เอกสารการจัดการความรู้
เรื่อง
“การรักษาความปลอดภัยทางคอมพิวเตอร์”

จัดทำเมื่อ ๑๐ ส.ค. ๕๗

รายชื่อคณะผู้จัดทำ

พันโท วีระพงค์	ตั้นเจริญ
พันตรี ตุลวัตร	ชุณห์วิจิตรา
ร้อยโท ณรงค์	ภูมิสุข

โดย

ส่วนการศึกษา

โรงเรียนนายร้อยพระจุลจอมเกล้า

แบบฟอร์มรายงานแผนการจัดการความรู้ รร.จปร.ปีงบประมาณ ๒๕๕๗

หน่วย สกศ.รร.จปร. วันที่ ๑๐ เดือนสิงหาคม พ.ศ.๒๕๕๗

เรียน ประธานคณะกรรมการจัดการความรู้ รร.จปร.

คณะกรรมการจัดการความรู้ สกศ.รร.จปร. ขอส่งแผนการจัดการความรู้ แผนที่ ๑ ประจำปีงบประมาณ ๒๕๕๗

เรื่อง การรักษาความปลอดภัยทางคอมพิวเตอร์

จัดทำโดย พ.ท.วีระพงศ์ ตั้นเจริญ

เบอร์ติดต่อ ภายใน ๖๒๒๙๒ มือถือ ๐๘๓-๓๑๑๑๖๘๓

ลำดับ	รายการ รูปเล่ม	เอกสาร	ไฟล์ PDF	หมายเหตุ
๑	- ปก	√	√	เอกสาร ๑-๔ เย็บเล่ม ตามลำดับ จำนวน ๒ ชุด
๒	แบบฟอร์มรายงานแผนการจัดการความรู้ รร.จปร. ปีงบประมาณ ๒๕๕๗	√		
	- คำนำ	√	√	
	- บทสรุปการจัดการความรู้	√	√	
	- สารบัญ	√	√	
	- เนื้อหา -บทที่๑ /-บทที่๒	√	√	
	- บรรณานุกรม	√	√	
๓	แบบฟอร์มที่ ๑	√	√	
๔	แบบฟอร์มที่ ๒	√	√	

☐ ได้ดำเนินการนำไฟล์ PDF ขึ้นบน web sit การจัดการความรู้ รร.จปร.แล้ว

ทั้งนี้ คณะกรรมการจัดการความรู้ สกศ.รร.จปร.
ได้ตรวจสอบถูกต้องและเอกสารครบถ้วนของเอกสารแล้ว

จึงเรียนมาเพื่อกรุณาพิจารณา

พ.อ.องอาจ พิมพ์ทนต์
(องอาจ พิมพ์ทนต์)
ประธานคณะกรรมการจัดการความรู้ สกศ.รร.จปร.

บทนำ

ปัจจุบันนี้มีการใช้อุปกรณ์คอมพิวเตอร์กันอย่างแพร่หลาย ซึ่งแน่นอนว่าอุปกรณ์คอมพิวเตอร์เหล่านั้นมีการเชื่อมต่อกับอินเตอร์เน็ท ผู้ใช้จึงควรมีความรู้ความเข้าใจเกี่ยวกับภัยอันตรายต่าง ๆ รวมถึงการรักษาความปลอดภัยทางไซเบอร์เบื้อต้น เพื่อที่จะได้ป้องกันตนเองให้พ้นจากเงื้อมมือของผู้ไม่ประสงค์ดี ซึ่งนับวันมีแต่จะเพิ่มจำนวนขึ้นเป็นทวีคูณ

Basic Computer Security

แนวทางการรักษาความปลอดภัยของข้อมูล และคอมพิวเตอร์ส่วนบุคคล

สถิติการถูกจู่โจมทางคอมพิวเตอร์เพิ่มขึ้นอย่างรวดเร็ว โดยเฉพาะอย่างยิ่งการจู่โจมผู้ใช้อุปกรณ์อิเล็กทรอนิกส์แบบพกพา

ผู้ใช้งานคอมพิวเตอร์ควรมีความรู้และปฏิบัติตามมาตรการในการรักษาคอมพิวเตอร์ ข้อมูลส่วนตัว ประวัติการท่องอินเทอร์เน็ต เลขบัตรเครดิตและข้อมูลอื่นๆ ให้ปลอดภัย โดยผู้ใช้งานควรระมัดระวังในเรื่องของโปรแกรมหรือผู้คนที่ให้ความมั่นใจว่าสามารถที่จะปกป้องดูแลความปลอดภัยได้ร้อยเปอร์เซ็นต์ เพราะการดูแลรักษาความปลอดภัยนั้นต้องมีทั้งโปรแกรมป้องกันภัยที่ดีและลักษณะพฤติกรรมการใช้งานที่ดีด้วย เช่น ควรที่จะต้องรู้ว่าสิ่งใดไม่ควรให้ผู้อื่นเข้าถึงได้ในขณะที่มีการเชื่อมต่ออินเทอร์เน็ต ใครที่ควรไว้วางใจ และการรักษาความปลอดภัยอื่นๆที่เทคโนโลยีไม่สามารถตอบโจทย์ได้ ซึ่งผู้ใช้งานควรจะต้องมองหาโปรแกรมที่ตอบโจทย์การใช้งานของตัวผู้ใช้เองมากที่สุดและในขณะเดียวกันต้องสามารถปกป้องคอมพิวเตอร์ได้อย่างมีประสิทธิภาพอีกด้วย

แนวทางการรักษาคอมพิวเตอร์ส่วนบุคคลให้ปลอดภัยมีดังนี้

ระบบปฏิบัติการต้องอัพเดตอยู่เสมอ

ผู้ใช้งานต้องคอยหมั่นตรวจสอบดูแลให้ระบบปฏิบัติการ (Operating system) ของคอมพิวเตอร์นั้นทันสมัยอยู่เสมอ ผู้พัฒนาระบบจะมีการแจ้งเตือนให้ผู้ใช้งานอัพเดตระบบอยู่เป็นระยะๆ ซึ่งอาจจะเป็นการแจ้งเตือนโดยอัตโนมัติเมื่อ

ถึงช่วงเวลาที่ต้องอัพเดตระบบหรือผู้ใช้งานอาจส่งคำขอไปที่ผู้พัฒนาระบบเพื่อขออัพเดตระบบได้ด้วยตนเองหรือปรับตั้งค่าที่หน้าการตั้งค่าของระบบเองก็ได้ การอัพเดตระบบเหล่านี้จะช่วยทำให้คอมพิวเตอร์ของคุณมีประสิทธิภาพมากขึ้น ง่ายต่อการใช้งานมากขึ้น และสามารถแก้ไขช่องโหว่ของความปลอดภัยที่บางครั้งโปรแกรมตัวก่อนๆ นั้นไม่สามารถปกป้องได้ แต่อาชญากรนั้นก็สามารถที่จะเรียนรู้และค้นพบช่องโหว่ของความปลอดภัยได้อย่างรวดเร็ว บางครั้งก็ก่อนที่ผู้พัฒนาโปรแกรมจะแก้ไขได้ทัน ดังนั้นการแก้ไขหรือซ่อมแซมโปรแกรมอย่างรวดเร็วและทันท่วงทีถือเป็นสิ่งที่ดี และถือเป็นโชคดีที่ระบบปฏิบัติการส่วนใหญ่สามารถที่จะดูแลระบบของตนเองให้ทันสมัยอยู่เสมอและปลอดภัยได้เป็นอย่างดี และคอมพิวเตอร์ของผู้ใช้งานก็จะปลอดภัยหากคุณหมั่นอัพเดตระบบปฏิบัติการคอมพิวเตอร์อยู่เสมอ

การติดตั้งโปรแกรมอัพเดตระบบปฏิบัติการลงบนคอมพิวเตอร์เครื่องใหม่เป็นสิ่งที่จำเป็นมาก เหตุเพราะคอมพิวเตอร์เครื่องใหม่ที่ซื้อมาจากร้านนั้นอาจวางอยู่ที่ร้านมาเป็นเวลาหลายเดือนแล้วก็เป็นได้ เพราะฉะนั้นจึงหมายความว่า ระบบปฏิบัติการในคอมพิวเตอร์เครื่องนั้นอาจล้าหลังและไม่ได้รับการอัพเดต ดังนั้นเมื่อซื้อคอมพิวเตอร์เครื่องใหม่ ผู้ใช้งานควรสละเวลาอัพเดตระบบปฏิบัติการของเครื่องเพื่อช่วยให้คอมพิวเตอร์ปลอดภัยยิ่งขึ้น

บัญชีผู้ใช้และพาสเวิร์ด

คอมพิวเตอร์ทุกเครื่องควรจะมีบัญชีผู้ใช้ไว้สำหรับทำการล็อกอินเข้าสู่เครื่องคอมพิวเตอร์ ซึ่งบัญชีผู้ใช้จะเปรียบเสมือนปราการด่านแรกในการเข้าถึงข้อมูลส่วนตัวและฟังก์ชั่นต่างๆในคอมพิวเตอร์ ดังนั้น ผู้ใช้งานควรสร้างรหัสผ่านหรือพาสเวิร์ดของทุกๆบัญชีผู้ใช้ด้วยเพื่อให้ยากต่อการที่ผู้ใช้งานคนอื่นๆจะสามารถเข้าถึงข้อมูลส่วนตัวของผู้ใช้งาน หลักการตั้งรหัสผ่านที่ดีคือต้องตั้งรหัสเป็นตัวอักษรผสมกับตัวเลขที่คาดเดาได้ยากและควรมีจำนวนอย่างน้อย 8 ตัว และหากเป็นในส่วนการเข้าถึงข้อมูลหรือเพื่อดาวน์โหลดเอกสารสำคัญของหน่วยงาน ควรมีการเปลี่ยนแปลงรหัสผ่านอย่างสม่ำเสมอเพื่อเพิ่มความปลอดภัยมากยิ่งขึ้นไปอีก

ล็อกไว้แบบนี้ แน่ใจได้เลยว่าไม่หายไปไหน

การป้องกันทางกายภาพ

ผู้คนมากมายไม่ได้ตระหนักเลยว่าข้อมูลส่วนตัวของตนเองนั้นมีมูลค่ามหาศาลสำหรับบุคคลอื่น หากผู้ใช้งานกำลังกำลังทำงานอยู่ในสภาพแวดล้อมหรือสถานที่ที่ไม่รู้จักคุ้นเคยหรือที่คุณไม่สามารถควบคุมได้ ผู้ใช้งานก็จะต้องคอยดูแลทรัพย์สินเป็นอย่างดีโดยไม่ให้คลาดสายตา ซึ่งคอมพิวเตอร์ก็ใช้หลักการเดียวกัน ลองคิดสักนิดว่าจะอันตรายมากแค่ไหนถ้าหากข้อมูลในคอมพิวเตอร์ตกไปอยู่ในมือของผู้ไม่หวังดี ผู้ใช้งานควรระลึกเสมอว่าได้เก็บข้อมูลสำคัญอะไรเอาไว้ใน

คอมพิวเตอร์ และหากมีคนมาขโมยข้อมูลนั้นไป เขาจะเอามันไปทำอะไรหรือใช้ประโยชน์อะไรได้บ้าง ผู้ใช้งานควรตระหนักด้วยว่า พาสเวิร์ดนั้นเพียงแค่ช่วยปกป้องให้ผู้ไม่หวังดีเข้าถึงข้อมูลในคอมพิวเตอร์ได้ช้าลงเท่านั้น แต่มันจะไม่สามารถช่วยปกป้องข้อมูลของผู้ใช้งานได้ถ้าหากระบบทั้งระบบถูกทำลายไป การเข้าถึงคอมพิวเตอร์โดยตรงคือวิธีที่ง่ายที่สุดในการเข้าถึงข้อมูลในฮาร์ดดิสก์ (โดยการใช้คอมพิวเตอร์อีกเครื่องหนึ่ง) โ ดยที่ไม่มีความจำเป็นจะต้องรู้แม้กระทั่งพาสเวิร์ดตัวแรกของผู้ใช้งานด้วยซ้ำ ถ้าหากข้อมูลในโน้ตบุ๊คของผู้ใช้งานมีมูลค่ามาก ผู้ใช้งานยิ่งต้องให้ความสนใจเกี่ยวกับการรักษาความปลอดภัยของข้อมูลส่วนตัว และยิ่งต้องให้ความสนใจมากขึ้นไปอีก หากผู้ใช้งานให้คนอื่นยืมคอมพิวเตอร์หรืออุปกรณ์อื่นๆ เพราะถึงแม้ว่าผู้ใช้งานจะเชื่อใจบุคคลที่ให้ยืมมากแค่ไหน ก็ไม่สามารถที่จะคอยควบคุมให้เขาใช้งานคอมพิวเตอร์อย่างระมัดระวังและปลอดภัยเท่าตัวเอง

ใช้โปรแกรมแอนติไวรัส

ถ้าหากผู้ใช้งานใช้โปรแกรมวินโดวส์ของไมโครซอฟต์ ควรใช้โปรแกรมแอนติไวรัสและหมั่นอัพเดตมันอยู่เสมอ เพราะมีโปรแกรมชนิดหนึ่งที่ชื่อว่ามัลแวร์ถูกเขียนขึ้นมาเพื่อขโมยข้อมูลหรือเพื่อใช้คอมพิวเตอร์ของผู้ใช้งานในทางที่ไม่ดี ไ ว รัสและมัลแวร์เหล่านี้สามารถเข้าถึงระบบ เปลี่ยนแปลงระบบและฝังตัวอยู่ในคอมพิวเตอร์ มันสามารถเข้ามาอยู่ในคอมพิวเตอร์ผ่านทางอีเมล์ เว็บไซต์ที่ผู้ใช้งานเข้าชม หรือมาพร้อมกับไฟล์ที่ผู้ใช้งานไม่คิดว่ามันจะเป็นอันตราย ผู้ให้บริการโปรแกรมแอนติไวรัสจะทำการศึกษาค้นคว้าเกี่ยวกับตัวคุกคาม (Threat) ที่ขึ้นเกิดขึ้นอยู่เสมอและเพิ่มมันเข้าไปในบัญชีที่คอมพิวเตอร์ของผู้ใช้งานต้องสกัดกั้น ใ นการที่จะทำให้โปรแกรมสามารถตรวจจับตัวคุกคามใหม่ๆได้ตลอด ผู้ใช้จึงจำเป็นที่จะต้องอัพเดตโปรแกรมแอนติไวรัสอย่างสม่ำเสมอ

อุปกรณ์บันทึกข้อมูลภายนอกและอุปกรณ์บันทึกข้อมูลขนาดพกพา

การส่งผ่านของไวรัสผ่านทางแฟลชไดร์ฟหรือช่องแนบข้อมูลของอีเมล์สามารถทำได้อย่างง่ายดายและส่วนใหญ่ตัวไวรัสเองมักจะเป็นตัวที่ส่งข้อมูลหรืออีเมล์ด้วยตัวของมันเองแทนที่จะเป็นเจ้าของอีเมล์หรือแฟลชไดร์ฟนั้นๆ โ ดยเฉพาะอย่างยิ่งในระบบปฏิบัติการของไมโครซอฟต์วินโดวส์ ผู้ใช้ควรระมัดระวังในการเสียบแฟลชไดร์ฟเข้ากับเครื่องคอมพิวเตอร์หรือให้บุคคลอื่นยืมไปใช้ ซึ่งบริษัทไมโครซอฟต์เองก็ได้มีการเปลี่ยนแปลงนโยบายเกี่ยวกับการที่คอมพิวเตอร์มีการตั้งค่าให้เปิดแฟลชไดร์ฟเองโดยอัตโนมัติ ซึ่งนั่นทำให้วินโดวส์มีความปลอดภัยมากยิ่งขึ้น แต่อย่างไรก็ดี ผู้ใช้ก็ไม่ควรที่จะเปิดไฟล์ที่ตนเองไม่รู้จักหรือไม่น่าไว้วางใจ

เลือกใช้ซอฟต์แวร์ที่น่าเชื่อถือและซอฟต์แวร์แบบโอเพ่นซอร์ส

ผู้ใช้ควรเลือกใช้โปรแกรมจากผู้ผลิตหรือผู้จัดจำหน่ายที่มีความน่าเชื่อถือ หรือเลือกใช้โปรแกรมแบบโอเพ่นซอร์ส (Open source software) คือซอฟต์แวร์ลิขสิทธิ์ที่มีไลเซนส์แบบโอเพ่นซอร์ส ซึ่งมีลักษณะต่างจากซอฟต์แวร์ทั่วไป คือผู้พัฒนาซอฟต์แวร์จะอนุญาตให้ผู้ใช้ติดตั้งและใช้งานได้โดยไม่จำกัดจำนวนและรูปแบบการใช้งาน ไม่ว่าจะเป็นการใช้งานส่วนตัว ในเชิงธุรกิจหรือในองค์กร มีการเผยแพร่ต้นฉบับ (Source code) ของซอฟต์แวร์เพื่อให้ผู้ใช้งานสามารถแก้ไขดัดแปลงให้ตรงความต้องการได้ ซึ่งซอฟต์แวร์แบบโอเพ่นซอร์สนี้มีข้อดีอยู่ด้วยกันหลายประการ ยกตัวอย่างเช่น ประหยัดค่าใช้จ่ายเพราะไม่มีค่าใบอนุญาต (License) และไม่เสี่ยงต่อการละเมิดลิขสิทธิ์ สามารถแก้ไขโปรแกรมให้ตรงกับความต้องการของตัวเองหรือขององค์กรได้ทันที สามารถทำร่วมกันกับซอฟต์แวร์อื่นๆได้เป็นอย่างดี ไม่เหมือนกับซอฟต์แวร์แบบโคลสซอร์ส (Closed source software) หรือซอฟท์แวร์ลิขสิทธ์ที่มีค่าใช้จ่าย ซึ่งบางครั้งประเทศที่ผู้ใช้งานอาศัยอยู่ก็ไม่สามารถโหลดซอฟต์แวร์นั้นๆ หรือตัวอัพเดตซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ได้ และซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ส่วนมากมักมีไวรัสติดมาด้วย

การทำลายข้อมูลในคอมพิวเตอร์อย่างปลอดภัย

คลิปหลุดออกมาแบบนี้ ไม่เชื่อก็ต้องเชื่อ ลบแล้ว ฟอร์แมตแล้ว ก็ยังสามารถกู้มาได้

ทุกวันนี้คนส่วนใหญ่ใช้คอมพิวเตอร์ในการทำงานและจัดเก็บข้อมูล ใ น เวลาที่เราดาวน์โหลดรูปภาพหรือคลิปวีดิโอ รูปภาพหรือคลิปวีดิโอเหล่านั้นก็จะถูกจัดเก็บเอาไว้ในฮาร์ดดิสก์ของเครื่องหรือที่เก็บข้อมูลขนาดพกพาจนกว่าผู้ใช้จะไม่ต้องการและจัดการลบข้อมูลทิ้งไป อย่างไรก็ตาม ข้อมูลต่างๆ ที่ผู้ใช้ลบด้วยวิธีการลบแบบเบื้องต้นอาจไม่เพียงพอหากข้อมูลนั้นเป็นข้อมูลที่เป็นความลับสำคัญหรือเป็นข้อมูลที่ไม่อยากเปิดเผยให้ใครรู้ เพราะข้อมูลที่ถูกลบไปแล้วนั้น ยังสามารถกู้กลับมาได้ใหม่อีกครั้งหากไม่ใช้วิธีการลบขั้นสูงหรือใช้โปรแกรมที่ช่วยในการลบข้อมูลโดยสมบูรณ์ ดังนั้น ผู้ใช้งานจึงควรมีโปรแกรมช่วยลบติดคอมพิวเตอร์ไว้สักหนึ่งตัวหากต้องการลบไฟล์ข้อมูลที่สำคัญหรือเป็นความลับ

โปรแกรมช่วยลบข้อมูลโดยสมบูรณ์มีอยู่หลายโปรแกรม มีคุณสมบัติช่วยลบไฟล์ข้อมูลที่ไม่ต้องการได้อย่างถาวร โ ดยไม่สามารถกู้กลับคืนมาได้อีก โ ดย แต่ละตัวนั้นก็จะมีวิธีการดำเนินการลบข้อมูลที่หลากหลาย และมีขั้นตอนการใช้งานที่ยากง่ายแตกต่างกันออกไป โ ดยในที่นี้จะขอยกตัวอย่างบางโปรแกรมที่สามารถใช้งานได้อย่างมีประสิทธิภาพและมีขั้นตอนที่ไม่ยุ่งยากในการใช้งาน

Data Shredder

เดต้า เชร็ดเดอร์ คือโปรแกรมทำลายข้อมูลที่ออกแบบมาเพื่อช่วยในการลบข้อมูลที่ถูกเก็บไว้ในฮาร์ดดิสก์ (Hard disk) หรือที่เก็บข้อมูลขนาดพกพาอื่นๆ เช่น USB โดยโปรแกรมนี้จะช่วยให้เราลบข้อมูลที่เราไม่ต้องการโดยสมบูรณ์และไม่สามารถกู้กลับคืนมาได้ใหม่ โ ปรแกรมนี้จะมีวิธีการทำงานที่แตกต่างออกไปจากโปรแกรมลบข้อมูลตัวอื่นๆ เพราะมันจะใช้วิธีการเขียนทับไฟล์ข้อมูลที่ต้องการลบ ทำให้ข้อมูลเก่าเสียไปและไม่สามารถเรียกกลับคืนมาได้อีก โ ดยผู้ที่ใช้งานระบบวินโดวส์ (Windows) สามารถเข้าดาวน์โหลดได้ที่ www.fileshredder.org วิธีเรียกใช้งานโปรแกรมก็ง่าย เพียงแค่คลิกขวาบนไฟล์ โ ปรแกรมก็จะปรากฏขึ้นมาให้เลือกใช้ได้โดยสะดวก การลบไฟล์ด้วย Data Shredder มีขั้นตอนดังนี้

1. คลิกขวาบนไฟล์ที่ต้องการลบ > เลือก File Shredder > เลือก Secure delete files
2. จะปรากฏหน้าต่างถามว่าต้องการที่จะลบไฟล์ดังกล่าวจริงๆหรือไม่
3. หลังจากกดยืนยัน โปรแกรมจะทำการลบไฟล์ดังกล่าว เวลาในการดำเนินงานจะขึ้นอยู่กับขนาดของไฟล์นั้นๆ

เปิดใช้งาน Firewall

Firewall คือ สิ่งควบคุมการเข้าออกของข้อมูล

สำหรับคอมพิวเตอร์ส่วนบุคคล Firewall (ไฟร์วอลล์) จัดเป็นโปรแกรมพื้นฐานอีกหนึ่งอย่างที่จำเป็นต้องติดตั้งเอาไว้ในเครื่อง เพราะ Firewall จะทำหน้าที่เสมือนเป็นกำแพงผู้พิทักษ์ในการตรวจสอบการส่งผ่านข้อมูลจากระบบเน็ตเวิร์กมายังตัวเครื่องและจากตัวเครื่องออกไปสู่ระบบเน็ตเวิร์ก โ ดยช่วยบล็อกการส่งข้อมูลที่ไม่จำเป็นรวมถึงการเข้าถึงข้อมูลภายในเครื่องคอมพิวเตอร์จากภายนอกโดยไม่ได้รับอนุญาตตามที่เราตั้งค่าเอาไว้ ช่วยให้ข้อมูลภายในเครื่องคอมพิวเตอร์ปลอดภัยและไม่ถูกเจาะระบบเพื่อดูดเอาข้อมูลความลับทางธุรกิจออกไปอย่างแน่นอน

ใช้ระบบ VPN เพิ่มความปลอดภัยในระบบเครือข่าย

การติดต่อสื่อสารระหว่างกันภายในหน่วยงานไม่ว่าจะอยู่ในสถานที่เดียวกันหรือต่างสถานที่ผ่านระบบเครือข่ายของหน่วยงานจำเป็นต้องมีมาตรการรักษาความปลอดภัยที่รัดกุมมากเป็นพิเศษ เพราะข้อมูลลับของหน่วยงานส่วนหนึ่ง

จะถูกส่งผ่านช่องทางนี้เช่นกัน การใช้ระบบเครือข่าย VPN (Virtual Private Network) จะช่วยให้การส่งข้อมูลผ่านเครือข่ายของหน่วยงานมีความปลอดภัยและรัดกุมมากขึ้น เพราะมีการเข้ารหัสด้วยตัวระบบก่อนที่ทำการส่งข้อมูลเสมอ จึงเป็นเรื่องยากหากผู้ไม่ประสงค์ดีจะมาดักจับข้อมูลไปจากเครือข่าย

วิธีการป้องกันข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานให้รอดพ้นจากการโจมตีด้วยไวรัสและการล้วงข้อมูลของเหล่าบรรดานักแฮกเกอร์ที่ดีที่สุด ต้องเริ่มต้นที่ตัวของผู้ใช้งานก่อนเป็นสำคัญ เพราะวิธีการที่นำเสนอมาจะไม่มีประโยชน์อะไรเลยหากผู้ใช้งานยังขาดซึ่งความรู้และทำตัวไม่ภักดีต่อหน่วยงานด้วยการนำข้อมูลที่เป็นความลับจากภายในออกไปยังภายนอก ดังนั้นนอกจากการสแกนคอมพิวเตอร์เพื่อหาไวรัสแล้ว ก็ควรสแกนเจ้าหน้าที่เพื่อหาสายลับควบคู่กันไปในตัวด้วย จึงจะเป็นการป้องการรั่วไหลของข้อมูลที่ดีที่สุด เพราะถึงอย่างไรเสียไวรัสที่ว่าร้ายก็ยังมิอาจสู้ใจคนที่คิดคดเป็นแน่แท้

.....

อ้างอิง :

- Master in Security, จตุชัย แพงจันทร์, info press, 2550
- www.ictkm.info
- www.thaicert.or.th

บรรณานุกรม

- Charles P. Pfleeger and Shari Lawrence Pfleeger, “Analyzing Computer Security.” Pearson Education Internation, December 2011.
- คู่มือ Linux Security พิมพ์ครั้งที่ 4, อ.บัณฑิต จามรภูติ, บริษัท เอช.เอ็น กรุ๊ป จำกัด, 2556
- คู่มือแก้ไขปัญหาเครือข่าย CISCO สไตล์อาจารย์วิรินทร์ เล่ม 1, ดร.วิรินทร์ เมฆประดิษฐสิน, บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน), 2552
- ตำราผู้ดูแลระบบยูนิซ์ / ลินุกซ์และการเขียนโปรแกรมระบบเครือข่ายคอมพิวเตอร์, ดร.สานนท์ ฉิมมณี, บริษัท เอเชียดิจิตอล การพิมพ์ จำกัด, 2551
- Master in Security, จตุชัย แพงจันทร์, info press,2550
- www.ictkm.info
- www.thaicert.or.th

แบบฟอร์มที่ ๑ การจำแนกองค์ความรู้ที่จำเป็นต่อการผลักดันตามประเด็นยุทธศาสตร์ของส่วนราชการ/จังหวัด (KM Action Plan)

ชื่อส่วนราชการ : กคศ.สกศ.รร.จปร.

ประเด็นยุทธศาสตร์	**เป้าประสงค์ (objective)**	**ตัวชี้วัด (KPI) ตามคำรับรอง**	**เป้าหมายของตัวชี้วัด**	**องค์ความรู้ที่จำเป็นต่อการปฏิบัติงานตามประเด็นยุทธศาสตร์**
การรักษาความมั่นคงของรัฐ				การรักษาความปลอดภัยทางคอมพิวเตอร์
องค์ความรู้ที่จำเป็นต่อการปฏิบัติราชการตามประเด็นยุทธศาสตร์ที่เลือกมาจัดทำแผนการจัดการความรู้ คือ				
แผนการจัดการความรู้	ประเด็นยุทธศาสตร์ : การรักษาความมั่นคงของรัฐ			
แผนที่ ๑	องค์ความรู้ที่จำเป็น : การรักษาความปลอดภัยทางคอมพิวเตอร์			
	เหตุผลที่เลือกองค์ความรู้ : กำลังพลทบ. ส่วนมากไม่ตระหนักถึงภัยอันตรายทางคอมพิวเตอร์ เป็นเหตุให้ตนเองอาจตกเป็นเป้าหมายของผู้ไม่ประสงค์ดี หรืออาจเป็นเหตุให้เกิดความไม่ปลอดภัยแก่ข้อมูลความลับทางราชการ			
	ตัวชี้วัดตามคำรับรองและเป้าหมายที่เลือกใช้วัดการทำ KM :			

แบบฟอร์มที่ ๒ แผนการจัดการความรู้ (KM Action Plan)

ชื่อส่วนราชการ : กคศ.สกศ.รร.จปร.

ประเด็นยุทธศาสตร์ : การรักษาความมั่นคงของรัฐ

องค์ความรู้ที่จำเป็น : การรักษาความปลอดภัยทางคอมพิวเตอร์

ลำดับ	กิจกรรม	ระยะเวลา	ตัวชี้วัด	เป้าหมาย	กลุ่มเป้าหมาย	เครื่องมือ/อุปกรณ์	งบประมาณ	ผู้รับผิดชอบ	CMP
๑	**การบ่งชี้ความรู้** -สมาชิกกลุ่มได้ร่วมกันระดมสมองเพื่อค้นหาความรู้ที่พึงประสงค์	ม.ค. ๕๗	จำนวนสมาชิกของ KM Team	๓ คน	KM Team	สถานที่ฐานความรู้	-	กคศ.	๑,๒,๓
๒	**การสร้างและแสวงหาความรู้** -ค้นคว้าข้อมูลจากระบบสารสนเทศ -ทดลองปฏิบัติ -ค้นคว้า case study จากข่าวสารต่าง ๆ	ก.พ.-เม.ย. ๕๗	จำนวนแหล่งข้อมูล	ไม่น้อยกว่า ๔ แหล่งข้อมูล	ห้องสมุด รร.จปร., ห้องสมุด กคศ., ระบบสืบค้น	ฐานความรู้, การเชื่อมต่ออินเตอร์เน็ต	-	กคศ.	๑,๒,๓,๔
๓	**การจัดความรู้ให้เป็นระบบ** - Security threat - Security prevention	เม.ย.-พ.ค.๕๗	ความชัดเจนและการเข้าถึงข้อมูล	ร้อยละ ๑๐๐	ความรู้เกี่ยวกับภัยคุยคามทางคอมพิวเตอร์ , แนวทางการป้องกันตนเองเบื้องต้น	ฐานความรู้	-	กคศ.	๑,๒,๓,๔
๔	**การประมวลและกลั่นกรองความรู้** -นำคู่มือที่จัดทำขึ้นให้ผู้เชี่ยวชาญตรวจสอบ	มิ.ย.-ก.ค. ๕๖	จำนวนผู้เชี่ยวชาญที่ตรวจสอบ	ไม่น้อยกว่า ๓ คน	ผู้เชี่ยวชาญด้านคอมพิวเตอร์	อินเตอร์เน็ต, หนังสือ	-	กคศ.	๑,๒,๓,๔,๕
๕	**การเข้าถึงความรู้** -นำร่างคู่มือที่ให้ผู้เชี่ยวชาญตรวจสอบแล้วให้กำลังพลในแต่ละหน่วยได้ศึกษา	ส.ค. ๕๖	จำนวนช่องทาง	ไม่น้อยกว่า ๒ ช่องทาง	อินเตอร์เน็ท, คู่มือ	อินเตอร์เน็ท , คู่มือ	-	กคศ.	๑,๒,๓,๔,๕

ลำดับ	กิจกรรม	ระยะเวลา	ตัวชี้วัด	เป้าหมาย	กลุ่มเป้าหมาย	เครื่องมือ/อุปกรณ์	งบประมาณ	ผู้รับผิดชอบ	CMP
๖	**การแบ่งปันแลกเปลี่ยนเรียนรู้** -พูดคุยสอบถามผ่านเว็บบอร์ด	ก.ย. ๕๖	จำนวนเว็บบอร์ดที่เข้าร่วม	ไม่น้อยกว่า 5	ผู้สนใจทั่วไป	เครื่องแม่ข่าย, เอกสาร	-	กคศ.	๑,๒,๓,๔,๕
๗	**๗.๑ การเรียนรู้** จัดอบรม cyber security เผยแพร่แจกจ่ายคู่มือทั้งทางอินเตอร์เน็ทและพิมพ์แจก	ต.ค. ๕๖	จำนวนเอกสารที่แจกจ่าย/ยอดการดาวโหลด	ไม่น้อยกว่า 5	กำลังพลรร.จปร. และผู้สนใจทั่วไป	เครื่องแม่ข่าย, เอกสาร	-	กคศ.	๖
	๗.๒ การยกย่องชมเชย								