การติดตั้ง patch บนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ หน่วยงานกำหนดเพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

๕. ทบทวนและปรับปรุงกระบวนการบริหารจัดการ patch อย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าหน่วยงานสามารถทดสอบและติดตั้ง patch ด้านการรักษาความปลอดภัยได้ทันต่อสถานการณ์ที่เปลี่ยนไปและสามารถรองรับความเสี่ยงที่เพิ่มขึ้นได้อย่างรวดเร็ว

๗. การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System acquisition and development)

๗.๑ การจัดหาระบบ (System acquisition)

วัตถุประสงค์

เพื่อให้หน่วยงานดำเนินการจัดหาหรือพัฒนาระบบสารสนเทศที่มีประสิทธิภาพ และสร้างความปลอดภัยให้กับระบบสารสนเทศ

นโยบายและแนวปฏิบัติ

การจัดหาเพื่อให้ได้มาซึ่งระบบสารสนเทศ จะต้องดำเนินการตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของการกีฬาแห่งประเทศไทย ดังนี้

๑. การเชื่อมโยงหรือทำงานร่วมกันกับระบบงานเดิมที่กกท. มีการใช้งานอยู่

๒. การจัดหาเครื่องแม่ข่าย เพื่อรองรับระบบสารสนเทศใหม่ให้รวมอยู่ในการจัดหาด้วย รวมถึงการดูแลระบบ การดูแลข้อมูล การสำรองข้อมูล และการ Update ระบบต่างๆ ให้เป็นหน้าที่ของผู้พัฒนาระบบ

๓. การจัดหาระบบงานจะต้องรวมถึงการอบรม หรือการแนะนำการใช้งาน

๗.๒ การพัฒนาระบบ (System development)

วัตถุประสงค์

เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบและดำเนินการตลอดช่วงระยะเวลาของการพัฒนาระบบ

นโยบายและแนวปฏิบัติ

๑. ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง เช่น

- ต้องมีการอนุมัติโดยผู้มีอำนาจ
- ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
- ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

๒. ผู้พัฒนาระบบสารสนเทศต้องจัดทำแนวปฏิบัติการควบคุมการเปลี่ยนแปลงระบบสารสนเทศ

๓. เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่างๆ ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

๔. เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

๕. ควรนำหลักการวิศวกรรมระบบมาประยุกต์ใช้กับงานการพัฒนาระบบ เช่น

๑) ควรนำระบบงานที่สำคัญไปอยู่หลัง Firewall

๒) ปิดช่องโหว่ของระบบให้เหลือน้อยที่สุด

๓) การออกแบบด้านความปลอดภัยต้องให้ง่ายสำหรับการทำความเข้าใจ

๖. หากมีความจำเป็นต้องให้หน่วยงานภายนอกเข้ามาพัฒนาระบบภายในหน่วยงาน ต้องกำหนดสภาพแวดล้อมที่มีความมั่นคงปลอดภัย เช่น ตัดการเชื่อมต่อเครือข่ายออกสู่ภายนอกเพื่อป้องกันการนำข้อมูลลับออกสู่ภายนอก

๗. มีการแบ่งสิทธิตามหน้าที่การทำงานอย่างชัดเจน เช่น ผู้พัฒนาระบบ ผู้ดูแลฐานข้อมูล

๘. ต้องตรวจสอบประวัติของหน่วยงานภายนอกที่มารับจ้าง

๙. หน่วยงานภายนอกต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

๑๐. ต้องมีการประชุมติดตาม และบันทึกการประชุมกิจกรรมการพัฒนาระบบอย่างสม่ำเสมอ

๑๑. หากพบการละเมิดความมั่นคงปลอดภัยต้องแจ้งให้ผู้บังคับบัญชาทราบ

๑๒. การทดสอบด้านความมั่นคงปลอดภัยต้องทำการทดสอบการใช้งานในช่วงของการพัฒนาหากไม่ผ่านการทดสอบต้องแก้ไขให้แล้วเสร็จก่อนการส่งมอบ

๑๓. การทำงานของฟังก์ชันทุกฟังก์ชันการทำงาน ต้องทำงานถูกต้อง และสามารถทำงานได้

๑๔. มีการจัดทำคู่มือและฝึกอบรมให้แก่เจ้าหน้าสารสนเทศและผู้ใช้งานระบบ

๘. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem management)

วัตถุประสงค์

เพื่อแก้ไขปัญหาที่เกิดขึ้นแก่ระบบสารสนเทศภายในกกท. ให้กลับคืนสู่สภาวะปกติได้โดยเร็วที่สุด และลดผลกระทบต่อกระบวนการทำงาน ที่จะส่งผลกระทบต่อองค์กรให้น้อยที่สุด รวมถึงให้ระบบมีความพร้อมใช้งานและการให้บริการเป็นไปตามมาตรฐานที่ตกลงไว้กับผู้ใช้งาน

นโยบายและแนวปฏิบัติ

๑. กำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน และมีความเป็นระบบระเบียบที่ดี โดยให้เป็นไปตามแนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

๒. มีการรายงานสถานการณ์โดยต้องกำหนดช่องทางการติดต่อเพื่อรายงานเหตุการณ์ที่ผิดปกติอย่างชัดเจน

๓. หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลกระทบต่อระบบสารสนเทศกกท. ต้องแจ้งเหตุการณ์ดังกล่าวต่อฝ่ายสารสนเทศและวิชาการกีฬา

๔. มีการตรวจสอบเหตุการณ์ผิดปกติ หรือปัญหาที่เกิดให้ชัดเจน ก่อนรายงานแก่ผู้บริหาร

๕. กำหนดให้มีการรายงานเหตุการณ์ผิดปกติ หรือปัญหาตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว

๖. ต้องมีการบันทึกเหตุการณ์และปัญหาระบบสารสนเทศที่เกิดขึ้น โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อจะได้เรียนรู้และเตรียมการป้องกัน

๗. ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางกฎหมาย

๙. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศภายใน

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

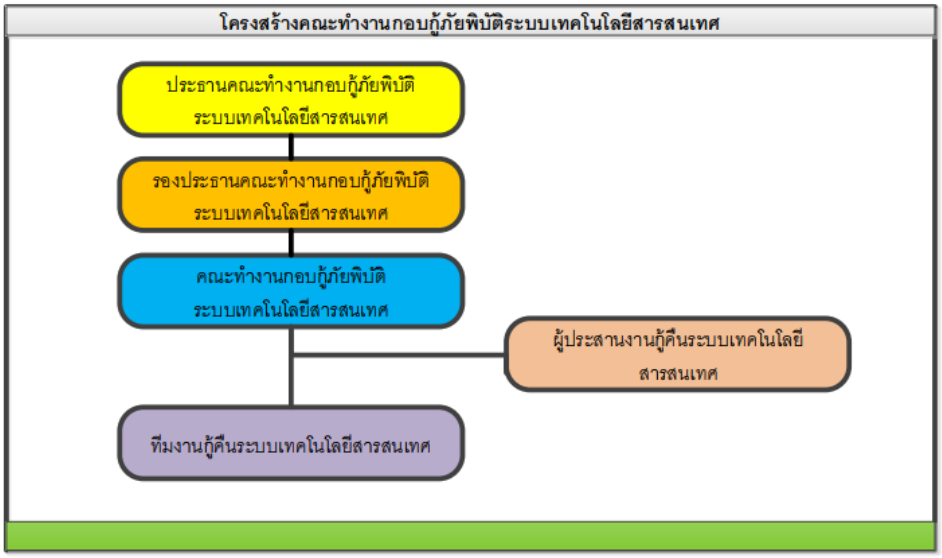
๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของกรมคุ้มครองสิทธิและเสรีภาพ

กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๑. คณะทำงานและบทบาทหน้าที่

เพื่อให้แผนการบริหารจัดการความต่อเนื่องทางธุรกิจ กองสารสนเทศ การกีฬาแห่งประเทศไทยสามารถดำเนินการได้อย่างมีประสิทธิภาพ จึงจำเป็นต้องกำหนดผู้มีหน้าที่ความรับผิดชอบในการกู้คืนระบบให้มีความชัดเจน โดยสามารถแบ่งได้ดังต่อไปนี้

- ประธานคณะทำงานกอบกู้ภัยพิบัติระบบเทคโนโลยีสารสนเทศ
- รองประธานคณะทำงานกอบกู้ภัยพิบัติระบบเทคโนโลยีสารสนเทศ
- คณะทำงานกอบกู้ภัยพิบัติระบบเทคโนโลยีสารสนเทศ
- ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศ
- ทีมงานกู้คืนระบบเทคโนโลยีสารสนเทศ



บทบาทหน้าที่ความรับผิดชอบ

ประธานคณะทำงานกอบกู้ภัยพิบัติระบบเทคโนโลยีสารสนเทศ

มีหน้าที่ดังนี้

- กำหนดนโยบายและเป้าหมายเกี่ยวกับการกู้คืนระบบ
- ให้ความสำคัญและจัดสรรงบประมาณและทรัพยากรต่างๆ ที่จำเป็นสำหรับการกู้คืนระบบ
- กำหนดและแต่งตั้งทีมที่เกี่ยวข้องกับการกู้คืนระบบและหน้าที่ความรับผิดชอบเช่น ทีมกู้คืนระบบ และทีมอื่นๆ ตามความจำเป็น
- สั่งการให้มีการเตรียมความพร้อมหรือเตรียมการพื้นฐานต่างๆ ที่จำเป็นสำหรับการรับมือกับเหตุการณ์หยุดชะงักที่อาจเกิดขึ้น
- สั่งการให้มีการนำแผนกู้คืนระบบมาใช้งาน
- บริหารจัดการเพื่อดำเนินการรับมือกับเหตุการณ์หยุดชะงักที่เกิดขึ้น
- วิเคราะห์ ติดตามสถานการณ์ที่เกิดขึ้นอย่างต่อเนื่อง ตัดสินใจ และสั่งการต่างๆ เพิ่มเติมตามที่เห็นสมควร
- สั่งการให้มีการแจ้งหรือสื่อสารข้อมูลที่ถูกต้องและทันสมัยต่อผู้บริหารหน่วยงานภายใน พนักงาน ญาติพี่น้องของพนักงาน ผู้ใช้บริการ หรือผู้ที่เกี่ยวข้องอื่นๆ
- สั่งการให้มีการจัดหาระบบ อุปกรณ์ หรือทรัพยากรเพิ่มเติมตามความจำเป็น
- สั่งการให้สิ้นสุดภารกิจของการกู้คืนระบบ

รองประธานคณะทำงานกอบกู้ภัยพิบัติระบบเทคโนโลยีสารสนเทศ

มีหน้าที่ดังนี้

- ปฏิบัติการแทนประธานคณะทำงานกอบกู้ภัยพิบัติระบบเทคโนโลยีสารสนเทศ
- ร่วมกำหนดนโยบายและเป้าหมายเกี่ยวกับการกู้คืนระบบ
- ร่วมให้ความสำคัญและจัดสรรงบประมาณและทรัพยากรต่างๆ ที่จำเป็นสำหรับการกู้คืนระบบ
- ร่วมกำหนดและแต่งตั้งทีมที่เกี่ยวข้องกับการกู้คืนระบบและหน้าที่ความรับผิดชอบเช่น ทีมกู้คืนระบบ และทีมอื่นๆ ตามความจำเป็น
- ร่วมสั่งการให้มีการเตรียมความพร้อมหรือเตรียมการพื้นฐานต่างๆ ที่จำเป็นสำหรับการรับมือกับเหตุการณ์หยุดชะงักที่อาจเกิดขึ้น
- ร่วมสั่งการให้มีการนำแผนกู้คืนระบบมาใช้งาน
- ร่วมบริหารจัดการเพื่อดำเนินการรับมือกับเหตุการณ์หยุดชะงักที่เกิดขึ้น
- ร่วมวิเคราะห์ ติดตามสถานการณ์ที่เกิดขึ้นอย่างต่อเนื่อง ตัดสินใจ และสั่งการต่างๆ เพิ่มเติมตามที่เห็นสมควร

- ร่วมสั่งการให้มีการแจ้งหรือสื่อสารข้อมูลที่ถูกต้องและทันสมัยต่อผู้บริหาร หน่วยงานภายใน พนักงาน ญาติพี่น้องของพนักงาน ผู้ใช้บริการ หรือผู้ที่เกี่ยวข้องอื่นๆ
- ร่วมสั่งการให้มีการจัดหาระบบ อุปกรณ์ หรือทรัพยากรเพิ่มเติมตามความจำเป็น
- ร่วมสั่งการให้สิ้นสุดภารกิจของการกู้คืนระบบ

คณะทำงานกู้คืนระบบเทคโนโลยีสารสนเทศ

มีหน้าที่ดังนี้

- ร่วมกำหนดนโยบายและเป้าหมายเกี่ยวกับการกู้คืนระบบ
- ร่วมให้ความสำคัญและจัดสรรงบประมาณและทรัพยากรต่างๆ ที่จำเป็นสำหรับการกู้คืนระบบ
- ร่วมกำหนดและแต่งตั้งทีมที่เกี่ยวข้องกับการกู้คืนระบบและหน้าที่ความรับผิดชอบเช่น ทีมกู้คืนระบบ และทีมอื่นๆ ตามความจำเป็น
- ร่วมสั่งการให้มีการเตรียมความพร้อมหรือเตรียมการพื้นฐานต่างๆ ที่จำเป็นสำหรับการรับมือกับเหตุการณ์หยุดชะงักที่อาจเกิดขึ้น
- ร่วมสั่งการให้มีการนำแผนกู้คืนระบบมาใช้งาน
- ร่วมบริหารจัดการเพื่อดำเนินการรับมือกับเหตุการณ์หยุดชะงักที่เกิดขึ้น
- ร่วมวิเคราะห์ ติดตามสถานการณ์ที่เกิดขึ้นอย่างต่อเนื่อง ตัดสินใจ และสั่งการต่างๆ เพิ่มเติมตามที่เห็นสมควร
- ร่วมสั่งการให้มีการแจ้งหรือสื่อสารข้อมูลที่ถูกต้องและทันสมัยต่อผู้บริหาร หน่วยงานภายใน พนักงาน ญาติพี่น้องของพนักงาน ผู้ใช้บริการ หรือผู้ที่เกี่ยวข้องอื่นๆ
- ร่วมสั่งการให้มีการจัดหาระบบ อุปกรณ์ หรือทรัพยากรเพิ่มเติมตามความจำเป็น
- ร่วมสั่งการให้สิ้นสุดภารกิจของการกู้คืนระบบ

ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศ

มีหน้าที่ดังนี้

- ประเมินสถานการณ์ที่เกิดขึ้นว่ามีผลกระทบและความรุนแรงในระดับใด
- รายงานหรือประสานงานเพื่อแจ้งประธานคณะทำงานให้ได้รับทราบ
- ประสานงานติดต่อทีมกู้คืนระบบเพื่อให้ลงพื้นที่ปฏิบัติการกู้คืนระบบ
- ระดมทีมกู้คืนระบบทั้งหมดเพื่อลงพื้นที่ปฏิบัติการประสานงาน และสั่งการทีมกู้คืนระบบเพื่อขอให้ดำเนินการต่างๆ ตามที่เห็นสมควร
- สั่งการให้ตรวจสอบและเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศต่างๆ ในศูนย์คอมพิวเตอร์สำรอง
- ติดตามและแจ้งข้อมูลเกี่ยวกับสถานภาพการดำเนินการกู้คืนระบบให้พนักงานและผู้ที่เกี่ยวข้องได้รับทราบ

- ประสานงานกับหน่วยงานภายในที่เกี่ยวข้องเพื่อขอให้ช่วยดำเนินการในเรื่องต่างๆ อาทิตรวจสอบระบบไฟฟ้า ระบบโทรศัพท์ ระบบปรับอากาศ การรักษาความปลอดภัย หรืออื่นๆที่เกี่ยวข้อง

ทีมกู้คืนระบบเทคโนโลยีสารสนเทศ

มีหน้าที่แยกตามฟังก์ชันงานดังนี้

การติดตั้งระบบ

- สำรวจและประเมินความเสียหายของฮาร์ดแวร์ อุปกรณ์ ข้อมูล และ/หรือ ซอฟต์แวร์ต่างๆ ของระบบที่เกิดความเสียหายและจำเป็นต้องติดตั้งกลับคืน
- กำหนดรายการของฮาร์ดแวร์ อุปกรณ์ ข้อมูล และ/หรือ ซอฟต์แวร์ต่างๆ ที่จำเป็นต้องใช้ในการกู้คืนระบบ
- แจ้งรายการฮาร์ดแวร์หรืออุปกรณ์ที่ต้องการพร้อมทั้งคุณลักษณะให้เลขาทีมกู้คืนระบบช่วยจัดหาหรือจัดเตรียมให้
- ติดตั้งฮาร์ดแวร์ อุปกรณ์ และ/หรือ ซอฟต์แวร์ที่เกี่ยวข้องกับระบบ โดยติดตั้งให้เหมือนเดิม หรือใกล้เคียงกับระบบเดิมให้มากที่สุด
- นำข้อมูลล่าสุดที่สำรองเก็บไว้มาทำการติดตั้งระบบกลับคืนตามความจำเป็น
- พยายามกู้คืนข้อมูลของระบบให้กลับไปสู่จุดเวลาที่เหตุหยุดชะงักเกิดขึ้น
- ตรวจสอบความเสียหายของอุปกรณ์เครือข่ายและดำเนินการแก้ไขระบบเครือข่ายตามความจำเป็น รวมทั้งทำการเชื่อมโยงเครือข่ายส่วนต่างๆ ของสำนักงานฯ เข้าด้วยกัน เพื่อให้สามารถกลับมาใช้งานได้ตามปกติ
- ติดตั้งอุปกรณ์เครือข่ายและสายสัญญาณเครือข่ายต่างๆ ตามความจำเป็น

การติดตั้งข้อมูล

- ติดตั้งและปรับแต่งแอพพลิเคชันให้เหมือนระบบเดิมมากที่สุด
- ทดสอบฟังก์ชันการทำงานต่างๆ ของระบบเพื่อดูว่าสามารถใช้งานได้ครบถ้วนหรือไม่
- นำข้อมูลล่าสุด (ของฐานข้อมูล) ที่สำรองเก็บไว้มาทำการติดตั้งระบบกลับคืนตามความจำเป็น
- พยายามกู้คืนข้อมูลของระบบให้กลับไปสู่จุดเวลาที่เหตุหยุดชะงักเกิดขึ้น
- ตรวจสอบดูความถูกต้องของข้อมูลที่ทำการติดตั้งกลับคืนนั้นเท่าที่ทำได้
- ทดสอบระบบร่วมกับผู้ใช้งาน

การให้บริการผู้ใช้งาน

มีหน้าที่ดังนี้

- รับแจ้งปัญหาการใช้งานเกี่ยวกับระบบเทคโนโลยีสารสนเทศของสำนักงานฯ ซึ่งรวมถึงเหตุหยุดชะงักที่เกิดขึ้นกับระบบต่างๆ

- วิเคราะห์ปัญหาที่ได้รับแจ้งร่วมกับทีมอื่นๆ เช่น ทีมติดตั้งระบบ ทีมกู้คืนระบบงาน เพื่อหาทางในการแก้ปัญหา
- กำหนดแนวทางหรือวิธีการในการแก้ปัญหา แก้ปัญหา และปิดปัญหา
- ประสานงานกับผู้ใช้งานเพื่อขอให้ร่วมทดสอบระบบต่างๆ

๒. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของการกีฬาแห่งประเทศไทย เทคโนโลยีสารสนเทศจึงเข้ามามี บทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการ ป้องกันปัญหาและลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความ เสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของกกท. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศของกกท. พบ ประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดีถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๒. ความเสี่ยงด้านบุคคล เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการ เข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูล ต่างๆ ของกกท. เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหาย ต่อข้อมูลสารสนเทศได้

๓. ความเสี่ยงด้านภัยพิบัติหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือ สถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม อัคคีภัย การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๔. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจ ส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศของกกท. ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกกท. มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับ สถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่ อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของกกท.

๓. แผนรองรับสถานการณ์ฉุกเฉิน

๓.๑ การเตรียมการก่อนเหตุการณ์ภัยพิบัติ

- กำหนดให้มีสถานที่ที่เป็นจุดรวมพลเมื่อมีเหตุการณภัยพิบัติเกิดขึ้น โดยมีการกำหนดสถานการณ์ตามกรณีต่างๆ เช่น ในกรณีที่เข้าพื้นที่การกีฬาแห่งประเทศไทยได้, ในกรณีที่ไม่สามารถเข้าพื้นที่การกีฬาแห่งประเทศไทยได้

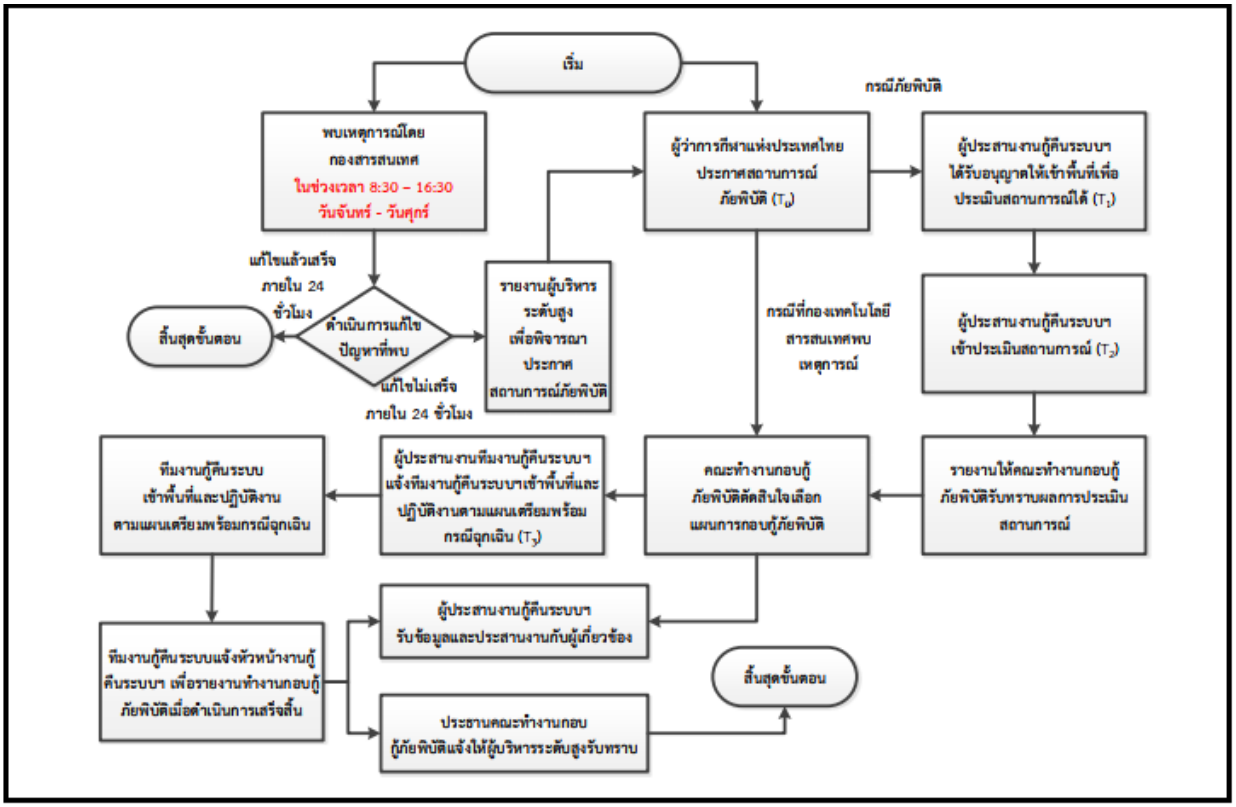
- มีการจัดตั้งศูนย์สั่งการ และเตรียมอุปกรณ์ต่างๆ เพื่อใช้ในการดำเนินงาน หากมีความจำเป็นต้องจัดตั้งศูนย์สั่งการ โดยจะต้องมีการทบทวนรายการดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

- จะต้องดำเนินการสำรองข้อมูลและเอกสารที่สำคัญ และจัดเก็บไว้ที่ศูนย์สั่งการทุกครั้งที่เอกสารดังกล่าวมีการเปลี่ยนแปลง

๓.๒ การรับมือกับภัยพิบัติ

เพื่อให้เกิดความพร้อมเมื่อภัยพิบัติเกิดขึ้น กองสารสนเทศ การกีฬาแห่งประเทศไทย จึงได้กำหนดแนวทางการรับมือไว้ดังต่อไปนี้

๑) การยกระดับเหตุภัยพิบัติและเริ่มแผนเตรียมพร้อมกรณีฉุกเฉิน



๒) ในการยกระดับเหตุการณ์ภัยพิบัติและเริ่มแผนการบริหารจัดการความต่อเนื่องทางธุรกิจนั้นจะแยกออกเป็น ๒ สถานการณ์ กล่าวคือ

- เมื่อผู้ว่าการกีฬาแห่งประเทศไทย ได้พิจารณาแล้วว่าเหตุการณ์ที่มีลักษณะดังต่อไปนี้

- ระบบไฟฟ้าล่ม เนื่องจากพายุฝนฟ้าคะนอง / อุปกรณ์ชำรุดเสียหาย
- ไฟไหม้
- อุปกรณ์ที่สำคัญล้มเหลว เนื่องระบบเกิดความชำรุดเสียหายไม่สามารถทำงานได้
- ไม่สามารถเข้ามาในการกีฬาแห่งประเทศไทยได้ เนื่องจากเกิดการก่อการร้าย/การประท้วง
- มีผู้เสียชีวิตจำนวนมาก เนื่องจากเกิดโรคระบาด เช่น ไข้หวัดนก โรคโควิด ๑๙
- อุปกรณ์เสียหายเนื่องจากไฟไหม้
- มีการโจมตีที่ระบบเครือข่ายของการกีฬาแห่งประเทศไทย
- ระบบเครือข่ายหลักห้องคอมพิวเตอร์ แผนกประมวลผลล่ม เนื่องจากเกิดพายุ

มีผลกระทบโดยตรงหรือทางอ้อมกับ การกีฬาแห่งประเทศไทยและมีความจาเป็นที่จะต้องประกาศสถานการณ์ภัยพิบัติ (T๐) เพื่อให้พนักงานและเจ้าหน้าที่เตรียมพร้อมรับมือ

- เมื่อกองสารสนเทศ การกีฬาแห่งประเทศไทย พบเหตุการณ์ เช่น อุปกรณ์เครื่องแม่ข่ายเกิดขัดข้องไม่สามารถใช้งานได้ เป็นระยะเวลาเกินกว่า ๒๔ ชั่วโมง ในช่วงเวลา ๘:๓๐–๑๖:๓๐ วันจันทร์–วันศุกร์ และได้แจ้งให้ผู้ว่าการกีฬาแห่งประเทศไทย พิจารณาแล้วเห็นว่าสามารถประกาศสถานการณ์ภัยพิบัติ (T๐) ได้

๓) ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศรอจนกว่าจะได้รับการอนุญาตให้เข้าพื้นที่ได้ (T๑) = (T๐) + ๑ ชม.

๔) ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศเข้าประเมินสถานการณ์ (T๒) = (T๑) + ๑ ชม. โดยใช้เอกสารข้อมูลแบบฟอร์มรายงานประเมินสถานการณ์ ทั้งนี้สามารถคัดเลือกทีมที่มีความเชี่ยวชาญในระบบที่มีความสำคัญเข้าไปประเมินสถานการณ์พร้อมกัน

๕) ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศรายงานผลการประเมินความเสียหายอันเกิดจากเหตุการณ์ดังกล่าวให้คณะกรรมการกอบกู้ภัยพิบัติรับทราบ

๖) คณะทำงานกอบกู้ภัยพิบัติพิจารณาเลือกแผนที่เหมาะสมในการกอบกู้ภัยพิบัติโดยอนุมัติจากข้อมูลที่ได้รับจากแบบฟอร์มรายงานประเมินสถานการณ์และแจ้งให้ผู้ประสานงานกอบกู้ภัยพิบัติจัดกลุ่มกู้คืนระบบที่เกี่ยวข้องเข้าปฏิบัติงานตามแผนการบริหารจัดการความต่อเนื่องทางธุรกิจ (T๓) = (T๒) + ๒ ชม.

๗) ทีมงานกู้คืนระบบเทคโนโลยีสารสนเทศดำเนินการกู้คืนระบบตามแผนการบริหารจัดการความต่อเนื่องทางธุรกิจและเมื่อดำเนินการแล้วเสร็จให้แจ้งหัวหน้าทีมงานกู้คืนระบบเทคโนโลยีสารสนเทศ

๘) ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศรายงานผลการปฏิบัติงานให้กับคณะทำงานกอบกู้ภัยพิบัติรับทราบ

๙) ประธานคณะทำงานกอบกู้ภัยพิบัติรายงานผลการดำเนินงานให้ผู้ว่าการกีฬาแห่งประเทศไทยรับทราบ

๑๐.) ทั้งนี้ ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศมีหน้าที่ประสานงานและแจ้งผลการแก้ไขระบบเทคโนโลยีสารสนเทศให้กับผู้เกี่ยวข้องรับทราบเป็นระยะๆ

<u>การติดต่อผู้ที่เกี่ยวข้อง</u>

๑) เมื่อมีการประกาศเหตุการณ์ภัยพิบัติ ให้ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศติดต่อผู้ที่เกี่ยวข้องตามที่ได้ระบุไว้ในแผนการบริการจัดการความต่อเนื่องทางธุรกิจ ตามภาคผนวกที่ ๑

๒) เมื่อสามารถติดต่อได้แล้ว ให้แจ้งข้อมูลดังต่อไปนี้ให้แก่บุคคลที่มีรายชื่ออยู่ใน ระบุไว้ในแผนการบริการจัดการความต่อเนื่องทางธุรกิจ ตามภาคผนวกที่ ๑ ทราบ:

- สถานะของภัยพิบัติที่เกิดขึ้น
- สิ่งที่ต้องดำเนินการ
- เตรียมพร้อมจนกว่าจะได้รับการติดต่อเพื่อแจ้งให้ทราบถึงขั้นตอนที่ต้องดำเนินการต่อไป หรือ
- ไปรายงานตัวที่ (สถานที่) และ (เวลา) โดยนำบัตรประจำตัวเจ้าหน้าที่และบัตรผ่านต่างๆ ไปด้วย
- กำชับไม่ให้เผยแพร่ข้อมูลสถานการณ์ออกสู่สาธารณะ
- หากไม่สามารถติดต่อบุคคลดังกล่าวได้ ให้ฝากข้อความให้โทรกลับ
- หากไม่สามารถติดต่อได้นานกว่าห้านาที ให้โทรหารายชื่อถัดไป
- รายงานรายชื่อบุคคลที่ไม่สามารถติดต่อได้ ให้กับคณะทำงานกอบกู้ภัยพิบัติทราบ

<u>การจัดตั้งศูนย์สั่งการ</u>

๑) เมื่อมีการประกาศเหตุภัยพิบัติ ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศจะกำหนดเจ้าหน้าที่อย่างน้อย ๒ คน ที่จะต้องเดินทางไปยังสถานที่ตั้งของศูนย์สั่งการและศูนย์สำรองข้อมูลให้พร้อมใช้งาน

๒) ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศ เป็นผู้ให้ข้อมูลสรุปแก่หน่วยงานที่เกี่ยวข้องให้ทราบเกี่ยวกับภัยพิบัติที่เกิดขึ้น โดยมีรายละเอียดข้อมูลที่จะต้องแจ้งดังต่อไปนี้

- ข้อมูลเกี่ยวกับภัยพิบัติที่เกิดขึ้น

- ข้อมูลเกี่ยวกับการตัดสินใจของคณะทำงานกอบกู้ภัยพิบัติ
- ข้อมูลเกี่ยวกับการติดต่อประสานงาน
- ข้อมูลอื่นๆ เพื่อให้หน่วยงานที่เกี่ยวข้องเตรียมพร้อมสำหรับกู้คืนจากภัยพิบัติ

<u>การสื่อสารกับบุคคลภายนอกการกีฬาแห่งประเทศไทย</u>

๑) ผู้อำนวยการฝ่ายสารสนเทศและวิชาการกีฬา และฝ่ายประชาสัมพันธ์จะเป็นผู้รับผิดชอบหลักในการแถลงข่าว หรือสื่อสารให้กับหน่วยงานภายนอกถึงเหตุการณ์วิกฤติที่เกิดขึ้น

๒) เจ้าหน้าที่ที่ไม่เกี่ยวข้องจะต้องไม่ให้ข้อมูลแก่บุคคลภายนอกรวมทั้งผู้สื่อข่าวเกี่ยวกับเหตุการณ์ที่เกิดขึ้นไม่ว่าจะในเรื่องใด

๓.๓ สถานการณ์และการกู้คืนระบบ

๑. การจัดกลุ่มเหตุการณ์สมมุติ

ตารางดังต่อไปนี้ เป็นรายละเอียดของสถานการณ์ต่างๆ โดยจึงจัดเป็นกลุ่มจำแนกตามประเภทของสถานการณ์ เพื่อให้ง่ายต่อการทำความเข้าใจและการดำเนินการ

ประเภท	สถานการณ์ความเสี่ยง	ประเภทภัยพิบัติ
IT-SAT – ๑	เข้าพื้นที่ได้ อุปกรณ์ไม่เสียหาย จำเป็นต้องย้ายระบบไปศูนย์สำรอง	มีการ Hack ระบบ ระบบไฟฟ้าขัดข้องเป็นระยะเวลานาน
IT- SAT – ๒	เข้าพื้นที่ไม่ได้ อุปกรณ์ไม่เสียหาย ไม่จำเป็นต้องย้ายระบบไปศูนย์สำรอง	เกิดจลาจลและการประท้วง โรคระบาด
IT- SAT – ๓	เข้าพื้นที่ไม่ได้ อุปกรณ์ไม่เสียหาย จำเป็นต้องย้ายระบบไปศูนย์สำรอง	น้ำท่วม เกิดจลาจลและการประท้วง เป็นระยะเวลานาน ระบบไฟฟ้าขัดข้อง
IT- SAT – ๔	เข้าพื้นที่ได้ อุปกรณ์เสียหาย จำเป็นต้องย้ายระบบไปศูนย์สำรอง	ไฟฟ้าลัดวงจร อุปกรณ์เสียหาย
IT- SAT – ๕	เข้าพื้นที่ไม่ได้ อุปกรณ์เสียหาย จำเป็นต้องย้ายระบบไปศูนย์สำรอง	ตึกถล่ม ไฟไหม้ พายุ สึนามิ

๒. ระยะเวลาในการกู้ระบบและการเลือกกลยุทธ์ที่จะนำมาใช้ในการกู้คืนระบบ

การกำหนดระยะเวลาในการกู้คืนระบบ จะต้องพิจารณาเวลาในแต่ละประเภทดังต่อไปนี้

๑) MTPD (Maximum Tolerable Period of Disruption) หมายถึง ระยะเวลาตั้งแต่ประกาศเหตุการณ์ภัยพิบัติ จนกระทั่งสามารถกลับมาปฏิบัติงาน หรือดำเนินงานได้ตามปกติ โดยไม่ก่อให้เกิดความเสียหายต่อองค์กร หรือการให้บริการ

๒) MBCO (Maximum Business Continuity Objective) หมายถึง ระดับการให้บริการขั้นต่ำที่สามารถให้ได้เมื่อดำเนินการตามแผนเตรียมพร้อมกรณีฉุกเฉินได้สำเร็จ

๓) RTO (Recovery Time Objective) หมายถึง ระยะเวลาที่สามารถกู้คืนระบบเพื่อให้สามารถปฏิบัติงานหรือให้บริการได้

๔) RPO (Recovery Point Objective) หมายถึง ศักยภาพการให้บริการที่ยอมรับได้หากเกิดเหตุการณ์ภัยพิบัติ

๕) (T๐) หมายถึง เวลาที่ปลัดกระทรวงสาธารณสุข ประกาศว่าเป็นเหตุภัยพิบัติ

๖) (T๑) หมายถึง เวลาที่ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศได้รับแจ้งให้สามารถเข้าพื้นที่เพื่อประเมินความเสียหายได้

๗) (T๒) หมายถึง เวลาที่ผู้ประสานงานกู้คืนระบบเทคโนโลยีสารสนเทศเข้าประเมินความเสียหายระบบเทคโนโลยีสารสนเทศ

๘) (T๓) หมายถึง เวลาที่เริ่มกระบวนการกอบกู้ระบบเทคโนโลยีสารสนเทศตามแผนเตรียมพร้อมกรณีฉุกเฉิน

๙) เวลาสำหรับค่าต่างๆ ที่ได้ระบุไว้ข้างต้นนั้น จะถูกนำมาใช้ในการพิจารณากลยุทธ์ในการกู้คืนระบบต่อไป

๓. กลยุทธ์ในการกู้คืนระบบ

กลยุทธ์ในการกู้คืนระบบ มีดังต่อไปนี้

๑) Hot Site: สถานที่สำรองจะต้องมีระบบสำรองเหมือนระบบงานหลัก รวมถึงข้อมูลของสถานที่หลักและสถานที่สำรองจะต้องมีเหมือนกันทั้งสองแห่งเพื่อให้สามารถให้บริการแทนได้ทันทีเมื่อเกิดเหตุการณ์ภัยพิบัติ

๒) Warm Site: สถานที่สำรองจะต้องมีการติดตั้งระบบเหมือนระบบงานหลัก แต่จะต้องมีการRestore ข้อมูลของแต่ละระบบ หรือตั้งค่าระบบของอุปกรณ์ต่างๆ เสียก่อนจึงจะสามารถให้บริการต่อไปได้

๓) Cold Site: สถานที่สำรองจะติดตั้งเฉพาะระบบโครงสร้างพื้นฐานที่จ าเป็น เช่น ระบบเครือข่าย ระบบปรับอากาศ ระบบไฟฟ้า หรือสายโทรศัพท์ เมื่อเกิดเหตุการณ์ภัยพิบัติ จะต้องจัดหาอุปกรณ์ต่างๆ มาติดตั้ง เพื่อให้สามารถให้บริการต่อไปได้

๓.๔ คู่มือและเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๑) มีการจัดทำคู่มือและแนวปฏิบัติในการดำเนินการตามแผน ตามตัวอย่างในภาคผนวกที่ ๑

๒) ฝึกอบรมเจ้าหน้าที่ บุคลากรเกี่ยวข้องกับระบบสารสนเทศภายในกกท.

๓.๕ การทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๑) ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงต่างๆ เกิดขึ้นดังนี้

- การเปลี่ยนแปลงลักษณะการปฏิบัติงานและระบบสารสนเทศที่สนับสนุนการดำเนินงาน
- การเปลี่ยนแปลงของสถานที่
- การเปลี่ยนแปลงผู้รับผิดชอบในส่วนต่างๆ
- การเปลี่ยนแปลงใดๆ ที่มีผลต่อการดำเนินงานตามแผนปฏิบัติการฉุกเฉิน

๓.๖ การจัดตั้งศูนย์คอมพิวเตอร์สำรอง

จัดให้มีการจัดตั้งศูนย์คอมพิวเตอร์สำรอง (Disaster recovery Site : DR Site) เพื่อรองรับแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ขององค์กร โดยมีการติดตั้งอุปกรณ์ระบบการสำรองข้อมูลรวมถึงอุปกรณ์ต่างๆ ที่จำเป็นให้การดำเนินการตามแผน

๑๐ การบริหารจัดการผู้ให้บริการภายนอก (Third party management)

วัตถุประสงค์

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย ป้องกันสินทรัพย์ขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

นโยบายและแนวปฏิบัติ

การใช้บริการด้านงานสารสนเทศจากหน่วยงานภายนอก บางครั้งหน่วยงานภายนอกอาจเข้าถึงระบบสารสนเทศ แก้ไข เปลี่ยนแปลง และประมวลผลระบบงานโดยไม่ได้รับอนุญาต ดังนั้น จึงต้องกำหนดแนวทางในการปฏิบัติงานของหน่วยงานภายนอกเพื่อความมั่นคง ปลอดภัย ของระบบสารสนเทศของการกีฬาแห่งประเทศไทย โดยนโยบายและแนวปฏิบัตินี้ต้องตรวจสอบ และประเมินตามระยะเวลา ๑ ครั้งต่อปี

๑. หน่วยงานภายนอก ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศและการสื่อสารของการกีฬาแห่งประเทศไทย จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้บริหารของหน่วยงาน

๒. จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

๑) เหตุผลในการขอใช้งาน

๒) ระยะเวลาในการใช้งาน

๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๔) การตรวจสอบ Mac Address ของอุปกรณ์ที่เชื่อมต่อ

๕) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓. หน่วยงานภายนอกที่ทำงานให้กับการกีฬาแห่งประเทศไทยทุกหน่วยงาน จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของการกีฬาแห่งประเทศไทย โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

๔. ผู้ให้บริการจากหน่วยงานภายนอก ต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งปรับปรุงให้ทันสมัย และหากมีการปรับเปลี่ยนจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

๕. เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๖. การกีฬาแห่งประเทศไทยมีสิทธิในการตรวจสอบตามสัญญาการใช้บริการด้านสารสนเทศ เพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานอย่างทั่วถึงตามข้อกำหนด

๗. ในการจ้างเหมาพัฒนา บำรุงรักษาระบบผู้ดูแลระบบต้องกำหนดการเข้าถึงระบบสารสนเทศสำหรับผู้ปฏิบัติงานจากภายนอก ได้แก่

๑) ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิ์ในการใช้งานเฉพาะที่จำเป็นขั้นต่ำ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๒) ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งานภายนอก ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศ ได้แก่ การกำหนดชื่อผู้ใช้ และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ

๓) ต้องบันทึกกิจกรรมการใช้งานข้อมูลเก็บเป็น Log File

๔) ในระบบที่มีความสำคัญสูงไม่อนุญาตให้ทดสอบบนระบบจริง (Production) แต่ต้องทดสอบบนระบบทดสอบ (Test) ให้เสร็จสิ้นก่อนจึงจะนำมาติดตั้งบนระบบจริง และก่อนการติดตั้งระบบจริงต้องได้รับอนุญาตจากผู้บริหารก่อน

ภาคผนวก

แบบฟอร์มขอใช้บริการระบบสารสนเทศ กกท.

กองสารสนเทศ ฝ่ายสารสนเทศและวิชาการกีฬา การกีฬาแห่งประเทศไทย

<u>ส่วนที่ 1</u> **สำหรับผู้ใช้ระบบ** **วันที่เริ่มขอใช้บริการ**.....

หน่วยงาน ฝ่าย/สำนัก.....**กอง**.....**งาน**.....

ข้อมูลผู้ข้อใช้บริการ

ชื่อ - สกุล (ภาษาไทย).....

ชื่อ - สกุล (ภาษาอังกฤษ).....

เลขที่บัตรพนักงาน / เลขที่บัตรประชาชน .....

ประเภทของผู้ขอใช้บริการ

☐ พนักงาน ☐ ผู้ช่วยปฏิบัติงาน ☐ อื่นๆ .....

มีความประสงค์ขอใช้ระบบสารสนเทศ :

☐ เปิดสิทธิ์ใช้งานระบบ (User Account, E-mail, Internet, WIFI, Intranet)

☐ ERP (กรอกแบบฟอร์มเพิ่มเติมที่เอกสาร FM-ITSAT-002)

☐ BPM (กรอกแบบฟอร์มเพิ่มเติมที่เอกสาร FM-ITSAT-003)

ทั้งนี้ข้าพเจ้าได้แนบสำเนาบัตรประจำตัวประชาชน / บัตรประจำตัวพนักงานมาพร้อมนี้แล้ว

ลงชื่อ.....(ผู้ขอใช้บริการ)
(.....)
ตำแหน่ง .....
วันที่.....

ลงชื่อ.....(ผู้บังคับบัญชา)
(.....)
ตำแหน่ง .....
วันที่.....

<u>ส่วนที่ 2</u> **สำหรับเจ้าหน้าที่ วันที่รับเรื่อง**...../...../..... เวลา .....

ชื่อ ..... หัวหน้างานบริการเทคโนโลยีสารสนเทศ

เห็นควร ☐ อนุมัติ ☐ ไม่อนุมัติ เนื่องจาก .....

ผู้อนุมัติ

☐ อนุมัติ ☐ ไม่อนุมัติ

ลงชื่อ.....(ผู้อำนวยการกองสารสนเทศ)
(.....)
วันที่.....

<u>ส่วนที่ 3</u> **สำหรับผู้ขอใช้ระบบ**

User: .....

*** กองสารสนเทศจะใช้ชื่อตามด้วย "." (จุด) และนามสกุล 1 ตัวแรกใน ภาษาอังกฤษเป็น username และ password ให้ท่าน เช่น นายสมชาย ใจดี username และ password จะเป็น somchai.j โดยระบบจะบังคับให้เปลี่ยน password ด้วยตนเองเมื่อเข้าสู่ระบบครั้งแรก**

ติดต่อสอบถามรายละเอียดได้ที่ งานบริการเทคโนโลยีสารสนเทศ กองสารสนเทศ โทร 8734