สารบัญ

การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

แนวปฏิบัติในการควบคุมสิทธิการเข้าถึงข้อมูลที่สำคัญของหน่วยงาน (Access Control) สำนักงานโครงการ TO BE NUMBER ONE

ตามประกาศกรมสุขภาพจิต เรื่องนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสุขภาพจิต กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสุขภาพจิต เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมสุขภาพจิตเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อนให้เกิดความเสียหายต่อกรมสุขภาพจิต นั้น

สำนักงานโครงการ TO BE NUMBER ONE จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมสุขภาพจิต ดังนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศสำนักงานโครงการ TO BE NUMBER ONE เรื่อง แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์สำนักงานโครงการ TO BE NUMBER ONE พ.ศ. 2567”

ข้อ 2 ประกาศนี้ให้ใช้บังคับ ตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ 3 คำนิยาม

“หน่วยงาน” หมายถึง สำนักงานโครงการ TO BE NUMBER ONE

“ผู้บริหาร” หมายถึง ผู้อำนวยการสำนักงานโครงการ TO BE NUMBER ONE

“หัวหน้ากลุ่ม” หมายถึง หัวหน้ากลุ่มงานอำนวยการ, หัวหน้ากลุ่มงานแผนงาน, หัวหน้ากลุ่มงานผลิตและถ่ายทอดเผยแพร่เทคโนโลยี, หัวหน้ากลุ่มงานรณรงค์เผยแพร่และประชาสัมพันธ์, หัวหน้ากลุ่มงานที่ปรึกษา

“นโยบาย” หมายถึง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติมพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และรวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้องกับภารกิจของกรมสุขภาพจิต เพื่อเป็นทิศทางให้ผู้ดูแลระบบ (Administrator) ผู้ใช้งาน (User) ได้ถือปฏิบัติ

“แนวปฏิบัติ” หมายถึง แนวทางหรือข้อกำหนดให้ผู้ใช้งาน (User) และบุคคลภายนอกได้ถือปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

“ผู้ดูแลระบบ” หมายถึง บุคลากร สำนักงานโครงการ TO BE NUMBER ONE ผู้ซึ่งได้รับมอบหมายจากเจ้าของระบบ (System Owner) หรือจากผู้อำนวยการของหน่วยงานให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และการบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศของระบบเทคโนโลยีสารสนเทศ

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“ผู้ใช้งาน” หมายถึง บุคลากรสำนักงานโครงการ TO BE NUMBER ONE ทุกคน ซึ่งเป็นข้าราชการ พนักงานราชการ

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข่องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์

“สินทรัพย์” หมายถึง ฮาร์ดแวร์ ซอฟท์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศหรือสิ่งอื่นใดก็ตามที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของสำนักงานโครงการ TO BE NUMBER ONE ประกอบด้วย

1. ฮาร์ดแวร์ (Hardware) หมายถึง อุปกรณ์คุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้

- เครื่องคอมพิวเตอร์ลูกข่าย (Client) อันได้แก่ เครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Laptop) อุปกรณ์สื่อสารแบบพกพา (Tablet / Smart phone) รวมถึงอุปกรณ์สนับสนุนเครื่องพิมพ์ (Printer / Scanner) และอุปกรณ์สำรองข้อมูลของสำนักงานโครงการ TO BE NUMBER ONE
- อุปกรณ์โครงข่าย (Network) หรือ อุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) หรืออุปกรณ์สำหรับเชื่อมต่อระบบสื่อสาร (Router, Switch, Access Point) หรืออุปกรณ์จัดเก็บบันทึกการใช้งาน (Log File)

2. โปรแกรมประยุกต์หรือแอพพลิเคชั่น (Program or Application) หมายถึง ระบบคุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้ ระบบ, System Software, Database Software, Software Tool และ Application Software ที่ใช้งานร่วมกับอุปกรณ์ในหัวข้อ Hardware

“ระบบคอมพิวเตอร์” หมายถึง ระบบคอมพิวเตอร์ลูกข่ายแบบเสมือน (Virtualization System) ที่ติดตั้งบนอุปกรณ์ในการประมวลผลข้อมูล (Process Device) โดยเข้าถึงด้วยเทคโนโลยีแบบ Cloud Computing และระบบปฏิบัติการ (Operating System) ที่ติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) พร้อมด้วยโปรแกรมประยุกต์ (Application Software)

“ระบบสารสนเทศ” หมายถึง ระบบงานคอมพิวเตอร์ เช่น เว็บไซต์ จดหมายอิเล็กทรอนิกส์ (E-Mail) และระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น หรืออุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับการพัฒนาหรือติดตั้งหรือการนำมาประยุกต์ใช้เพื่อสนับสนุนการปฏิบัติงาน

“ข้อมูลสารสนเทศ” หมายถึง ข้อมูล (Data) หรือสารสนเทศ (Information) ที่อยู่ในรูปของเอกสารอิเล็กทรอนิกส์ เช่น แฟ้มข้อมูล (File) ฐานข้อมูล (Database) และเอกสารที่มีการแปลงให้อยู่ในรูปแบบอิเล็กทรอนิกส์ (E-Document)

“พื้นที่ปฏิบัติงานทั่วไป” (General Working Area) หมายถึง พื้นที่สำหรับการปฏิบัติงานภายในสำนักงานโครงการ TO BE NUMBER ONE ซึ่งได้รับการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์ลูกข่ายเสมือน เครื่องคอมพิวเตอร์พกพา อุปกรณ์ต่อพ่วง และเครือข่ายแบบไร้สาย (Wireless LAN)

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง (Information Security) การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูล

สารสนเทศ รวมทั้งคุณสมบัติอื่นๆ ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบคอมพิวเตอร์และระบบสารสนเทศถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

การสร้างความตระหนักรู้ด้าน Cyber security ของหน่วยงาน : ในสถานที่ทำงาน

ด้านการใช้งานคอมพิวเตอร์ (Computer) เจ้าหน้าที่พึงตระหนักในสิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ดังนี้

1. ให้มีการแยก user ใช้งานกันของแต่ละบุคคล
2. ให้เจ้าหน้าที่ทำการ logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
4. มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. มีการเน้นยำไม่ให้เจ้าหน้าที่จด password และติด password ไว้ที่หน้าจอคอมพิวเตอร์
7. มีการใช้ password ที่ดีและไม่ให้บอก password แก่เจ้าหน้าที่อื่น

การใช้งานการตั้งค่าเกี่ยวกับ Password ที่ดีเน้นยำให้เจ้าหน้าที่สำนักงานโครงการ TO BE NUMBER ONE ให้ตั้งค่าอย่างน้อยเบื้องต้น ดังนี้

1. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ
2. มีความยาวของ Password อย่างน้อย 8 ตัวอักษร
3. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password,123456,วันเกิด,หมายเลขโทรศัพท์
4. มีการเปลี่ยน Password อย่างสม่ำเสมอ
5. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
6. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
7. ไม่ควรบอก Password แก่ผู้อื่น

เหตุผลที่ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password,123456,วันเกิด,หมายเลขโทรศัพท์

ด้านการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

หน่วยงานได้ประชาสัมพันธ์และชี้แจงเรื่องการในงานที่เชื่อมต่อกับระบบ Network อยู่สม่ำเสมอ ให้พึงระวังเกี่ยวกับความมั่นคงปลอดภัยโดยให้ถือปฏิบัติเพื่อความปลอดภัย ดังนี้

1. ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
2. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
3. ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค
4. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

ด้านการใช้งานเว็บไซต์ (Website)

เว็บไซต์เป็นหนึ่งรูปแบบที่ทำให้ไวรัสคอมพิวเตอร์ ที่เป็นสื่อในการที่ทำให้เครื่องคอมพิวเตอร์ของเจ้าหน้าที่หน่วยงานติดไวรัสคอมพิวเตอร์ได้ง่าย เพราะหากไม่มีการระวังหรือตระหนักอาจทำให้เครื่องคอมพิวเตอร์หรือข้อมูลที่สำคัญเสียหายหรือสูญเสียได้ โดยให้เจ้าหน้าควรปฏิบัติเพื่อความปลอดภัย ดังนี้

1. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง social ต่างๆ
2. ไม่ควรทำการบันทึก Password ต่างๆบน Browser
3. เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
4. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น google chrome mozilla firefox เป็นต้น
5. ควรมีการอัพเดทเวอร์ชั่นของ Browser อย่างสม่ำเสมอ
6. ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน browser ในโหมด safe web browsing
7. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ

เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน browser ในโหมด safe web browsing

การใช้งานด้านข้อความ (Messaging) สิ่งที่ให้เจ้าหน้าที่หน่วยงานถือปฏิบัติเพื่อความปลอดภัย คือ

1. ไม่ควรบันทึก password ของตนเองไว้ที่โปรแกรมที่ใช้งานที่เครื่องคอมพิวเตอร์
2. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่างๆ ที่เป็นข้อมูลบุคคลที่สำคัญไว้บนเครื่อง
3. มีความตระหนักก่อนเปิดลิงค์หรือไฟล์ต่างๆที่ได้รับมาเสมอ
4. มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ

และไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆโดยไม่ทราบที่มาของข้อมูล โดยเฉพาะ Fake News เพราะ Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือจึงทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ทางช่องทางออนไลน์ เช่น LINE,Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

1. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
2. ระบุที่มาของข่าวไม่ได้
3. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
4. สำนวนการเขียนออกแนวการโฆษณา

ที่มา http://www.antifakenewcenter.com ศูนย์ต่อต้านข่าวปลอมประเทศไทย

การใช้งานเกี่ยวกับงานด้าน Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ใช้สถานที่เหมาะสมกับการ Conference
2. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
3. แชร์เอกสารต่างๆ อย่างระมัดระวัง
4. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
5. มีการอัพเดทเวอร์ชั่นของโปรแกรม Conference อย่างสม่ำเสมอ

การใช้งานด้าน Cloud Storage เป็นอีกรูปแบบหนึ่งที่มีการใช้งานที่มากขึ้นเรื่อยๆ ตัวอย่างเช่น google drive One Drive และระบบแชร์ไฟล์ต่าง นั่นเป็นอีกหนึ่งเหตุผลที่อาจทำให้มีความปลอดภัยลดลงได้หากมีการเข้าถึงข้อมูลส่วนตัวและรหัสผ่านของเจ้าหน้าที่นั้นๆได้ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ

1. ให้เจ้าหน้าที่แยก User ในการใช้งานของแต่ละบุคคล
2. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
3. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
4. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ
5. มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ
6. มีการตั้ง Password ที่ดีและไม่บอก Password แก่ผู้อื่น

การสร้างความตระหนักรู้ด้าน Cyber security ของหน่วยงาน : ในสถานที่ทำงาน

การใช้งานคอมพิวเตอร์ (Computer) สิ่งที่เจ้าหน้าที่ควรปฏิบัติเพื่อความปลอดภัย ดังนี้

1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง anti-malware และมีการอัพเดตอย่างสม่ำเสมอ
4. มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
7. มีการใช้ Password ที่ดีและไม่ควรบอก Password แก่ผู้อื่น

การใช้งาน Free WIFI สิ่งที่เจ้าหน้าที่ควรตระหนักและปฏิบัติเพื่อความปลอดภัย ดังนี้

1. ไม่ควรใช้งาน WiFi ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
2. หลีกเลี่ยงการใช้งาน WiFi ที่ไม่รู้ที่มาในการให้บริการMobileสิ่งที่ควรปฏิบัติเพื่อความปลอดภัย
1. เปิดการใช้งาน PIN/Password,Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
2. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
3. กำหนด Application permission ให้เหมาะสม
4. มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างเหมาะสม
5. มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ กำหนด Application permission ให้เหมาะสม

การเชื่อต่อและการใช้งาน Internet Connection : ภายนอกสถานที่ทำงาน

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
2. เปลี่ยน SSID และรหัสผ่านของ WiFi ที่กำหนดมาจากผู้ให้บริการ
3. กำหนดผู้ที่สามารถเข้าใช้งานอินเทอร์เน็ตเท่าที่จำเป็น

การเชื่อต่อกับ อุปกรณ์ IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่างๆ หรือ Application ต่างๆ ได้ เช่น หลอดไฟ,พัดลม,เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปลี่ยน Default Password ที่มาจากโรงงาน
2. ควรมีการอัพเดทเฟิร์มแวร์ให้เป็นเวอร์ชั่นล่าสุด
3. ใช้ application ที่ใช้ในการคอนโทรลกับอุปกรณ์ต่างๆให้เป็นเวอร์ชั่นล่าสุด กล้องวงจรปิดที่ดูผ่านอินเตอร์เน็ตควรมีการเปลี่ยน password ที่ไม่ใช่ default password จากโรงงาน ตัวอย่าง IoT Devices เช่น เตาแม่เหล็กไฟฟ้ารุ่นใหม่ต้องต่อกับสมาร์ทโฟนเพื่อทำการคอนโทรล

สรุปเรื่องการสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์ในส่วนของความปลอดภัยกับความสะดวกสบาย จะให้เห็นว่าสิ่งที่เจ้าหน้าที่ต้องทำคือต้องพยายามถ่วงน้ำหนักให้เท่ากันในส่วนของเรื่องความปลอดภัยทางด้านไซเบอร์และความสะดวกสบาย ซึ่งจะเป็นการสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์ให้เจ้าหน้าที่หน่วยงานทุกคน โดยให้ถือปฏิบัติตามเพื่อความปลอดภัยการใช้งานในยุคของข้อมูลข่าวสารเทคโนโลยีในชีวิตประจำวัน

การอบรมการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

คำอธิบาย

เรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานให้กับเจ้าหน้าที่ของสำนักงานโครงการ TO BE NUMBER ONE และชีวิตประจำวัน

วัตถุประสงค์

1. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
2. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆและแนวทางป้องกันแก้ไข
3. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

หัวข้อ

- แนะนำบทเรียน
- Cybersecurity คืออะไร
- ความรู้พื้นฐานของ Cybersecurity
- รูปแบบภัยคุกคามของ Cybersecurity
- ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

รูปแบบ

- ศึกษาผ่านระบบหลักสูตรออนไลน์ของ สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy ที่เว็บไซต์หน่วยงาน https://tdga.dga.or.th/knowledge/e-learning/detail/?content_id=27

หมวดที่ 1
การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

วัตถุประสงค์

1. เพื่อกำหนดการเข้าถึงข้อมูลสารสนเทศ โดยคำนึงถึงการใช้งานและความมั่งคงปลอดภัยด้านสารสนเทศ
2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิและการมอบอำนาจของหน่วยงานของรัฐ
3. เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
4. เพื่อให้การตรวจสอบและติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศได้อย่างถูกต้อง

นโยบาย

บุคลากรสำนักงานโครงการ TO BE NUMBER ONE และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

1. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ก็ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ / เจ้าของข้อมูล ตามความจำเป็นต่อการใช้งานเท่านั้น
2. ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น
3. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวน สิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

3.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

3.1.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ

- ไม่มีสิทธิ์

3.1.2 กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

3.1.3 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหนาหน่วยงานหรือ ผู้ดูแลระบบที่ได้รับมอบหมาย

3.2 การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

3.2.1 จัดแบ่งประเภทของข้อมูลออกเป็น ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

3.2.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

3.2.3 จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง
- ข้อมูลลับ หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ
- ข้อมูลใช้งานภายในหน่วยงาน หมายถึง ข้อมูลที่ใช้งานภายในหน่วยงานและไม่ได้รับอนุญาตให้นำไปใช้งานภายนอกหน่วยงาน
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่ไม่จำเป็นต้องได้รับการคุ้มครองความมั่นคงปลอดภัย ข้อมูลที่เผยแพร่สู่สาธารณะ ผ่านช่องทางที่เหมาะสมซึ่งองค์กรพิจารณาอนุมัติ หากข้อมูลสูญหายหรือถูกเปิดเผยจะไม่ส่งผลเสียหายต่อองค์กร

3.2.4 จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

3.2.5 รูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น TEXT Format, Document Format, PDF Format (Portable Document Format)

- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ มีรูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

4. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

5. เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ และอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ทั้งทางกายภาพ (Physical Access) และจากระยะไกล (Remote Access) บุคคลภายนอกดังกล่าวต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากสำนักงานโครงการ TO BE NUMBER ONE และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหายบุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

6. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

7. การจัดการสื่อบันทึกข้อมูล (Media Handing)

7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยก/เคลื่อนย้ายได้ (Management of Removable Media) กรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูล ต้องจัดให้มีกระบวนการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูลและไม่ให้สามารถกู้คืนข้อมูลได้

7.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

7.2.1 ผู้ดูแลระบบ / ผู้ใช้งานต้องทำลายข้อมูลที่เป็นความลับ ที่บันทึกในอุปกรณ์สื่อบันทึกข้อมูลแฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบ หรือเขียนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูล ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันการรั่วไหลของข้อมูล หรือป้องกันไม่ให้ข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้เครื่องหั่นแผ่น CD/DVD หรือกรรไกตัดทำลาย
ฮารดดิสก์	- ให้การทำลายข้อมูลบน ฮารดดิสก์ ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

7.2.2 กรณีที่จัดเก็บเป็นระยะเวลานาน ต้องคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใหม่

8.3 การขนย้ายสื่อบันทึก (Physical Media Transfer)

8.3.1 ผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึกที่มีข้อมูลออกจากพื้นที่ทำการจะต้องดูแลรักษาความปลอดภัย จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์ หรือทำให้เสียหายระหว่างการขนย้าย

8.3.2 ผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึกที่มีข้อมูลออกจากพื้นที่ทำการต้องชดใช้ค่าเสียหาย ไม่ว่าทรัพย์สินนั้นจะชำรุด หรือ สูญหายตามมูลค่าของทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทเลินเล่อของผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึก

หมวดที่ 2
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งาน (User) ที่ได้รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศ และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

1. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนบุคลากรใหม่ (User Registration) เพื่อรับสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

2. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อบุคลากรไม่ได้ปฏิบัติงานแล้ว

3. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการควบคุม จำกัด และเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

4. กำหนดให้มีการบริหารจัดการรหัสผ่าน (User Password Management) อย่างรัดกุมโดยเริ่มตั้งแต่กระบวนการสร้างรหัสผ่านชั่วคราว (Temporary Password) ตามสิทธิที่ได้รับของผู้ใช้งาน (User) การส่งมอบรหัสผ่านชั่วคราว (Temporary Password) การเปลี่ยนรหัสผ่าน เงื่อนไขการเปลี่ยนรหัสผ่าน และการ กำหนดรหัสผ่านใหม่ในกรณีลืมรหัสผ่าน

5. กำหนดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง

6. กำหนดให้มีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักและความเข้าใจเรื่องภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

7. กำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

แนวปฏิบัติ

1. การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

1.1 กรณีบุคลากรสำนักงานโครงการ TO BE NUMBER ONE

1.1.1 บุคลากรใหม่กรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กลุ่มงานแผนงาน เพื่อสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่าน (Password) การใช้งาน

1.1.2 ผู้ดูแลระบบ (Administrator) กำหนดสิทธิการใช้งานระบบฯ ให้บุคลากรใหม่ตามสิทธิ พร้อมทั้งแจ้งให้บุคลากรใหม่ได้รับทราบ

1.2 การสร้างบัญชีผู้ใช้งาน (Username) และการกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

1.2.1 การสร้างบัญชีผู้ใช้งาน (Username) ให้ใช้ชื่อภาษาอังกฤษ ผู้ดูแลระบบจะต้องตรวจสอบบัญชีผู้ใช้งานเพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

1.2.2 การกำหนดรหัสผ่าน (Password) ชุดของตัวอักษร ตัวเลข และอักขระพิเศษอย่างน้อย 8 ตัวขึ้นไป ซึ่งต้องประกอบด้วยตัวเลข (Numerical character), ตัวอักษร (Alphabet) ประกอบด้วย ตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก และตัวอักษรพิเศษ (Special character)

– ตัวอักษร (a-z, A-Z)

– ตัวเลข (0-9)

– เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./) และยากต่อการคาดเดา โดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตน (Authentication) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

1.2.3 ให้ผู้ดูแลระบบ (Administrator) แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ผู้ใช้งาน (User) ทราบโดยตรง

1.2.4 เมื่อบุคลากรมีการเปลี่ยนชื่อหรือนามสกุล ให้แจ้งกลุ่มงานแผนงาน เพื่อเปลี่ยนแปลงข้อมูลส่วนบุคคลให้ถูกต้อง

1.3 การยกเลิกสิทธิการใช้งานของบุคลากรสำนักงานโครงการ TO BE NUMBER ONE ให้ดำเนินการ ดังนี้

1.3.1 ให้หัวหน้ากลุ่มงาน หรือเจ้าหน้าที่ในกลุ่มงานนั้น แจ้งกลุ่มงานแผนงาน เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก ให้โอน ย้าย หรือสิ้นสุดการจ้าง

1.3.2 กลุ่มงานแผนงานจะปิดบัญชีผู้ใช้งาน (Username) ชั่วคราวเป็นระยะเวลา 90 วัน ทั้งนี้เมื่อครบ 90 วัน นับจากมีคำสั่งเป็นลายลักษณ์อักษร กลุ่มงานแผนงานจะลบข้อมูลสารสนเทศของบัญชีผู้ใช้งาน (Username) ดังกล่าวเป็นการถาวร

2. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้ใช้งาน (User) ให้ดำเนินการ ดังนี้

2.1 ผู้ดูแลระบบ (Administrator) ตรวจสอบสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศตามแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ให้สอดคลองกับคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ หรือเหตุผลความจำเป็นของสำนักงานโครงการ TO BE NUMBER ONE ที่ได้แจ้งความประสงค์ในการให้บุคคลากรเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ แล้วแต่กรณี

2.2 ในกรณีที่มีการเปลี่ยนแปลงตำแหน่ง หรือหน้าที่ที่ได้รับมอบหมาย ให้บุคลากรแต่ละกลุ่มแจ้งกลุ่มงานแผนงานเพื่อเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้สอดคล่องกับการเปลี่ยนแปลงดังกล่าว

2.3 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้ากลุ่มงาน หรือผู้อำนวยการฯ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดได้บ้าง

3. ให้กลุ่มงานแผนงานจัดฝึกอบรมให้แก่ผู้ใช้งาน (User) เพื่อให้มีความรู้ ความเข้าใจและเกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ อย่างน้อยปีละ 1 ครั้ง หรือจัดให้ผู้ใช้งาน (User) เข้าร่วมการฝึกอบรมที่หน่วยงานอื่นจัดขึ้น

4. ให้กลุ่มงานแผนงานกำหนดมาตรการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศตามความเหมาะสม ได้แก่ ยกเลิกการใช้งาน Internet กรณีที่มีการตรวจพบ Package จาก Users นั้นๆ มากผิดปกติ หรือการแจ้งเตือนผู้ใช้งาน (User) เมื่อมีไวรัสแพร่ระบาด

5. เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

หมวดที่ 3
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมย อุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

1. กำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)

2. กำหนดแนวปฏิบัติในการป้องกันระบบคอมพิวเตอร์ และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ในขณะที่ไม่มีผู้ใช้งาน (User) ดูแล

3. กำหนดแนวปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ได้แก เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศเพื่อไม่ให้สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งาน (User) ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

4. กำหนดให้ผู้ใช้งาน (User) อาจนำการเข้ารหัสข้อมูล (Encryption) มาใช้กับการรับ-ส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. 2544

แนวปฏิบัติ

1. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้

1.1 ผู้ใช้งาน (User) ต้องกำหนดรหัสผ่าน (Password) ชุดของตัวอักษร ตัวเลข และอักขระพิเศษอย่างน้อย 8 ตัวขึ้นไป ซึ่งต้องประกอบด้วยตัวเลข (Numerical character), ตัวอักษร (Alphabet) ประกอบด้วย ตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก และตัวอักษรพิเศษ (Special character) – ตัวอักษร (a-z, A-Z) – ตัวเลข (0-9) – เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

1.2 ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก 9 เดือน และรหัสผ่าน (Password) ใหม่ ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

1.3 ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพรแจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

1.4 ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

1.5 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

1.6 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

1.7 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

1.8 กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการสงมอบรหัสผ่าน ให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

1.9 การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

1.10 การกระทำใดๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

2. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อค หรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

2.1 คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

2.2 การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

2.3 การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

2.4 เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

2.5 เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาไม่เกิน 15 นาที

3. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของสำนักงานโครงการ TO BE NUMBER ONE หรือเป็นข้อมูลของบุคคลภายนอก

4. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง / ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

5. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของหน่วยงาน หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

6. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่างๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

7. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร หน่วยงาน จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้น ในกรณีที่หน่วยงานต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับสำนักงานโครงการ TO BE NUMBER ONE ซึ่งหน่วยงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

8. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่งที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า

แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอรแรนท (Bit torrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

9. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เล่นเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

10. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้เพื่อการเผยแพรข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของสำนักงานโครงการ TO BE NUMBER ONE

11. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใด อันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของสำนักงานโครงการ TO BE NUMBER ONE

12. ห้ามใช้สินทรัพย์ของสำนักงานโครงการ TO BE NUMBER ONE เพื่อประโยชน์ทางการค้า

13. ห้ามกระทำการใดๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศ สำนักงานโครงการ TO BE NUMBER ONE โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

14. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

15. ห้ามใช้ระบบสารสนเทศสำนักงานโครงการ TO BE NUMBER ONE เพื่อการควบคุมคอมพิวเตอร์หรือระบบ สารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

16. ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

17. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเข้าถึงระบบสารสนเทศของสำนักงานโครงการ TO BE NUMBER ONE โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

หมวดที่ 4
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศ และการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของสำนักงานโครงการ TO BE NUMBER ONE ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินและการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่อง แม้ในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลา ที่เหมาะสมและสามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง

นโยบาย

1. พิจารณาคัดเลือกระบบสารสนเทศที่เหมาะสมในการจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน
2. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของสำนักงานโครงการ TO BE NUMBER ONE เพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
3. กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบตามแผนบริหารความต่อเนื่องของสำนักงานโครงการ TO BE NUMBER ONE ด้านสารสนเทศ
4. ทดสอบสภาพพร้อมใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ และระบบสำรองตามแผน
5. บริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของสำนักงานโครงการ TO BE NUMBER ONE อย่างน้อยปีละ 1 ครั้ง
6. กำหนดความถี่ของการปฏิบัติในแต่ละข้อ โดยต้องมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของหน่วยงาน

แนวปฏิบัติ

1. สำนักงานโครงการ TO BE NUMBER ONE ต้องจัดทำระบบสารสนเทศและระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน โดยมีขั้นตอน ดังนี้

1.1 ผู้ดูแลระบบ (Administrator) จัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูลและการกู้คืนข้อมูลสารสนเทศ

1.3 ผู้ดูแลระบบ (Administrator) ต้องพิมพ์รายละเอียดไว้บนตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรือ External Disk และอื่นๆ ที่ใช้สำหรับการสำรองข้อมูลได้แก่รูปแบบการสำรองข้อมูลแบบรายวันหรือรายสัปดาห์หรือรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล

1.4 ผู้ดูแลระบบ (Administrator) ต้องกำหนดรูปแบบการกู้คืนข้อมูลของระบบการสำรองข้อมูล (Backup System) โดยมีความถี่และรูปแบบ ดังนี้

1.4.1 การกู้คืนข้อมูลรายวันจากอุปกรณ์ที่ใช้ในการสำรองข้อมูล เฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) หรือที่สำรองข้อมูลเฉพาะส่วนที่มีการเปลี่ยนแปลง (Differential Backup)

1.4.2 การกู้คืนข้อมูลรายสัปดาห์หรือรายเดือนจากอุปกรณ์ที่ใช้ในการสำรองข้อมูลแบบสมบูรณ์ (Full Backup)

2. สำนักงานโครงการ TO BE NUMBER ONE ดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของหน่วยงาน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ดังนี้

2.1 กำหนดผู้มีหน้าที่รับผิดชอบระบบสารสนเทศ

2.2 กำหนดผู้มีหน้าที่รับผิดชอบระบบสำรองข้อมูลสารสนเทศ

2.3 กำหนดผู้มีหน้าที่รับผิดชอบการจัดทำแผนดังกล่าว

2.4 กำหนดให้ปรับปรุงแผนดังกล่าวทุก 2 ปี

3. สำนักงานโครงการ TO BE NUMBER ONE ต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้อย่างน้อยปีละ 1 ครั้ง ทั้งนี้ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์และแผนการสำรองข้อมูลสำนักงานโครงการ TO BE NUMBER ONE รวมถึงการทดสอบสภาพความพร้อมใช้งาน ได้นำข้อมูลไปรวมไว้ในแผนบริหารความต่อเนื่องในสภาวะวิกฤต ด้านสารสนเทศของสำนักงานโครงการ TO BE NUMBER ONE

หมวดที่ 5
การบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศ

สำนักงานโครงการ TO BE NUMBER ONE ได้นำเทคโนโลยีสารสนเทศและการสื่อสารเข้ามาใช้ในการปฏิบัติงานของหน่วยงานจึงมีความจำเป็นต้องมีแผนบริหารจัดการความเสี่ยงด้านสารสนเทศ ภายใต้แผนบริหารจัดการความเสี่ยงของกรมสุขภาพจิตอีกลำดับหนึ่งเพื่อป้องกันปัญหาที่อาจเกิดขึ้น อันส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงาน เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานอันจะเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น ด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงเกิดขึ้นจริงและนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในการดำเนินการ

วัตถุประสงค์

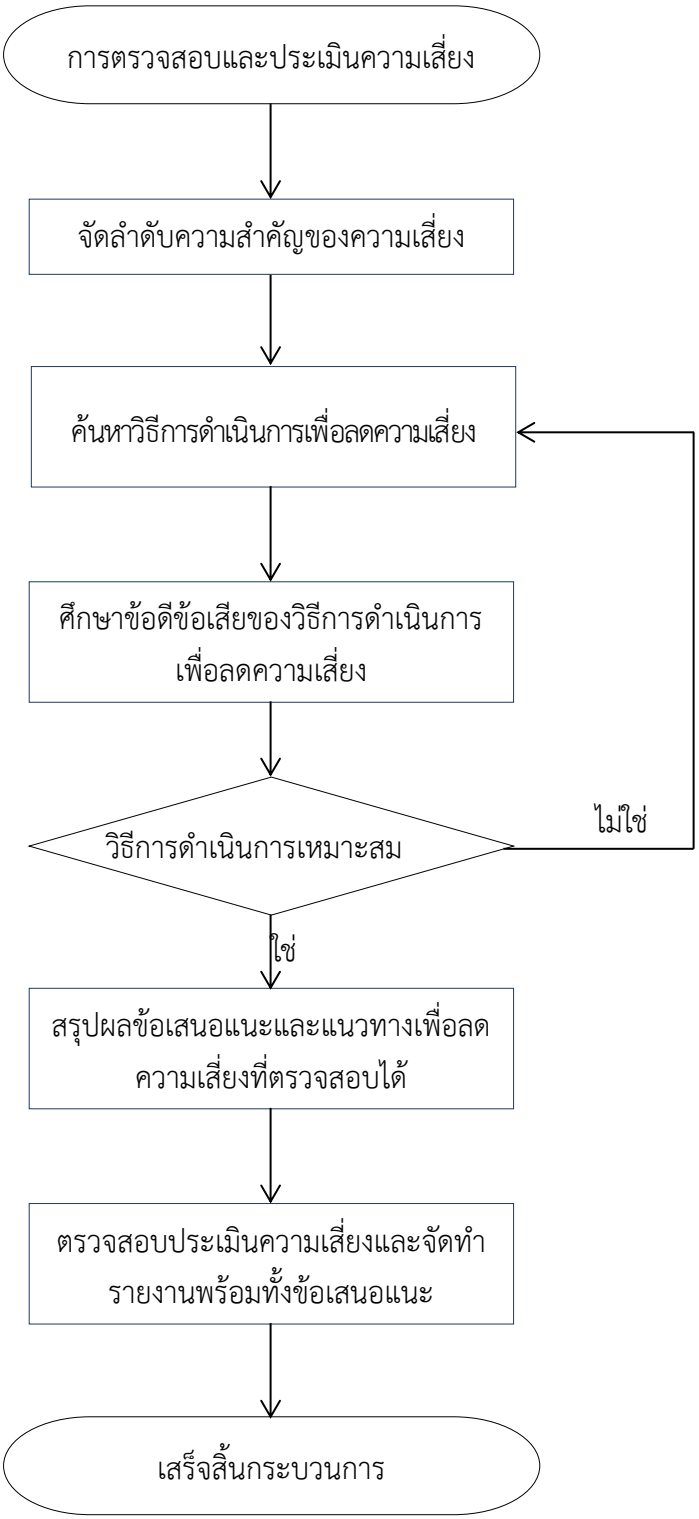
1. เพื่อเป็นแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศภายในหน่วยงาน
2. เพื่อเป็นแนวทางในการลดความเสี่ยงที่อาจส่งผลกระทบต่อระบบสารสนเทศภายในหน่วยงาน
3. เพื่อเป็นแนวทางปฏิบัติเมื่อมีความเสี่ยงเกิดขึ้นกับระบบสารสนเทศในหน่วยงาน

การตรวจสอบและประเมินความเสี่ยง

ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศภายในสำนักงานโครงการ TO BE NUMBER ONEจากผู้รับผิดชอบการตรวจสอบภายในหน่วยงาน(Internal Auditor) โดยมีแนวทางในการตรวจและประเมินความเสี่ยงดังนี้

1. จัดลำดับความสำคัญของความเสี่ยง
2. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง
3. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง
4. สรุปผลข้อเสนอแนะและแนวทางเพื่อลดความเสี่ยงที่ตรวจสอบได้
5. มีการตรวจสอบประเมินความเสี่ยงและจัดทำรายงานพร้อมข้อเสนอแนะ

ผังงานการตรวจสอบและประเมินความเสี่ยง



แผนปฏิบัติที่ 1 อุปกรณ์คอมพิวเตอร์เสียหาย

คำอธิบายความเสี่ยง อุปกรณ์คอมพิวเตอร์เสียหาย

สาเหตุความเสี่ยง

-อายุการใช้งานของเครื่องคอมพิวเตอร์

-การใช้งานหนัก

-ขาดการดูแล บำรุงรักษา

-ขาดแผนการจัดซื้อทดแทน

ผลกระทบของความเสี่ยง

-เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้

-อุปกรณ์ภายในคอมพิวเตอร์เสียหาย

แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

-ดำเนินการอบรมให้ความรู้ในการดูแลรักษาเครื่องคอมพิวเตอร์ การใช้งานเครื่องคอมพิวเตอร์อย่างถูกต้อง การ
สำรองข้อมูลภายในเครื่องคอมพิวเตอร์ แก่บุคลากรของของสำนักงานโครงการ TO BE NUMBER ONE

-กลุ่มงานแผนงาน จัดทำคู่มือการดูแลรักษาคอมพิวเตอร์ ระเบียบปฏิบัติการซ่อมบำรุงคอมพิวเตอร์และประกาศให้บุคลากรของสำนักงานโครงการ TO BE NUMBER ONEทราบ

- การสำรองข้อมูลที่สำคัญภายในเครื่องคอมพิวเตอร์

-จัดทำแผนการจัดซื้อทดแทนเมื่อครุภัณฑ์มีอายุการใช้งาน 5 ปีขึ้นไป

ผู้รับผิดชอบ

- กลุ่มงานแผนงาน และบุคลากรของของสำนักงานโครงการ TO BE NUMBER ONE

แผนปฏิบัติที่ 2 อุปกรณ์เครือข่ายเสียหาย

คำอธิบายความเสี่ยง อุปกรณ์เครือข่ายเสียหาย

สาเหตุความเสี่ยง

-สภาพแวดล้อมที่ใช้งาน

-อุปกรณ์ชำรุด ขาดการตรวจสอบ ซ่อมบำรุง

-ปัญหาที่เกิดจากภายนอก ซึ่งไม่สามารถควบคุมได้

ผลกระทบของความเสี่ยง

-เครือข่ายอินเตอร์เน็ตในหน่วยงานไม่สามารถใช้งานได้

แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

-อบรมและทำคู่มือวิธีการดูแลอุปกรณ์เครือข่ายคอมพิวเตอร์ และประกาศให้บุคลากรในหน่วยงานทราบ

-ตรวจสอบการทำงานของอุปกรณ์เครือข่ายภายในหน่วยงานเป็นประจำ

-เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศของหน่วยงานดำเนินการตรวจสอบการทำงานของอุปกรณ์เครือข่ายคอมพิวเตอร์ เป็นประจำ

-จัดทำแผนการจัดซื้อทดแทนเมื่อครุภัณฑ์มีอายุการใช้งาน 5 ปีขึ้นไป

ผู้รับผิดชอบ

กลุ่มงานแผนงาน สำนักงานโครงการ TO BE NUMBER ONE

แผนปฏิบัติที่ 3 อุปกรณ์คอมพิวเตอร์แม่ข่ายเสียหาย

คำอธิบายความเสี่ยง อุปกรณ์คอมพิวเตอร์แม่ข่ายเสียหาย

สาเหตุความเสี่ยง

-ขาดการดูแล บำรุงรักษา

-อายุการใช้งานของเครื่องคอมพิวเตอร์แม่ข่าย

-แผนการจัดซื้ออุปกรณ์ทดแทนไม่ได้ตามแผนที่กำหนด

ผลกระทบของความเสี่ยง

-อุปกรณ์คอมพิวเตอร์แม่ข่ายเสียหาย

-เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถใช้งานได้

แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

-จัดทำคู่มือการดูแลบำรุงรักษาและตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย

-จัดทำแผนการกู้คืนระบบ และซ้อมการกู้คืนระบบอย่างสม่ำเสมอ

-ดำเนินการตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายอย่างน้อยวันละ 1 ครั้ง

-ดำเนินการสำรองข้อมูลที่อยู่ภายในเครื่องคอมพิวเตอร์แม่ข่าย

-จัดทำแผนการจัดซื้อทดแทนเมื่อครุภัณฑ์มีอายุการใช้งาน 5 ปีขึ้นไป

ผู้รับผิดชอบ

- กลุ่มงานแผนงาน สำนักงานโครงการ TO BE NUMBER ONE

แผนปฏิบัติที่ 4 อุปกรณ์จัดเก็บข้อมูลกลางเสียหาย

คำอธิบายความเสี่ยง อุปกรณ์จัดเก็บข้อมูลกลางเสียหาย

สาเหตุความเสี่ยง

-ขาดการดูแล บำรุงรักษา

-อายุการใช้งานของอุปกรณ์

-ขาดแผนการจัดซื้อทดแทน

ผลกระทบของความเสี่ยง

-อุปกรณ์จัดเก็บข้อมูลกลางเสียหายไม่สามารถใช้งานได้

-ข้อมูลที่ถูกจัดเก็บไว้สูญหาย

แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

-ดำเนินการตรวจสอบการทำงานของอุปกรณ์จัดเก็บข้อมูลกลางอย่างสม่ำเสมอ

-ดำเนินการสำรองข้อมูลอย่างน้อย 1 ครั้งต่อเดือน

-จัดทำแผนการจัดซื้อทดแทนเมื่อครุภัณฑ์มีอายุการใช้งาน 5 ปีขึ้นไป

ผู้รับผิดชอบ กลุ่มงานแผนงาน สำนักงานโครงการ TO BE NUMBER ONE

แผนปฏิบัติที่ 5 ระบบปฏิบัติการคอมพิวเตอร์(Operating System)เสียหาย

คำอธิบายความเสี่ยง ระบบปฏิบัติการคอมพิวเตอร์(Operating System)เสียหายเสียหาย

สาเหตุความเสี่ยง

-อายุการใช้งานของเครื่องคอมพิวเตอร์

-อายุการใช้งานของระบบปฏิบัติการ

-การติดไวรัส มัลแวร์

-การลงซอฟแวร์ การติดตั้ง Driver ต่างๆ

-ขาดการ Update ระบบปฏิบัติการ

-ระบบปฏิบัติการที่สิ้นสุดการ support

-การใช้ระบบปฏิบัติการ ที่ละเมิดลิขสิทธิ์

-การใช้งานเครื่องคอมพิวเตอร์ที่ไม่ถูกวิธี

-ไม่ติดตั้ง Antivirus และ Updateให้เป็นปัจจุบัน

ผลกระทบของความเสี่ยง

-เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้

-ระบบปฏิบัติการไม่สามารถใช้งานได้

-ข้อมูลที่อยู่ภายในเครื่องสูญหาย

แนวปฏิบัติเพื่อป้องกันความเสี่ยง

-ใช้ระบบปฏิบัติการที่ถูกลิขสิทธิ์

-Update ระบบปฏิบัติการอยู่เสมอ

-ติดตั้ง Antivirus และดำเนินการ Update Antivirus ให้ทันสมัยอยู่เสมอ

-สแกนไวรัสอย่างสม่ำเสมอ

-ระมัดระวังในการใช้งานอุปกรณ์จัดเก็บข้อมูลแบบพกพา (Flash Drive / External Hard Drive) และควรสแกนไวรัสก่อนการใช้งานทุกครั้ง

-จัดอบรมบุคลากรของสถาบันสุขภาพจิตเด็กและวัยรุ่นราชนครินทร์ ในการใช้เครื่องคอมพิวเตอร์และการ

บำรุงรักษาอย่างถูกวิธี

-ดำเนินการสำรองข้อมูลในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ

ผู้รับผิดชอบ กลุ่มงานแผนงาน และบุคลากรของสำนักงานโครงการ TOBE NUMBER ONE

แผนปฏิบัติที่ 6 ซอฟแวร์การใช้ประโยชน์งานอื่นๆเสียหาย

คำอธิบายความเสี่ยง ซอฟแวร์การใช้ประโยชน์งานอื่นๆเสียหาย

สาเหตุความเสี่ยง

-การลงซอฟแวร์ที่ไม่สมบูรณ์

-การติดไวรัส มัลแวร์

-การติดตั้งซอฟแวร์ที่ไม่รู้แหล่งที่มา

-การติดตั้งซอฟแวร์ผิดลิขสิทธิ์

-บุคลากรดำเนินการติดตั้งซอฟแวร์ด้วยตนเอง

ผลกระทบของความเสี่ยง

-ไม่สามารถใช้งานโปรแกรมได้

-ระบบปฏิบัติการไม่สามารถใช้งานได้

-ติดไวรัส มัลแวร์

-ถูก Hack เครื่องคอมพิวเตอร์ที่ใช้งาน

แนวปฏิบัติเพื่อป้องกันความเสี่ยง

-ใช้ซอฟแวร์ที่ถูกลิขสิทธิ์ หรือใช้ซอฟแวร์ประเภท Open Source เพื่อทดแทนการละเมิดลิขสิทธิ์

-ชี้แจงบุคลากร เรื่องห้ามดำเนินการติดตั้งซอฟแวร์ด้วยตนเอง

ผู้รับผิดชอบ

กลุ่มงานแผนงาน และบุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

แผนปฏิบัติที่ 7 บุคลากรของสถาบันฯขาดความรู้ความเข้าใจเรื่องของความปลอดภัยทางด้านสารสนเทศ

คำอธิบายความเสี่ยง บุคลากรของหน่วยงานขาดความรู้ความเข้าใจเรื่องของความปลอดภัยทางด้านสารสนเทศ

สาเหตุความเสี่ยง

-ไม่ทำตามระเบียบปฏิบัติที่ถูกกำหนดไว้

-ขาดความรู้ความเข้าใจเกี่ยวกับความปลอดภัยทางด้านสารสนเทศในการทำงาน

-บุคลากรขาดความระมัดระวังในการจัดเก็บ การเข้าถึงข้อมูล การเรียกใช้ข้อมูล การทำลายข้อมูล ที่ไม่ถูกวิธี

ผลกระทบของความเสี่ยง

-ถูกโจมตี หรือถูก Hack ข้อมูล

-ข้อมูลรั่วไหลไปยังภายนอกและส่งผลกระทบต่อสถาบันสุขภาพจิตเด็กและวัยรุ่นราชนครินทร์

แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

-จัดทำระเบียบปฏิบัติด้านการเข้าถึงข้อมูลทางด้านกายภาพ และทางด้านดิจิทัล และดำเนินการสื่อสารแก่บุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

ผู้รับผิดชอบ

กลุ่มงานแผนงาน และบุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

แผนปฏิบัติที่ 8 ความปลอดภัยของข้อมูล

คำอธิบายความเสี่ยง ความปลอดภัยของข้อมูล

สาเหตุความเสี่ยง

-เครื่องคอมพิวเตอร์ติดไวรัส มัลแวร์

-อุปกรณ์ภายในเสียหาย

-การปฏิบัติงานที่ผิดพลาด

-บุคลากรละเลยความปลอดภัยทางด้านสารสนเทศ

-การจัดเก็บข้อมูลทางด้านกายภาพ และทางด้านดิจิทัล ยังไม่มีความปลอดภัย

-การทำลายเอกสารและข้อมูลที่ไม่ถูกวิธี

ผลกระทบของความเสี่ยง

-ข้อมูลสูญหาย

-ข้อมูลความสำคัญรั่วไหลหรือสูญหายเอกสาร และทางด้านดิจิทัล

-การโจมตีทางด้าน Cyber Security

-เอกสารถูกโจรกรรม

-ข้อมูลรั่วไหลไปยังภายนอกและส่งผลกระทบต่อสำนักงานโครงการ TO BE NUMBER ONE

แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

-จัดทำระเบียบปฏิบัติด้านการเข้าถึงข้อมูลทางด้านกายภาพ และทางด้านดิจิทัล และดำเนินการสื่อสารแก่บุคลากรของสำนักงานโครงการ TO BE NUMBER ONEให้ทราบ

-สื่อสารเรื่องการทำลายเอกสารและข้อมูล

ผู้รับผิดชอบ

- กลุ่มงานแผนงาน และกลุ่มงานต่างๆ ของสำนักงานโครงการ TO BE NUMBER ONE ที่ดำเนินการจัดเก็บข้อมูล

สรุปแนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

การบริหารความเสี่ยงของระบบสารสนเทศ เป็นหน้าที่ความรับผิดชอบของบุคลากรทุกคน และ เป็นการป้องกันความเสี่ยงที่ทุกคนต้องช่วยกันปฏิบัติ เพื่อป้องกันความเสี่ยง ดังนี้

1. ด้านฮาร์ดแวร์ (hardware)

1.1เครื่องแม่ข่าย อุปกรณ์เครือข่าย

-ไม่อนุญาตให้บุคคลภายนอกเข้า

-เลือกสถานที่เหมาะสม ทั้งสถานที่ และ สภาพอากาศ

1.2 ไม่อนุญาตให้ผู้อื่นใช้เครื่องของตนเอง

1.3 ตั้งรหัสผ่านเพื่อป้องกันเครื่องคอมพิวเตอร์ และ ข้อมูลความลับของแต่ละฝ่าย

1.4 หมั่นดูแลรักษา สังเกตความผิดปกติของเครื่องตนเอง

2. ด้านซอฟแวร์ (software)

-ไม่ควรติดตั้งโปรแกรมที่ไม่รู้จักแหล่งที่มา

3. ด้านข้อมูล (Data)

3.1 ต้องมีการสำรองข้อมูลที่สำคัญ

3.2 ต้องมีความรักษาความปลอดภัยของข้อมูลในแต่ละฝ่าย

3.3 มีการจำกัดสิทธิ์ในการเข้าถึงข้อมูล

4. ด้านบุคลากร (people)

4.1 ผู้บริหารระบบ

-ดูแลรักษาเครื่องคอมพิวเตอร์ ระบบเครือข่ายภายในองค์กร

-ควบคุม ดูแล การใช้งานระบบ

-รักษาความปลอดภัยของระบบ

4.2 ผู้ใช้งาน

-ดูแลรักษาเครื่องคอมพิวเตอร์ของตนเอง

-รักษาข้อมูลที่สำคัญของตนเอง/ฝ่าย

หมวดที่ 6
การใช้งานซอฟต์แวร์ที่มีลิขสิทธ์ถูกต้องและซอฟต์แวร์ป้องกันไวรัส

ปัจจัยที่ส่งผลต่อการใช้งานซอฟต์แวร์ถูกลิขสิทธิ์ในการทำงานที่สำคัญที่สุดของ ทั้งสามกลุ่ม คือ ผู้ใช้งาน นักพัฒนาโปรแกรม และผู้ดูแลสิทธิ์ เป็นปัจจัยทางด้านราคา หากราคาของซอฟต์แวร์ถูกลิขสิทธิ์มีราคาที่ไม่สูงจนเกินไป จะส่งผลให้มีการใช้งานซอฟต์แวร์ถูกลิขสิทธิ์ในการทำงานมากขึ้น ปัจจัยที่สสำคัญรองลงมาที่ส่งผลต่อการใช้งานซอฟต์แวร์ถูกลิขสิทธิ์ในการประกอบธุรกิจ คือ ปัจจัย การสนับสนุนจากผู้บริหารระดับสูง ปัจจัยความคาดหวังถึงสมรรถนะ และปัจจัยกฎหมายลิขสิทธิ์ซอฟต์แวร์ ตามลำดับ

สำนักงานโครงการ TO BE NUMBER ONE จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การใช้งานซอฟท์แวร์ที่มีลิขสิทธิ์ถูกต้องและการใช้งานซอฟแวร์ป้องกันไวรัส ดังนี้

"ลิขสิทธิ์" คือ สิทธิแต่ผู้เดียวที่จะทำการใดๆ ตามพระราชบัญญัติฯ เกี่ยวกับงานที่ "ผู้สร้างสรรค์" ได้ทำขึ้น

"ผู้สร้างสรรค์" คือ ผู้ทำ หรือ ผู้ก่อให้เกิดงานสร้างสรรค์อย่างใดอย่างหนึ่งที่เป็นงานอันมีลิขสิทธิ์ตามพระราชบัญญัติฯ

"โปรแกรมคอมพิวเตอร์" คือ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่นำไปใช้กับเครื่องคอมพิวเตอร์ เพื่อให้เครื่องคอมพิวเตอร์ทำงานหรือเพื่อให้ได้รับผลอย่างใดอย่างหนึ่ง ทั้งนี้ไม่ว่าจะเป็นภาษาโปรแกรมคอมพิวเตอร์ในลักษณะใด

"การดัดแปลง" ในส่วนที่เกี่ยวกับโปรแกรมคอมพิวเตอร์ คือ การทำซ้ำโดยเปลี่ยนรูปแบบใหม่ ปรับปรุง แก้ไขเพิ่มเติมโปรแกรมคอมพิวเตอร์ในส่วนอันเป็นสาระสำคัญ โดยไม่มีลักษณะเป็นการจัดทำขึ้นใหม่

“ข้อมูลการบริหารสิทธิ” คือ ข้อมูลที่บ่งชี้ถึงผู้สร้างสรรค์ งานสร้างสรรค์ นักแสดง การแสดง เจ้าของลิขสิทธิ์ หรือระยะเวลาและเงื่อนไขการใช้งานอันมีลิขสิทธิ์ ตลอดจนตัวเลขหรือรหัสแทนข้อมูลดังกล่าว โดยข้อมูลเช่นว่านี้ติดอยู่หรือปรากฏเกี่ยวข้องกับงานอันมีลิขสิทธิ์หรือสิ่งบันทึกการแสดง

“มาตรการทางเทคโนโลยี” หมายความว่า เทคโนโลยีที่ออกแบบมาเพื่อป้องกันการทำซ้ำหรือควบคุมการเข้าถึงงานอันมีลิขสิทธิ์หรือสิ่งบันทึกการแสดง โดยเทคโนโลยีเช่นว่านี้ได้นำมาใช้กับงานอันมีลิขสิทธิ์หรือสิ่งบันทึกการแสดงนั้นอย่างมีประสิทธิภาพ

“การหลบเลี่ยงมาตรการทางเทคโนโลยี” หมายความว่า การกระทำด้วยประการใด ๆ ที่ทำให้มาตรการทางเทคโนโลยีไม่เกิดผล”

“ซอฟต์แวร์” เรียกตามกฎหมาย คือ "โปรแกรมคอมพิวเตอร์" เพราะเป็นสิ่งที่ทำให้คอมพิเตอร์ทำงานได้ (เช่น ใส่ Windows ลงบนเครื่องแล้วเครื่องสามารถตอบสนองได้ หรือ ใส่ Office ลงเครื่องแล้ว เครื่องสามารถประมวลผลการพิมพ์ได้)

"ไวรัสคอมพิวเตอร์" ถูกนำมาใช้ในความหมายของ "มาลแวร์" ซึ่งนอกจากจะหมายถึงไวรัสคอมพิวเตอร์ในรูปแบบต่างๆ แล้วนั้น ตัวอย่างไวรัสคอมพิวเตอร์ประเภทต่างๆ ดังนี้

หนอนอินเทอร์เน็ต (Internet Worm) ซึ่งหมายถึงโปรแกรมที่ออกแบบมาให้สามารถแพร่ กระจายไปยังเครื่องคอมพิวเตอร์เครื่องอื่นได้ด้วยตัวเอง โดยอาศัยระบบเครือข่ายคอมพิวเตอร์ เช่น อี-เมล์ หรือ การแชร์ไฟล์ ทำให้การแพร่กระจายเป็นไปอย่างรวดเร็วและเป็นวงกว้าง

โทรจัน (Trojan) ซึ่งหมายถึงโปรแกรมที่ออกแบบมาให้แฝงเข้าไปสู่ระบบคอมพิวเตอร์ของผู้ใช้อื่นในหลากหลายรูปแบบ เช่น โปรแกรม หรือ การ์ดอวยพร เป็นต้น เพื่อดักจับ ติดตาม หรือควบคุมการทำงานของเครื่องคอมพิวเตอร์ที่ถูกคุกคาม

โค้ด Exploit ซึ่งหมายถึงโปรแกรมที่ออกแบบมาให้สามารถเจาะระบบโดยอาศัยช่องโหว่ของระบบปฏิบัติการหรือแอพพลิเคชันที่ทำงานอยู่บนระบบ เพื่อให้ไวรัสหรือผู้บุกรุกสามารถครอบครอง ควบคุม หรือกระทำการอย่างหนึ่งอย่างใดบนระบบได้

ไวรัสหลอกลวง (Hoax) ซึ่งมักจะอยู่ในรูปแบบของการส่งข้อความต่อๆ กันไป เหมือนกับการส่งจดหมายลูกโซ่ โดยข้อความประเภทนี้จะใช้หลักจิตวิทยา ทำให้ข่าวสารนั้นน่าเชื่อถือ ถ้าผู้ที่ได้รับข้อความปฏิบัติตามอาจจะทำให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ เช่น การให้ลบไฟล์ข้อมูลที่จำเป็นของระบบปฏิบัติการโดยหลอกว่าเป็นไวรัสคอมพิวเตอร์ ทำให้ระบบปฏิบัติการทำงานผิดปกติ เป็นต้น

บู๊ตเซกเตอร์ไวรัส (Boot Sector Viruses หรือ Boot Infector Viruses) คือไวรัสที่แพรากระจายในตอนที่ทำการบู๊ตเครื่อง โดยเก็บตัวเองอยู่ในบู๊ตเซกเตอร์ของฮาร์ดดิสก์ การทำงานของบู๊ตเซกเตอร์ไวรัส บู๊ตเซ็กเตอร์ไวรัสจะทำงานได้ก็ต่อเมื่อเราเสียบแผ่นดิสก์เก็ตคาไว้ที่ไดรว์ พอเราเปิดเครื่องคอมพิวเตอร์ขึ้นมาเครื่องจะบู๊ตข้อมูลจากแผ่นดิสก์ก่อน

มาโครไวรัส (Macro Viruses) ไวรัสที่แทรกมากับไฟล์เอกกสารที่มีการฝังคำสั่งควบคุมการทำงานไว้

วัตถุประสงค์

เพื่อให้เจ้าหน้าที่สำนักงานโครงการ TO BE NUMBER ONE ได้ใช้ซอฟท์แวร์ที่ถูกต้องตามกฎหมายในการทำงาน และเพื่อเพิ่มประสิทธิภาพในการทำงานของเจ้าหน้าที่ ทั้งเพื่อป้องกันไวรัสคอมพิวเตอร์ที่จะทำให้คอมพิวเตอร์และข้อมูลได้รับความเสียหายได้

นโยบาย

1. บุคลากรสำนักงานโครงการ TO BE NUMBER ONE ได้ใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องมีใช้ในการทำงานภายในหน่วยหน่วยงานอย่างถูกต้อง และการใช้ซอฟต์แวร์ป้องกันไวรัสอย่างมีประสิทธิภาพ เพื่อสนับสนุนการักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

แนวปฏิบัติ

การใช้ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์

วิธีการป้องกันไวรัสคอมพิวเตอร์(Computer Virus Protection)

1. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทฐานข้อมูลไวรัสใหม่ๆ อยู่เสมอ (Install Antivirus Program)
2. สแกนไวรัสในเครื่องคอมพิวเตอร์อย่างน้อย 1 ครั้งต่อสัปดาห์ โดยใช้โปรแกรมจากข้อ 1 (Scan Virus at least 1 time/week)
3. ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูล (Media) ต่าง ๆ
   - การบันทึกข้อมูลแบบ USB เป็นต้น
   - สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
   - ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลก ๆ ที่น่าสงสัย เช่น .pif เป็นต้น รวมทั้งไฟล์ที่มีนามสกุลซ้อนกัน เช่น .jpg.exe, .gif.scr , txt.exe เป็นต้น
   - ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา
4. ใช้ความระมัดระวังในการเปิดอ่าน E-mail
   - ไม่เปิดไฟล์ที่แนบมากับ E-mail จนกว่าจะรู้ที่มา
   - ไม่เปิดอ่าน E-mail ที่มี Subject ที่มีข้อความจูงใจ
   - ลบ E-mail ที่ไม่ทราบแหล่งที่มาทิ้งทันที เพื่อตัดปัญหาทั้งปวงที่มาจากผู้ไม่หวังดี
5. ตระหนักถึงความเสี่ยงของไฟล์ที่ดาวน์โหลด หรือได้รับจากทางอินเทอร์เน็ต
   - ไม่ควรเปิดไฟล์ที่แนบมากับโปรแกรมที่ใช้สนทนา เช่น Skype, Facebook, ICQ, Web Chat ต่างๆ ที่มีการแลกเปลี่ยนไฟล์ โดยเฉพาะไฟล์ที่สามารถรันได้ เช่น ไฟล์ที่นามสกุล .exe, .pif, .com, .bat, .vbs เป็นต้น (โดยไม่ทราบแหล่งที่มา)
   - ไม่เข้าเว็บไซต์ที่มากับ E-mail หรือโปรแกรมสนทนาต่างๆ รวมทั้งโฆษณาชวนเชื่อ หรือหน้าเว็บที่ปรากฏขึ้นมาโดยไม่ได้ตั้งใจ
   - ไม่ดาวน์โหลดไฟล์ต่างๆ จากเว็บไซต์ที่ไม่มั่นใจ หรือไม่น่าเชื่อถือ
   - หลีกเลี่ยงการแชร์ไฟล์โดยไม่จ าเป็น ถ้าต้องการแชร์ไฟล์ ควรตั้งค่าการแชร์แบบอ่านอย่างเดียว (Read only) หรืออาจตั้งรหัสผ่านด้วยก็ได้ข้อมูลโปรแกรมป้องกันไวรัส (Virus Program)

โปรแกรมป้องกันไวรัสที่ทางสำนักนักโครงการ TO BE NUMBER ONE ได้ติดตั้งใช้งาน คือ ESET Antivirus

ปัยจัยที่ส่งผลต่อการใช้ซอฟต์แวร์ที่มีลิขสิทธ์ถูกต้องมาใช้งาน

1. มีความเข้ากันได้ของโปรแกรมกับการทำงาน (Compatibility) มีคุณสมบัติเหมาะสม และครบครัน สามารถใช้งานร่วมกับโปรแกรมอื่นๆได

2. ซอฟต์แวร์ถูกลิขสิทธิ์มีฟังก์ชั่นการใช้งานต่างๆ ที่ง่าย และมีเครื่องมือที่หลากหลายเพียงพอกับบริบทของงาน มีการอัพเดทเครื่องมือ และฟีเจอร์ต่างๆ เพื่อการใช้งานที่ง่ายกว่าเดิม

3. การมีการสนับสนุนด้านเทคนิคจากซอฟต์แวร์ที่ถูกลิขสิทธิ์ (Technical Support) ทำให้ผู้ใช้งานเพิ่มประสิทธิภาพ ในการทำงาน เพิ่ม ความมั่นใจในการใช้งานซอฟต์แวร์ถูกลิขสิทธิ์