ประกาศการกีฬาแห่งประเทศไทย

เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศและข้อมูลสารสนเทศ (Data and Information Security Management)

.....

เพื่อให้ระบบสารสนเทศของการกีฬาแห่งประเทศไทย มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างมีประสิทธิภาพ และมิให้มีผู้กระทำด้วยประการใด ๆ ให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่ง หรือผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อการเผยแพร่ข้อมูลอันเป็นเท็จซึ่งอาจก่อให้เกิดความเสียหายแก่การกีฬาแห่งประเทศไทย และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายอื่นที่เกี่ยวข้องได้ รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการถูกคุกคามจากภัยต่าง ๆ

การกีฬาแห่งประเทศไทย จึงได้จัดทำนโยบายและแนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อเผยแพร่ให้บุคลากรทุกระดับปฏิบัติตามอย่างเคร่งครัด และกำหนดให้มีการทบทวนอย่างสม่ำเสมอ ปีละ ๑ ครั้ง

อาศัยอำนาจตามความในมาตรา ๒๓ แห่งพระราชบัญญัติการกีฬาแห่งประเทศไทย พ.ศ. ๒๕๕๘ และที่แก้ไขเพิ่มเติม การกีฬาแห่งประเทศไทย จึงออกประกาศการกีฬาแห่งประเทศไทย เรื่อ นโยบายและแนวปฏิบัติในการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศและข้อมูลสารสนเทศ (Data and Information Security Management) ดังต่อไปนี้

๑. นโยบายและแนวปฏิบัติในการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศและข้อมูลสารสนเทศ (Data and Information Security Management) ของการกีฬาแห่งประเทศไทย มีวัตถุประสงค์ดังต่อไปนี้

๑.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของการกีฬาแห่งประเทศไทย ให้ดำเนินงานได้อย่างมี ประสิทธิภาพ และประสิทธิผล

๑.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงาน ได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๑.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับการกีฬาแห่งประเทศไทย ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการใช้งานด้านสารสนเทศ

๒. นโยบาย ...

๒. นโยบายและแนวปฏิบัติในการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศและข้อมูลสารสนเทศ ของการกีฬาแห่งประเทศไทย สามารถแบ่งออกได้ดังนี้

๒.๑ มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ

๒.๒ บทบาทหน้าที่ความรับผิดชอบในการบริหารจัดการ

๒.๓ การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information security)

๒.๔ แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

๒.๕ การทำลาย ข้อมูลข่าวสาร ระบบภายใน ข้อมูลภายในระบบ

๓. การกำหนดผู้รับผิดชอบ

๓.๑ ระดับนโยบาย

ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) เป็นผู้กำหนดแผนการดำเนินงาน แนวนโยบายและแนวปฏิบัติ รวมถึงกำกับดูแล ให้เป็นไปตามนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) เป็นผู้รับผิดชอบในการสั่งการตามแนวนโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย

ผู้อำนวยการฝ่ายสารสนเทศและวิชาการกีฬา เป็นผู้รับผิดชอบติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ ให้คำปรึกษา แก่เจ้าหน้าที่ระดับปฏิบัติ

๓.๒ ระดับปฏิบัติ

เพื่อให้การปฏิบัติตามแนวนโยบายและแนวการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศและข้อมูลสารสนเทศ การกีฬาแห่งประเทศไทยเป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้ฝ่ายสารสนเทศและวิชาการกีฬา ผู้ดูแลระบบ ผู้รับผิดชอบระบบสารสนเทศและผู้ที่ได้รับมอบหมายเป็นผู้รับผิดชอบ ดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุง นโยบายและแนวปฏิบัติในการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ และข้อมูลสารสนเทศให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง และหากมีการเปลี่ยนแปลงนโยบายและแนวปฏิบัติให้ประกาศให้เจ้าหน้าที่ทุกระดับในหน่วยงานการกีฬาแห่งประเทศไทย รับทราบทุกครั้ง

๔. ฝ่ายสารสนเทศและวิชาการกีฬา มีหน้าที่ออกระเบียบข้อบังคับ เพื่อปฏิบัติในการจำกัด ระงับ หรือเพิกถอนสิทธิการใช้เครือข่ายของผู้ฝ่าฝืนระเบียบข้อบังคับ ตลอดจนระงับหรือจำกัดการเข้าถึงคอมพิวเตอร์ที่มีข้อมูลขัดต่อระเบียบข้อบังคับ นโยบาย พระราชบัญญัติการกีฬาแห่งประเทศไทย พ.ศ. ๒๕๕๘ และที่แก้ไขเพิ่มเติมซึ่งรวมถึงกฎหมายอื่นที่เกี่ยวข้องในกรณีจำเป็นให้ฝ่ายสารสนเทศและวิชาการกีฬา รายงานการฝ่าฝืนระเบียบข้อบังคับให้หน่วยงานต้นสังกัดหรือการกีฬาแห่งประเทศไทย เพื่อพิจารณาลงโทษต่อไป

๕.นโยบาย ...

๕. นโยบายและแนวการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศและข้อมูลสารสนเทศ จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของการกีฬาแห่งประเทศไทย เพื่อใช้เป็นแนวทางในการดำเนินงานในระบบสารสนเทศให้มีความปลอดภัย เชื่อถือได้เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง จึงให้ใช้แนวปฏิบัติการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศและข้อมูลสารสนเทศ เอกสารแนบท้ายประกาศนี้ ซึ่งเจ้าหน้าที่ของการกีฬาแห่งประเทศไทย และหน่วยงานที่เกี่ยวข้องต้องถือปฏิบัติอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๓ สิงหาคม พ.ศ. ๒๕๖๓

(นายก้องศักด ยอดมณี)
ผู้ว่าการการกีฬาแห่งประเทศไทย

เอกสารแนบท้ายประกาศ

การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศ

(Data and Information Security Management)

ของการกีฬาแห่งประเทศไทย

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

การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศ

๑. ระบบสารสนเทศ (Information System) หมายถึง

การประมวลผลข่าวสารที่มีอยู่ ให้อยู่ในรูปของข่าวสารที่ เป็นประโยชน์สูงสุด เพื่อเป็นข้อสรุปที่ใช้สนับสนุนการตัดสินใจของบุคคลระดับบริหาร การที่ทำให้เกิดข่าวสารสารสนเทศนี้ เรียกว่า การประมวลผลผลสารสนเทศ (Information Processing) และเรียกวิธีการประมวลผลสารสนเทศด้วยเครื่องมือทางอีเล็กทรอนิกส์หรือระบบสารสนเทศ ในการจัดเก็บข้อมูล หรือการได้มาจากประสบการณ์ทำงานของพนักงาน ผู้เชี่ยวชาญ ในรูปแบบของข้อมูลในระบบสารสนเทศ

๒. เทคโนโลยีสารสนเทศ (Information Technology : IT) เทคโนโลยีสารสนเทศ หมายถึง

เทคโนโลยีที่ประกอบขึ้นด้วยระบบจัดเก็บและประมวลผลข้อมูล ระบบสื่อสารโทรคมนาคม และอุปกรณ์สนับสนุนการปฏิบัติงานด้านสารสนเทศที่มีการวางแผน จัดการ และใช้ง่านร่วมกันอย่างมีประสิทธิภาพ

๒.๑. เทคโนโลยีสารสนเทศ มีองค์ประกอบสำคัญ ๓ ประการ

๒.๑.๑. ระบบประมวลผล ความซับซ้อนในการปฏิบัติงานและความต้องการสารสนเทศที่หลากหลาย ทำให้การจัดการและการประมวลผลข้อมูลด้วยมือ ไม่สะดวก ช้า และอาจผิดพลาด ปัจจุบันองค์การจึงต้องทำการจัดเก็บและการประมวลผลข้อมูลด้วยระบบอีเล็กทรอนิกส์ โดยใช้คอมพิวเตอร์และอุปกรณ์สนับสนุนในการจัดการข้อมูล เพื่อให้การทำงานถูกต้องและรวดเร็วขึ้น

๒.๑.๒. ระบบสื่อสารโทรคมนาคม การสื่อสารข้อมูลเป็นเรื่องสำคัญสำหรับการจัดการและประมวลผล ตลอดจนการใช้ ข้อมูลในการตัดสินใจ ระบบสารสนเทศที่ดีต้องประยุกต์เทคโนโลยีอีเล็กทรอนิกส์ในการสื่อสารข้อมูลระหว่างระบบคอมพิวเตอร์ อุปกรณ์อีเล็กทรอนิกส์ และผู้ใช้ที่อยู่ห่างกัน ให้สามารถสื่อสารกันได้อย่างมีประสิทธิภาพ

๒.๑.๓. การจัดการข้อมูลปกติบุคคลที่ให้ความสนใจกับเทคโนโลยีจะอธิบายความหมายของเทคโนโลยีสาร สนเทศโดยให้ความสำคัญกับส่วนประกอบสองประการแรก แต่ผู้ที่สนใจด้านการจัดการข้อมูล (Data/Information Management) จะให้ความสำคัญกับส่วนประกอบที่สาม ซึ่งมีความเป็นศิลปะ ในการจัดรูปแบบและการใช้งานเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ

สามารถสรุปได้ว่า เทคโนโลยีสารสนเทศเป็นเทคโนโลยีทุกรูปแบบที่นำมาประยุกต์ ในการประมวลผล การจัดเก็บ การสื่อสาร และการส่งผ่านสารสนเทศด้วยระบบอีเล็กทรอนิกส์ โดยที่ระบบทางกายภาพประกอบด้วยคอมพิวเตอร์ อุปกรณ์ติดต่อสื่อสาร และระบบเครือข่าย ขณะที่ระบบนามธรรมเกี่ยวข้องกับการจัดรูปแบบของการปฏิสัมพันธ์ด้านสารสนทศ ทั้งภายในและภายนอกระบบ ให้สามารถดำเนินร่วมกันอย่างประสิทธิภาพ

๓. ประโยชน์ของระบบสารสนเทศเพื่อการจัดการ

๓.๑. ช่วยให้ผู้ใช้สามารถเข้าถึงสารสนเทศที่ต้องการได้อย่างรวดเร็วและทันต่อเหตุการณ์เนื่องจากข้อมูลถูกจัดเก็บและบริหารเป็นระบบ ทำให้ผู้บริหารสามารถจะเข้าถึงข้อมูลได้อย่างรวดเร็วในรูปแบบที่เหมาะสม และสามารถนำข้อมูลมาใช้ประโยชน์ได้ทันต่อความต้องการ

๓.๒. ช่วยผู้ใช้ในการกำหนดเป้าหมายกลยุทธ์และการวางแผนปฏิบัติการ โดยผู้บริหารจะสามารถนำข้อมูลที่ได้จากระบบ สารสนเทศมาช่วยในการวางแผนและกำหนดเป้าหมายในการดำเนินงาน เนื่องจากสารสนเทศถูกเก็บรวบรวมและจัดการ อย่างเหมาะสม ทำให้มีประวัติของข้อมูลอย่างต่อเนื่อง สามารถที่จำชี้แนวโน้มของการดำเนินงานได้ว่าน่าจะเป็นไปในลักษณะใด

๓.๓. ช่วยผู้ใช้ในการตรวจสอบประเมินผลการดำเนินงาน เมื่อแผนงานถูกนำไปปฏิบัติในช่วงระยะเวลาหนึ่ง ผู้ควบคุมจะต้องตรวจสอบผลการดำเนินงานโดยนำข้อมูลบางส่วนมาประมวลผลประกอบการประเมิน สารสนเทศที่ได้จะแสดงให้เห็นผลการดำเนินงานว่าสอดคล้องกับเป้าหมายที่ต้องการเพียงไร

๓.๔. ช่วยผู้ใช้ในการศึกษาและวิเคราะห์สาเหตุของปัญหา ผู้บริหารสามารถใช้ระบบสารสนเทศประกอบการศึกษาและการค้นหาสาเหตุ หรือข้อผิดพลาดที่เกิดขึ้นในการดำเนินงาน ถ้าการดำเนินงานไม่เป็นไปตามแผนที่วางเอาไว้ อาจจะเรียกข้อมูลเพิ่มเติมออกมาจากระบบ เพื่อให้ทราบว่าข้อผิดพลาดในการทำงานเกิดขึ้นมาจากสาเหตุใด หรือจัดรูปแบบสารสนเทศในการวิเคราะห์ปัญหาใหม่

๓.๕. ช่วยให้ผู้ใช้สามารถวิเคราะห์ปัญหาหรืออุปสรรคที่เกิดขึ้น เพื่อหาวิธีควบคุม ปรับปรุงและแก้ไขปัญหา สารสนเทศที่ได้จากการประมวลผลจะช่วยให้ผู้บริหาร วิเคราะห์ว่าการดำเนินงานในแต่ละทางเลือกจะช่วยแก้ไข หรือควบคุมปัญหาที่เกิดขึ้นได้อย่างไร ธุรกิจต้องทำอย่างไรเพื่อปรับเปลี่ยนหรือพัฒนาให้การดำเนินงานเป็นไปตามแผนงานหรือเป้าหมาย

๓.๖. ช่วยลดค่าใช้จ่าย ระบบสารสนเทศที่มีประสิทธิภาพ ช่วยให้ธุรกิจลดเวลา แรงงานและค่าใช้จ่ายในการทำงานลง เนื่องจากระบบสารสนเทศสามารถรับภาระงานที่ต้องใช้แรงงาน จำนวนมากตลอดจนช่วยลดขั้นตอนในการทำงาน ส่งผลให้ธุรกิจสามารถลดจำนวนคนและระยะเวลาในการประสานงานให้น้อยลง โดยผลงานที่ออกมาอาจเท่าหรือดีกว่าเดิม ซึ่งจะเป็นการเพิ่มประสิทธิภาพและศักยภาพในการแข่งขันทางธุรกิจ

๔. <u>องค์ประกอบของระบบสารสนเทศกับความมั่นคง</u>

๔.๑. Software อยู่ภายใต้เงื่อนไขของการบริหารโครงการ ภายใต้เวลา ต้นทุน และกำลังคนที่จำกัด

๔.๒. Hardware ใช้นโยบายเดียวกับสินทรัพย์ที่จับต้องได้ขององค์กร คือการป้องกันจากการลักขโมยหรือภัยอันตรายต่าง ๆ รวมถึงการจัดสถานที่ที่ปลอดภัยให้กับอุปกรณ์หรือฮาร์ดแวร์

๔.๓. Data ข้อมูล/สารสนเทศ เป็นทรัพยากรที่มีค่าขององค์กร การป้องกันที่แน่นหนาก็มีความจำเป็นสำหรับข้อมูลที่เป็นความลับ ซึ่งต้องอาศัยนโยบายความปลอดภัยและกลไกป้องกันที่ดีควบคู่กัน

๔.๔. People บุคลากร คือภัยคุกคามต่อสารสนเทศที่ถูกมองข้ามมากที่สุด โดยเฉพาะบุคลากรที่ไม่มีจรรยาบรรณในอาชีพ ก็เป็นจุดอ่อนต่อการโจมตีได้ จึงได้มีการศึกษากันอย่างจริงจัง เรียกว่า Social Engineering ซึ่งเป็นการป้องการการหลอกหลวงบุคลากร เพื่อเปิดเผยข้อมูลบางอย่างเข้าสู่ระบบได้

๔.๕. Procedure ขั้นตอนการทำงาน เป็นอีกหนึ่งองค์ประกอบที่ถูกมองข้าม หากมิจฉาชีพทราบขั้นตอนการทำงาน ก็จะสามารถค้นหาจุดอ่อนเพื่อนกระทำการอันก่อนให้เกิดความเสียหายต่อองค์กรและลูกค้าขององค์กรได้

๔.๖. Network เครือข่ายคอมพิวเตอร์ การเชื่อมต่อระหว่างคอมพิวเตอร์และระหว่างเครือข่ายคอมพิวเตอร์ ทำให้เกิดอาชญากรรมและภัยคุกคามคอมพิวเตอร์ โดยเฉพาะการเชื่อมต่อระบบสารสนเทศเข้ากับเครือข่ายอินเตอร์เน็ต

๕. จุดประสงค์ของการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ

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

๕.๑.การรักษาความลับ (confidentiality) คือการรักษาความลับ มีการเก็บข้อมูลไว้เป็นความลับให้เฉพาะผู้มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้

๕.๒.การรักษาความสมบูรณ์ (integrity) คือความครบถ้วน ความถูกต้องสมบูรณ์ ไม่มีการแก้ไขเปลี่ยนแปลงหรือทำลายจากผู้ไม่มีสิทธิไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา

๕.๓.ความพร้อมใช้ (availability) คือความพร้อมใช้งานของข้อมูลและบริการการสื่อสารต่างๆ สามารถตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ

๖. มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ

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

๗. บทบาทหน้าที่ความรับผิดชอบในการบริหารจัดการ

เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศภายในองค์กร นโยบาย

๗.๑ การกำหนดบทบาทและหน้าที่ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ ผู้บริหารระดับสูงสุดต้องแต่งตั้งกลุ่มหรือคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ และมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

๗.๒ การแบ่งแยกหน้าที่ความรับผิดชอบ

๗.๒.๑ ผู้บริหารด้านไอทีต้องกำหนดตำแหน่งด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดความรับผิดชอบให้เหมาะสม พร้อมทั้งควบคุมการปฏิบัติงานเพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย

๗.๒.๒ ผู้บริหารด้านไอทีเป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ การกีฬาแห่งประเทศไทย

๗.๒.๓ ผู้บริหารต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย

๗.๒.๔ ผู้ใช้งาน และหน่วยงานภายนอกต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของ การกีฬาแห่งประเทศไทย ในการรักษาความมั่นคงปลอดภัยสารสนเทศของการกีฬาแห่งประเทศไทย

๘. การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information security)

เพื่อป้องกันข้อมูลสารสนเทศที่เกิดขึ้นจากการใช้ระบบ ควบคุมและป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต รวมถึงองค์ประกอบอื่นๆ ที่เกี่ยวข้องเช่น ระบบและฮาร์ดแวร์ที่ใช้ในการจัดเก็บและถ่ายโอนข้อมูลสารสนเทศนั้นให้รอดพ้นจากภัยคุกคามต่างๆ

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 การดำเนินงานตามภารกิจ กกท. กฎหมาย ระเบียบ, 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

๙. 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 ให้พิจารณาในระดับฐานข้อมูล ด้วยการประเมินมูลค่าความเสียหายต่อหน่วยงานหากข้อมูลมีปัญหา 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

๑๐. การทำลาย ข้อมูลข่าวสาร ระบบภายใน ข้อมูลภายในระบบ

ข้อมูลข่าวสารลับจะทำลายได้ใน ๒ กรณีดังนี้

๑. ในกรณีที่การเก็บรักษาข้อมูลข่าวสารข้อมูลข่าวสาร ระบบภายใน ข้อมูลภายในระบบ ชั้นลับที่สุดจะเสี่ยงต่อการรั่วไหลอันจะก่อให้เกิด อันตรายแก่ประโยชน์ของหน่วยงาน หัวหน้าหน่วยงานของรัฐจะพิจารณาสั่งทำลายข้อมูลข่าวสารลับชั้นลับที่สุดนั้นได้ หากพิจารณาเห็นว่ามีความจำเป็นอย่างยิ่งที่จะต้องทำลาย

๒. ครบอายุการใช้งาน หรือได้รับการพิจารณาให้ตัดครุภัณฑ์ โดยต้องให้ผู้อำนวยการฝ่ายที่รับผิดชอบระบบหรือข้อมูล เป็นผู้เห็นชอบเสนอหัวหน้าหน่วยงาน เพื่อขออนุมัติในการตัดครุภัณฑ์

ขั้นตอนการทำลายข้อมูลข่าวสารลับ

๑) จัดทำบัญชีรายชื่อหนังสือขอทำลาย (ข้อมูลข่าวสาร ระบบภายใน ข้อมูลภายในระบบ)

๒) จัดทำคำขออนุมัติทำลายข้อมูลข่าวสาร ระบบภายใน ข้อมูลภายในระบบ พร้อมทั้งเสนอหัวหน้าหน่วยงานของรัฐ แต่งตั้งคณะกรรมการทำลาย โดยมีนายทะเบียนข้อมูลข่าวสาร ระบบภายใน ข้อมูลภายในระบบของหน่วยงานเป็นประธาน และผู้เกี่ยวข้อง อย่างน้อย ๒ คน เป็นกรรมการ และเมื่อคณะกรรมการดังกล่าวได้ทำลายข้อมูลข่าวสาร ระบบภายใน ข้อมูลภายในระบบเสร็จแล้ว ให้จด แจ้งการทำลายไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับและจัดทำใบรับรองการทำลายข้อมูลข่าวสาร ระบบภายใน ข้อมูลภายในระบบด้วย ใบรับรองการทำลายให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่าหนึ่งปี

๓) จัดทำใบรับรองการทำลายข้อมูลข่าวสาร ระบบภายใน ข้อมูลภายในระบบ และเก็บรักษาไว้เป็นหลักฐานอย่างน้อย ๑ ปี

(เอกสารเพิ่มเติม)

๑. **แบบฟอร์มผู้ดูแลระบบ มีแล้ว ข้อ ๖.๑**
๒. **ฟอร์มขออนุมัติตัดครุภัณฑ์ ระบบ**
๓. **<u>แบบฟอร์มขอใช้บริการห้องคอมพิวเตอร์แม่ข่าย (Datacenter</u>) ของกอล์ฟ**