เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคง ในการติดต่อสื่อสารและเครือข่ายขององค์กร

การกีฬาแห่งประเทศไทย

ประกาศการกีฬาแห่งประเทศไทย

เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงในการติดต่อสื่อสารและเครือข่าย ของการกีฬาแห่งประเทศไทย (Communications and Network Security Management)

.....

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ผ่านเครือข่ายคอมพิวเตอร์ของการกีฬาแห่งประเทศไทย เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว การกีฬาแห่งประเทศไทย จึงกำหนดนโยบายและแนวปฏิบัติในการบริหารจัดการความมั่นคงในการติดต่อสื่อสารและเครือข่ายของการกีฬาแห่งประเทศไทย

อาศัยอำนาจตามความในมาตรา ๒๓ แห่งพระราชบัญญัติการกีฬาแห่งประเทศไทย พ.ศ. ๒๕๕๘ และที่แก้ไขเพิ่มเติม การกีฬาแห่งประเทศไทย จึงออกประกาศการกีฬาแห่งประเทศไทย เรื่องนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงในการติดต่อสื่อสารและเครือข่ายของการกีฬาแห่งประเทศไทย (Communications and Network Security Management) ดังต่อไปนี้

๑. การบริหารจัดการความมั่นคงในการติดต่อสื่อสารและเครือข่ายของการกีฬาแห่งประเทศไทย ตามประกาศนี้ประกอบด้วย ๒ ส่วน ดังนี้

๑.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร พนักงาน เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการจัดทำนโยบาย

(๒) นโยบายได้รับการจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวก ผ่านทางเว็บไซต์ของการกีฬาแห่งประเทศไทย

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๑.๒ ส่วนที่ว่าจะด้วยรายละเอียดของนโยบายประกอบด้วย ๒ ส่วน คือ

ส่วนที่ ๑ ความหมายและคำจำกัดความ

ส่วนที่ ๒ นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงในการติดต่อสื่อสารและเครือข่ายของการกีฬาแห่งประเทศไทย ซึ่งกำหนดผู้รับผิดชอบตามนโยบาย แบ่งสาระสำคัญออกเป็น ๖ หมวด ซึ่งมีสาระสำคัญสอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ดังนี้

(๑) นโยบาย ...

(๑) นโยบายและแนวปฏิบัติการติดตั้งซอฟแวร์ป้องกันโปรแกรมไม่ประสงค์ดี แนวทางตรวจหาการป้องกันการกู้คืน การให้ความเข้าใจและความตระหนักต่อผู้ใช้งาน

(๒) นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ต

(๓) นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

(๔) นโยบายการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน

(๕) นโยบายการควบคุมการเข้าถึง

(๖) การสื่อสารนโยบายบริหารจัดการความมั่นคงปลอดภัยในการติดต่อสื่อสารและเครือข่าย

๒.กำหนดให้ผู้บริหารเป็นผู้รับผิดชอบตามนโยบาย มีมาตรการและควบคุมตามแนวปฏิบัติดังต่อไปนี้

๒.๑ กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้ผู้บริหารระดับสูงสุดเป็นผู้รับผิดชอบต่อความเสี่ยง และความเสียหายหรืออันตรายที่เกิดขึ้น

๒.๒ การกีฬาแห่งประเทศไทย มีนโยบายไม่ตรวจตราการใช้เครือข่ายของผู้ใช้รายหนึ่งในกรณีปกติ แต่การกีฬาแห่งประเทศไทยสงวนสิทธิ์ในการติดตั้งเครื่องมือฮาร์ดแวร์ หรือซอฟต์แวร์เพื่อบันทึกและเฝ้าระวังการใช้คอมพิวเตอร์และเครือข่าย เพื่อคงไว้ซึ่งการให้บริการอย่างปลอดภัย มีประสิทธิภาพและเป็นไปตามกฎหมายบัญญัติไว้ ทั้งนี้ การกีฬาแห่งประเทศไทยคงไว้ซึ่งอำนาจในการจำกัด ระงับหรือเพิกถอนสิทธิการใช้ระบบสารสนเทศและดำเนินการสอบสวน เมื่อได้รับรายงานการแจ้งเตือน หรือการตรวจพบการกระทำประการใด ๆ ที่อาจก่อให้เกิดปัญหาความมั่นคงปลอดภัย ปัญหาเสถียรภาพหรือการกระทำที่ขัดต่อนโยบายหรือพระราชบัญญัติการกีฬาแห่งประเทศไทย หรือกฎหมายที่เกี่ยวข้อง

๒.๓ ฝ่ายสารสนเทศและวิชาการกีฬา มีหน้าที่ออกระเบียบข้อบังคับในการจำกัด ระงับ หรือเพิกถอนสิทธิการใช้เครือข่ายของผู้ฝ่าฝืนระเบียบข้อบังคับ ตลอดจนระงับหรือจำกัดการเข้าถึงคอมพิวเตอร์ที่มีข้อมูลขัดต่อระเบียบข้อบังคับ นโยบาย พระราชบัญญัติการกีฬาแห่งประเทศไทย พ.ศ. ๒๕๕๘ และที่แก้ไขเพิ่มเติม หรือกฎหมายที่เกี่ยวข้อง ในกรณีสำคัญให้ฝ่ายสารสนเทศและวิชาการกีฬา รายงานการฝ่าฝืนระเบียบข้อบังคับให้หน่วยงานต้นสังกัดหรือการกีฬาแห่งประเทศไทย เพื่อพิจารณาลงโทษ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๓ สิงหาคม พ.ศ. ๒๕๖๓

(นายก้องศักด ยอดมณี)
ผู้ว่าการการกีฬาแห่งประเทศไทย

บทนำ

เพื่อให้การติดต่อสื่อสารและเครือข่ายของการกีฬาแห่งประเทศไทยมีความมั่นคงปลอดภัย เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ๒๕๕๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ๒๕๔๔ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ การกีฬาแห่งประเทศไทย จึงกำหนดนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงในการติดต่อสื่อสารและเครือข่ายขององค์กรประกอบด้วยนโยบายและแนวปฏิบัติ หลัก ๖ ด้าน ดังต่อไปนี้

หมวดที่ ๑ การติดตั้งซอฟแวร์ป้องกันป้องกันโปรแกรมไม่ประสงค์ดี แนวทางตรวจหาการป้องกัน การกู้คืน การให้ความเข้าใจและความตระหนักต่อผู้ใช้งาน

๑.๑ นโยบายการติดตั้งซอฟแวร์ป้องกันป้องกันโปรแกรมไม่ประสงค์ดีและแนวทางตรวจหา (Network Security Management)

๑.๒ นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy)

๑.๓ นโยบายการให้ความรู้ ความเข้าใจและความตระหนักของผู้ใช้งาน

หมวดที่ ๒ การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ต (Website and Internet Security Policy)

หมวดที่ ๓ การรักษาความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communication Security Management)

๓.๑ การบริหารจัดการความมั่นคงเครือข่าย (Network Security Management)

๓.๒ การถ่ายโอนข้อมูลสารสนเทศ (Information Transfer)

หมวดที่ ๔ การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)

หมวดที่ ๕ การควบคุมการเข้าถึง (Access Control)

๕.๑ นโยบายการควบคุมการเข้าถึง (Access Control Policy)

๕.๒ การเข้าถึงเครือข่ายและบริการคอมพิวเตอร์ (Access to network and network services)

หมวดที่ ๖ การสื่อสารนโยบายการบริหารจัดการความมั่นคงปลอดภัยในการติดต่อสื่อสารและเครือข่าย (Communications And Network Security Management)

สารบัญ

ส่วนที่ ๑
ความหมายและคำจำกัดความ

๑. **กกท.** หมายความว่า การกีฬาแห่งประเทศไทย

๒. **หน่วยงาน** หมายความว่า ฝ่าย/สำนัก/กอง/งาน ที่เป็นส่วนงานตามโครงสร้างของการกีฬาแห่งประเทศไทย

๓. **หน่วยงานภายนอก** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของการกีฬาแห่งประเทศไทยโดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

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

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

๖. **ผู้บังคับบัญชา** หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

๗. **ผู้ดูแลระบบ (System administrator)** หมายความว่า ผู้ซึ่งได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่ดูแลเซิร์ฟเวอร์ ระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ให้บริการได้อย่างมีเสถียรภาพ

๘. **ผู้พัฒนาระบบ** หมายความว่า ผู้ซึ่งได้รับมอบหมายให้รับผิดชอบในการพัฒนาระบบสารสนเทศ

๙. **เจ้าหน้าที่** หมายความว่า บุคลากรทุกประเภทของการกีฬาแห่งประเทศไทย

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

๑๑. **การรักษาความมั่นคงปลอดภัย** หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑๒. **มาตรฐาน (Standard)** หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

๑๓. **วิธีการปฏิบัติ (Procedure)** หมายความว่า รายละเอียดที่บอกขั้นตอนเป็นข้อๆที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

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

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

๑๖. **เจ้าของข้อมูล** หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๑๗. **สินทรัพย์** หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เซิร์ฟเวอร์ ระบบสารสนเทศ ระบบเครือข่ายอุปกรณ์เครือข่าย เลขที่อยู่ไอพีโดเมนเนม รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อหน่วยงาน

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

๑๙. **ระบบสารสนเทศ** หมายความว่า ระบบงานของการกีฬาแห่งประเทศไทย ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศในองค์กร สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุม การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการโปรแกรมประยุกต์ ข้อมูลสารสนเทศ ฯลฯ

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

๒๑. **จดหมายอิเล็กทรอนิกส์ (e-mail)** หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่ายภาพกราฟิกภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับผ่านโพรโทคอลต่าง ๆ เช่น SMTP, POP๓, IMAP ฯลฯ

๒๒. **สื่อบันทึกพกพา (portable media)** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD , DVD , flash drive, external hard disk ฯลฯ

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

๒๔. **รหัสผ่าน (password)** หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือ ในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

๒๕. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานและหน่วยงานภายนอก เข้าถึงหรือใช้งานระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบเครือข่าย ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

๒๖. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายความว่า การรักษาไว้ซึ่งความลับ (confidentiality) ความครบถ้วนถูกต้อง (integrity) และความพร้อมใช้ (availability) ของสารสนเทศและระบบเครือข่ายรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธ ความรับผิด(non-repudiation) และความน่าเชื่อถือ (reliability)

๒๗. **การพิสูจน์ยืนยันตัวตน (authentication)** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ยืนยันตัวตนของผู้ใช้บริการระบบทั่วไป แล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน

๒๘. **WEP (wired equivalent privacy)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

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

๓๐. **VPN (virtual private network)** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ - ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่ สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๓๑. **แผนผังระบบเครือข่าย (network diagram)** หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของการกีฬาแห่งประเทศไทย

ส่วนที่ ๒
นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศการกีฬาแห่งประเทศไทย

หมวดที่ ๑ การติดตั้งซอฟแวร์ป้องกันป้องกันโปรแกรมไม่ประสงค์ดีและแนวทางตรวจหาป้องกันและการกู้คืน รวมถึงสร้างความรู้ ความเข้าใจและความตระหนักต่อผู้ใช้งาน

๑.๑ นโยบายการติดตั้งซอฟแวร์ป้องกันป้องกันโปรแกรมไม่ประสงค์ดีและแนวทางตรวจหาและป้องกัน (Malicious Software Prevention)

วัตถุประสงค์ เพื่อควบคุมและป้องกันซอฟต์แวร์และข้อมูลขององค์กร จากซอฟต์แวร์อันตรายหรือไวรัสคอมพิวเตอร์รวมถึงมีแนวทางการตรวจสอบโปรแกรมไม่ประสงค์ดี

แนวปฏิบัติ

๑.๑.๑. การนำซอฟต์แวร์จากภายนอกมาใช้งานภายในองค์กร ผู้ใช้งานต้องทำการตรวจสอบซอฟแวร์ ดังกล่าวให้แน่ใจว่าซอฟต์แวร์นั้นๆ ไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่ โดยให้กองสารสนเทศตรวจสอบให้

๑.๑.๒. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งซอฟแวร์ป้องกันโปรแกรมไม่ประสงค์ดีในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และเครื่องเซิร์ฟเวอร์ทุกเครื่อง

๑.๑.๓. ผู้ดูแลระบบต้องกำหนดให้โปรแกรมไม่ประสงค์ดีทำงานพร้อมกันกับการเริ่มทำงานของระบบ ประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะที่มีการใช้ระบบด้วยนอกจากนี้ผู้ดูแลระบบ ต้องมีการปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ

๑.๑.๔. มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

๑.๑.๕. ผู้ดูแลระบบต้องทำการตรวจทานระบบข้อมูลเพื่อตรวจหาไวรัสและซอฟต์แวร์อันตรายอยู่เป็นประจำ

๑.๑.๖. ห้ามมิให้เจ้าหน้าที่ดำเนินการใด ๆ ที่เกี่ยวกับการพัฒนาไวรัสหรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ

๑.๑.๗. ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกองค์กรมาใช้ผู้ใช้งานสื่อข้อมูลนั้นต้อง ตรวจสอบไวรัสคอมพิวเตอร์ก่อนใช้งานทุกครั้ง

๑.๑.๘. มีเจ้าหน้าที่ติดตามและแจ้งเหตุภัยคุกคามการแจ้งเตือนภัยจากช่องโหว่ต่าง ๆ มีการตรวจสอบช่องโหว่และให้ข้อแนะนำในการป้องกันภัยคุกคามสารสนเทศ

๑.๒ นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy)

วัตถุประสงค์ เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย หรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้

แนวปฏิบัติ

ในการคัดเลือกการสำรองข้อมูล ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพ พร้อมใช้งานตามแนวทางต่อไปนี้

๑.๒.๑. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบ สารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒.๒. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

๑.๒.๒.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้และความถี่ในการสำรอง

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

๑.๒.๒.๓ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๑.๒.๒.๔ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูล Configuration ข้อมูลในฐานข้อมูล เป็นต้น

๑.๒.๒.๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๑.๒.๒.๖ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๑.๒.๒.๗ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๑.๒.๒.๘ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูล ที่ได้สำรองเก็บไว้ตรวจสอบ และทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติ ในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๑.๒.๒.๙ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒.๒. แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติ

อย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียม ความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งาน ตามภารกิจต่อไปนี้

๑.๒.๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์โดยมีรายละเอียดอย่างน้อย ดังนี้

๑.๒.๒.๑.๑ มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๑.๒.๒.๑.๒ มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น

๑.๒.๒.๑.๓ มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๑.๒.๒.๑.๔ มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

๑.๒.๒.๑.๕ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ซอฟต์แวร์เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๑.๒.๒.๑.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๑.๒.๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่าง เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๑.๒.๓. แนวปฏิบัติในการสำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูลและสามารถนำข้อมูลกลับมาใช้งานได้ ในกรณีที่ ไวรัสคอมพิวเตอร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล โดยมีมาตรการ ดังนี้

๑.๒.๓.๑ การสำรองข้อมูล

๑.๒.๓.๑.๑ ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเองตามความเหมาะสมของแต่ละระบบไม่ต่ำกว่า ๑ ครั้งต่อเดือน

๑.๒.๓.๑.๒ ผู้ดูแลระบบต้องตั้งค่าสำรองข้อมูลอัตโนมัติสำหรับเครื่องคอมพิวเตอร์แม่ข่ายของเว็บไซต์ (Web Server)

๑.๒.๓.๑.๓ ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป จะต้องทำการสำรองข้อมูล ในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม ไม่ต่ำกว่า ๑ ครั้งต่อเดือน ตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒.๓.๑.๔ หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญมากให้พิมพ์ (Print) ออกมาเก็บสำรองไว้ในรูปของเอกสารกระดาษ (Hard Copy)

๑.๒.๓.๑.๕ แผนกผู้ดูแลระบบต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบที่สำคัญ โดยต้องมีการทดสอบอย่างน้อยปีละหนึ่งครั้ง ซึ่งการทดสอบดังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริงแต่ทดสอบบนระบบทดสอบ

๑.๒.๓.๑.๖ ผู้ดูแลระบบต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์ขององค์กรและเก็บรักษาไว้ตาม แนวทางปฏิบัติการเก็บรักษาข้อมูลขององค์กร

๑.๒.๓.๑.๗ การกู้คืนข้อมูล เพื่อให้การฟื้นฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการหยุดทำงานของการประมวลผลโปรแกรม ทำให้ไม่สามารถบันทึกข้อมูลได้ทันเวลา หรือไม่สามารถใช้งานคอมพิวเตอร์ได้ตามปกติ มีมาตรการในการกู้คืนข้อมูล ดังนี้

๑.๒.๓.๑.๘ ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา

๑.๒.๓.๑.๙ ผู้ดูแลระบบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟต์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหาย

๑.๒.๓.๑.๑๐ ผู้ดูแลระบบจะต้องทำการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

๑.๓ นโยบายการให้ความรู้ความเข้าใจและความตระหนักต่อผู้ใช้งาน

วัตถุประสงค์ เพื่อให้ความรู้ความเข้าใจ และความตระหนักในการใช้งานระบบคอมพิวเตอร์ระบบเครือข่ายและการสื่อสารของ กกท. ให้มีความมั่นคงปลอดภัยจากภัยคุกคามสารสนเทศ

แนวปฏิบัติ

๑.๓.๑ เจ้าหน้าที่ กกท. ฯ เจ้าหน้าที่ กกท. ฯ ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานและมีรายการดังต่อไปนี้เป็นอย่างน้อย

- นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสารของการกีฬาแห่งประเทศไทย
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
- พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
- มีการสอดแทรกเนื้อหา ด้านความปลอดภัยทางระบบสารสนเทศลงในการอบรมการใช้งานระบบสารสนเทศต่างๆ ของ กกท.

๑.๓.๒ ให้ความรู้ความเข้าใจ ในลักษณะของเกร็ดความรู้ที่ผู้ใช้สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยประชาสัมพันธ์ตามบอร์ดความรู้ ในสถานที่ต่างๆ ในองค์กร

๑.๓.๓ สนับสนุนให้ผู้ใช้มีส่วนร่วม และนำสู่การปฏิบัติตลอดจนติดตามประเมินผลและสำรวจความต้องการของผู้ใช้บริการ

หมวดที่ ๒ การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ต

วัตถุประสงค์ เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย หรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูลสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้

แนวปฏิบัติ

๑. ให้จัดทำ Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของ กกท. และเครือข่ายข้อมูลทั้งหมด

๒. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๓. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

๔. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีการรายงานให้ ผู้บังคับบัญชาทราบ

๕. มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต

๖. กกท. มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุก รุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๗. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย ได้แก่ Proxy, Firewall และ IPS/IDS

๘. เครื่องคอมพิวเตอร์ทุกเครื่อง ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส

๙. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ กกท. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

๑๐. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ กกท. โดยผ่านความเห็นชอบจากผู้บริหารของหน่วยงานต้นสังกัด

๑๑. ผู้ใช้งานต้องไม่กระทำการเปิดเผยข้อมูลสำคัญเกี่ยวกับงานของ กกท. ที่ไม่เข้าหลักเกณฑ์ การเปิดเผยประกาศอย่างเป็นทางการ ผ่านทางอินเทอร์เน็ต

๑๒. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บน อินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๑๓. ผู้ใช้งานต้องปฏิบัติตามพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ อย่างเคร่งครัด

๒.๑ มาตรการเครือข่าย

๒.๑.๑. สิทธิการใช้เครือข่าย

๒.๑.๑.๑. สิทธิการใช้เครือข่ายเป็นสิทธิพิเศษเฉพาะ (privilege) ที่การกีฬาแห่งประเทศไทย มอบให้บุคคลหรือหน่วยงานที่ได้รับสิทธิไม่สามารถโอนสิทธิให้แก่บุคคลอื่นหรือหน่วยงานอื่นได้

๒.๑.๑.๒. ผู้ใช้ต้องเคารพในสิทธิส่วนบุคคลและไม่ละเมิดความเป็นส่วนตัวของผู้ใช้รายอื่น

๒.๑.๑.๓. ผู้ใช้ต้องใช้ระบบเครือข่ายคอมพิวเตอร์ตามมารยาทและจรรยาบรรณของการใช้เครือข่ายตามที่การกีฬาแห่งประเทศไทยกำหนดและตามวิถีสากล

๒.๑.๒. การใช้งานที่ไม่อนุญาตให้ปฏิบัติ

๒.๑.๒.๑. การใช้ระบบเครือข่ายคอมพิวเตอร์เพื่อกระทำสิ่งที่ผิดกฎหมาย

๒.๑.๒..๒. การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ด้วยบัญชีของผู้อื่นทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของบัญชี

๒.๑.๒..๓. การเข้าถึงข้อมูลของผู้อื่นเพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม โดยไม่ได้รับอนุญาต

๒.๑.๒..๔. การเผยแพร่ข้อมูลของผู้ใช้หรือของหน่วยงานโดยไม่ได้รับอนุญาต

๒.๑.๒..๕. การใช้งานที่เป็นสาเหตุให้ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เสียหายหรือมีผลต่อประสิทธิภาพการทำงานของระบบ

๒.๑.๒..๖. การพยายามทำลายหรือทำลายระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

๒.๑.๒..๗. การใช้หรือเผยแพร่ซอฟต์แวร์โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

๒.๑.๒.๘. การลักลอบดักจับข้อมูลในระบบเครือข่ายคอมพิวเตอร์

๒.๑.๒..๙. การปลอมแปลงเป็นบุคคลอื่นเพื่อสร้างความเข้าใจผิดให้แก่ระบบคอมพิวเตอร์และผู้ใช้อื่น

๒.๑.๒..๑๐. การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อสร้างความเสียหายแก่ระบบคอมพิวเตอร์หรือเครือข่ายอื่น

๒.๑.๒.๑๑. การเผยแพร่และ/หรือการเข้าถึงสื่อลามกอนาจาร

๒.๑.๒.๑๒. การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อเปิดให้บริการใด ๆ โดยไม่ได้รับอนุญาต

๒.๑.๒.๑๓. การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อประกอบธุรกิจ

๒.๑.๒.๑๔. การนำไอพีแอดเดรสของการกีฬาแห่งประเทศไทยไปจดทะเบียนชื่อโดเมนอื่นนอกเหนือจากชื่อโดเมน sat.or.th โดยไม่ได้รับอนุญาต

๒.๑.๒.๑๕. การใช้ระบบเครือข่ายคอมพิวเตอร์อื่นใดที่ขัดต่อนโยบายและระเบียบของการกีฬาแห่งประเทศไทย

๒.๒ การจัดแบ่งเครือข่ายภายใน (Segregation in Network)

๒.๒.๑ ออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) โซนพิเศษ (DMZ Zone) และ โซนภายนอก (External Zone) เพื่อทำให้การควบคุม และปูองกันการบุกรุกได้อย่างเป็นระบบ

๒.๒.๒ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

หมวดที่ ๓ การรักษาความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

๓.๑ การบริหารจัดการความมั่นคงเครือข่าย

วัตถุประสงค์

เพื่อควบคุมการใช้งานเครือข่าย และกรองแพ็กเก็ตและบริการที่ผ่านเข้ามาในเครือข่ายองค์กร

แนวปฏิบัติ

๓.๑.๑ อนุญาตเฉพาะบริการเครือขายที่จำเป็นต่อการใช้งาน บริการเครือขายอื่น ๆ ที่เหลือปิดให้หมด

๓.๑.๒ ไม่อนุญาตให้สแกนเพื่อตรวจสอบเครือข่ายด้วยโปรแกรมประเภท Network Scanning Tools เช่น Nmap เป็นต้น

๓.๑.๓ ปิดบริการที่ไม่จำเป็นบนไฟรวอลล์

๓.๑.๔ จำกัดบริการเครือข่ายที่ทำงานบนไฟร์วอลล์ให้มีน้อยที่สุด โดยให้แยกบริการอื่น ๆ เหล่านั้น โดยเจาะจงเครื่องที่ต้องใช้งานตามความจำเป็น

๓.๑.๕ จำกัดชื่อบัญชีผู้ใช้บนเครื่องไฟร์วอลล์ให้มีน้อยที่สุด และไม่เข้าถึงไฟร์วอลล์ โดยใช้ชื่อบัญชีผู้ใช้ที่เป็น Root หรือ Administrator

๓.๑.๖ เปลี่ยนรหัสผ่านสำหรับ Root หรือ Administrator ที่ผู้ขายกำหนดมาให้เป็นรหัสอื่นที่ยากต่อการเดา

๓.๑.๗ ควรใช้ระบบอื่นทำงานรวมกับไฟร์วอลล์ ได้แก่ ระบบป้องกันการบุกรุก (IPS) ไฟร์วอลล์ส่วนตัว (Personal Firewall) โปรแกรมป้องกันไวรัส (Antivirus) ซึ่งเป็นการเสริมการรักษาความมั่นคงปลอดภัยภาพรวมได้สูงขึ้น

๓.๑.๘ กำหนดกฎในไฟร์วอลล์ให้กรองทิ้งแพ็กเก็ตที่ไม่ประสงค์ดีตามรายการช่องโหว่ที่แพร่ระบาดอยู่เสมอ

๓.๑.๙ ป้องกันการเขาถึงทางกายภาพต่อไฟร์วอลล์ให้มีความแข็งแกร่ง โดยจัดทำเป็นห้องที่มีการควบคุม การเข้า-ออกอย่างเข้มงวด

๓.๑.๑๐ หมั่นตรวจสอบกฎของไฟร์วอลล์เพื่อกำจัดกฎที่ไม่มีความจำเป็นทิ้งไป เพื่อเพิ่มประสิทธิภาพของการประมวลผลกฎที่กำหนดไว้ของไฟร์วอลล์

๓.๑.๑๑ เมื่อเพิ่มกฎข้อใหม่เข้าไปในไฟร์วอลล์ ตรวจสอบว่ากฎที่ใส่เขาไปนั้นไมขัดแย้งกับกฎที่มีอยู่แล้ว เดิมรวมทั้งทดสอบด้วยว่าไฟร์วอลล์สามารถป้องกันได้จริงตามกฎข้อใหม่นั้น

๓.๑.๑๒ ตรวจสอบว่ากฎที่กำหนดไวบนไฟร์วอลล์ไม่มีข้อใดขัดแย้งกับนโยบายความมั่นคงปลอดภัยขององค์กรอย่างน้อยควรทำปีละครั้ง

๓.๑.๑๓ ไม่อนุญาตให้เข้าถึงไฟร์วอลล์จากทางไกลโดยโปรแกรมประเภท Telnet หรือแม้แต่โดยการเข้าถึงให้ทำได้จากตัวเครื่องไฟร์วอลล์โดยตรง

๓.๑.๑๔ สร้างความแข็งแกร่งให้กับระบบปฏิบัติการของไฟร์วอลล์ โดยการ Update Patch อยู่เสมอตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๑.๑๕ ตรวจสอบโปรแกรมสำหรับระบบปฏิบัติการของไฟร์วอลล์อย่างสม่ำเสมอ

๓.๑.๑๖ ก่อนการอัพเกรดหรือแก้ไขของโหว่ของไฟร์วอลล์ให้ทำการสำรองข้อมูลแบบ Full Backup ของเครื่อง ไฟร์วอลล์นั้นเก็บไว้ก่อน หากมีปัญหาจะได้นำกลับมาติดตั้งและใช้งานได้อย่างรวดเร็ว

๓.๑.๑๗ ใช้ไฟร์วอลล์รวมกับเราท์เตอร์เพื่อป้องกันปัญหา DoS (Denial of Service) และปัญหาการเจาะ ระบบเข้าสู่ไฟร์วอลล์ได้โดยตรง

๓.๑.๑๘ใช้ไฟร์วอลล์เพื่อกั้นเครือข่ายภายใน เช่น เครือข่ายส่วนนั้นอนุญาตให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นในการเข้าถึง

๓.๑.๑๙ บันทึกข้อมูล Log ของการเข้าถึงไฟร์วอลล์เก็บไว้รวมทั้งหากไฟร์วอลล์มีขีดความสามารถในการแจ้งเตือนให้เปิดใช้ขีดความสามารถนี้ด้วย

๓.๑.๒๐ ใช้เซิร์ฟเวอร์ เช่น Syslog แยกต่างหากอีกเครื่องหนึ่งจากเครื่องของไฟร์วอลล์เพื่อเก็บบันทึกข้อมูล Log ไว้บนเซิร์ฟเวอร์นั้น ซึ่งจะทำให้การเปลี่ยนแปลงแก้ไขข้อมูล Log โดยผู้บุกรุกทำได้ยากขึ้น

๓.๑.๒๑ หากหน่วยงานอื่นต้องการนำระบบขึ้น จะต้องทำเป็นหนังสือผ่านผู้อำนวยการกองสารสนเทศแจ้งเจ้าหน้าที่ให้ดำเนินการเป็นกรณีไป

๓.๒ การถ่ายโอนข้อมูลสารสนเทศ

วัตถุประสงค์ เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กรและถ่ายโอน
กับหน่วยงานภายนอก

แนวปฏิบัติ

๓.๒.๑ นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

๓.๒.๑.๑. หน่วยงานภายนอก ที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศและการสื่อสารของการกีฬาแห่งประเทศไทย จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้บริหารของหน่วยงาน

๓.๒.๑.๒. จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

- เหตุผลในการขอใช้งาน
- ระยะเวลาในการใช้งาน
- การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
- การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓.๒.๑.๓. หน่วยงานภายนอกที่ทำงานให้กับการกีฬาแห่งประเทศไทยทุกหน่วยงาน จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของการกีฬาแห่งประเทศไทย โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

๓.๒.๑.๔. ผู้ให้บริการจากหน่วยงานภายนอก ต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งปรับปรุงให้ทันสมัย และหากมีการปรับเปลี่ยนจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

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

๓.๒.๑.๖. การกีฬาแห่งประเทศไทยมีสิทธิในการตรวจสอบตามสัญญาการใช้บริการด้านไอซีที เพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานอย่างทั่วถึงตามข้อกำหนด

๓.๒.๑.๗. ในการจ้างเหมาพัฒนา บำรุงรักษาระบบผู้ดูแลระบบต้องกำหนดการเข้าถึงระบบสารสนเทศสำหรับผู้ปฏิบัติงานจากภายนอก ได้แก่

๓.๒.๑.๗.๑. ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิในการใช้งานเฉพาะที่จำเป็นขั้นต่ำ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๓.๒.๑.๗.๒. ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งานภายนอก ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศ ได้แก่ การกำหนดชื่อผู้ใช้ และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ

๓.๒.๑.๗.๓. ต้องบันทึกกิจกรรมการใช้งานข้อมูลเก็บเป็น Log File

๓.๒.๑.๗.๔. ในระบบที่มีความสำคัญสูงไม่อนุญาตให้ทดสอบบนระบบจริง (Production) แต่ต้องทดสอบบนระบบทดสอบ (Test) ให้เสร็จสิ้นก่อนจึงจะนำมาติดตั้งบนระบบจริง และก่อนการติดตั้งระบบจริงต้องได้รับอนุญาตจากผู้บริหารก่อน

๓.๒.๒ ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer) การทำข้อตกลงต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๓.๒.๓ ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements) ต้องจัดให้มีการลงนามในสัญญาระหว่างหน่วยงานและหน่วยงานภายนอกว่าจะไม่เปิดเผยความลับของหน่วยงาน (Non-Disclosure Agreement : NDA)

หมวดที่ ๔ การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน

วัตถุประสงค์ เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ โดยผู้ประกอบธุรกิจต้องจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโดยคำนึงถึงลักษณะ ขนาด และความซับซ้อนของการประกอบธุรกิจ รวมทั้งกฎเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง

แนวทางปฏิบัติ

๔.๑ เครื่องคอมพิวเตอร์ที่ กกท. อนุญาตให้ผู้ใช้งาน ใช้งานเป็นสินทรัพย์ของ กกท. ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของ กกท.

๔.๒ ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆของ กกท. และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๔.๓ ไม่อนุญาตให้ ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ในเครื่องคอมพิวเตอร์ส่วนบุคคลของ กกท. เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่ของกองสารสนเทศ หรือผู้ดูแลระบบของ กกท.

๔.๔ การส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องได้รับการพิจารณาจากกองสารสนเทศ

๔.๕ ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๔.๖ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น

๔.๗ ผู้ใช้งาน ต้องใช้งานโปรแกรมรักษาจอภาพ (Screen saver) เพื่อให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

๔.๘ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของ กกท. ยกเว้นจะได้รับการพิจารณาอนุญาตจากกองสารสนเทศก่อนการใช้งาน

๔.๙ ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ส่วนบุคคลต้องมีการ Update service pack และhot fix ที่เป็น version ล่าสุดเสมอ โดยอัตโนมัติหรือมีเจ้าหน้าที่ดำเนินการ

๔.๑๐ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลจะต้องกำหนดโดยเจ้าหน้าที่ของกองสารสนเทศ หรือผู้ดูแลระบบของหน่วยงานใน กกท. ที่มีศูนย์สารสนเทศ เท่านั้น

๔.๑๑ การเคลื่อนย้ายเครื่องคอมพิวเตอร์จากจุดเชื่อมต่อเครือข่ายเดิมไปยังจุดเชื่อมต่อเครือข่ายใหม่ภายในหน่วยงานใน กกท. จะต้องแจ้งกองสารสนเทศดำเนินการให้เท่านั้น

๔.๑๒ กรณีส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมเสร็จแล้วต้องให้เจ้าหน้าที่กองสารสนเทศ หรือผู้ดูแลระบบของหน่วยงานใน กกท. ที่มีศูนย์สารสนเทศ เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของ กกท.

๔.๑๓ ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ส่วนบุคคลของ กกท. ทุกเครื่องเว้นแต่ได้รับความเห็นชอบจากกองสารสนเทศ

๔.๑๔ เครื่องคอมพิวเตอร์ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสโดยโปรแกรมป้องกันไวรัสของ กกท. จากเจ้าหน้าที่ของกองสารสนเทศ

๔.๑๕ ผู้ใช้งานไม่ควรสร้าง short-cut หรือปุ่มกดง่าย บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ กกท.

๔.๑๖ ต้องทำการล้างข้อมูลในเครื่องคอมพิวเตอร์ทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง

หมวดที่ ๕ การควบคุมการเข้าถึง

วัตถุประสงค์ เพื่อป้องกันให้ผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูลทำการเข้าถึงระบบสารสนเทศและข้อมูลบนระบบสารสนเทศโดยไม่ได้รับอนุญาต

๕.๑ นโยบายการควบคุมการเข้าถึง

แนวทางปฏิบัติ

๕.๑.๑ ออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งานกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External zone) และโซนพิเศษ (DMZ Zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๕.๑.๒ จำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๑.๓ จำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๕.๑.๔ มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

๕.๑.๕ กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบ

๕.๑.๖ ระบบเครือข่ายทั้งหมดของ กกท. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก กกท. ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๕.๑.๗ มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของ กกท. ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่าน ระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๕.๑.๘ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๑.๑๑ ใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๑.๑๒ การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่กองสารสนเทศเท่านั้น

๕.๑.๑๓ ผู้ใช้งาน ที่ต้องการนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด เพื่อให้การเชื่อมต่ออุปกรณ์ต่างๆ เป็นไปตามมาตรฐาน และไม่เกิดผลกระทบกับระบบเครือข่ายคอมพิวเตอร์ส่วนรวมของ กกท.

๕.๑.๑๔ ห้ามบุคคลใดกระทำการเคลื่อนย้าย หรือทำการใดๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการ เพราะอาจก่อให้เกิดความเสียหายแก่ระบบเครือข่ายหลักของ กกท. ได้

๕.๑.๑๕ ในกรณีที่ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติต่อระบบเครือข่ายหลักของ กกท. กองสารสนเทศ อาจจะหยุดให้บริการจากระบบเครือข่ายกลางโดยไม่มีการแจ้งให้ทราบล่วงหน้า จนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน

๕.๑.๑๗ ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายแบบไร้สายด้วย (Wireless Network)

๕.๒ การเข้าถึงเครือข่ายและบริการคอมพิวเตอร์

๕.๒.๑ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

แนวทางปฏิบัติ

๕.๒.๑.๑ การใช้บริการเครือข่าย ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของการให้บริการ ได้แก่ โซนภายใน (Internal Zone) และโซนภายนอก (External Zone) และโซนพิเศษ (DMZ Zone) เพื่อควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ และต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) ผู้ดูและระบบต้องกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งาน ให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาต ให้เข้าถึงเท่านั้น พร้อมทั้งจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการกองสารสนเทศหรือ ผู้ดูแลระบบที่ได้รับมอบหมาย ก่อนที่จะใช้งานในทุกกรณี

(๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยผู้ดูแลระบบต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

๕.๒.๑.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงานจะต้องได้รับการอนุมัติจากผู้อำนวยการกองสารสนเทศก่อนทุกครั้ง และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานจะต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการขออนุญาตอย่างเพียงพอ

(๒) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (User Name) ทุกครั้ง และผู้ดูแลระบบจะต้องตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของการกีฬาแห่งประเทศไทย

(๓) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของการกีฬาแห่งประเทศไทยโดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

(๔) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตที่ใช้ไว้ตลอดเวลาโดยไม่จำเป็น ควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๕.๒.๑.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ผู้ดูและระบบต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๑) การควบคุมการใช้งานอย่างเหมาะสม และจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้โดยผู้ขอใช้บริการ จะต้องได้รับการอนุญาตจากผู้อำนวยการกองสารสนเทศก่อนทุกครั้ง

(๒) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์ โดยผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย เช่น รายชื่อผู้ขอใช้บริการ IP Address และผังเครือข่าย เป็นต้น

(๓) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของต้นทางและปลายทางได้

๕.๒.๑.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

(๑) ผู้ดูแลระบบ ต้องกำหนดการเปิด - ปิด พอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงของอุปกรณ์เครือข่ายต่าง ๆ และปิดพอร์ตที่เสี่ยงต่อการก่อให้เกิดความเสียหายต่อระบบเครือข่ายและอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๒) บุคคลภายนอกที่เข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายต้องได้รับการอนุญาตจากผู้ดูแลระบบ

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๕.๒.๑.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายภายในหน่วยงาน และเครือข่ายภายนอกหน่วยงาน

๕.๒.๑.๖ การควบคุมการเชื่อมต่อเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ดังนี้

(๑) ผู้ดูแลระบบต้องมีการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิของผู้ใช้ในการเชื่อมต่อเครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) ผู้ดูแลระบบต้องมีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ผู้ดูแลระบบต้องควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๕.๒.๑.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลสารสนเทศ ดังนี้

(๑) ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address)

(๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๕.๒.๑.๘ การควบคุมการเข้าใช้งานระบบจากระยะไกล (Remote Access)

(๑) ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) ต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัสเป็นต้น

(๓) ผู้ใช้งานต้องแสดงหลักฐานและเหตุผลความจำเป็น และต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๔) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ต้องดูแลและจัดการโดยผู้ดูแลระบบ และต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๕.๒.๒ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

แนวทางปฏิบัติ

๑. ห้ามใช้ระบบเครือข่ายไร้สายภายในอาคารของ กกท. ในระหว่างที่ กกท. ยังไม่มีการติดตั้งระบบบริหารจัดการและระบบรักษาความปลอดภัยสำหรับระบบเครือข่ายไร้สายโดยเฉพาะ

๒. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายชั่วคราวของ กกท. จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุมัติจาก ผอ.กองสารสนเทศ ตามความจำเป็นในการใช้งาน

๓. ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๔. ผู้ดูแลระบบต้องต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้ สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจาก ภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๕. ผู้ดูแลระบบต้องต้องกำหนดค่าใช้ Wep (wired equivalent privacy) หรือ WPA (Wi-Fi protected access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจายสัญญาณ (access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

๖. ผู้ดูแลระบบต้องควรเลือกใช้วิธีการควบคุมชื่อผู้ใช้ (username) รหัสผ่าน (password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะ อุปกรณ์ที่มีชื่อผู้ใช้(username) รหัสผ่าน (password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้ สายได้อย่างถูกต้อง

๗. ผู้ดูแลระบบต้องควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สาย กับ เครือข่ายภายในหน่วยงาน

๘. ผู้ดูแลระบบต้องต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่าย ไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึง อย่างสม่ำเสมอ

๙. ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย อย่างสม่ำ เสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการ ใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อหัวหน้างานทราบทันที

หมวดที่ ๖ การสื่อสารนโยบายบริหารจัดการความมั่นคงปลอดภัยในการติดต่อสื่อสารและเครือข่าย

วัตถุประสงค์ เพื่อถ่ายทอดนโยบายทีจัดทำขึ้นให้มีประสิทธิภาพในการกระจายนโยบายลงสู่ผู้ปฏิบัติงาน และหวังผลให้ผู้ปฏิบัติมีความเข้าใจ เข้าถึงนโยบายได้ง่ายและมีความตระหนักต่อผลที่เกิดจากนโยบาย โดยนโยบายการสื่อสารซึ่งอาจจัดเป็น ๓ วิธี มีรายละเอียด ดังนี้

๑) **การให้ข้อมูลข่าวสาร** (Information) การให้ข่าวสารข้อมูลความมั่นคงปลอดภัยในการติดต่อสื่อสารและเครือข่าย ช่วยให้ผู้ใช้งานตระหนักถึงปัญหาการบริหารจัดการความมั่นคงปลอดภัยในการติดต่อสื่อสารและเครือข่าย ความสำคัญของการให้ข่าวสารข้อมูล คือ การเลือกใช้การประชาสัมพันธ์ที่สามารถเข้าถึงผู้ใช้งานให้มากที่สุดการประชาสัมพันธ์ที่มีประสิทธิภาพจะต้องเป็นสื่อที่สอดคล้องกับระดับการปฏิบัติงานของผู้ใช้งาน

๒) **การอำนวยความสะดวก** (Facilitation) การให้ความสะดวกหมายถึงการเอื้ออำนวยให้กลุ่มผู้ใช้ กลุ่มเป้าหมายของนโยบายมีความสะดวกที่จะปฏิบัติตามนโยบาย หรือสะดวกที่จะเข้ามารับรู้บริการจากนโยบาย หรือสะดวกที่จะให้ความร่วมมือกับนโยบายในและปฏิบัติตามนโยบาย โดยที่ผู้ใช้งานและผู้เกี่ยวข้องอาจเห็นด้วยอย่างมากกับนโยบายที่ประกาศใช้แต่นโยบายนั้นอาจถูกปฏิเสธจากผู้ใช้งาน หรือผู้ใช้งานอาจให้ความร่วมมือน้อยกว่าที่ควรจะเป็นเพราะเห็นว่ามีข้อยุ่งยากในทางปฏิบัติ

๓) **กลยุทธ์การสร้างความตระหนัก** (Awareness Strategies) เป็นกลยุทธ์ที่ใช้เพื่อสร้างความตระหนัก (Awareness) ต่อผู้ใช้ซึ่งไม่ปฏิบัติตามนโยบาย มุ่งเน้นให้เห็นผลความเสียหายต่อผู้ใช้เองและองค์กรหากผู้ใช้ไม่ปฏิบัติตามนโยบาย กลยุทธ์นั้นมีจุดมุ่งหมายเพื่อให้บุคคลและกลุ่มบุคคลปฏิบัติหรือละเว้นการปฏิบัติอย่างใด อย่างหนึ่ง เพื่อให้เกิดสิ่งที่ดีงามแก่สังคมนโยบายจำนวนมากจำเป็นต้องอาศัยกลยุทธ์นี้รวมทั้งนโยบายด้านการศึกษาด้วย เช่น นโยบายควบคุมคุณภาพ

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) ลงชื่อ.....(ผู้บังคับบัญชา)

(.....) (.....)

ตำแหน่ง ..... ตำแหน่ง .....

วันที่..... 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

แบบฟอร์มขออนุญาตเปิดบริการบนไฟร์วอล์
การกีฬาแห่งประเทศไทย

วันที่.....เดือน.....พ.ศ.....

ข้าพเจ้า นาย/นาง/นางสาว.....เลขประจำตัวประชาชน.....

ตำแหน่ง..... สังกัดหน่วยงาน.....

โทรศัพท์.....อีเมล์.....

ขอแจ้งความประสงค์

☐ เปิด Port หมายเลข..... เป็นแบบ ○ UDP ○ TCP ○ ทั้ง ๒ รูปแบบ

หมายเลข..... เป็นแบบ ○ UDP ○ TCP ○ ทั้ง ๒ รูปแบบ

หมายเลข..... เป็นแบบ ○ UDP ○ TCP ○ ทั้ง ๒ รูปแบบ

หมายเลข..... เป็นแบบ ○ UDP ○ TCP ○ ทั้ง ๒ รูปแบบ

หมายเลข..... เป็นแบบ ○ UDP ○ TCP ○ ทั้ง ๒ รูปแบบ

เหตุผล : ○ ใช้งานเว็บไซต์ (ระบุ URL).....
(เช่น www.sat.or.th)

○ เพื่อใช้โปรแกรมหรือซอร์ฟแวร์หรือโปรแกรมประยุกต์(ระบุชื่อ).....

โดยขอเปิดใช้งานเครื่อง IP Address หมายเลข.....

☐ เปิดหมายเลขประจำเครื่องคอมพิวเตอร์(IP Address)

○ IP ภายนอก สำหรับเครื่องคอมพิวเตอร์แม่ข่ายให้บริการ.....

จำนวน.....เครื่อง /หมายเลข โดยสถานที่ติดตั้งใช้งานคือ.....

กำหนดชื่อเครื่องคอมพิวเตอร์แม่ข่าย (โดเมนเนม) เป็น.....

○ IP ภายใน

สำหรับเครื่องคอมพิวเตอร์แม่ข่ายให้บริการ.....

จำนวน.....เครื่อง /หมายเลข โดยสถานที่ติดตั้งใช้งาน คือ.....

กำหนดชื่อเครื่องคอมพิวเตอร์แม่ข่าย (โดเมนเนม) เป็น.....

☐ อื่น ๆ (ระบุเช่น Remote).....

โดยข้าพเจ้าจะปฏิบัติตามนโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy) ดังนี้

ข้อ ๑ ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของ Firewall ทั้งหมด การเปลี่ยนแปลงค่าต่าง ๆ ของอุปกรณ์Firewall ในแต่ละครั้ง ได้แก่ค่าพารามิเตอร์การกำหนดค่าใช้บริการ และการกำหนดระบบเครือข่ายสื่อสารต่าง ๆ ให้สามารถเชื่อมต่อกับระบบเครือข่ายสื่อสารของการกีฬาแห่งประเทศไทยโดยได้รับอนุญาตจากผู้อำนวยการกองสารสนเทศหรือผู้ได้รับมอบหมาย

ข้อ ๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกระบบเครือข่ายสื่อสาร จะต้องเป็นการปฏิเสธทั้งหมด

- ทุกเส้นทางการเชื่อมต่อระบบอินเทอร์เน็ตและบริการระบบอินเทอร์เน็ตที่ไม่ได้รับการอนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดย Firewall
- การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
- ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้องจัดเก็บไว้ที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่น่าเชื่อถือและมีการเข้ารหัสข้อมูลเพื่อป้องกันการแก้ไขหรือเปลี่ยนแปลงและต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า ๙๐ วัน
- มีการตรวจสอบเหตุการณ์ข้อมูลจราจรทางคอมพิวเตอร์พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลการเข้าใช้งานระบบเครือข่ายเป็นประจำทุกวัน โดยผู้ดูแลระบบ
- การกำหนดการให้บริการระบบอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตใน Firewall สำหรับการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานนอกเหนือจากที่กำหนดไว้จะต้องมีการเปิดพอร์ตให้เป็นกรณีพิเศษ ต้องทำหนังสือและได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมาย
- การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของระบบเครือข่ายสื่อสาร จะต้องกำหนดค่าอนุญาตในไฟล์วอลล์เฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้นโดยจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ ให้บริการจริง
- เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานระบบอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป
- การสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟล์วอลล์จะต้องสำรองข้อมูลเป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงการกำหนดค่าในอุปกรณ์ไฟล์วอลล์
- ผู้ดูแลระบบมีสิทธิที่จะระงับการใช้งานของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข
- การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกผ่านระบบเครือข่ายสื่อสารมายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ระบบเครือข่ายสื่อสารภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบคำขออนุญาตเปิดบริการใน Firewall และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน
- ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานระบบอินเทอร์เน็ตหรือการเชื่อมต่อระบบเครือข่ายสื่อสารภายในโดยทันที

ทั้งนี้ข้าพเจ้ายินดีรับผิดชอบผลที่เกิดจากการเข้าใช้ระบบสารสนเทศของการกีฬาแห่งประเทศไทยกรณีที่เกิดความเสียหายในส่วนที่ข้าพเจ้าได้รับสิทธิให้เข้าใช้งาน

.....

(.....)

ผู้ขอใช้บริการ

ส่วนนี้สำหรับผู้ดูแลระบบ

เรียน ผู้อำนวยการกองสารสนเทศ

ข้าพเจ้า.....

พิจารณาแล้วเห็นควร ○ อนุญาต ○ ไม่อนุญาต

เนื่องจาก.....

ให้เปิดบริการ Firewall ตามคำขอดังกล่าวข้างต้น

จึงเรียนมาเพื่อโปรดพิจารณา

.....

(.....)

ตำแหน่ง.....

วันที่.....

○ อนุญาต ○ ไม่อนุญาต

.....

(.....)

ผู้อำนวยการกองสารสนเทศ

วันที่.....

แบบฟอร์มผลการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายภายในการกีฬาแห่งประเทศไทย ประจำเดือน.................ปี...........

วันที่	เวลา	ระบบ				แหล่งจัดเก็บข้อมูลสำรอง	ผู้ปฏิบัติ
		ชื่อเครื่อง / การสำรองข้อมูล					
		ผลการสำรองข้อมูล					
		ขนาด (GB)					
		ผลการสำรองข้อมูล					
		ขนาด (GB)					
		ผลการสำรองข้อมูล					
		ขนาด (GB)					
		ผลการสำรองข้อมูล					
		ขนาด (GB)					
		ผลการสำรองข้อมูล					
		ขนาด (GB)					
		ผลการสำรองข้อมูล					
		ขนาด (GB)					
		ผลการสำรองข้อมูล					
		ขนาด (GB)					
		ผลการสำรองข้อมูล					
		ขนาด (GB)					