อยู่อย่างไร?

ให้ปลอดภัยในโลกไซเบอร์

ตอน PASSWORD SECURITY

กลุ่มนักปฏิบัติ “ปิดทองหลังพระ”
สำนักตรวจสอบ

สารบัญ

อยู่อย่างไรให้ปลอดภัยในโลกไซเบอร์

ตอน “Password Security”

บทคัดย่อ

การจัดการความรู้ หรือเคเอ็ม (KM = Knowledge Management) คือ การรวบรวมองค์ความรู้ที่มีอยู่ภายในองค์กร ซึ่งกระจัดกระจายอยู่ในตัวบุคคลหรือเอกสารมาพัฒนาให้เป็นระบบ เพื่อให้ทุกคนในองค์กรสามารถเข้าถึงความรู้และพัฒนาตนเองให้เป็นผู้รู้ รวมทั้งสามารถนำเอาความรู้ที่มีมาถ่ายทอดหรือพัฒนาต่อยอดเพื่อใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ อันจะส่งผลให้องค์กรมีการพัฒนาความสามารถในเชิงแข่งขันสูงสุด โดยที่องค์ความรู้มี 2 ประเภท คือ

1) ความรู้ที่ฝังอยู่ในคน (Tacit Knowledge) เป็นความรู้ที่ได้จากประสบการณ์ พรสวรรค์หรือสัญชาติญาณของแต่ละบุคคลในการทำความเข้าใจในสิ่งต่างๆ ซึ่งเป็นความรู้ที่ไม่สามารถถ่ายทอดออกมาเป็นคำพูดหรือลายลักษณ์อักษรได้โดยง่าย เช่น ทักษะในการทำงาน งานฝีมือ หรือการคิดเชิงวิเคราะห์ บางครั้ง จึงเรียกว่าเป็นความรู้แบบนามธรรม

2) ความรู้ที่ชัดแจ้ง (Explicit Knowledge) เป็นความรู้ที่สามารถรวบรวม ถ่ายทอดได้ โดยผ่านทางวิธีการต่างๆ เช่น การบันทึกเป็นลายลักษณ์อักษร ทฤษฎี คู่มือต่างๆ ซึ่งบางครั้งเรียกว่าเป็นความรู้แบบรูปธรรม

ปัจจุบันการประปานครหลวง (กปน.) ได้นำระบบสารสนเทศมาใช้สนับสนุนการทำงานในด้านต่างๆ ขององค์กร โดยที่การเข้าใช้งานระบบสารสนเทศที่สำคัญต้องมีการยืนยันตัวตนของผู้ใช้งานระบบด้วยรหัสผู้ใช้งานและรหัสผ่าน (Username / Password) แต่ในปัจจุบันพบว่าในองค์กรมีภัยคุกคามมากขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ทั้งจากไวรัสคอมพิวเตอร์ หรือจากผู้ไม่ประสงค์ดีหรือแฮกเกอร์ (Hacker) แม้ว่า กปน. จะมีระเบียบ กปน. ฉบับที่ 18 ว่าด้วยการรักษาความปลอดภัยสารสนเทศ พ.ศ.2557 เพื่อให้พนักงาน ลูกจ้าง และผู้เกี่ยวข้องได้ปฏิบัติตาม เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัย (Security) และช่วยป้องกันเครื่องคอมพิวเตอร์ อุปกรณ์ต่างๆที่เกี่ยวข้อง รวมถึงข้อมูล(Information) สำคัญที่ได้จัดเก็บไว้ภายในระบบ

อย่างไรก็ตามรูปแบบของภัยคุกคามทางเทคโนโลยีสารสนเทศในปัจจุบันมีการปรับเปลี่ยนรูปแบบที่หลากหลายและมีความซับซ้อนมากขึ้น เพื่อล่อหลอกหรือหลีกเลี่ยงการตรวจจับ รวมถึงขโมยหรือนำรหัสผู้ใช้งานและรหัสผ่านไปใช้งานโดยไม่มีสิทธ์ ทำให้หลายๆองค์กรได้รับผลกระทบและความเสียหายทั้งที่เป็นตัว

เงินและไม่เป็นตัวเงิน หรือด้านชื่อเสียงและภาพลักษณ์ขององค์กร ดังนั้นหากพนักงานทุกคนที่ปฏิบัติงานในองค์กร มีความรู้และเข้าใจในการรักษารหัสผู้ใช้งานและรหัสผ่านอย่างเหมาะสมและรู้เท่าทันผู้ไม่ประสงค์ดีแล้วจะสามารถป้องกันหรือหลีกเลี่ยงผลกระทบที่อาจตามมาจากการที่บุคคลอื่นนำรหัสผู้ใช้งานและรหัสผ่านของบุคคลอื่นไปใช้งานได้

กลุ่ม “ปิดทองหลังพระ” เล็งเห็นโอกาสในการพัฒนาความรู้ที่ชัดแจ้ง ที่ได้จากผลงานการตรวจสอบระบบสารสนเทศในการประปานครหลวง ประกอบกับความรู้จากเอกสารตำรา มาตราฐานที่เกี่ยวข้อง และการค้นคว้าจากโลกออนไลน์ ผ่านการคัดสรรและนำมาร้อยเรียงและจัดทำเป็นคลิปวีดีโอ ความยาวประมาณ 5 นาที เพื่อถ่ายทอดเรื่องราวเกี่ยวกับ อยู่อย่างไรให้ปลอดภัยในโลกไซเบอร์ ตอน “Password Security” เพื่อเป็นสื่อกลางในการปลุกจิตสำนึกให้ผู้รับชมได้ตระหนักถึงภัยคุกคาม และความเสียหายที่จะมาถึงตัวหากไม่ระมัดการใช้งาน Password ให้ปลอดภัย

แต่เนื่องจากเนื้อหาด้านความปลอดภัยในโลกไซเบอร์มีเป็นจำนวนมาก กลุ่มฯ จึงเลือกนำเสนอเรื่องที่สำคัญใกล้ตัวผู้ใช้มากที่สุดมาจัดทำและนำเสนอเป็น “ตอน” ที่มีชื่อว่า “Password Security” เนื่องจากเวลามีจำกัด โดยหวังว่าจะเป็นต้นแบบในการรวบรวมและจัดการความรู้ ซึ่งหากมีผู้สนใจนำไปต่อยอดก็สามารถเติมเต็มเนื้อหาให้สมบูรณ์ยิ่งขึ้นใน ”ตอน” อื่นๆ ต่อไปได้ในอนาคต

สาเหตุ ความเป็นมาและความสำคัญของความรู้

เนื่องจากในปัจจุบันการประปานครหลวงได้นำระบบเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานในทุกๆด้านไม่ว่าจะเป็นด้านการผลิตและจ่ายน้ำ ด้านบริการลูกค้า หรือด้านการปฏิบัติงานภายในองค์กร เป็นต้น ซึ่งสำหรับสำนักตรวจสอบ (สตส.) นั้นมีภาระกิจในการตรวจสอบสารสนเทศภายในองค์กร ซึ่งจากการตรวจสอบที่ผ่านมาพบความสำคัญที่เกี่ยวข้องกับความตระหนักในการใช้งานระบบสารสนเทศ สืบเนื่องมาจากการประปานครหลวงได้มีการประกาศใช้ ระเบียบการประปานครหลวงฉบับที่ 18 ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.2557 โดยมีการระบุเกี่ยวกับวิธีปฏิบัติในการใช้รหัสผ่าน แต่พนักงานภายในองค์กรอาจจะยังไม่ทราบหรือยังขาดความตะหนักในเรื่องดังกล่าว จึงเป็นที่มาของการจัดทำเคเอ็ม (Knowledge Management : KM) ในครั้งนี้เพื่อถ่ายทอดให้พนักงานภายในองค์กรทราบถึงความสำคัญในการใช้งานรหัสผ่าน การดูแลรักษารหัสผู้ใช้งานและรหัสผ่านให้มีความมั่นคงปลอดภัยจากภัยคุกคามบนโลกไซเบอร์ (Cyber)

ประโยชน์ของความรู้

เพื่อบรรลุเป้าหมายขององค์กรในการดูแลสารสนเทศ (Information) ซึ่งเป็นทรัพยากรที่มีค่ายิ่งในองค์กร การตรวจสอบเพื่อให้ความเชื่อมั่นว่าผู้ที่มีสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลในระบบสารสนเทศได้ สตส. ในฐานะที่เป็นหน่วยงานที่มีบทบาทในการให้ความเชื่อมั่นและให้คำปรึกษากับทุกหน่วยงาน การตรวจสอบด้านเทคโนโลยีสารสนเทศก็เป็นอีกบทบาทที่สำคัญอย่างยิ่งอีกบทบาทหนึ่งของ สตส. ซึ่งนับวันยิ่งมีบทบาทสำคัญมากยิ่งขึ้น เนื่องจากการนำเทคโนโลยีสารสนเทศเข้ามาใช้ใน กปน. อย่างต่อเนื่อง วิธีการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบสารสนเทศด้วยรหัสผู้ใช้งานและรหัสผ่าน (Username / Password) กลายเป็นเรื่องจำเป็นพื้นฐานสำหรับระบบสารสนเทศเกือบทุกระบบงาน เนื่องจากเป็นวิธีการที่ง่าย ประหยัด และเป็นวิธีพื้นฐานที่สำคัญเพื่อพิสูจน์ว่าเป็นเจ้าของรายการ (Transaction) ที่เกิดขึ้นในระบบ แต่ในปัจจุบันกลับพบว่าพนักงาน กปน. ส่วนมากยังขาดความรู้ความเข้าใจในเรื่องของการเก็บรักษารหัสผู้ใช้งานและรหัสผ่าน ไม่ว่าจะเป็นการจดบันทึกรหัสผ่านไว้ใกล้กับคอมพิวเตอร์ที่ใช้งานเป็นประจำ หรือใช้รหัสผ่านที่คาดเดาได้ง่าย เช่น วันเกิด ชื่อเล่น เป็นต้น

การจัดการความรู้ในหัวข้อเรื่อง อยู่อย่างไรให้ปลอดภัยในโลกไซเบอร์ ตอน “Password Security” ได้นำเรื่องราวเกี่ยวกับภัยอันตรายที่เกิดจากการไม่ระมัดระวังการเก็บรักษา Password ให้ปลอดภัยไม่ให้ผู้อื่นล่วงรู้ ผลกระทบที่อาจเกิดขึ้นหากมีผู้ไม่หวังดีนำรหัสผ่านแล้วนำไปใช้ในทางมิชอบ และเคล็ดลับการตั้ง

Password ให้ปลอดภัย โดยมีความมุ่งหวังให้พนัก กปน. รวมทั้งผู้ที่สนใจได้รับความรู้จากการชมคลิป ส่งผลเกิดความตระหนัก (Awareness) ในการรักษา Password ซึ่งจะทำให้เกิดการปรับเปลี่ยนพฤติกรรมในการรักษา Password เป็นความลับให้ปลอดภัยทั้งในที่ทำงานและในชีวิตประจำวัน

เนื้อหาและสาระสำคัญของความรู้

การดำเนินงาน

เคล็ดลับที่ทำให้การดำเนินการจัดทำ KM ในครั้งนี้สำเร็จไปด้วยดีคือ การร่วมมือร่วมใจจากทีมงานทั้ง 4 ท่าน ที่เต็มเปี่ยมไปด้วยความเสียสละ ทุ่มเท ช่วยเหลือเกื้อกูลเติมเต็มในสิ่งที่แต่ละคนมีความถนัดและเชี่ยวชาญ เช่น ถนัดทำ CLIP ถนัดนำเสนอ และถนัดสร้างเรื่องราว เป็นต้น จนทำให้การจัดการความรู้ด้านสารสนเทศซึ่งจัดอยู่เป็นกระบวนงานหลักที่สำคัญของ กปน. สำเร็จลุล่วงแม้จะมีปัญหาหรืออุปสรรคอยู่บ้างในเรื่องระยะเวลา และภาระงานประจำก็ตาม

ข้อคิด ข้อเสนอแนะ

การจัดทำ KM ในครั้งนี้ สืบเนื่องจากนโยบายของผู้บริหารในการเร่งดำเนินการจัดทำ โดยหลักการแล้วการจัดการความรู้ ควรหามาตรการส่งเสริมให้ COPs ดำเนินการอย่างต่อเนื่องตลอดทั้งปี ไม่ควรมาเร่งรีบให้ดำเนินการในช่วงที่จะมีการประกวดหรือแข่งขัน

เนื้อหาของความรู้

ในปัจจุบันระบบคอมพิวเตอร์ได้ถูกคุกคามมากขึ้นจากผู้ไม่ประสงค์ดี ซึ่งความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security) ช่วยปกป้องเครื่องคอมพิวเตอร์รวมไปถึงอุปกรณ์ต่างๆ ที่เกี่ยวข้อง และที่สำคัญยังสามารถช่วยปกป้องข้อมูลที่ได้จัดเก็บไว้ภายในระบบ หรือใช้ในความหมายความปลอดภัยทางข้อมูลสารสนเทศ (Information Security) ก็ได้ จุดประสงค์หลักของความปลอดภัยทางข้อมูลคือ ความลับ (Confidentiality) ความสมบูรณ์ (Integrity) ความพร้อมใช้ (Availability) และการห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) ของข้อมูลต่างๆภายในองค์กร โดยมีรายละเอียด ดังนี้

การรักษาความลับ (Confidentiality) คือการรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ และผู้มีสิทธิเท่านั้นจึงจะเข้าถึงข้อมูลนั้นได้

การรักษาความสมบูรณ์ (Integrity) คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา

ความพร้อมใช้ (Availability) คือการรับรองว่าข้อมูลและบริการการสื่อสารต่างๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้งาน

การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) คือวิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

ในทางปฏิบัตินั้นสามารถกำหนดลักษณะของการควบคุมความมั่นคงปลอดภัย (Security Controls) และถือเป็นองค์ประกอบที่สำคัญส่วนหนึ่งของความมั่นคงปลอดภัยคอมพิวเตอร์ เพราะจัดเป็นการกำหนดและควบคุมทั้งบุคคลที่สามารถเข้าสู่ระบบ เข้าถึงข้อมูลภายในระบบ เพื่อกระทำการใดได้บ้าง ซึ่งจะอนุญาตตามระดับชั้นของความสำคัญของข้อมูล รวมไปถึงการจัดเก็บพฤติกรรมการใช้งานระบบของบุคคลนั้นต่อข้อมูลบนระบบทั้งหมด

การพิสูจน์ตัวตน (Authentication) คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (Username)

การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

กระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ ซึ่งในขั้นนี้คือการระบุตัวตน และในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้าง ซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธจากระบบ

<u>เคล็ดลับ สร้าง Password ยังไง ให้ปลอดภัยจากผู้ไม่ประสงค์ดี</u>

1. ไม่ใช้คำที่จะพบในพจนานุกรม
2. ไม่ใช้ข้อมูลส่วนตัว
3. ไม่ใช้ Password ซ้ำกันสำหรับหลายๆ บัญชี
4. ไม่สร้าง Password ที่สั้นเกินไป อย่างน้อยควรมี 8 ตัวอักษรเป็นอย่างต่ำ
5. ไม่ใช้ Password เดิมนานเกินไป

(แหล่งค้นคว้า **http://www.chillpainai.com/scoop/**5030/)

สิ่งที่ควรทำใน การสร้าง Password

1. Password ควรมีตัวอักษรอย่างน้อย 8 ตัว และประกอบด้วยอักษรตัวใหญ่ ตัวเล็ก ตลอดจนตัวเลข และสัญลักษณ์ ยิ่งผสมกันได้มากเท่าไร password จะยิ่งปลอดภัยเท่านั้น

2. หลีกเลี่ยงการใช้วัน เดือน ปีเกิด ชื่อตัว(ชื่อแฟน เพื่อนสนิท พ่อแม่พี่น้อง ฯลฯ) ชื่อจังหวัด หรือข้อมูลต่างๆ ที่เกี่ยวข้องกับตัวเรามาใช้ในการตั้งรหัสผ่าน

3. ควรใช้รหัสผ่านแยกกัน หากเป็นคนละบัญชีผู้ใช้งาน โดยเฉพาะรหัสผ่านที่ใช้เข้าถึงข้อมูลสำคัญ เช่น ธนาคารออนไลน์ แต่ถ้าหากไม่สามารถจดจำได้ อาจจะใช้วลีในการตั้ง Password เป็นพวกเดียวกัน โดยใช้ตัวเลขที่ตามหลังเป็นตัวแยกความแตกต่างของแต่ละบัญชีผู้ใช้

4.อย่าเลือกตัวเลือก (Option) จัดเก็บรหัสผ่านอัตโนมัติของบราวเซอร์ หากใช้เครื่องคอมพิวเตอร์ร่วมกับผู้อื่นหรือเครื่องสาธารณะ

5. อย่าส่งรหัสผ่านให้ใครไม่ว่ากรณีใดๆ เช่น ทางวาจา อีเมล์ line และ sms ให้จำไว้เสมอว่า มันคือ รหัสลับที่ไม่ควรส่งไปให้ใครเด็ดขาด

6. อย่าจดรหัสผ่านลงในกระดาษ หรือสมุดโน้ตใดๆ แต่ถ้าหากจำเป็นต้องจดควรเก็บเอกสารที่จดไว้ในที่ปลอดภัยไม่ใกล้เครื่องคอมพิวเตอร์

7. เปลี่ยนรหัสผ่านทุกๆ 3 เดือน เพื่อลดโอกาสที่ผู้ไม่ประสงค์ดีจะแกะรหัสออก

8. พิมพ์รหัสผ่านเป็นภาษาไทย แต่แป้นพิมพ์ภาษาอังกฤษ เช่น คำว่า “okpgdkgs]k” ซึ่งหมายถึง “นายเกาเหลา”

(แหล่งค้นคว้า http://library.stou.ac.th/blog/?p=1087)

การได้มาซึ่งความรู้

กลุ่มปิดทองหลังพระ ได้เสาะแสวงหาความรู้ทั้งจากภายในและภายนอกองค์กรที่เป็น (Explicit Knowledge) ประกอบด้วยแหล่งข้อมูลภายในคือผลการตรวจสอบตามแผนการตรวจสอบประจำปีด้านเทคโนโลยีสารสนเทศ และจากแหล่งภายนอกอื่น ประกอบด้วยการรักษาความปลอดภัยบนโลกไซเบอร์ภาคประชาชน ของ กสทช. และการค้นคว้าบนโลกไซเบอร์ (Internet) นำมาประมวล เพื่อให้ได้องค์ความรู้ที่เหมาะสม ดังนี้

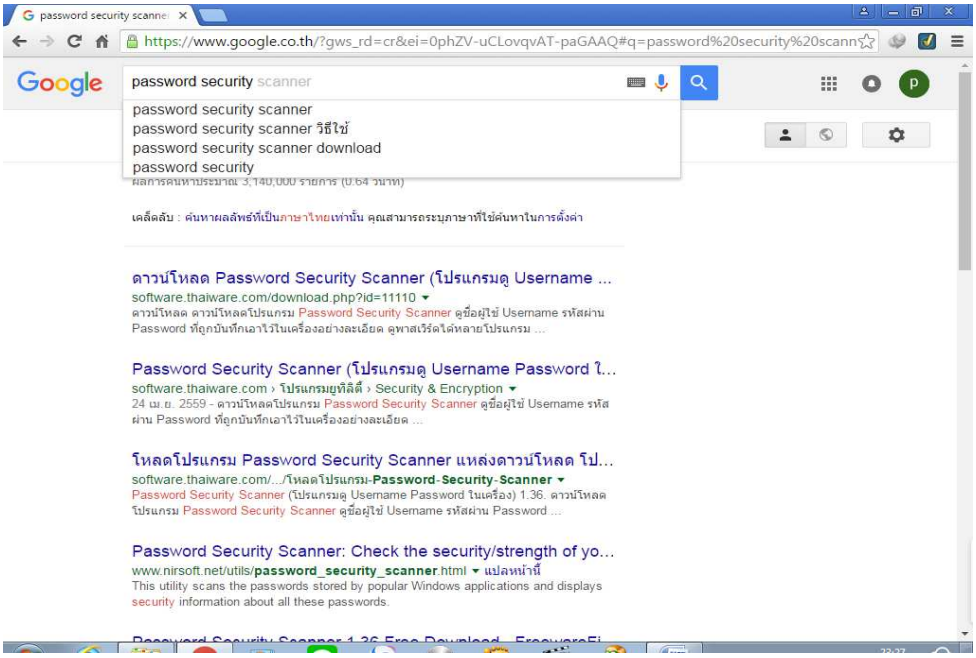
1. ผลการตรวจสอบของสำนักตรวจสอบ ในผลงานการตรวจสอบเรื่องการควบคุมทั่วไปด้านสารสนเทศ (Information Technology General Controls) และการตรวจสอบเฉพาะระบบงาน (Application Controls) เช่น การตรวจสอบระบบ CIS ระบบ SAP ระบบผลิตและสูบจ่ายน้ำ เป็นต้น

NO	ลำดับตามแผนกลยุทธ์	กิจกรรมตรวจสอบ (Audit Activity : AA) เลขที่ AA	กิจกรรมตรวจสอบ (Audit Activity : AA)	หน่วยตรวจสอบ	ระดับความสำคัญ	จำนวนวันปฏิบัติงาน (MAN-DAY)	ระยะเวลาตรวจสอบและรายงานผลการตรวจสอบ												วัตถุประสงค์
							ไตรมาสที่ 1			ไตรมาสที่ 2			ไตรมาสที่ 3			ไตรมาสที่ 4			
							ต.ค. 2558	พ.ย. 2558	ธ.ค. 2558	ม.ค. 2559	ก.พ. 2559	มี.ค. 2559	เม.ย. 2559	พ.ค. 2559	มิ.ย. 2559	ก.ค. 2559	ส.ค. 2559	ก.ย. 2559	
8	AA7	I-03	การบริหารความต่อเนื่องธุรกิจและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ - แผนที่ 7 การทบทวนการบริหารความต่อเนื่องทางธุรกิจ (BCM) ด้าน IT - แผนที่ 8 ความปลอดภัยและความพร้อมใช้งานของข้อมูลสารสนเทศ	กสส.	ปานกลาง	150	1					25							การดำเนินธุรกิจต่อเนื่อง (BCM) ด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ เหมาะสม เพียงพอ เพื่อให้ข้อมูลต่าง ๆ และระบบเทคโนโลยีสารสนเทศของ กปน. มีความปลอดภัย เชื่อถือได้ ถูกต้องสมบูรณ์และใช้งานได้อย่างต่อเนื่อง
9	AA8	I-04	ระบบ SAP (System App & Products in data Processing) - Business Audit - Module 1	กสส.	ปานกลาง	140				4			11						ระบบงานมีการออกแบบให้มีการควบคุมและการรักษาความปลอดภัยอย่างเพียงพอ การนำเข้าข้อมูล การประมวลผล การควบคุมผลลัพธ์และการรายงานผลข้อมูลสารสนเทศที่ได้จากระบบมีความถูกต้องครบถ้วนและเชื่อถือได้
10			- Module 2	กสส.	ปานกลาง	140				4			8						
11	AA16	I-12	ความปลอดภัยของระบบเครือข่ายและการสื่อสาร - แผนที่ 7 การทบทวนการบริหารความต่อเนื่องทางธุรกิจ (BCM) ด้าน IT - แผนที่ 8 ความปลอดภัยและความพร้อมใช้งานของข้อมูลสารสนเทศ	กสส.	สูง	130										1		26	ระบบเครือข่ายและการสื่อสารมีการออกแบบสถาปัตยกรรมเครือข่ายที่ดีมีการรักษาความปลอดภัยไม่ให้เกิดช่องโหว่ (Vulnerability) รวมถึงมาตรการการควบคุม และรักษาความปลอดภัยเครือข่ายเพื่อป้องกันการถูกโจมตีจากภายนอกและภายในองค์กรได้อย่างมีประสิทธิภาพ
12	AA18	M-02	การบริหารทรัพยากรบุคคล - แผนที่ 10 การเตรียมความพร้อมบุคลากรให้ที่มีความรู้ความเชี่ยวชาญเฉพาะด้าน	กคอ.	ปานกลาง	120									1			15	เพื่อให้มั่นใจว่ากระบวนการวิเคราะห์อัตรากำลัง สรรหา คัดเลือก บรรจุบุคคลมีความเหมาะสมกับตำแหน่งงาน และสอดคล้องกับยุทธศาสตร์ มีความโปร่งใส เป็นธรรม เป็นไปตาม กฎ ระเบียบที่เกี่ยวข้อง
	AA67	P-02-02	การติดตามประเมินผลบุคคล																เพื่อให้มั่นใจว่ากระบวนการประเมินผลการปฏิบัติงานสอดคล้องกับภารกิจของงาน รวมทั้งนโยบายหลักเกณฑ์ที่เกี่ยวข้องและนำผลการประเมินมาใช้ประโยชน์ในการบริหารในส่วนที่เกี่ยวข้องอย่างมีประสิทธิภาพ
13	AA20	M-04	การดำเนินการทางกฎหมาย	กคอ.	ปานกลาง	169								16				31	เพื่อให้มั่นใจว่าการพิจารณาข้อหารือทางกฎหมายมีกระบวนการที่เชื่อถือได้ ปฏิบัติงานร่วม/สนับสนุนการปฏิบัติงานของหน่วยงานอื่นด้วยความรวดเร็ว
14	AA21	M-05	การบริหารการจัดซื้อจัดจ้าง	กคอ.	สูง	189	1			20	10			25					เพื่อให้มั่นใจว่ากระบวนการจัดซื้อจัดจ้าง เป็นไปตามกฎ ระเบียบที่เกี่ยวข้อง โปร่งใส มีคุณภาพและทันตามความต้องการของผู้ใช้งาน

2. จากคู่มือแนวทางการรักษาความปลอดภัยบนโลกไซเบอร์ภาคประชาชน ของ กสทช.

สามารถดาวน์โหลดได้ฟรีที่ http://physics.ipst.ac.th/?p=2541

3. จากการค้นคว้าจากโลกออนไลน์



การประยุกต์ใช้ความรู้ในการปฏิบัติงาน

การตรวจสอบระบบสารสนเทศในเรื่องการพิสูจน์ตัวตนของผู้ใช้งานด้วยรหัสผู้ใช้งานและรหัสผ่าน นั้นนับได้ว่าเป็นหัวข้อพื้นฐานที่สำคัญในทุกงานตรวจสอบ และจำเป็นอย่างยิ่งที่ทุกๆระบบสารสนเทศต้องมีการกำหนดไว้อย่างเหมาะ สำนักตรวจสอบจึงเล็งเห็นความสำคัญของความรู้ในเรื่องนี้ จึงได้ประยุกต์ความรู้ที่ได้จากผลการตรวจสอบ เอกสารตำรา มาตรฐานที่เกี่ยวข้องและจาก Internet นำมาปรับปรุง ดัดแปลงเนื้อหาให้เหมาะสมให้ง่ายแก่การเรียนรู้และทำความเข้าใจ เพื่อป้องกันภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศจากผู้ไม่ประสงค์ดี (Hacker) ที่เพิ่มขึ้นอย่างต่อเนื่อง แม้ กปน. จะได้ประกาศใช้ระเบียบ กปน. ฉบับที่ 18 ว่าด้วยการรักษาความปลอดภัยสารสนเทศ เพื่อให้พนักงาน ลูกจ้าง และผู้เกี่ยวข้องปฏิบัติตามเพื่อความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security) เพื่อช่วยปกป้องเครื่องคอมพิวเตอร์รวมไปถึงอุปกรณ์ต่างๆ ที่เกี่ยวข้อง และข้อมูลที่ได้จัดเก็บไว้ภายในระบบ

การจัดให้มีการจัดการความรู้ในเรื่องอยู่อย่างไรให้ปลอดภัยในโลกไซเบอร์ ตอน “Password Security” นอกจากจะเป็นแหล่งที่เสริมสร้างความรู้ ความเข้าใจ และให้พนักงานได้เกิดความตระหนักถึงภัย

อันตรายและผลกระทบที่อาจจะเกิดขึ้นกับการไม่รักษา Password ให้เป็นความลับในการปฏิบัติงานใน กปน. แล้วผู้เรียนรู้ยังสามารถนำไปปรับใช้ในชีวิตประจำวันได้อีกด้วย

วิธีการถ่ายทอดองค์ความรู้และเครื่องมือที่ใช้

ใช้วิธีการถ่ายทอดความรู้ โดยใช้วิธีการจัดประชุมระดมสมองโดยคณะทำงาน และหารือกับผู้บริหารของสำนักตรวจสอบ และเสาะแสวงหาความรู้เพิ่มเติมจากคู่มือ เอกสาร ตำรา และค้นคว้าในโลกออนไลน์ เพื่อให้ได้ข้อสรุปในองค์ความรู้ที่เหมาะสม เพียงพอ และนำมาเรียบเรียงเนื้อหาแล้วจัดทำเป็นคลิปวีดีโอ ที่มีเนื้อหาเกี่ยวกับ “Password Security” เครื่องมือที่ใช้ในการพัฒนา คือ PowToon

ตัวอย่างภาพจาก CLIP สามารถดูได้จากภาคผนวก

การเผยแพร่ความรู้

- Intranet ของ กปน.
- ICONNEX
- Facebook ของ สตส.
- การสัมมนา โครงการพี่เลี้ยง ของ สคร. และ บริษัททริส คอร์ปอเรชั่น จำกัด จัดเมื่อ 15 มิถุนายน 2559

ผู้เรียนรู้

พนักงาน ลูกจ้าง และผู้เกี่ยวข้องที่ต้องใช้ระบบสารสนเทศในการประปานครหลวง และหรือผู้สนใจทั่วไปเช่นผู้ใช้น้ำ ผู้รับจ้าง คู่ค้ากับการประปานครหลวง