รายงานฉบับสมบูรณ์

โครงการขอรับการส่งเสริมและสนับสนุนจากเงินกองทุนวิจัยและพัฒนา
กิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ

ประจำงวดที่ 3 (งวดสุดท้าย)

(โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชน)

(นายสมทบ แก้วเชื้อ)

ได้รับทุนอุดหนุนจาก
กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ
(สำนักงาน กสทช.)

กทปส

คำนำ

รายงานการศึกษาวิจัย “โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ สำหรับองค์กรขนาดเล็กในระดับชุมชน” ฉบับนี้เป็นรายงานฉบับสมบูรณ์ซึ่งคณะผู้วิจัยได้รวบรวมข้อมูลและทำการสำรวจการใช้งานระบบเทคโนโลยีสารสนเทศของท้องถิ่น ศึกษาวิเคราะห์ผลการสำรวจ พร้อมแนวทางการวิจัยพัฒนาระบบเครือข่ายความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน/รายงานผลพร้อมตัวแบบจำลอง อีกทั้งจัดเสวนาแลกเปลี่ยนเรียนรู้ เผยแพร่ และสร้างความตระหนักให้รู้เท่าทันภัยคุกคามทางไซเบอร์และจัดทำข้อเสนอแนะเชิงนโยบายเพื่อเป็นแนวทางในการการป้องกันภัยคุกคามข้อมูลสารสนเทศที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน

คณะผู้วิจัย ขอขอบคุณกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ที่ได้มอบความไว้วางใจให้มหาวิทยาลัยราชภัฏสวนสุนันทา ทำโครงการสำหรับการศึกษาวิจัยดังกล่าวนี้ และขอขอบคุณท่านอธิการบดี มหาวิทยาลัยราชภัฏสวนสุนันทา ที่ให้การสนับสนุน คณะผู้วิจัยอย่างดียิ่งมาโดยตลอด ขอขอบคุณบุคลากรที่เกี่ยวข้องทุกท่านของมหาวิทยาลัยราชภัฏสวนสุนันทาที่ช่วยดูแลงานด้านเอกสารต่าง ๆ และสุดท้ายขอขอบคุณผู้บริหารองค์กรปกครองส่วนท้องถิ่น ผู้นำชุมชน ข้าราชการและประชาชนผู้เกี่ยวข้องทุกท่านที่ให้กรุณาให้ข้อมูลที่เป็นประโยชน์ให้งานวิจัยฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี

คณะผู้วิจัย

สารบัญ

แบบรายงานความก้าวหน้า

โครงการขอรับการส่งเสริมและสนับสนุนจากเงินกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ

❒ ไตรมาสที่ 1/2560 ❒ ไตรมาสที่ 2/2560
☑ ไตรมาสที่ 3/2560 ❒ ไตรมาสที่ 4/25.....

ชื่อโครงการ (ไทย) :	**การศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ สำหรับองค์กรขนาดเล็กในระดับชุมชน**			
ชื่อโครงการ (อังกฤษ) :				
สัญญารับทุนเลขที่ :	B๒-๒-๒๐/๕๘			
หน่วยงาน :	**มหาวิทยาลัยราชภัฏสวนสุนันทา**			
ชื่อ – นามสกุล : (หัวหน้าโครงการ)	**นาย สมทบ แก้วเชื้อ**			
เบอร์ติดต่อ :		**E-Mail :**		
ระยะเวลาดำเนินการ : (เริ่มต้น – สิ้นสุด)	**20 กุมภาพันธ์ – 18 ตุลาคม 2560**	**ปี**	**8**	**เดือน**
งบประมาณรวม :	**รวมทั้งสิ้น**	**จำนวน**	**2,614,300**	**บาท**

ส่วนที่ ๑ สาระสำคัญของโครงการ (Project Hilight)

๑.๑ วัตถุประสงค์

๑.๑.๑ เพื่อส่งเสริมบุคลากรในองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน รวมถึงประชาชนทั่วไปที่มีส่วนร่วมกับองค์กรให้มีความตระหนักรู้ ความรู้ ความเข้าใจพื้นฐานทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๑.๒ เพื่อศึกษาและรวบรวมปัญหา วิเคราะห์ความเสี่ยงและผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน

๑.๑.๓ เพื่อจัดทำข้อเสนอแนะเชิงนโยบายและตัวแบบจำลองสำหรับองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชนในการผลักดันให้เกิดการป้องกันภัยคุกคามทางไซเบอร์อย่างเป็นระบบอย่างบูรณาการ

๑.๒ เป้าหมาย

เป้าหมายในการดำเนินงานการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชน เพื่อหาแนวทางที่เป็นรูปธรรมในรูปแบบการปฏิบัติงาน ที่ชัดเจนในการสร้างความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรและผู้เกี่ยวข้องในองค์กรปกครองส่วนท้องถิ่นได้อย่างเหมาะสมและมีประสิทธิภาพสูงสุด ทำให้ประชาชนในท้องถิ่นเกิดความตระหนักรู้ถึงปัญหาภัยคุกคามที่มาจากระบบเครือข่ายสารสนเทศ และวิธีการเฝ้าระวังความปลอดภัยทางไซเบอร์ รวมถึงแนวทางในการรับมือที่คาดว่าจะเกิดขึ้นกับความมั่นคงทางไซเบอร์ได้ในอนาคต และสามารถนำมาต่อยอดในการวิจัยครั้งต่อไปในการสร้างมาตรฐานในการกำหนดสมรรถนะทางความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นมาตราการในการใช้งานและการตรวจสอบอย่างมีมาตรฐาน

<u>บทบาทภาครัฐในการผลักดันให้เกิดการขยายตัวการใช้งานอินเทอร์เน็ต</u>

จากความสำคัญดังกล่าวนี้ภาครัฐจึงได้ศึกษาแนวทางและได้กำหนดเป็นแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด ฉบับนำเสนอคณะรัฐมนตรี ๕ เมษายน ๒๕๕๙ เพื่อใช้เป็นกรอบในการผลักดันให้เทคโนโลยีดิจิทัลเป็นกลไกสำคัญในการพัฒนาเศรษฐกิจและสังคมของประเทศ ซึ่งรวมถึงการปรับเปลี่ยนกระบวนทัศน์ทางความคิดใน ทุกภาคส่วนเพราะเทคโนโลยีดิจิทัลจะไม่ได้เป็นเพียงเครื่องมือสนับสนุนการทำงานเฉกเช่นที่ผ่านมาอีกต่อไป จากนโยบายการผลักดันของรัฐบาลทำให้หน่วยงานของภาครัฐเองได้เริ่มดำเนินการเตรียมการเข้าสู่การเป็นรัฐบาลดิจิทัล โดยเฉพาะอย่างยิ่งหน่วยงานของภาครัฐระดับองค์กรขนาดเล็ก เช่น องค์กรปกครองส่วนท้องถิ่นได้มีการจัดทำแผนพัฒนาท้องถิ่น การบริหารงานบุคคล การเงินการคลัง และการบริหารจัดการเพื่อให้องค์กรปกครองส่วนท้องถิ่นมีความเข้มแข็งและมีศักยภาพในการให้บริการสาธารณะโดยการนำเทคโนโลยีดิจิทัลเข้ามาสนับสนุนมากยิ่งขึ้น อาทิเช่น ระบบแผนที่ภาษีและทะเบียนทรัพย์สิน (LTAX GIS และ LTAX 3000) ระบบบัญชีคอมพิวเตอร์ของกรมส่งเสริมการปกครองส่วนท้องถิ่น (Electronic Administration Accounting System)และระบบโครงข่ายพื้นฐานเพื่อชุมชน เป็นต้น ซึ่งขณะที่เร่งขับเคลื่อนเพื่อเข้าสู่การเป็นรัฐบาลดิจิทัลแต่กลับต้องเผชิญกับปัญหาความปลอดภัยของระบบสารสนเทศหรือปัญหาภัยคุกคามทางไซเบอร์รุนแรงมากขึ้นทุกๆ ปี เริ่มตั้งแต่การถูกบุกรุกเข้าสู่ระบบคอมพิวเตอร์ในรูปแบบต่าง ๆ อาทิเช่น ไวรัสคอมพิวเตอร์ มัลแวร์ สปายแวร์ หนอนคอมพิวเตอร์ การแฮ็กเข้าสู่ระบบคอมพิวเตอร์ซึ่งเป็นปัญหาที่กระทบต่อระบบการสื่อสารและทำลายระบบฐานข้อมูล ซึ่งภัยคุกคามรูปแบบนี้มีมาเป็นระยะเวลานาน แต่ในระดับองค์กรขนาดเล็กหรือระดับท้องถิ่นยังไม่ได้ถูกแก้ไขอย่างมีระบบ ประกอบกับในช่วงระยะ ๒ ปีที่ผ่านมา ปัญหาการกระทำความผิดในการนำเข้าข้อมูลที่ผิดกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ซึ่งกระทบต่อความมั่นคงของประเทศที่ปรากฏขึ้นเป็นจำนวนมาก

ปัจจุบันการป้องกันภัยคุกคามยังต้องอาศัย Hardware และ software ของต่างประเทศ ซึ่งยังมีราคาค่อนข้างสูง การใช้งานค่อนข้างยาก แต่การป้องกันการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พบว่า Hardware และ software ของต่างประเทศมิได้รองรับในส่วนนี้ ถึงแม้ว่าในประเทศไทยเอง ได้เริ่มมีการพัฒนา Hardware และ software สำหรับการป้องกันภัยคุกคามทางไซเบอร์มาระยะหนึ่งแล้ว แต่ยังไม่ค่อยได้รับความนิยมมากนัก

สำหรับหน่วยงานของรัฐระดับองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน นั้น พบว่ายังขาดความพร้อมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในด้านความรู้ความเข้าใจ ด้านบุคลากร และด้านการพัฒนาเครื่องมือเพื่อป้องกันภัยคุกคามอย่างเป็นระบบ ดังนั้น มหาวิทยาลัยราชภัฏสวนสุนันทา จึงเล็งเห็นความสำคัญในการดำเนิน “โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือเฝ้าระวังความมั่นคงปลอดภัย

ทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชน” เพื่อการศึกษาวิจัย เพื่อวิเคราะห์ความเสี่ยง เพื่อพัฒนาเครื่องมือสารสนเทศสำหรับการป้องกันภัยคุกคามทางไซเบอร์ พร้อมทั้งสร้างความรู้ความเข้าใจให้แก่บุคลากรในองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน ซึ่งองค์กรปกครองส่วนท้องถิ่นน่าจะเป็นแบบอย่างหรือเป็นต้นแบบให้กับหน่วยงานหรือองค์กรขนาดเล็กในระดับชุมชนได้เป็นอย่างดี

โดยที่ผ่านมาทางมหาวิทยาลัยได้มีการวิจัยเรื่องรูปแบบและมาตรการแก้ไขปัญหาทางไซเบอร์ (Model and measure of Solving Problem Cyber Crime) (ได้รับทุนจาก สกว. ปี ๒๕๕๗) ซึ่งได้รับรางวัลวิจัยดีเด่นด้านวิทยาศาสตร์และเทคโนโลยี ในงานวิจัยมีแนวทางหลักที่สำคัญเพื่อป้องกันภัยคุกคามทางไซเบอร์และอาชญากรรมทางไซเบอร์ โดยสำหรับการพัฒนาเครื่องมือที่มีประสิทธิภาพนั้น ประกอบด้วยการค้นหา (Detection) การป้องกัน (Protection) การเตือนภัย (Response) การบันทึกข้อมูลจราจรคอมพิวเตอร์ (Record) โดยเฉพาะอย่างยิ่งสถิติจากงานวิจัยสำหรับองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน มีอาชญากรรมทางไซเบอร์สูงและมีการป้องกันภัยคุกคามไซเบอร์ที่ค่อนข้างต่ำกว่าองค์กรขนาดใหญ่หรือองค์กรในระดับประเทศ/ชุมชนเมือง ทั้งนี้องค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชนนั้นยังขาดความพร้อมด้านบุคลากรและการพัฒนาเครื่องมือสำหรับป้องกันภัยคุมคามจึงควรต้องมีกระบวนการใช้งานและคู่มือที่ใช้งานได้ง่าย สะดวก เหมาะสม และมีประสิทธิภาพสูงสุด ซึ่งองค์กรปกครองส่วนท้องถิ่นน่าจะเป็นแบบอย่างหรือเป็นต้นแบบให้กับหน่วยงานหรือองค์กรขนาดเล็กในระดับชุมชนได้เป็นอย่างดี

๑.๓ ผลผลิตสำคัญ

ลำดับ	ชื่อผลผลิต	หน่วยวัด	ตัวชี้วัด (เชิงคุณภาพ/เชิงคุณภาพ)
๑	รายงานการศึกษาวิเคราะห์ความเสี่ยงรูปแบบภัยคุกคามต่าง ๆ เว็บไซต์และเนื้อหาที่ไม่เหมาะสมหรือเสี่ยงต่อการกระทำผิดทางกฎหมายสำหรับองค์กรขนาดเล็ก ระดับชุมชน จากกลุ่มตัวอย่าง 1,000 กลุ่มตัวอย่าง พร้อมด้วยตัวแบบจำลอง	๑ ฉบับ	ได้แนวทางในการพัฒนาอุปกรณ์ป้องกันภัยคุกคามข้อมูลสารสนเทศที่เหมาะสมสำหรับชุมชนขนาดเล็ก จำนวน 1 ชุด
๒	บุคลากรในองค์กรท้องถิ่นและประชาชนในท้องถิ่นมีความตระหนักรู้ให้รู้เท่าทันภัยคุกคามทางไซเบอร์	๑๕๐ คน	เจ้าหน้าที่ที่เกี่ยวข้องในชุมชนเข้าใจเรื่องภัยคุกคามข้อมูลสารสนเทศ รู้จักและใช้งานอุปกรณ์จากหลักสูตรสำหรับอบรม
๓	ข้อเสนอแนะเชิงนโยบาย	๑ ฉบับ	แนวทางในการพัฒนาอุปกรณ์ป้องกันภัยคุกคามข้อมูลสารสนเทศที่ใช้งานง่ายเหมาะสำหรับชุมชนขนาดเล็กที่ขาดผู้เชี่ยวชาญในการดูแล

๑.๔ แผนปฏิบัติการโครงการ

ลำดับ	กิจกรรมที่สำคัญ	ระยะเวลาการดำเนินกิจกรรม				
		ประจำปี 2560				น้ำหนัก
		Q1	Q2	Q3	Q4	(%)
๑	นำเสนอรายงานแผนการดำเนินงาน (Project Plan)	√				10
๒	สำรวจการใช้งานระบบเทคโนโลยีสารสนเทศของท้องถิ่น		√			40
๓	ศึกษาวิเคราะห์ผลการสำรวจ พร้อมแนวทางการวิจัยพัฒนาระบบเครือข่ายความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน/รายงานผลพร้อมตัวแบบจำลอง		√			35
๔	จัดเสวนาแลกเปลี่ยนเรียนรู้ เผยแพร่ และสร้างความตระหนักให้รู้เท่าทันภัยคุกคามทางไซเบอร์			√		10
๕	จัดทำข้อเสนอแนะเชิงนโยบาย และเอกสารแนวทางในการพัฒนาอุปกรณ์ป้องกันภัยคุกคามข้อมูลสารสนเทศที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน/นำเสนอผลการดำเนินงานโครงการ			√		5
รวม						**100 %**

ส่วนที่ ๒ ความก้าวหน้าในการดำเนินโครงการ

๒.๑ สรุปผลการดำเนินงานประจำงวด

จากการดำเนินโครงการในแต่ละไตรมาสของการทำงานตามเงื่อนไขการเบิกจ่ายเงินในแต่ละไตรมาสโดยคณะผู้วิจัยได้ดำเนินการนำเสนอแผนการดำเนินงานในโครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชน ซึ่งประกอบประกอบด้วยรูปแบบ /วิธีการดำเนินงาน ขั้นตอนและระยะเวลาการดำเนินงานตลอดทั้งโครงการดังนี้

๑. นำเสนอรายงานแผนการดำเนินงาน (Project Plan)

๒. สำรวจการใช้งานระบบเทคโนโลยีสารสนเทศของท้องถิ่น

๓. ศึกษาวิเคราะห์ผลการสำรวจ พร้อมแนวทางการวิจัยพัฒนาระบบเครือข่ายความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน/รายงานผลพร้อมตัวแบบจำลอง

๔. จัดเสวนาแลกเปลี่ยนเรียนรู้ เผยแพร่ และสร้างความตระหนักให้รู้เท่าทันภัยคุกคามทางไซเบอร์

๕. จัดทำข้อเสนอแนะเชิงนโยบาย และเอกสารแนวทางในการพัฒนาอุปกรณ์ป้องกันภัยคุกคามข้อมูลสารสนเทศที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน/นำเสนอผลการดำเนินงานโครงการ

ส่วนในไตรมาสที่ ๒ คณะผู้วิจัยได้ดำเนินการได้ดำเนินการสำรวจการใช้งานระบบเทคโนโลยีสารสนเทศของท้องถิ่นในด้านต่างๆทั้งปัญหาภัยคุกคามทางไซเบอร์ของท้องถิ่น วิธีการแก้ไขปัญหา รวมถึงอุปสรรค์และข้อจำกัดต่างๆขององค์กรขนาดเล็กจำนวน ๑,๐๐๐ กลุ่มตัวอย่างโดยคณะดำเนินการได้ทำการเก็บรวบรวมข้อมูลได้จากกลุ่มตัวอย่างทั่วประเทศได้ทั้งสิ้น ๑,๕๐๐ กลุ่มอย่าง และได้ทำการคัดเลือกตัวแทนเพื่อทำการสัมภาษณ์เชิงลึกกับผู้เกี่ยวข้องลงโดยการลงพื้นที่ทั้งวิธีการสนทนาซักถามประเด็นที่เกี่ยวข้องและตอบแบบสัมภาษณ์โดยสามารถได้ข้อสรุปดังนี้

การดำเนินโครงการนี้คณะผู้ดำเนินโครงการจัดทำบันทึกข้อตกลงความร่วมมือทางวิชาการร่วมกับองค์การปกครองส่วนท้องถิ่นหรือหน่วยงานที่เกี่ยวข้อง และจะดำเนินการสำรวจศึกษาปัจจัยที่เกี่ยวข้องกับการดำเนินงานด้วยวิธีการแบบสอบถามและลงพื้นที่สัมภาษณ์จำนวน ๑,๐๐๐ กลุ่มตัวอย่างจากองค์การปกครองส่วนท้องถิ่นทั้ง ๗๖ จังหวัดทั่วประเทศไทยโดยประมาณ ๗,๘๓๕ แห่ง และคัดเลือกกลุ่มตัวอย่างในการดำเนินการพัฒนาเครื่องมือและระบบในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรปกครองส่วนท้องถิ่น จำนวน ๓๐ แห่ง

รายงานสรุปผลการดำเนินงานการสำรวจการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรส่วนท้องถิ่น

สรุปผลการดำเนินงานการสำรวจการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรส่วนท้องถิ่น ฉบับนี้มีวัตถุประสงค์เพื่อศึกษา รวบรวมปัญหา วิเคราะห์ความเสี่ยงและผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กรขนาดเล็กหรือในระดับท้องถิ่น/ชุมชน

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลเพื่อทำสรุปประเด็นสำคัญในครั้งนี้ คือ แบบสอบถามแบบที่กลุ่มตัวอย่าง (บุคลากรในองค์กรหรือประชาชนในชุมชน) เป็นผู้กรอกข้อมูลเอง (self-administrative questionnaire) ซึ่งได้จัดทำกับกลุ่มตัวอย่างทั้งสิ้น ๑,๕๐๐ คน โดยแบ่งแบบสอบถามออกเป็น ๕ ส่วน คือ

ส่วนที่ ๑ ข้อมูลทั่วไป

ส่วนที่ ๒ สรุปข้อมูลการใช้งานระบบเทคโนโลยีระบบสารสนเทศภายในองค์กร

ส่วนที่ ๓ แบบทดสอบความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ ๔ สถานภาพด้านการรักษาความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

ส่วนที่ ๕ แบบทดสอบความรู้เกี่ยวกับด้านกฎหมาย ว่าด้วยการกระทำผิด พรบ. เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

เมื่อเก็บรวบรวมข้อมูลเรียบร้อยแล้ว ผู้สรุปประเด็นสำคัญได้นำแบบสอบถามตรวจสอบความเรียบร้อยของการตอบรายข้อคำถาม จากนั้นจึงนำมาสรุปเป็นข้อๆ

ส่วนที่ ๑ ข้อมูลทั่วไป

ตารางที่ ๑.๑ จำนวนและร้อยละ จำแนกตามเพศของกลุ่มตัวอย่าง

เพศ	จำนวน/คน	ร้อยละ
ชาย	๕๘๘	๓๙.๐๒
หญิง	๙๑๒	๖๐.๐๘
รวม	**๑,๕๐๐**	**๑๐๐**

ตารางที่ ๑.๒ จำนวนและร้อยละ จำแนกตามอายุของกลุ่มตัวอย่าง

อายุ	จำนวน/คน	ร้อยละ
ต่ำกว่า ๒๐ ปี	๔๒	๒.๘๐
๒๑ – ๓๐ ปี	๑๐๒	๖.๘๐
๓๑ – ๔๐ ปี	๒๗๓	๑๘.๒๐
๔๑ – ๕๐ ปี	๖๒๑	๔๑.๔๐
ตั้งแต่ ๕๑ ปีขึ้นไป	๔๖๒	๓๐.๘๐
รวม	**๑,๕๐๐**	**๑๐๐**

ตารางที่ ๑.๓ จำนวนและร้อยละ จำแนกตามระดับการศึกษาของกลุ่มตัวอย่าง

ระดับการศึกษา	จำนวน/คน	ร้อยละ
มัธยมศึกษา/ปวช./ปวส.	๔๒	๒.๘๐
ปริญญาตรี	๔๖๒	๓๐.๘๐
ปริญญาโท	๘๗๘	๕๘.๕๓
ปริญญาเอก	๑๑๘	๗.๘๗
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๑.๑ – ๑.๓ พบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นผู้หญิง ซึ่งคิดเป็นร้อยละ ๖๐.๐๘ โดยมีอายุตั้งแต่ ๔๑ ปีขึ้นไปหรือกลุ่มวัยทำงานที่มีอายุงานพอสมควรแล้ว ซึ่งคิดเป็นร้อยละ ๗๒.๒๐ ระดับการศึกษาอยู่ระดับปริญญาโท ซึ่งคิดเป็นร้อยละ ๕๘.๕๓

ตารางที่ ๑.๔ จำนวนและร้อยละ จำแนกตามสังกัดหน่วยงานของกลุ่มตัวอย่าง

หน่วยงาน	จำนวน/คน	ร้อยละ
อบจ.	๓๕๑	๒๓.๔๐
เทศบาลตำบล/อบต.	๖๖๓	๔๔.๒๐
หน่วยงานที่เกี่ยวข้องกับเทศบาลตำบล/อบต./อบจ.	๓๗๒	๒๔.๘๐
ไม่ระบุสังกัด/ประชาชนทั่วไปในชุมชน	๑๑๔	๗.๖๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๑.๔ พบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นผู้ที่อยู่ในหน่วยงานเทศบาล อบต. อบจ. ซึ่งคิดเป็นร้อยละ ๖๗.๖๐ โดยมีหน่วยงานที่เกี่ยวข้องกับเทศบาล/อบต./อบจ. ร้อยละ ๒๔.๘๐ เป็นหน่วยงานที่เกี่ยวกับการศึกษาและการบริการสังคมที่ให้บริการบริเวณใกล้เคียงหรือระแวกเดียวกันกับเทศบาล/อบต./อบจ. อาทิ เช่น โรงเรียน สถานศึกษา โรงพยาบาล สถานีอนามัย เป็นต้น และมีประชาชนทั่วไปในชุมชน ร้อยละ ๗.๖๐ โดยเป็นสัดส่วนที่ทางผู้วิจัยอยากวัดความรู้ที่เกี่ยวข้องกับ Cyber Security ในทุกภาคส่วนของชุมชน

ตารางที่ ๑.๕ จำนวนและร้อยละ จำแนกตามงานที่ได้รับมอบหมายของกลุ่มตัวอย่าง

งาน	จำนวน/คน	ร้อยละ
ฝ่ายเทคโนโลยีสารสนเทศ (IT)	๓๔๔	๒๒.๙๓
ฝ่ายบริหาร*	๖๓๗	๔๒.๔๗
ฝ่ายบริการสังคม/การศึกษา	๔๓๑	๒๘.๗๓
ไม่ระบุ	๘๘	๕.๘๗
รวม	**๑,๕๐๐**	**๑๐๐**

*หมายเหตุ ฝ่ายบริหารเป็นฝ่ายบริหารเกี่ยวกับ อาทิเช่น งานปกครอง งานการพัสดุ งานการบัญชี เป็นต้น

ตารางที่ ๑.๖ จำนวนและร้อยละ จำแนกการเคยฝึกอบรมเกี่ยวกับ Cyber Security ของกลุ่มตัวอย่าง

การฝึกอบรม	จำนวน/คน	ร้อยละ
เคย	๒๘๘	๑๙.๒๐
ไม่เคย	๑,๒๑๒	๘๐.๘๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๑.๕ – ๑.๖ พบว่า กลุ่มตัวอย่างส่วนใหญ่ปฏิบัติหน้าที่เกี่ยวข้องกับฝ่ายบริหาร ร้อยละ ๔๒.๔๗ โดยรองลงมาฝ่ายเทคโนโลยีสารสนเทศและฝ่ายบริการสังคม/การศึกษา ค่อนข้างใกล้เคียงกัน ร้อยละ ๒๒.๙๓ และ ๒๘.๗๓ ตามลำดับ ซึ่งส่วนใหญ่ไม่เคยฝึกอบรมเกี่ยวกับ Cyber Security คิดเป็นร้อยละ ๘๐.๘๐ โดยผู้ที่เคยได้รับการฝึกอบรมเกี่ยวกับ Cyber Security ส่วนใหญ่เป็นผู้ที่ปฏิบัติหน้าที่เกี่ยวกับฝ่ายเทคโนโลยีสารสนเทศ (IT) และฝ่ายบริหาร

ส่วนที่ ๒ ข้อมูลการใช้งานระบบเทคโนโลยีสารสนเทศภายในองค์กร

ตารางที่ ๒.๑ จำนวนและร้อยละ จำแนกการใช้คอมพิวเตอร์ของกลุ่มตัวอย่าง

การใช้คอมพิวเตอร์	จำนวน/คน	ร้อยละ
คอมพิวเตอร์สำนักงาน	๑,๐๑๘	๖๗.๘๗
คอมพิวเตอร์ส่วนตัว	๔๘๒	๓๒.๑๓
รวม	**๑,๕๐๐**	**๑๐๐**

ตารางที่ ๒.๒ จำนวนและร้อยละ จำแนกการมีคนอื่นใช้คอมพิวเตอร์ของกลุ่มตัวอย่าง

คนอื่นใช้คอมพิวเตอร์	จำนวน/คน	ร้อยละ
ใช่	๖๔๓	๔๒.๘๗
ไม่ใช่	๘๕๗	๕๗.๑๓
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๒.๑ – ๒.๒ พบว่า กลุ่มตัวอย่างส่วนใหญ่ใช้คอมพิวเตอร์สำนักงานในการปฏิบัติงานคิดเป็นร้อยละ ๖๗.๘๗ แต่เป็นส่วนน้อยที่มีการใช้งานคอมพิวเตอร์จากคนอื่นคิดเป็นร้อยละ ๔๒.๘๗ จากข้อมูลพบว่ากว่าครึ่งของการใช้คอมพิวเตอร์สำนักงานมีบุคคลอื่นใช้คอมพิวเตอร์ร่วมด้วย

ตารางที่ ๒.๓ จำนวนและร้อยละ จำแนกการใช้งานโปรแกรมเฉพาะด้านบริหารจัดการของกลุ่มตัวอย่าง

โปรแกรมเฉพาะด้านบริหารจัดการ	จำนวน/คน	ร้อยละ
มี	๓๒๔	๒๑.๖๐
ไม่มี	๗๔๒	๔๙.๔๗
ไม่ระบุ/ไม่ทราบ	๔๓๔	๒๘.๙๓
รวม	**๑,๕๐๐**	**๑๐๐**

ตารางที่ ๒.๔ จำนวนและร้อยละ จำแนกการใช้งานรับส่งข้อมูลระหว่างหน่วยงานผ่านทางอินเทอร์เน็ตของกลุ่มตัวอย่าง

รับส่งข้อมูลผ่านทางอินเทอร์เน็ต	จำนวน/คน	ร้อยละ
มี	๑,๓๕๒	๙๐.๑๓
ไม่มี	๑๔๘	๙.๘๗
รวม	**๑,๕๐๐**	**๑๐๐**

ตารางที่ ๒.๕ จำนวนและร้อยละ จำแนกการนำอุปกรณ์สื่อสารชนิดอื่นมาเชื่อมต่อของกลุ่มตัวอย่าง

การนำอุปกรณ์สื่อสารอื่นเชื่อมต่อ	จำนวน/คน	ร้อยละ
เคย	๑,๑๒๔	๗๔.๙๓
ไม่เคย	๓๗๖	๒๕.๐๗
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๒.๓ – ๒.๕ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่มีโปรแกรมเฉพาะด้านบริหารจัดการ คิดเป็นร้อยละ ๔๙.๔๗ และไม่ทราบหรือไม่ระบุ คิดเป็นร้อยละ ๒๘.๙๓ แต่การรับส่งข้อมูลผ่านอินเทอร์เน็ตสูงถึงร้อยละ ๙๐.๑๓ โดยการรับส่งข้อมูลผ่านทางอินเทอร์เน็ต อาทิเช่น E-mail E-file E-office ระบบภาษี ระบบบัญชี ระบบทะเบียนทรัพย์สิน เป็นต้น ทั้งนี้ ยังมีการนำอุปกรณ์สื่อสารชนิดอื่นมาเชื่อมต่อคิดเป็นร้อยละ ๗๔.๙๓ ซึ่งถือว่าช่องทางและความเสี่ยงจากการใช้งานอินเทอร์เน็ตค่อนข้างสูง แต่หน่วยงานยังขาดโปรแกรมเฉพาะด้านบริหารจัดการในการป้องกันการรับส่งข้อมูลผ่านทางอินเทอร์เน็ตและการเชื่อมต่อจากอุปกรณ์ชนิดอื่นที่ไม่มีการป้องกันก็เป็นได้

ตารางที่ ๒.๖ จำนวนการใช้งานคอมพิวเตอร์เกี่ยวกับเรื่องต่างๆ ของกลุ่มตัวอย่าง

การใช้งานคอมพิวเตอร์เกี่ยวกับเรื่อง	จำนวน
- พิมพ์งานเอกสาร	๑,๒๕๖
- จัดเก็บข้อมูล	๑,๐๓๔
- ดูหนังฟังเพลง	๑,๔๘๗
- ใช้งานอีเมล์	๑,๔๓๗
- ค้นหาข้อมูล	๑,๐๒๗
- ดาวน์โหลดข้อมูล	๘๗๗
- Social Network	๗๙๘
- web site	๙๘๒
- ข่าวสาร	๗๘๖
- ซื้อขายออนไลน์	๓๔๘
- เกมส์	๑๒๖
- อื่นๆ	๑๒

จากตารางที่ ๒.๖ พบว่าการใช้งานคอมพิวเตอร์เกี่ยวกับเรื่องต่างๆ ๕ ลำดับแรกที่พบมากที่สุด ได้แก่ ดูหนังฟังเพลง การใช้งานอีเมล์ พิมพ์งานเอกสาร จัดเก็บข้อมูล และค้นหาข้อมูลตามลำดับ โดย ๓ ลำดับท้ายที่พบน้อยที่สุด ได้แก่ อื่นๆ เกมส์ และซื้อขายออนไลน์ตามลำดับ ซึ่งยังถือว่าการใช้งานอินเทร์เน็ตและคอมพิวเตอร์ยังคงมีความเสี่ยงการใช้งานอีเมล์และการจัดเก็บข้อมูลมีความถี่ค่อนข้างสูง

ส่วนที่ ๓ ข้อมูลการทดสอบความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

ตารางที่ ๓.๑ จำนวนและร้อยละ จำแนกการตั้งรหัสคอมพิวเตอร์ของกลุ่มตัวอย่าง

การตั้งรหัสคอมพิวเตอร์	จำนวน/คน	ร้อยละ
อย่างน้อย ๘ ตัวอักษร ทั้งตัวหนังสือและตัวเลข	๕๒๔	๓๔.๙๓
ง่ายต่อการจำของตนเอง	๘๑๔	๕๔.๒๗
จดบันทึกไว้กันลืม	๑๖๒	๑๐.๘๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๓.๑ พบว่า กลุ่มตัวอย่างส่วนใหญ่ตั้งรหัสคอมพิวเตอร์ที่ง่ายต่อการจำของตนเอง คิดเป็นร้อยละ ๕๔.๒๗ ทั้งนี้การตั้งรหัสที่เหมาะสมควรเป็นการตั้งรหัสอย่างน้อย ๘ ตัวอักษร ทั้งตัวหนังสือและตัวเลข คิดเป็นร้อยละเพียง ๓๔.๙๓ โดยกลุ่มตัวอย่างที่ตั้งรหัสที่เหมาะสมส่วนใหญ่เป็นผู้ปฏิบัติงานในฝ่าย IT ยังถือการตั้งรหัสคอมพิวเตอร์ของกลุ่มตัวอย่างยังมีความเสี่ยงพอสมควร

ตารางที่ ๓.๒ จำนวนและร้อยละ จำแนกการส่งซ่อมคอมพิวเตอร์ของกลุ่มตัวอย่าง

การส่งซ่อมคอมพิวเตอร์	จำนวน/คน	ร้อยละ
Backup และลบข้อมูลออกก่อน	๒๓๗	๑๕.๘๐
ส่งซ่อมกับเจ้าหน้าที่	๗๔๗	๔๙.๘๐
ส่งซ่อมตามร้านทั่วไป	๕๑๖	๓๔.๔๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๓.๒ พบว่า กลุ่มตัวอย่างส่วนใหญ่ส่งซ่อมกับเจ้าหน้าที่ซ่อมบำรุง คิดเป็นร้อยละ ๕๔.๒๖ ทั้งนี้การส่งซ่อมที่เหมาะสมควรเป็นการBackup และลบข้อมูลออกก่อน คิดเป็นร้อยละเพียง ๑๖.๑๔ โดยกลุ่มตัวอย่างที่มีการส่งซ่อมที่เหมาะสมส่วนใหญ่เป็นผู้ปฏิบัติงานในฝ่าย IT ยังถือว่าการส่งซ่อมคอมพิวเตอร์ของกลุ่มตัวอย่างยังมีความเสี่ยงพอสมควร ซึ่งการส่งซ่อมกับเจ้าหน้าที่ซ่อมบำรุงอาจมีการ Backup และลบข้อมูลออกก่อนแต่ข้อมูลนั้นๆ ก็จะผ่านเจ้าหน้าที่ซ่อมบำรุงซึ่งอาจมีการรั่วไหลของข้อมูลได้

ตารางที่ ๓.๓ จำนวนและร้อยละ จำแนกการแชร์ข้อมูลบนระบบเครือข่ายของกลุ่มตัวอย่าง

การแชร์ข้อมูลบนระบบเครือข่าย	จำนวน/คน	ร้อยละ
แบบ Full อ่านและเขียนได้	๑,๐๘๗	๗๒.๔๗
แบบอ่านได้อย่างเดียว	๙๙	๖.๖๐
แบบอ่านได้อย่างเดียวและตั้งรหัสในการแชร์ข้อมูล	๓๑๔	๒๐.๙๓
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๓.๓ พบว่า กลุ่มตัวอย่างส่วนใหญ่แชร์ข้อมูลบนระบบเครือข่ายแบบ Full อ่านและเขียนได้ คิดเป็นร้อยละ ๗๒.๔๗ ทั้งนี้การแชร์ข้อมูลบนระบบเครือข่ายที่เหมาะสมควรเป็นการแชร์ข้อมูลแบบอ่านได้อย่างเดียวและตั้งรหัสในการแชร์ข้อมูลหรือเป็นการแชร์ข้อมูลแบบเข้ารหัสไว้ คิดเป็นร้อยละเพียง ๒๐.๙๓ โดยกลุ่มตัวอย่างที่มีการแชร์ข้อมูลที่เหมาะสมส่วนใหญ่เป็นผู้ปฏิบัติงานในฝ่าย IT ยังถือว่าการการแชร์ข้อมูลบนระบบเครือข่ายของกลุ่มตัวอย่างยังมีความเสี่ยงค่อนข้างมาก

ตารางที่ ๓.๔ จำนวนและร้อยละ จำแนกการมีโปรแกรม Antivirus และการ update anti-virus ของกลุ่มตัวอย่าง

โปรแกรม Antivirus และการ update	จำนวน/คน	ร้อยละ
มี	๑,๓๒๖	๘๘.๔๐
ไม่มี	๙๐	๖.๐๐
ไม่ระบุ/ไม่ทราบ	๘๔	๕.๖๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๓.๔ พบว่า กลุ่มตัวอย่างส่วนใหญ่คอมพิวเตอร์มีโปรแกรม Antivirus คิดเป็นร้อยละ ๘๘.๔๐ แต่จากการสอบถามเพิ่มเติมพบว่า ส่วนใหญ่ไม่ได้มีการ update antivirus เนื่องจากการ update antivirus จะเป็นการส่งคอมพิวเตอร์ไปบำรุงรักษาโดยเจ้าหน้าที่ IT หรือบริษัทที่ทำหน้าที่ดังกล่าวทำการ update antivirus ให้แก่บุคลากรในหน่วยงาน ซึ่งถือว่าการ update antivirus อย่างสม่ำเสมอจะช่วยลดการติดสแปม การโจรกรรมข้อมูลส่วนบุคคลและข้อมูลส่วนราชการในคอมพิวเตอร์ของกลุ่มตัวอย่าง

ตารางที่ ๓.๕ จำนวนและร้อยละ จำแนกการใช้งาน Flash drive ไป save งานจากเครื่องอื่น แล้วนำมาเปิดที่คอมพิวเตอร์ของกลุ่มตัวอย่าง

การใช้งาน Flash drive	จำนวน/คน	ร้อยละ
Scan Virus ก่อนเปิดทุกครั้ง	๑,๓๐๘	๘๗.๒๐
เสียบแล้วเปิดใช้ทันที	๑๙๒	๑๒.๘๐
นำไปเสียบเครื่องอื่นก่อน เพื่อให้มั่นใจว่าไม่มี Virus	๐	๐.๐๐
ถามเจ้าของ Flash drive ว่ามีหรือไม่ เพื่อความมั่นใจ	๐	๐.๐๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๓.๕ พบว่า กลุ่มตัวอย่างส่วนใหญ่ Scan Virus ก่อนเปิดทุกครั้ง คิดเป็นร้อยละ ๘๗.๒๐ แต่หากเปรียบเทียบจากข้อมูลการ update antivirus ซึ่งไม่ค่อยมีการ update อย่างสม่ำเสมอ ยังถือว่ามีความเสี่ยงจากการใช้งาน Flash drive ถึงแม้ว่าพฤติกรรมการใช้งานของกลุ่มตัวอย่างค่อนข้างมีความปลอดภัยแล้วก็ตาม

จากข้อมูลในส่วนที่ ๓ ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ยังพบว่ากลุ่มตัวอย่างยังคงมีความเสี่ยงพอสมควร ถึงแม้ว่าพฤติกรรมการใช้งานบางประเด็นยังพอมีความปลอดภัยบ้างแล้วก็ตาม ทั้งนี้

กลุ่มตัวอย่างยังขาดความเข้าใจในประเด็นการตั้งรหัสคอมพิวเตอร์ การส่งซ่อมคอมพิวเตอร์ และแชร์ข้อมูลบนระบบเครือข่ายอยู่พอสมควร

ส่วนที่ ๔ สถานภาพด้านการรักษาความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

ตารางที่ ๔.๑ จำนวนและร้อยละ จำแนกการมีหน่วยงานที่ดูแลระบบสารสนเทศของกลุ่มตัวอย่าง

ผู้ดูแลระบบสารสนเทศ	จำนวน/คน	ร้อยละ
หน่วยงานภายใน	๗๔๕	๔๙.๖๗
หน่วยงานภายนอก	๖๔๑	๔๒.๗๓
ไม่ระบุ	๑๑๔	๗.๖๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๔.๑ พบว่า กลุ่มตัวอย่างส่วนใหญ่มีหน่วยงานภายในเป็นผู้ดูแลระบบสารสนเทศ คิดเป็นร้อยละ ๔๙.๖๗ และมีหน่วยงานภายนอกเป็นผู้ดูแล คิดเป็นร้อยละ ๔๒.๗๓ ทั้งนี้ กลุ่มตัวอย่างที่ไม่ระบุคิดเป็นร้อยละ ๗.๖๐ เป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๒ จำนวนและร้อยละ จำแนกการมีหน่วยงานที่รับผิดชอบในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นการเฉพาะของกลุ่มตัวอย่าง

การรับผิดชอบการรักษาความมั่นคงปลอดภัยสารสนเทศ	จำนวน/คน	ร้อยละ
หน่วยงานภายใน	๕๘๘	๓๙.๒๐
หน่วยงานภายนอก	๔๒๒	๒๘.๑๓
ไม่มี อยู่ระหว่างเตรียมการแผนงบประมาณปีถัดไป	๒๕๖	๑๗.๐๗
ไม่มี และยังไม่มีแผน	๑๒๐	๘.๐๐
ไม่ระบุ	๑๑๔	๗.๖๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๔.๒ พบว่า กลุ่มตัวอย่างส่วนใหญ่มีหน่วยงานภายในเป็นผู้รับผิดชอบในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ คิดเป็นร้อยละ ๓๙.๒๐ และมีการจ้างหน่วยงานภายนอก คิดเป็นร้อยละ ๒๘.๑๓ ตามลำดับ จากข้อมูลคิดเป็นร้อยละ ๒๕.๐๗ ยังไม่มีหน่วยงานผู้รับผิดชอบในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งอยู่ระหว่างการเตรียมแผนงบประมาณในปีถัดไปและไม่มีแผนงบประมาณในเรื่องดังกล่าวเลย ซึ่งการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรถือมีความสำคัญต้องสร้างความตระหนักให้แก่องค์กรเร่งดำเนินการในเรื่องดังกล่าว ทั้งนี้ กลุ่มตัวอย่างที่ไม่ระบุคิดเป็นร้อยละ ๗.๖๐ เป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๓ จำนวนการใช้งานระบบความมั่นคงปลอดภัยสารสนเทศของกลุ่มตัวอย่าง

ระบบความมั่นคงปลอดภัยสารสนเทศ	จำนวน
- ระบบ Firewall	๓๖๘
- ระบบ Antivirus	๑,๓๒๖
- Network Access Control	๒๔๖
- อื่นๆ	๑๓
- ไม่มี/ไม่ระบุ	๑๑๔

จากตารางที่ ๔.๓ พบว่า ลำดับมากที่สุดในการใช้งานระบบความมั่นคงปลอดภัยสารสนเทศเป็นระบบ Antivirus ลำดับรองลงมาเป็นระบบ Firewall และระบบ Network Access Control ตามลำดับ โดยส่วนใหญ่หากมีระบบ Firewall จะมีระบบ Antivirus ควบคู่ไปด้วย ทั้งนี้ ไม่มี/ไม่ระบุ เป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๔ จำนวนและร้อยละ จำแนกการทราบความหมาย “ไวรัสคอมพิวเตอร์”ของกลุ่มตัวอย่าง

การทราบความหมาย “ไวรัสคอมพิวเตอร์”	จำนวน/คน	ร้อยละ
ทราบ	๑,๒๘๔	๘๕.๖๐
ไม่ทราบ	๑๐๒	๖.๘๐
ไม่ระบุ	๑๑๔	๗.๖๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๔.๔ พบว่า กลุ่มตัวอย่างส่วนใหญ่ทราบความหมาย “ไวรัสคอมพิวเตอร์” คิดเป็นร้อยละ ๘๕.๖๐ แต่ยังไม่ทราบความหมายในเชิงลึก เนื่องจากส่วนใหญ่เป็นการตอบเกี่ยวกับการสร้างความเสียหายแก่ข้อมูลและระบบ ซึ่งไวรัสคอมพิวเตอร์บางชนิดรวมไปถึงการโจรกรรมข้อมูลและระบบด้วย ทั้งนี้ กลุ่มตัวอย่างที่ไม่ระบุคิดเป็นร้อยละ ๗.๖๐ เป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๕ จำนวนและร้อยละ จำแนกการทราบความหมาย “ฟิชชิ่ง”ของกลุ่มตัวอย่าง

การทราบความหมาย “ฟิชชิ่ง”	จำนวน/คน	ร้อยละ
ทราบ	๓๐๒	๒๐.๑๓
ไม่ทราบ	๑,๐๘๔	๗๒.๒๗
ไม่ระบุ	๑๑๔	๗.๖๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๔.๕ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่ทราบความหมาย “ฟิชชิ่ง” คิดเป็นร้อยละ ๗๒.๒๗ โดยกลุ่มที่ทราบความหมายส่วนใหญ่เป็นเป็นผู้ปฏิบัติงานในฝ่าย IT และเป็นผู้ที่เคยผ่านการอบรมด้าน Cyber security มาแล้ว ซึ่งการฟิชชิ่งนั้นคือการหลอกลวงทางอินเทอร์เน็ตหลายรูปแบบทั้งในเชิงทรัพย์สิน เชิงความรัก เชิงบุคคล เป็นต้น ทั้งนี้ กลุ่มตัวอย่างที่ไม่ระบุคิดเป็นร้อยละ ๗.๖๐ เป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๖ จำนวนและร้อยละ จำแนกการดำเนินการสอดคล้องกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ของกลุ่มตัวอย่าง

การดำเนินการสอดคล้องกับ พ.ร.บ. คอมพิวเตอร์	จำนวน/คน	ร้อยละ
ไม่ได้ดำเนินการ	๔๒๔	๒๘.๒๗
ได้ดำเนินการ อยู่ในขั้นตอนการวางแผนการดำเนินการ	๘๗๔	๕๘.๒๗
ได้ดำเนินการแล้วบางส่วนขององค์กร	๗๖	๕.๐๗
ได้ดำเนินการแล้วเต็มรูปแบบ	๑๒	๐.๘๐
ไม่ระบุ	๑๑๔	๗.๖๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๔.๖ พบว่า กลุ่มตัวอย่างส่วนใหญ่อยู่ระหว่างดำเนินการ คิดเป็นร้อยละ ๕๘.๒๗ และไม่ได้ดำเนินการเลย คิดเป็นร้อยละ ๒๘.๒๗ เป็นลำดับรองลงมา มีเพียงร้อยละ ๕.๘๗ ที่เริ่มดำเนินการไปบางส่วนและเต็มรูปแบบแล้ว จากข้อมูลส่งผลให้ทราบว่า พ.ร.บ. คอมพิวเตอร์ ยังคงเป็นเรื่องใหม่สำหรับองค์กรส่วนท้องถิ่น ซึ่งจากการสอบถามถึงการวางแผนการดำเนินการนั้น ยังคงไม่ทราบทิศทางที่ชัดเจนในการดำเนินการเรื่องดังกล่าวว่าต้องดำเนินการอย่างไร ทั้งนี้ กลุ่มตัวอย่างที่ไม่ระบุคิดเป็นร้อยละ ๗.๖๐ เป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๗ จำนวนและร้อยละ จำแนกการเก็บ Log ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ของกลุ่มตัวอย่าง

การเก็บ Log ตาม พ.ร.บ. คอมพิวเตอร์	จำนวน/คน	ร้อยละ
ไม่ได้ดำเนินการ	๑,๓๐๙	๘๗.๒๗
ดำเนินการ	๗๗	๕.๑๓
ไม่ระบุ	๑๑๔	๗.๖๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๔.๗ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่ได้ดำเนินการเก็บ Log ตาม พ.ร.บ. คอมพิวเตอร์ คิดเป็นร้อยละ ๘๗.๒๗ โดยมีเพียงร้อยละ ๕.๑๓ ที่ดำเนินการเก็บ Log แล้วเป็นกลุ่มที่ได้เริ่มดำเนินการไปบางส่วนและเต็มรูปแบบแล้ว ซึ่งการเก็บ Log เป็นเครื่องมืออย่างนึงในการช่วยกำกับดูแลการใช้งานคอมพิวเตอร์ให้เป็นไปตาม พ.ร.บ. คอมพิวเตอร์ ทั้งนี้ กลุ่มตัวอย่างที่ไม่ระบุคิดเป็นร้อยละ ๗.๖๐ เป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๘ จำนวนและร้อยละ จำแนกการให้มีนโยบาย/แนวทาง ที่สอดคล้องมาตรฐาน ISO/IEC ๒๗๐๐๑ ของกลุ่มตัวอย่าง

นโยบาย/แนวทางสอดคล้องมาตรฐาน ISO/IEC ๒๗๐๐๑	จำนวน/คน	ร้อยละ
ไม่ได้ดำเนินการ	๕๕๖	๓๗.๐๗
ได้ดำเนินการ อยู่ในขั้นตอนการวางแผนการดำเนินการ	๕๓๘	๓๕.๘๗
ได้ดำเนินการแล้วบางส่วนขององค์กร	๒๘๔	๑๘.๙๓
ได้ดำเนินการแล้วเต็มรูปแบบ	๘	๐.๕๓
ไม่ระบุ	๑๑๔	๗.๖๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๔.๘ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่ได้มีนโยบาย/แนวทาง ที่สอดคล้องมาตรฐาน ISO/IEC ๒๗๐๐๑ คิดเป็นร้อยละ ๓๗.๐๗ และอยู่ระหว่างการวางแผน คิดเป็นร้อยละ ๓๕.๘๗ โดยมีเพียงร้อยละ ๑๙.๔๖ ที่มีนโยบาย/แนวทางที่สอดคล้องมาตรฐาน ISO/IEC ๒๗๐๐๑ เป็นกลุ่มที่ได้เริ่มดำเนินการไปบางส่วนและเต็มรูปแบบแล้ว ทั้งนี้ กลุ่มตัวอย่างที่ไม่ระบุคิดเป็นร้อยละ ๗.๖๐ เป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๙ จำนวนการจัดกิจกรรมเพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศของกลุ่มตัวอย่าง

กิจกรรมเพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ	จำนวน
- จัดอบรม	๒๑๒
- ทำคู่มือแจกผ่านสิ่งพิมพ์ เว็บไซต์ หรือ intranet	๑๐๗
- รณรงค์ภายในองค์กร	๗๘๒
- อื่นๆ	๘๖
- ไม่มี/ไม่ระบุ	๖๘๙

จากตารางที่ ๔.๙ พบว่า ลำดับมากที่สุดคือ การรณรงค์ภายในองค์กร ลำดับรองลงมาคือไม่มีหรือไม่ระบุการจัดกิจกรรมเพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ กลุ่มตัวอย่างที่ไม่ระบุส่วนนึงเป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๑๐ จำนวนและร้อยละ จำแนกการประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศของกลุ่มตัวอย่าง

การประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศ	จำนวน/คน	ร้อยละ
ไม่ทราบ	๕๘๔	๓๘.๙๓
ไม่เคย	๗๗๘	๕๑.๘๗
เคย	๒๔	๑.๖๐
ไม่ระบุ	๑๑๔	๗.๖๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๔.๑๐ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่เคยประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศ คิดเป็นร้อยละ ๕๑.๘๗ และไม่ทราบว่าเคยประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศ คิดเป็นร้อยละ ๓๘.๙๓ ทั้งนี้ กลุ่มตัวอย่างที่ไม่ระบุคิดเป็นร้อยละ ๗.๖๐ เป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๑๑ จำแนกระดับการประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศของกลุ่มตัวอย่าง

การประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศ	ระดับจำนวน	ระดับความเสียหาย
- เนื้อหาที่เป็นภัยคุกคาม (Abusive Content)	๒.๔๘	๑.๒๖
- การโจมตีเพื่อให้ระบบสูญเสียประสิทธิภาพหรือใช้งานไม่ได้ตามปกติ	๒.๘๙	๑.๐๖
- การฉ้อฉล ฉ้อโกง หรือหลอกลวงเพื่อผลประโยชน์ (Fraud)	๒.๒๐	๒.๘๘
- ความพยายามในการรวบรวมข้อมลูของระบบ (Information Gathering)	๑.๘๙	๑.๙๓
- การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security)	๒.๕๖	๑.๓๔
- ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)	๒.๐๔	๑.๐๐
- การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)	๑.๔๓	๑.๐๐
- โปรแกรมประสงค์ร้าย (Malicious Code)	๑.๓๒	๑.๐๐
- อื่นๆ	๐.๐๐	๐.๐๐
ค่าเฉลี่ย	**๒.๑๐**	**๑.๔๓**

ตารางที่ ๔.๑๒ ระดับคะแนนจำนวน ครั้งที่เกิดเหตุ และระดับคะแนนความเสียหาย

จำนวนครั้งที่เกิดเหตุ	ความเสียหาย	ระดับ
ไม่ทราบหรือไม่เคยเกิดขึ้น	ไม่ทราบหรือน้อยกว่า ๑๐๐,๐๐๐ บาท	๑.๐๑ – ๒.๐๐
เกิดขึ้นน้อยกว่า ๑๐ ครั้งต่อเดือน	๑๐๐,๐๐๐ – ๑,๐๐๐,๐๐๐ บาท	๒.๐๑ – ๓.๐๐
เกิดขึ้น ๑๑ – ๕๐ ครั้งต่อเดือน	มากกว่า ๑,๐๐๐,๐๐๐ บาท	๓.๐๑ – ๔.๐๐
เกิดขึ้นมากกว่า ๕๐ ครั้งต่อเดือน	ประเมินค่าไม่ได้	๔.๐๑ – ๕.๐๐

จากตารางที่ ๔.๑๑ – ๔.๑๒ พบว่า จำนวนครั้งการประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศลำดับมากที่สุดคือ การโจมตีเพื่อให้ระบบสูญเสียประสิทธิภาพหรือใช้งานไม่ได้ตามปกติ และลำดับรองลงมาคือ การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security) โดยคะแนนเฉลี่ยของจำนวนครั้งอยู่ที่ระดับ ๒.๑๐ หมายถึงไม่ทราบว่าเกิดขึ้นมีเพียงส่วนน้อยที่เกิดขึ้นแต่ไม่มากนัก ส่วนความเสียหายจากการประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศ ลำดับมากที่สุดคือการฉ้อฉล ฉ้อโกง หรือหลอกลวงเพื่อผลประโยชน์ (Fraud) และลำดับรองลงมาคือ ความพยายามในการรวบรวมข้อมลูของระบบ (Information Gathering) โดยคะแนนเฉลี่ยระดับความเสียหายอยู่ที่ระดับ ๑.๔๓ หมายถึงไม่ทราบหรือน้อยกว่า ๑๐๐,๐๐๐ บาท ซึ่งส่วนใหญ่ไม่ทราบถึงความเสียหายที่เกิดขึ้น จากข้อมูลอาจสรุปได้ว่า ส่วนใหญ่ไม่ทราบถึงการเกิดขึ้นและการประเมินความเสียหายที่เกิดขึ้นจากการประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศ

ตารางที่ ๔.๑๓ จำนวนและร้อยละ จำแนกการใช้เวลาในการทราบว่าเกิดปัญหาภัยคุกคามของกลุ่มตัวอย่าง

การใช้เวลาในการทราบว่าเกิดปัญหาภัยคุกคาม	จำนวน/คน	ร้อยละ
ภายในระยะเวลาไม่เกิน ๒๔ ชั่วโมง	๒๔	๑.๖๐
ภายในระยะเวลาไม่เกิน ๗ วัน	๐	๐.๐๐
ภายในระยะเวลาไม่เกิน ๑ เดือนหรือ ๔ สัปดาห์	๐	๐.๐๐
อื่นๆ/ไม่เคยเกิดขึ้น/ไม่ทราบ/ไม่ระบุ	๑,๔๗๖	๙๘.๔๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๔.๑๓ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่เคยเกิดขึ้นหรือไม่ทราบหรือไม่ระบุการใช้เวลาในการทราบว่าเกิดปัญหาภัยคุกคามเมื่อประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศ คิดเป็นร้อยละ ๙๘.๔๐ และในส่วนที่เคยประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศทราบว่าเกิดปัญหาภายในระยะเวลา ๒๔ ชั่วโมง คิดเป็นร้อยละ ๑.๖๐ โดยกลุ่มนี้ระบุการทราบถึงปัญหาภัยคุกคามเฉลี่ย ๓๐ นาที ถึง ๒ ชั่วโมง ทั้งนี้ กลุ่มตัวอย่างที่ไม่เคยเกิดขึ้นหรือไม่ทราบหรือไม่ระบุมีบางส่วนเป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๑๔ จำนวนและร้อยละ จำแนกวิธีการทราบถึงปัญหาภัยคุกคามของกลุ่มตัวอย่าง

วิธีการทราบถึงปัญหาภัยคุกคาม	จำนวน/คน	ร้อยละ
ตรวจพบโดยฝ่ายที่ดูแลเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	๒๔	๑.๖๐
ได้รับการแจ้งเหตุจากพนักงานฝ่ายอื่น	๐	๐.๐๐
ได้รับการแจ้งเหตุโดยหน่วยงาน/บุคคลภายนอก	๐	๐.๐๐
อื่นๆ/ไม่เคยเกิดขึ้น/ไม่ทราบ/ไม่ระบุ	๑,๔๗๖	๙๘.๔๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๔.๑๔ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่เคยเกิดขึ้นหรือไม่ทราบหรือไม่ระบุการใช้เวลาในการทราบว่าเกิดปัญหาภัยคุกคามเมื่อประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศ คิดเป็นร้อยละ ๙๘.๔๐ และในส่วนที่เคยประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศทราบว่าเกิดปัญหาโดยการตรวจพบโดยฝ่ายที่ดูแลเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ คิดเป็นร้อยละ ๑.๖๐ ซึ่งเป็นสัดส่วนที่เป็นไปตามการใช้เวลาในการทราบว่าเกิดปัญหาภัยคุกคาม (ตารางที่ ๔.๑๓) ทั้งนี้ กลุ่มตัวอย่างที่ไม่เคยเกิดขึ้นหรือไม่ทราบหรือไม่ระบุมีบางส่วนเป็นกลุ่มตัวอย่างที่เป็นประชาชนทั่วไปในชุมชนซึ่งไม่ได้เป็นบุคลากรในองค์กร

ตารางที่ ๔.๑๕ จำแนกระดับคะแนนปัจจัยสำคัญที่ทำให้เกิดเหตุภัยคุกคามของกลุ่มตัวอย่าง

การประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศ	ระดับคะแนน
- ผู้ใช้เทคโนโลยีในองค์กรขาดความตระหนักถึงความสำคัญของการใช้เทคโนโลยีอย่างมั่นคงปลอดภัย	๓.๗๖
- ผู้ใช้เทคโนโลยีในองค์กรขาดความรู้ความเข้าใจในการใช้เทคโนโลยีอย่างมั่นคงปลอดภัย	๑.๕๔
- งบประมาณสำหรับการดูแลรักษาความมั่นคงปลอดภัยระบบสารสนเทศไม่เพียงพอ	๒.๘๘
- อุปกรณ์/ระบบ ที่ใช้งานมีช่องโหว่ให้สามารถโจมตีได้	๓.๙๒
- บุคลากรที่มีความเชี่ยวชาญในการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ไม่เพียงพอ	๓.๔๒
- อื่นๆ	๖.๐๐

ตารางที่ ๔.๑๖ ระดับคะแนนความสำคัญของปัจจัยที่ทำให้เกิดเหตุภัยคุกคาม

ลำดับความสำคัญ	ระดับ
มากที่สุด	๑.๐๑ – ๒.๐๐
มาก	๒.๐๑ – ๓.๐๐
ปานกลาง	๓.๐๑ – ๔.๐๐
น้อย	๔.๐๑ – ๕.๐๐
ไม่สำคัญ	๕.๐๑ – ๖.๐๐

จากตารางที่ ๔.๑๕ – ๔.๑๖ พบว่า ๓ ลำดับแรกสำหรับปัจจัยที่ทำให้เกิดภัยคุกคาม ได้แก่ปัจจัยสำคัญมากที่สุดที่ทำให้เกิดเหตุภัยคุกคามคือ ผู้ใช้เทคโนโลยีในองค์กรขาดความรู้ความเข้าใจในการใช้เทคโนโลยีอย่างมั่นคงปลอดภัย ลำดับรองลงมาอยู่ในเกณฑ์สำคัญมากคือ งบประมาณสำหรับการดูแลรักษาความมั่นคงปลอดภัยระบบสารสนเทศไม่เพียงพอ จำนวนครั้งการประสบปัญหาด้านการรักษาความปลอดภัยสารสนเทศ และลำดับที่ ๓ – ๕ อยู่ในเกณฑ์ระดับปานกลาง คือ บุคลากรที่มีความเชี่ยวชาญในการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ไม่เพียงพอ ผู้ใช้เทคโนโลยีในองค์กรขาดความตระหนักถึงความสำคัญของการใช้เทคโนโลยีอย่างมั่นคงปลอดภัย และอุปกรณ์/ระบบ ที่ใช้งานมีช่องโหว่ให้สามารถโจมตีได้ ตามลำดับ จากข้อมูลสะท้อนให้เห็นว่า องค์ความรู้และศักยภาพของบุคลากรเป็นปัจจัยที่สำคัญที่สุดถือเป็นความต้องการหลักของบุคลากรในองค์กรระดับท้องถิ่น เพราะฉะนั้นควรเร่งดำเนินการเสริมสร้างองค์ความรู้และบุคลากรให้เป็นผู้เชี่ยวชาญในด้านความมั่นคงปลอดภัยสารสนเทศ ประกอบกับการจัดหาอุปกรณ์และระบบมารองรับซึ่งถือว่ามีความจำเป็นสำหรับองค์กร

ส่วนที่ ๕ ความรู้ด้านกฎหมายเกี่ยวกับการรักษาความปลอดภัยสารสนเทศตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ตารางที่ ๕.๑ จำนวนและร้อยละ จำแนกการทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ของกลุ่มตัวอย่าง

การทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์	จำนวน/คน	ร้อยละ
ไม่ทราบ	๙๔๖	๖๓.๐๗
อย่างน้อย ๙๐ วัน	๓๔๘	๒๓.๒๐
อย่างน้อย ๙๐ วัน แต่กรณีจำเป็นที่พนักงานเจ้าหน้าที่สั่งให้เก็บไว้เกิน ๙๐ วัน แต่ไม่เกิน ๑ ปี เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้	๒๐๖	๑๓.๗๓
อื่นๆ/ไม่ระบุ	๐	๐.๐๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๕.๑ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่ทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ คิดเป็นร้อยละ ๖๓.๐๗ โดยส่วนที่ทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์นั้น คิดเป็นร้อยละ ๓๖.๙๓ ส่วนใหญ่เป็นผู้ปฏิบัติงานในฝ่าย IT และเป็นผู้ที่เคยผ่านการอบรมด้าน Cyber security หรือเป็นเจ้าหน้าที่ผู้ปฏิบัติงานฝ่ายบริหาร

ตารางที่ ๕.๒ จำนวนและร้อยละ จำแนกความสำคัญในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของกลุ่มตัวอย่าง

ความสำคัญ**ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์**	**จำนวน/คน**	**ร้อยละ**
ไม่สำคัญ เพราะยังไม่เกิดเหตุการณ์ดังกล่าว	๐	๐.๐๐
ไม่สำคัญ เพราะคิดว่าไม่น่าจะเหตุการ์ใดๆ ขึ้น	๐	๐.๐๐
สำคัญ เพราะเป็นพยานหลักฐานสำคัญในการดำเนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ	๗๘๔	๕๒.๒๗
สำคัญ เพราะได้เก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ แล้ว	๗๑๖	๔๗.๗๓
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๕.๒ พบว่า กลุ่มตัวอย่างทั้งหมดเห็นว่าสำคัญในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ถึงแม้ว่าสัดส่วนไม่สอดคล้องกับการทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (ตารางที่ ๕.๑) ก็ตาม ซึ่งสะท้อนให้เห็นว่าการไม่ทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แต่ก็ยังคงมีความสำคัญในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์สำหรับองค์กรระดับท้องถิ่น

ตารางที่ ๕.๓ จำนวนและร้อยละ จำแนกการทราบถึงบทลงโทษฐานความผิดเกี่ยวกับคอมพิวเตอร์ของกลุ่มตัวอย่าง

การทราบถึงบทลงโทษฐานความผิดเกี่ยวกับคอมพิวเตอร์	**จำนวน/คน**	**ร้อยละ**
ทราบ	๒๒๘	๑๕.๒๐
ไม่ทราบ/ไม่ระบุ	๑,๒๗๒	๘๔.๘๐
รวม	**๑,๕๐๐**	**๑๐๐**

จากตารางที่ ๕.๓ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่ทราบถึงบทลงโทษฐานความผิดเกี่ยวกับคอมพิวเตอร์ คิดเป็นร้อยละ ๘๔.๘๐ ซึ่งมีสัดส่วนที่สูงกว่าการไม่ทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ถึงร้อยละ ๒๑.๗๓ สะท้อนให้เห็นว่าถึงแม้ว่าจะทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ยังมีบางส่วนที่ไม่ทราบถึงบทบทลงโทษฐานความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งมีโทษจำคุก โทษปรับ และโทษทั้งจำคุกและปรับ

บทสรุปรวบรวมปัญหา วิเคราะห์ความเสี่ยงและผลกระทบจากแบบสอบถามของกลุ่มตัวอย่าง ๑,๕๐๐ คน สะท้อนถึงปัญหาจำนวน ๔ ประเด็นได้ดังนี้

<u>ประเด็นที่ ๑ การให้องค์ความรู้เกี่ยวกับ Cyber Security</u>

การให้องค์ความรู้เกี่ยวกับ Cyber Security ถือเป็นปัจจัยสำคัญลำดับต้นๆ ในการพัฒนาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยถือว่าจากผลการสำรวจพบว่าบุคลากรขาดองค์ความรู้ ขาดความเข้าใจเป็นสำคัญ ส่งผลกระทบให้ไม่ทราบถึงภัยคุกคามที่มีอยู่ภายในองค์กร อาจส่งผลกระทบถึงระดับประเทศได้ เนื่องจากองค์กรระดับท้องถิ่นมีช่องโหว่ในการถูกโจมตีได้ง่าย และมีเป็นจำนวนมากยากต่อการป้องกันทั้งหมด

<u>ประเด็นที่ ๒ การขาดแคลนทรัพยากรและงบประมาณ</u>

การขาดแคลนทรัพยากรได้แก่ ระบบการบริหารจัดการเฉพาะด้าน อาทิ เช่น ระบบ antivirus รวมไปถึงการอัพเดทโปรแกรม antivirus อย่างสม่ำเสมอ ระบบบริหารจัดการการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ระบบ Firewall เป็นต้น โดยระบบต่างๆ ถือมีความจำเป็นต้องกระทำควบคู่ไปกับการเสริมสร้างองค์ความรู้ เพื่อเป็นการป้องกันอย่างรวดเร็ว เพื่อไม่ให้ส่งผลกระทบในวงกว้าง

<u>ประเด็นที่ ๓ พฤติกรรมการใช้งานคอมพิวเตอร์</u>

การใช้งานคอมพิวเตอร์ของบุคลากรค่อนข้างมีความเสี่ยงพอสมควร เนื่องจากยังขาดความเข้าใจในการเข้ารหัสข้อมูลองค์กร การบริหารจัดการข้อมูลองค์กรอย่างมีประสิทธิภาพ การป้องกันข้อมูลรั่วไหลสู่มิจชีพหรือผู้ไม่ประสงค์ดีก็ตาม โดยในส่วนนี้ ควรกระทำควบคู่ไปกับการเสริมสร้างองค์ความรู้

<u>ประเด็นที่ ๔ พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐</u>

พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีบทลงโทษทั้งจำคุกและปรับ ซึ่งบุคลากรยังขาดความรู้ความเข้าใจใน พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อยู่เป็นจำนวนมาก ทั้งนี้ รวมไปถึงประชาชนในท้องถิ่น ซึ่งถือว่ามีความเสี่ยงในกระทำความผิดต่อ พ.ร.บ. ดังกล่าวเนื่องจากขาดความรู้ความเข้าใจในการเฝ้าระวังเรื่องดังกล่าว รวมไปถึงการหาวิธีป้องกัน/เครื่องมือและบริหารจัดการการใช้งานคอมพิวเตอร์ผ่านอินเทอร์เน็ต

สรุปผลการสัมภาษณ์โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ สำหรับองค์กรขนาดเล็กในระดับชุมชน

สรุปผลการสัมภาษณ์โครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ สำหรับองค์กรขนาดเล็กในระดับชุมชน

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลเพื่อทำสรุปประเด็นสำคัญในครั้งนี้ คือ แบบสัมภาษณ์แบบที่กลุ่มตัวอย่าง (บุคลากรในองค์กรหรือประชาชนในชุมชน) เป็นผู้กรอกข้อมูลเอง (self-administrative questionnaire) ประกอบกับการสัมภาษณ์เชิงลึก ซึ่งได้จัดทำกับกลุ่มตัวอย่างทั้งสิ้น ๕๐ คน โดยแบ่งแบบสัมภาษณ์ออกเป็น ๓ ส่วน คือ

ส่วนที่ ๑ ข้อมูลทั่วไป แบ่งเป็น ๒ หัวข้อ ได้แก่ ข้อมูลส่วนตัว และแนวคิด

ส่วนที่ ๒ โครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศในองค์กร

ส่วนที่ ๓ ระบบสารสนเทศขององค์กรปกครองส่วนท้องถิ่น

เมื่อเก็บรวบรวมข้อมูลเรียบร้อยแล้ว ผู้สรุปประเด็นสำคัญได้นำแบบสัมภาษณ์ตรวจสอบความเรียบร้อยของการตอบรายข้อคำถาม จากนั้นจึงนำมาสรุปเป็นข้อๆ

ส่วนที่ ๑ ข้อมูลทั่วไป

๑.๑ ข้อมูลส่วนตัว

ตารางที่ ๑.๑ จำนวนและร้อยละ จำแนกตามเพศของกลุ่มตัวอย่าง

เพศ	จำนวน/คน	ร้อยละ
ชาย	๑๑	๒๒.๐๐
หญิง	๓๙	๗๘.๐๐
รวม	**๕๐**	**๑๐๐**

จากกลุ่มตัวอย่างทั้งหมด ๕๐ คน อายุงานโดยเฉลี่ย ๑๒.๕๖ ปี อายุงานน้อยที่สุดคือ ๕ ปี อายุงานมากที่สุดคือ ๒๕ ปี สังกัดอบต./เทศบาลขนาดเล็ก

ตารางที่ ๑.๒ จำนวนและร้อยละ จำแนกตามตำแหน่งที่ปฏิบัติงานของกลุ่มตัวอย่าง

หน่วยงาน	จำนวน/คน	ร้อยละ
นายกอบต./รองนายกอบต./ปลัดเทศบาล	๑๓	๒๖.๐๐
ครูสังกัดกองงานการศึกษา	๓๗	๗๔.๐๐
รวม	**๕๐**	**๑๐๐**

จากตารางที่ ๑.๒ พบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นครูสังกัดกองงานการศึกษา คิดเป็นร้อยละ ๗๔ โดยครูเป็นผู้ดูแลระบบสารสนเทศภายในองค์กรเนื่องจากไม่มีตำแหน่งเฉพาะทาง และกลุ่มนายกอบต./รองนายกอบต./ปลัดเทศบาล คิดเป็นร้อยละ ๒๖

ตารางที่ ๑.๓ จำนวนและร้อยละ จำแนกตามระดับการศึกษาของกลุ่มตัวอย่าง

ระดับการศึกษา	จำนวน/คน	ร้อยละ
ปริญญาตรี	๑๘	๓๖.๐๐
ปริญญาโท	๒๔	๔๘.๐๐
ปริญญาเอก	๘	๑๖.๐๐
รวม	**๕๐**	**๑๐๐**

แนวคิดเรื่องการบริหารจัดการองค์กรบนพื้นฐานของการใช้ข้อมูลสารสนเทศ

ข้อคิดเห็นเกี่ยวกับการใช้ข้อมูลสารสนเทศ วิเคราะห์ตามบทบาทความสำคัญ การใช้ประโยชน์ และข้อเสนอแนะเพิ่มเติม โดยสรุปประเด็นได้ดังต่อไปนี้

- อยากให้พนักงานมีความรู้ด้านสารสนเทศเพิ่มมากขึ้น เนื่องจากพนักงานยังขาดความชำนาญความรู้ การใช้เครื่องมือสารสนเทศ การใช้สารสนเทศเพื่อการสืบค้นข้อมูล การใช้สารสนเทศเพื่อการประชาสัมพันธ์หน่วยงาน ขาดแคลนเครื่องมือสารสนเทศ (ระบบหรือโปรแกรมสำเร็จรูป)
- พนักงานยังขาดความรู้ด้านการป้องกันข้อมูลสารสนเทศต่างๆ จากไวรัส สแปมแวร์ รวมไปถึงการรับรู้ถึงอันตรายหรือความเสียหายจากไวรัส สแปมแวร์ต่างๆ
- การใช้งานระบบสารสนเทศภายในองค์กรไม่มีเครื่องมือสำหรับการป้องกันข้อมูลสารสนเทศต่างๆ จากไวรัส สแปมแวร์
- การติดตั้งระบบเครือข่ายอินเทอร์เน็ตไม่มีเครื่องแม่ข่ายและไม่มีระบบในการบริหารจัดการเครือข่ายภายในองค์กร
- มีการใช้ข้อมูลสารสนเทศเพื่อการสืบค้นและการสื่อสารที่สะดวกและรวดเร็วยิ่งขึ้น
- มีการใช้ข้อมูลสารสนเทศเพื่อเป็นช่องทางในการติดต่อสื่อสารทั้งภายในหน่วยงาน และระหว่างหน่วยงานรวมไปถึงระดับส่วนกลาง
- ข้อมูลสารสนเทศมีบทบาทสำคัญยิ่งในการบริหารจัดการท้องถิ่น อาทิเช่น ระเบียบ กฎหมายที่เกี่ยวข้อง ข้อมูลจากส่วนกลาง/สำนักงานใหญ่ เพื่อความทันสมัย สะดวกและรวดเร็ว และการประชาสัมพันธ์องค์กร
- เพื่อการดำเนินการสอดคล้องกับนโยบายภาครัฐ Thailand ๔.๐ ที่ข้อมูลต่างๆ ต้องถูกจัดเก็บไว้อย่างเป็นระบบ เพื่อการเผยแพร่ให้สาธารณชนทราบได้อย่างทั่วถึงและรวดเร็ว

ส่วนที่ ๒ โครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศในองค์กรฯ

ตารางที่ ๒.๑ จำนวนและร้อยละ จำแนกตามจำนวนของเจ้าหน้าที่บันทึกข้อมูลภายในหน่วยงานของกลุ่มตัวอย่าง

จำนวนเจ้าหน้าที่บันทึกข้อมูล/คน	จำนวน/คน	ร้อยละ
๑	๑๔	๒๘.๐๐
๒	๒๕	๕๐.๐๐
๓	๑๑	๒๒.๐๐
๔	-	
๕	-	
มากกว่า ๕	-	
ไม่มี	-	
รวม	**๕๐**	**๑๐๐**

จากตารางที่ ๒.๑ พบว่าหน่วยงานมีเจ้าหน้าที่บันทึกข้อมูลส่วนใหญ่จำนวน ๒ คน คิดเป็นร้อยละ ๕๐ โดยเฉลี่ยมีเจ้าหน้าที่บันทึกข้อมูลจำนวน ๑.๙๔ โดยเจ้าหน้าที่บันทึกข้อมูลส่วนใหญ่ปฏิบัติหน้าที่ในการส่งข้อมูลให้แก่สำนักงานใหญ่/ส่วนกลางเป็นประจำทุกวันและประจำทุกเดือน อาทิเช่น ข้อมูลภาษี ข้อมูลรายรับรายจ่าย ข้อมูลการศึกษา ข้อมูลเด็กเล็ก เป็นต้น

ตารางที่ ๒.๒ จำนวนและร้อยละ จำแนกตามจำนวนของเจ้าหน้าที่ระบบงานคอมพิวเตอร์ภายในหน่วยงานของกลุ่มตัวอย่าง

จำนวนเจ้าหน้าที่ระบบงานคอมพิวเตอร์/คน	จำนวน/คน	ร้อยละ
๑	๑๑	๒๒.๐๐
๒	๑๒	๒๔.๐๐
๓	๘	๑๖.๐๐
๔	-	-
๕	-	-
มากกว่า ๕	๑๐	๒๐.๐๐
ไม่มี	๙	๑๘.๐๐
รวม	**๕๐**	**๑๐๐**

จากตารางที่ ๒.๒ พบว่าหน่วยงานมีเจ้าหน้าที่ระบบงานคอมพิวเตอร์ส่วนใหญ่จำนวน ๒ คน คิดเป็นร้อยละ ๒๔ โดยเฉลี่ยมีเจ้าหน้าที่ระบบงานคอมพิวเตอร์จำนวน ๒.๑๘ หากเปรียบเทียบจากสัดส่วนเฉลี่ยระหว่างเจ้าหน้าที่บันทึกข้อมูลและเจ้าหน้าที่ระบบงานคอมพิวเตอร์ พบว่ามีความใกล้เคียงกัน แต่มีบางหน่วยงานไม่มีเจ้าหน้าที่งานระบบคอมพิวเตอร์เลย คิดเป็นร้อยละ ๑๘ ซึ่งเจ้าหน้าที่ระบบงานคอมพิวเตอร์ทำหน้าที่ดูแลด้านเทคนิคข้อมูลสารสนเทศแต่ยังไม่มีความชำนาญเฉพาะด้าน เนื่องจากเป็นหน่วยงานขนาดเล็ก เป็นเพียงการปฏิบัติหน้าที่ไปพลาง

หรือปฏิบัติหน้าที่ตามความจำเป็นเท่านั้นมิได้ปฏิบัติหน้าที่เป็นประจำ โดยบางหน่วยงานยังพบว่าเจ้าหน้าที่บันทึกข้อมูลเป็นเจ้าหน้าที่ระบบงานคอมพิวเตอร์ด้วยเช่นกัน

ตารางที่ ๒.๓ จำนวนและร้อยละ จำแนกตามจำนวนของเครื่องคอมพิวเตอร์แม่ข่ายภายในหน่วยงานของกลุ่มตัวอย่าง

จำนวนเครื่องคอมพิวเตอร์แม่ข่าย/เครื่อง	จำนวน/คน	ร้อยละ
๑	๓๒	๖๔.๐๐
๒	-	-
๓	-	-
๔	-	-
๕	-	-
มากกว่า ๕	-	-
ไม่มี	๑๘	๓๖.๐๐
รวม	**๕๐**	**๑๐๐**

จากตารางที่ ๒.๓ พบว่าหน่วยงานมีเครื่องคอมพิวแตอร์แม่ข่ายส่วนใหญ่จำนวน ๑ เครื่อง คิดเป็นร้อยละ ๖๔ โดยส่วนที่เหลือไม่มีเครื่องคอมพิวเตอร์แม่ข่าย แต่จากการสอบถามเพิ่มเติมส่วนใหญ่มีเครื่องคอมพิวเตอร์ลูกข่ายจำนวนโดยประมาณ ๑๐ – ๒๐ เครื่องสำหรับใช้ในการปฏิบัติหน้าที่ภายในหน่วยงาน

โปรแกรมสำเร็จรูปที่หน่วยงานใช้จัดทำเพื่อเป็นการบริหารจัดการเฉพาะด้าน ได้แก่

- ระบบจัดเก็บภาษี
- ระบบจัดเก็บพื้นที่
- ระบบจัดเก็บข้อมูลศูนย์เด็กเล็ก
- ระบบจัดเก็บข้อมูลบุคลากร
- ระบบสารบรรณอิเล็กทรอนิกส์
- ระบบการประเมินภาวะโภชนาการเด็ก
- ระบบ CCTV
- แอพพลิเคชั่นเฟสบุค
- แอพพลิเคชั่นไลน์
- แอพพลิเคชั่น Chorme
- แอพพลิเคชั่น e-mail ต่างๆ
- โปรแกรม Microsoft office
- เว็บไซด์ Google

โดยสรุปจะพบว่า เป็นการใช้ระบบเพื่อการปฏิบัติงานเฉพาะด้านในการรับ-ส่งข้อมูลไปยังหน่วยงานส่วนกลาง/สำนักงานใหญ่ โดยมีการใช้แอพพลิเคชั่นเพื่อการสื่อสารประชาสัมพันธ์การใช้โปรแกรม Microsoft office เพื่อการปฏิบัติงานทั่วไป และมีการใช้เว็บไซด์เพื่อการสืบค้นข้อมูลประกอบการทำงาน

ตารางที่ ๒.๔ จำนวนและร้อยละ จำแนกตามการปรับปรุง/อัพเดทเว็บไซต์ให้เป็นปัจจุบันอย่างต่อเนื่องของกลุ่มตัวอย่าง

การอัพเดทเว็บไซต์	จำนวน/คน	ร้อยละ
ทุกวัน	๒๔	๔๘.๐๐
ทุกสัปดาห์	๑๔	๒๘.๐๐
มากกว่า ๑ สัปดาห์	๑๒	๒๔.๐๐
รวม	**๕๐**	**๑๐๐**

จากตารางที่ ๒.๔ พบว่าหน่วยงานมีการปรับปรุง/อัพเดทเว็บไซต์ส่วนใหญ่ทุกวัน คิดเป็นร้อยละ ๔๘ โดยลำดับต่อมาคือทุกสัปดาห์ คิดเป็นรอยละ ๒๘ และมากกว่า ๑ สัปดาห์ คิดเป็นร้อยละ ๒๔ ตามลำดับ จากข้อมูลมีการอัพเดทข้อมูลเป็นประจำสำหรับหน่วยงานขนาดเล็กแต่การป้องกันและรักษาความปลอดภัยทางข้อมูลสารสนเทศยังถือว่ามีน้อยมาก หรือแทบไม่มีการป้องกันใดๆ เลย ซึ่งค่อนข้างมีความเสี่ยงสุงต่อข้อมุลสารสนเทศขององค์กร

ตารางที่ ๒.๕ จำนวนและร้อยละ จำแนกการทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ของกลุ่มตัวอย่าง

การทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์	จำนวน/คน	ร้อยละ
ไม่ทราบ	๒๖	๕๒.๐๐
อย่างน้อย ๙๐ วัน	-	-
อย่างน้อย ๙๐ วัน แต่กรณีจำเป็นที่พนักงานเจ้าหน้าที่สั่งให้เก็บไว้เกิน ๙๐ วัน แต่ไม่เกิน ๑ ปี เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้	๑๘	๓๖.๐๐
อื่นๆ	๖	๑๒.๐๐
รวม	**๕๐**	**๑๐๐**

จากตารางที่ ๒.๕ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่ทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ คิดเป็นร้อยละ ๕๒.๐๐ โดยส่วนที่ทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์นั้น คิดเป็นร้อยละ ๔๘.๐๐ ในส่วนที่เลือกอื่นๆ ระบุการเก็บรักษาข้อมูลบางประเภทต้องเก็บรักษา ๓ – ๑๐ ปี

ตารางที่ ๒.๖ จำนวนและร้อยละ จำแนกความสำคัญในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของกลุ่มตัวอย่าง

ความสำคัญ**ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์**	**จำนวน/คน**	**ร้อยละ**
ไม่สำคัญ เพราะยังไม่เกิดเหตุการณ์ดังกล่าว	-	-
ไม่สำคัญ เพราะคิดว่าไม่น่าจะเหตุการ์ใดๆ ขึ้น	-	-
สำคัญ เพราะเป็นพยานหลักฐานสำคัญในการดำเนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ	-	-
สำคัญ เพราะได้เก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ แล้ว	๕๐	๑๐๐.๐๐
รวม	**๕๐**	**๑๐๐**

จากตารางที่ ๒.๖ พบว่า กลุ่มตัวอย่างทั้งหมดเห็นว่าสำคัญในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ถึงแม้ว่าสัดส่วนไม่สอดคล้องกับการทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (ตารางที่ ๕.๑) ก็ตาม ซึ่งสะท้อนให้เห็นว่าการไม่ทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แต่ก็ยังคงมีความสำคัญในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์สำหรับองค์กรระดับท้องถิ่น

ตารางที่ ๒.๗ จำนวนและร้อยละ จำแนกการทราบถึงบทลงโทษฐานความผิดเกี่ยวกับคอมพิวเตอร์ของกลุ่มตัวอย่าง

การทราบถึงบทลงโทษฐานความผิดเกี่ยวกับคอมพิวเตอร์	**จำนวน/คน**	**ร้อยละ**
ทราบ	๑๖	๓๒.๐๐
ไม่ทราบ/ไม่ระบุ	๓๔	๖๘.๐๐
รวม	**๕๐**	**๑๐๐**

จากตารางที่ ๒.๗ พบว่า กลุ่มตัวอย่างส่วนใหญ่ไม่ทราบถึงบทลงโทษฐานความผิดเกี่ยวกับคอมพิวเตอร์ คิดเป็นร้อยละ ๖๘.๐๐ ซึ่งมีสัดส่วนที่สูงกว่าการไม่ทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ถึงร้อยละ ๑๖.๐๐ สะท้อนให้เห็นว่าถึงแม้ว่าจะทราบถึงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ยังมีบางส่วนที่ไม่ทราบถึงบทลงโทษฐานความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งมีโทษจำคุก โทษปรับ และโทษทั้งจำคุกและปรับ

ส่วนที่ ๓ ระบบสารสนเทศขององค์กรปกครองส่วนท้องถิ่นในปัจจุบัน

๓.๑ ระบบสารสนเทศที่มีอยู่ในปัจจุบันเกี่ยวกับสามารถสนับสนุนการบริหารจัดการท้องถิ่น จากข้อมูลพบว่าระบบสารสนเทศที่มีอยู่ในปัจจุบัน อาทิเช่น โปรแกรมและระบบต่างที่ได้กล่าวมาข้างต้นนั้น สามารถรองรับและสนับสนุนการปฏิบัติงานเกี่ยวกับการจัดเก็บข้อมูลของหน่วยงาน การรายงานข้อมูลของหน่วยงาน การประชาสัมพันธ์ขององค์กรได้บางส่วน เนื่องจากหน่วยงานมีอุปกรณ์หรือเครื่องมือสนับสนุนการปฏิบัติงาน แต่บุคลากรยังขาดองค์ความรู้ ขาดความเชี่ยวชาญเฉพาะด้าน ส่งผลให้การใช้ระบบสารสนเทศต่างๆ อาจใช้ได้ไม่เต็ม

ประสิทธิภาพ ประกอบกับระบบสารสนเทศที่มีอยู่ยังขาดระบบสารสนเทศหรือเครื่องมือต่างๆ ในการป้องกันภัยคุกคามทางไซเบอร์ มีเพียงระบบสารสนเทศเพื่อการปฏิบัติงานเท่านั้น

๓.๒ ปัญหา อุปสรรคและความต้องการพื้นฐานในการบริหารจัดการระบบสารสนเทศ จากข้อมูลพบว่าปัญหาและอุปสรรคส่วนใหญ่สืบเนื่องมาจากบุคลากรขาดความชำนาญในการใช้งาน เครื่องมือการใช้งานของระบบสารสนเทศต่างๆ มีความยุ่งยากซับซ้อนจนเกินไป เครือข่ายอินเทอร์เน็ตไม่เสถียรหรือไม่เพียงพอต่อการใช้งาน จากปัจจัยสะท้อนให้เห็นถึงปัญหาอุปสรรคหลักๆ ๓ ปัจจัย ได้แก่ บุคลากร (Human) องค์ความรู้ (Knowledge) โครงข่าย (Infra Structure) และยังพบความต้องการของผู้ใช้งาน (User) ในระดับองค์กรท้องถิ่นขนาดเล็ก มีความต้องการใช้งานเครื่องมือหรือระบบสารสนเทศที่ไม่มียุ่งยากซับซ้อนจนเกินไปเน้นการใช้งานที่ง่ายและรวดเร็ว ทั้งนี้ต้องมีความปลอดภัยสำหรับผู้ใช้งานและข้อมูลที่ใช้รับ-ส่งในการใช้งาน รวมไปถึงความต้องการด้านบุคลากรผู้เชี่ยวชาญในแต่ละด้าน ได้แก่ ด้านสารสนเทศ ด้านความปลอดภัยข้อมูลสารสนเทศ

สรุปผลการออกแบบและพัฒนาระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น

ปัจจุบันบทบาทหน้าในการพัฒนาท้องถิ่น ผ่านหน่วยงานองค์กรปกครองส่วนท้องถิ่น เป็นหัวใจสำคัญในการพัฒนา สภาพเศรษฐกิจ สังคม การรักษาวิถีชีวิตของชุมชน รวมถึงการผลักดันนโยบายการกระจายอำนาจปกครอง เพื่อให้สอดคล้องกับหลักการประชาธิปไตย ที่ประชาชนมีส่วนร่วมการบริหารจัดการท้องถิ่นของตนเอง โดยมีเป้าหมายในการส่งเสริมความมั่นคงและความผาสุกของประชาชน อย่างเท่าเทียมทั่วถึง การบริการประชาชนที่มีความละเอียดและสลับซับซ้อนด้วยปัญหาที่แตกต่างหลากหลาย องค์กรปกครองส่วนท้องถิ่นจึง เกี่ยวพันกับการใช้ประโยชน์จาก ๑. ระบบการสื่อสารผ่านอินเทอร์เน็ตความเร็วสูง ๒. ระบบฐานข้อมูลเพื่ออำนวยความสะดวกแก่ประชาชน ซึ่งหลีกเลี่ยงไม่พ้นที่จะต้องอาศัยความพร้อมด้านทักษะ ความรู้ และงบประมาณเพื่อใช้ในการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์

จากการสำรวจ องค์กรปกครองส่วนท้องถิ่น พบว่า ปัจจุบันมีการใช้งาน ระบบเครือข่ายคอมพิวเตอร์หลักๆ ๔ รูปแบบด้วยกันคือ

๑. ใช้ในการพิมพ์เอกสารและจัดเก็บข้อมูล เช่น เอกสารการเบิกจ่ายและฎีกาต่างๆ ซึ่ง จัดเก็บทั้งในรูปแบบ กระดาษ และ สแกนเป็นไฟล์ภาพ ไว้ในคอมพิวเตอร์สำนักงาน ประจำตัวเจ้าหน้าที่ การคลัง พัสดุ นอกจากนี้ ในส่วนของแบบ แปลน ขออนุญาต ก่อสร้างต่างๆของ ฝ่ายช่าง ปัจจุบัน ส่วนใหญ่ยังคงเก็บในรูปของกระดาษ เป็นหลัก

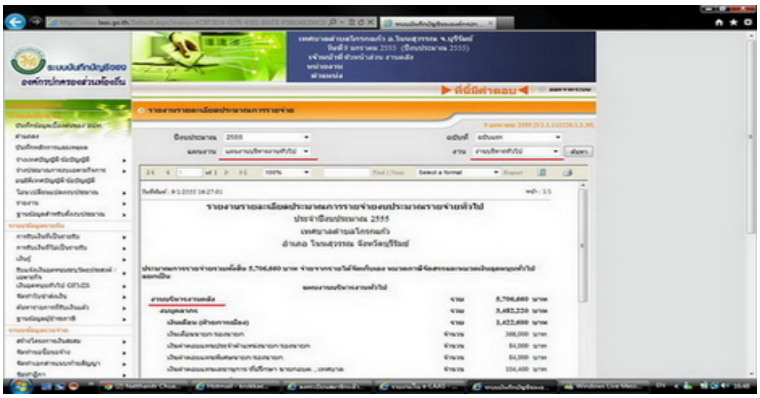
๒. ใช้ในการสื่อสารข้อมูลกับส่วนงานที่เกี่ยวข้อง เช่น การรับส่ง อีเมล์ หรือสอบถาม ปัญหาการทำงาน ในกรณีที่ ท้องถิ่น ไม่สามารถคลี่คลายปัญหาต่างๆได้ด้วยตนเอง เช่น ปัญหาการลงบันทึก ภาษีในระบบแผนที่ภาษี ฝ่ายการคลังของหน่วยงาน จำเป็นต้องสอบถามข้อมูล เชิงลึกกับเจ้าหน้าที่ที่เกี่ยวข้อของกรมส่งเสริมการปกครองส่วนท้องถิ่นโดยตรง

๓. การส่งรายงานกับหน่วยงานต้นสังกัดผ่านโปรแกรมสำเร็จรูป เนื่องจากองค์กรปกครองส่วนท้องถิ่น เป็นองค์กรที่บริหารมีโครงสร้างตำแหน่งงาน แบบ ฝ่ายนิติบัญญัติ และ ฝ่ายบริหาร อันประกอบไปด้วยส่วนงาน ๖ ฝ่ายด้วยกัน คือ ๑. สำนักงานปลัด ๒. ส่วนการคลัง ๓. ส่วนโยธา ๔. ส่วนการศึกษาและวัฒนธรรม ๕. ส่วนสวัสดิการสังคม ๖. ส่วนสาธารณสุขและสิ่งแวดล้อม โดยภายในองค์กรปกครองส่วนท้องถิ่นแต่ละแห่งมีการจัดองค์กรตามแบบ การจัดแผนกงานตามหน้าที่ (Departmentation by Function) ซึ่งได้แบ่งหน้าที่หลักๆ ออกจากกันชัดเจน แต่รับผิดชอบต่อเป้าหมายที่ควบคุมโดยผู้นำสูงสุดอันได้แก่นายกฯ แต่ละพื้นที่

ขณะเดียวกัน ส่วนงานทั้ง ๖ ด้าน ในฐานะเป็นข้าราชการประจำถูกกำหนดหน้าที่ในการรายงานความคืบหน้าของการปฏิบัติงานในตำแหน่งของตนเอง ไปยังส่วนงานต่างๆ ของกรมส่งเสริมการปกครองส่วนท้องถิ่น ส่วนกลาง ซึ่งเป็นรูปแบบ **การจัดองค์กรแบบแมทริกซ์ (Matrix organization)** โดยข้าราชการท้องถิ่น ขึ้นตรงและรายงานสายการบังคับบัญชา ๒ สาย

การรายงานความคืบหน้าและผลปฏิบัติงานในท้องถิ่นสู่ส่วนกลางปัจจุบัน ทำผ่านโปรแกรมสำเร็จรูป ได้แก่

๓.๑ โปรแกรม ระบบบัญชีคอมพิวเตอร์ของกรมส่งเสริมการปกครองท้องถิ่น (Electronic Administration Accounting System : e-LAAS) ซึ่งเจ้าหน้าที่คลัง มีหน้าที่ต้องส่งรายงาน ผ่านอินเทอร์เน็ตเพื่อสรุปรายงานงบประมาณทั้ง รายวัน รายเดือน และ รอบปีงบประมาณ โดยปัจจุบัน ระบบเสร็จสมบูรณ์องค์กรปกครองส่วนท้องถิ่นทุกแห่ง ใช้ระบบนี้เสร็จสมบูรณ์แล้ว



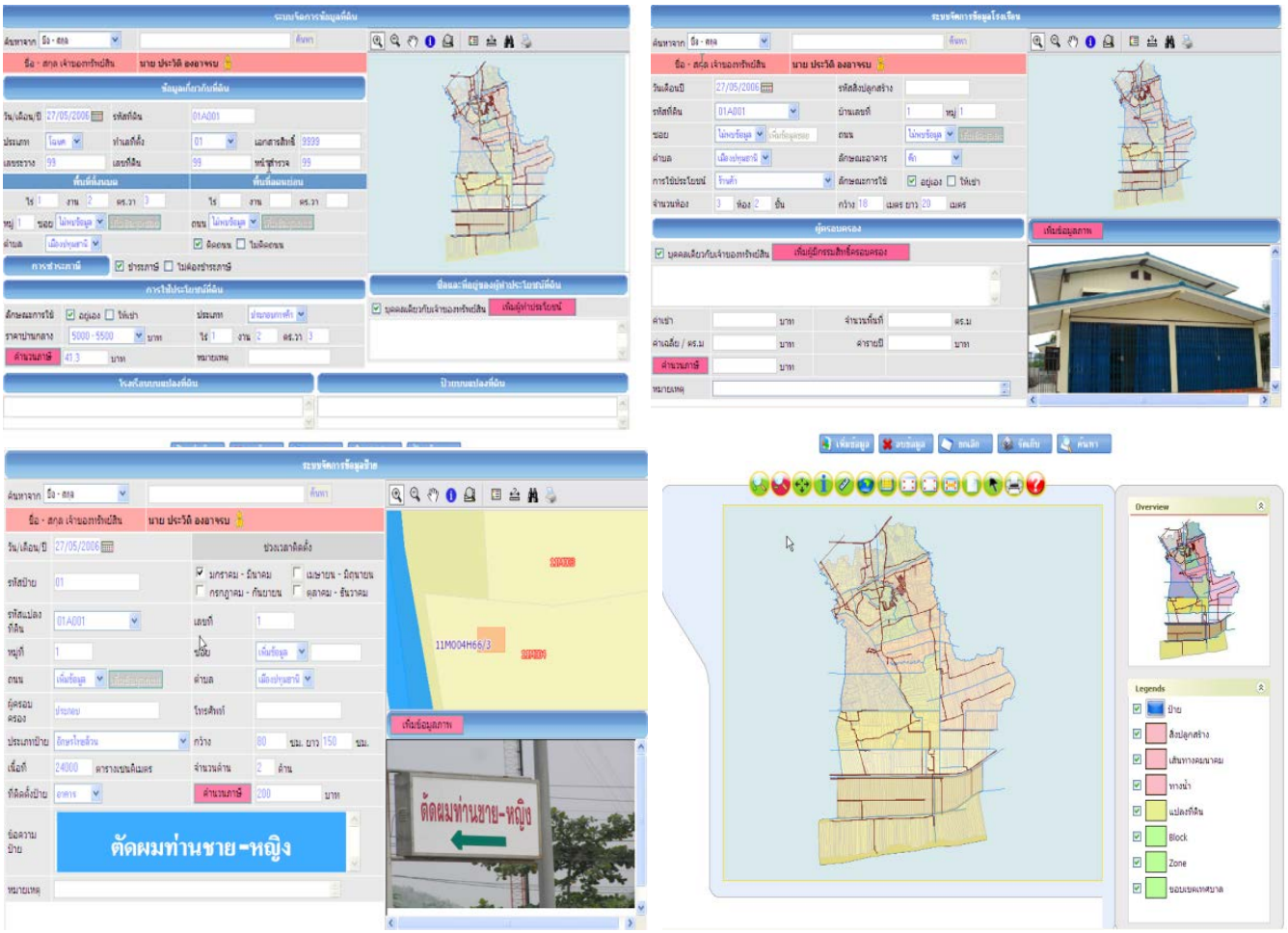
หน้ารายงานผล ระบบบัญชีคอมพิวเตอร์ของกรมส่งเสริมการปกครองท้องถิ่น

(Electronic Administration Accounting System : e-LAAS)

อุปกรณ์ Router ส่งรายงาน ระบบบัญชี ผ่านอินเทอร์เน็ต ADSL ของ TOT

๓.๒ โปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สินและโปรแกรมประยุกต์ระบบสารสนเทศภูมิศาสตร์(LTAX 3000 และLTAX GIS) เป็นโปรแกรมบันทึก และวิเคราะห์ข้อมูล ที่เกี่ยวข้องกับภาษีท้องถิ่นประเภทต่างๆ เช่น ป้าย โรงเรือน ที่ดิน และการคำนวณภาษีตามกฎหมาย โดยปัจจุบัน กรมส่งเสริมการปกครอง

ส่วนท้องถิ่น ได้แจกจ่ายและจัดอบรม เตรียมความพร้อม จึงเป็นเพียงการใช้งานในระบบปิด ไม่มีการส่งรายงานแบบ ออนไลน์เข้ามาที่ส่วนกลาง แต่มีการใช้งานแบบ StandAlone โดยในอนาคตกรมส่งเสริมการปกครองส่วนท้องถิ่น มีแนวทางพัฒนาไปสู่การเชื่อมต่อการรายงานข้อมูลในลักษณะเดียวกับ โปรแกรม ระบบบัญชีคอมพิวเตอร์ของกรมส่งเสริมการปกครองท้องถิ่น (Electronic Administration Accounting System : e-LAAS)



ตัวอย่าง ระบบแผนที่ภาษี และทะเบียนทรัพย์สิน และโปรแกรมประยุกต์ระบบสารสนเทศภูมิศาสตร์

ในอนาคต อันใกล้ โปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สินและโปรแกรมประยุกต์ระบบสารสนเทศภูมิศาสตร์ (LTAX 3000 และ LTAX GIS)มีความสมบูรณ์และเชื่อมต่อรับส่งข้อมูลผ่านระบบเครือข่ายอินเทอร์เน็ตทั่วไป อาจเกิดปัญหาทั้งปริมาณการรับส่งข้อมูล และการถูกลักลอบเข้าสู่ระบบฐานข้อมูล ที่มีความสำคัญของหน่วยงานได้

๔. การให้บริการ อินเทอร์เน็ตแก่ประชาชน โดยเฉพาะอย่างยิ่ง กลุ่มเยาวชนในท้องถิ่น เนื่องจากในหลายพื้นที่ การให้บริการอินเทอร์เน็ต ยังไม่มีความทั่วถึง ผู้ให้บริการอินเทอร์เน็ต (ISP) เชื่อมโยงระบบเครือข่ายไปถึงหน่วยงานองค์กรปกครองส่วนท้องถิ่นยังไม่ขยายบริการไปยังโรงเรียน หรือบ้านเรือนของประชาชนทั่วไป แต่เนื่องความจำเป็นในการใช้อินเทอร์เน็ตในชีวิตประจำวันของคนในท้องถิ่นมีเพิ่มมากขึ้น โดยเฉพาะด้านการศึกษา องค์กรปกครองท้องถิ่นในหลายพื้นที่ จึงจำเป็นต้องแบ่งปันการใช้งานอินเทอร์เน็ต เพื่อให้บริการแก่ประชาชนในพื้นที่อย่างหลีกเลี่ยงไม่ได้

ภาพจุดให้บริการอินเทอร์เน็ต แก่ประชาชน

โดยส่วนใหญ่การให้บริการอินเทอร์เน็ตแก่ประชาชนภายนอก ทางองค์กรปกครองส่วนท้องถิ่นจะกระจายสัญญาณอินเทอร์เน็ต ที่ใช้ภายสำนักงาน ให้แก่ประชาชนทั่วไป ได้ใช้งาน ร่วมกับ ข้าราชการ โดยไม่ได้ติดตั้งระบบรักษาความปลอดภัยใดๆ

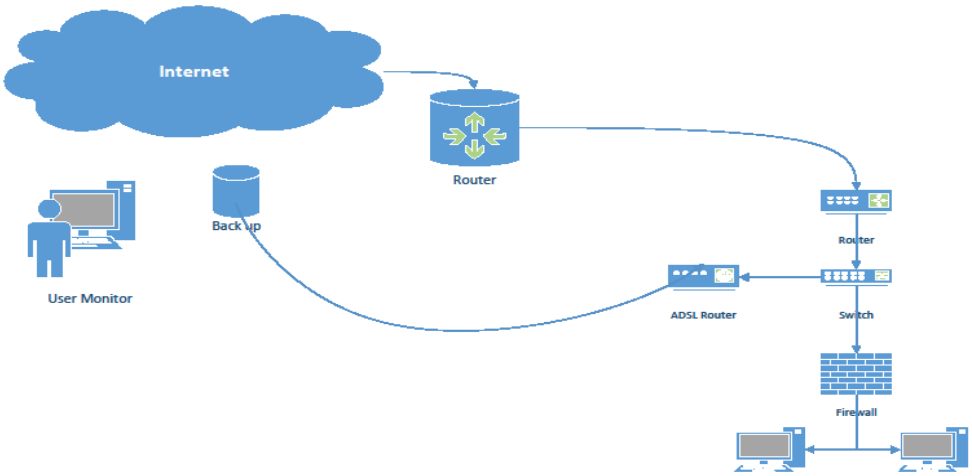
ภาพเด็กนักเรียน ที่เข้ามาใช้อินเทอร์เน็ต องค์กรปกครองส่วนท้องถิ่น

ด้วยเหตุนี้ความปลอดภัยและความมั่นคงของระบบเป็นเรื่องที่ต้องให้ความสำคัญมากขึ้น ตามไปด้วย โดยเฉพาะในองค์กรที่มีขนาดเล็กการต่อเชื่อมกับระบบอินเทอร์เน็ต เนื่องจากเป็นช่องทางหนึ่งที่ผู้บุกรุกทางไซเบอร์สามารถเข้ามาถึงข้อมูลโดยมิชอบหรือทำอันตรายกับระบบเครือข่ายได้ทุกเวลา ฉะนั้นการเฝ้าระวังและป้องกัน จึงเป็นเรื่องจำเป็นอย่างยิ่งสำหรับองค์กรปกครองส่วนท้องถิ่น ปัญหาและผลกระทบจากการบุกรุกหรือการโจมตีทางเครือข่ายในส่วนของโครงสร้างงานระบบพื้นฐานไปจนถึงระบบงานขั้นสูงเป็นประเด็นที่มีความสำคัญอย่างมาก หากข้อมูลที่ไหลเวียนอยู่ภายในภาวะวิกฤตภายใต้เครือข่ายที่ไม่มีการป้องกันหรืออ่อนแอต่อการบุรุกโจมตีทำให้ข้อมูลที่เกี่ยวข้องกับองค์กรขนาดเล็กมีความเสี่ยงในงานด้านต่างๆดังภาพ

ภาพโครงสร้างงานองค์การบริหารส่วนท้องถิ่น

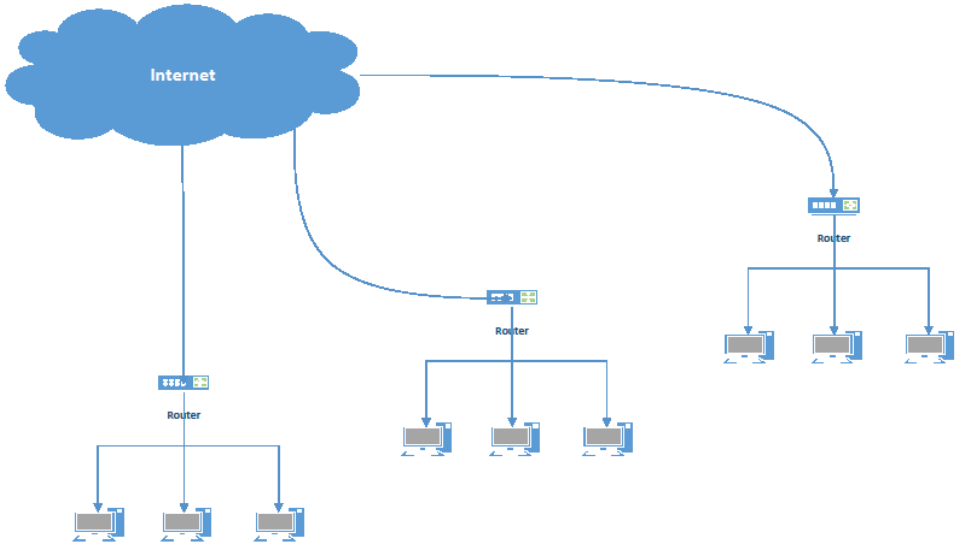
ทำให้คณะผู้วิจัยเล็งเห็นถึงความสำคัญข้อมูลสารสนเทศที่สำคัญในแต่ละภาคส่วนซึ่งเป็นข้อมูลพื้นฐานของประเทศไทยโดยได้ทำการสำรวจจากการลงพื้นที่สำรวจและสอบถาม อบต./เทศบาล จำนวน ๓๐ แห่ง โดยคณะทำงานคัดเลือกกลุ่ม อบต./เทศบาลขนาดเล็กเป็นส่วนใหญ่ เพื่อให้ทราบถึงปัจจัยแวดล้อมต่างๆ รวมไปถึงการใช้งานอินเทอร์เน็ตและการวางระบบโครงข่ายขององค์กรขนาดเล็กในท้องถิ่น โดยคำนึงถึงด้านการใช้งานเทคโนโลยีสารสนเทศและการใช้งานอินเทอร์เน็ตที่มีความเสี่ยงสูงต่อภัยคุกคามทางไซเบอร์ ด้านบุคลากรที่ยังขาดความพร้อมสำหรับการป้องกันภัยคุกคามทางไซเบอร์เป็นหลัก ซึ่งการวางระบบโครงข่ายขององค์กรขนาดเล็กในท้องถิ่น อาจจะแบ่งได้หลักๆ ๒ รูปแบบ

๑) อบต./เทศบาล ขนาดเล็กที่อยู่ในพื้นที่เขตเมืองหรือมีประชาชนในพื้นที่ค่อนข้างสูง จะมีการวางระบบโครงข่ายขององค์กรที่มีการป้องกันระดับนึง โดยมีการติดตั้ง firewall แต่ยังพบว่าการอัพเดท software ไม่ได้ดำเนินการยังสม่ำเสมอ



ภาพตัวอย่างการวางระบบโครงข่ายขององค์กรขนาดเล็กที่อยู่ในพื้นที่เขตเมือง

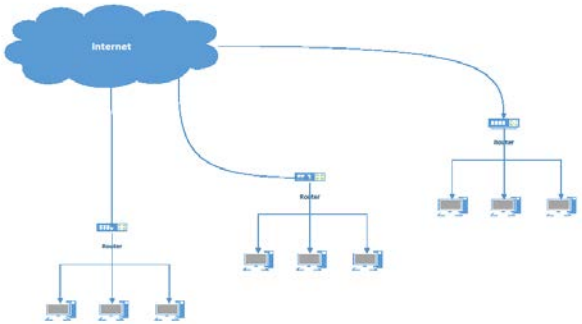
๒) อบต./เทศบาล ขนาดเล็กที่อยู่ในพื้นที่เขตชานเมือง การวางระบบโครงข่ายขององค์กรไม่มีการป้องกันใดๆ เลย มีเพียงการติดตั้ง Router แบบ ๔ port โดยเชื่อมต่อตรงกับคอมพิวเตอร์เลย



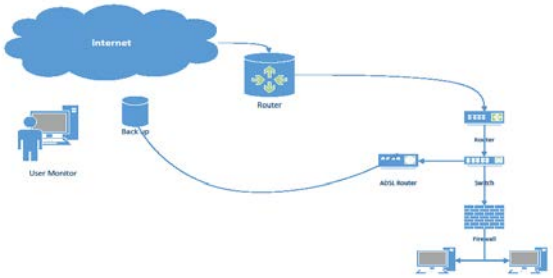
ภาพตัวอย่างการวางระบบโครงข่ายขององค์กรขนาดเล็กที่อยู่ในพื้นที่ชานเมือง

ภาพรวมข้อมูลการใช้งานระบบเครือข่ายและการป้องกันความปลอดภัยทางไซเบอร์

Existing Network



ระบบเครือข่าย อปท. ขนาดเล็ก
อบต. เทศบาลตำบล



ระบบเครือข่าย อปท ขนาดเล็ก
อบต. เทศบาลตำบล

Usage Analysis

รูปแบบการใช้งานภายในองค์กร

รับ-ส่งข้อมูล ผ่านโปรแกรมสำเร็จรูป
ของหน่วยงานต้นสังกัด

ระบบบัญชีคอมพิวเตอร์ e-LAAS

ระบบแผนที่ภาษีและทะเบียนทรัพย์สิน
และ โปรแกรมประยุกต์ระบบสารสนเทศ
ภูมิศาสตร์ (Ltax3000&LtaxGis)

บริการฟรี อินเทอร์เน็ตแก่ประชาชน

ใช้งานทั่วไปใน สำนักงาน

บริการอื่นๆ แก่หน่วยงานภายใต้ อปท.
เช่น โรงเรียน/สาธารณสุขตำบล
หรือกลุ่มอาชีพ & ศูนย์การเรียนรู้ เป็นต้น

ISP
Internet
Service
Provider

จากภาพการใช้ระบบสารสนเทศ และปัญหาด้านความปลอดภัย ของหน่วยงานท้องถิ่นสามารถสรุปได้แต่ละประเด็นดังนี้

๑. การให้บริการอินเทอร์เน็ตในระดับท้องถิ่น ไม่ครอบคลุม ทำให้หน่วยงานท้องถิ่นจำเป็นต้องเป็นจุดให้บริการ แก่ ประชาชน

๒. การเชื่อมต่อระบบอินเทอร์เน็ต ในหน่วยงานท้องถิ่น เป็นบริการ อินเทอร์เน็ตพื้นฐานโดยทั่วไปจากผู้ให้บริการ (ISP) ไม่ได้มีการติดตั้ง
อุปกรณ์ป้องกันภัยคุกคามทางไซเบอร์

๓. การให้บริการอินเทอร์เน็ต แก่ บุคคลภายนอก ของหน่วยงานท้องถิ่นไม่ได้ติดตั้งระบบ การพิสูจน์ตัวตน (Authentication)

๔. หน่วยงานท้องถิ่นมีพันธกิจ เชื่อมโยงกับ กรมส่งเสริมฯซึ่งเป็นต้นสังกัดในการ รายงานข้อมูลผ่านโปรแกรมสำเร็จรูปที่พัฒนาขึ้นมาโดยเฉพาะในงานแต่ละด้าน เช่น ระบบบัญชีคอมพิวเตอร์ และ ระบบแผนที่ภาษีและทะเบียนทรัพย์สิน และโปรแกรมประยุกต์ระบบสารสนเทศภูมิศาสตร์

๕. การรับส่งข้อมูล สำคัญ ระหว่าง หน่วยงานกลางกับ ท้องถิ่นด้วยโปรแกรมสำเร็จรูปที่พัฒนาขึ้น ผ่านเครือข่ายอินเทอร์เน็ตไม่ได้ ติดตั้งระบบความปลอดภัยรูปแบบต่างๆเพื่อใช้ระหว่างการรับส่งเช่น การติดตั้ง Private Network

๖. หน่วยงานต้นสังกัด ขาดการสนับสนุนด้านเทคโนโลยีเพื่อการป้องกันภัยทางไซเบอร์

๗. ขาดแคลน งบประมาณ ที่มุ่งเป้าหมายมาที่ ระบบป้องกัน

๘. ขาดแคลนบุคลากรด้านเทคโนโลยีสารสนเทศ

๙. ขาดความรู้ ความเข้าใจ ความตระหนัก ในภัยคุกคามทางไซเบอร์

จากประเด็นการใช้ระบบสารสนเทศ และปัญหาด้านความปลอดภัย ของหน่วยงานท้องถิ่นสามารถชี้บ่งกระบวนการด้านการจัดการความมั่นคงปลอดภัยทางไซเบอร์ที่สำคัญที่ไว้ ๔ ประเด็น ได้แก่

๑. สถานการณ์ความเสี่ยง(Risk Assessment)

๒. ผลกระทบต่อท้องถิ่น(Threat&Vulnerability Analysis)

๓. ความต้องการของท้องถิ่น(User Requirements)

๔. แนวทางการพัฒนาระบบ(Security Policy Design)

ซึ่งเป็นแนวทางในการการวิเคราะห์กลไกด้านความปลอดภัย(Security Mechanism Ananlysis)จนพัฒนาเป็นกลไกด้านความปลอดภัย(Security Mechanism Design) ตารางต่อไปนี้

สถานการณ์ความเสี่ยง Risk Assessment	ผลกระทบต่อท้องถิ่น Threat&Vulnerability Analysis	ความต้องการของท้องถิ่น User Requirements	แนวทางการพัฒนาระบบ Security Policy Design	การวิเคราะห์กลไกด้านความปลอดภัย Security Mechanism Analysis	กลไกด้านความปลอดภัย Security Mechanism Design
ด้านบุคลากร (Man Power) ๑.ขาดบุคลากรที่มีความรู้และความชำนาญในการใช้งาน อุปกรณ์ป้องกันภัยคุกคามทางไซเบอร์ ๒.ระบบสารสนเทศต่างๆ มีความยุ่งยากซับซ้อนต้องอาศัยคณะทำงานที่มีความชำนาญเฉพาะทางสนับสนุนให้เกิดเป็นรูปธรรม ปัญหาด้านบุคลากรส่งผลโดยภาพรวมให้หน่วยงานท้องถิ่นขาดความตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ไปด้วย	๑.องค์กรระดับท้องถิ่นขาดความตระหนักถึงการให้ความสำคัญกับนโยบายการรักษาความปลอดภัยทางไซเบอร์ ทำให้เกิดช่องว่างในการถูกโจมตีได้ง่าย ๒.ไม่ทราบถึงภัยคุกคามที่มีอยู่ภายในองค์กร อาจส่งผลกระทบถึงระดับประเทศได้ เนื่องจากองค์กรระดับท้องถิ่นมีช่องโหว่ในการถูกโจมตีได้ง่ายทำให้เข้าใจถึงที่มาปัญหา และ สามารถนำไปปรับปรุงเพิ่มพัฒนาระบบการรักษาความปลอดภัยที่เหมาะสมกับ หน่วยงานท้องถิ่น	๑.เพิ่มบุคลากรมีความรู้ด้านสารสนเทศและความปลอดภัยทางไซเบอร์เพื่อสนับสนุนให้การใช้เทคโนโลยีสารสนเทศในท้องถิ่นมีประสิทธิภาพมากยิ่งขึ้น ๒. คณะทำงานในการให้คำปรึกษา ด้านระบบสารสนเทศ และความปลอดภัยทางไซเบอร์เนื่องจากปัจจุบันหน่วยงานต้นสังกัดสนับสนุนเพียงการพัฒนาและฝึกอบรมการใช้โปรแกรมสำเร็จรูปเฉพาะทางแต่ยังไม่มี ทีมงานดูแลระบบสารสนเทศให้ท้องถิ่น	๑.พัฒนาศักยภาพด้านการการใช้เครื่องมือสารสนเทศ ทั้งความรู้ด้านการป้องกันภัยคุกคามทางไซเบอร์ การดูแลรักษาอุปกรณ์ และ ความรู้เบื้องต้นเกี่ยวกับระบบเครือข่าย ๒.ปลูกฝังความตระหนัก ต่อ มาตรการณ์รักษาความปลอดภัยของ ระบบคอมพิวเตอร์	ความตระหนักรู้/ทักษะและการนำไปใช้	๑.การพัฒนาบุคลากรสู่ความเป็นเลิศด้านความมั่นคงปลอดภัยทางไซเบอร์ ๒.พัฒนาองค์กรตามแนวทางมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศโดยอยู่ภายใต้แนวทางปฏิบัติของกรมส่งเสริมการปกครองส่วนท้องถิ่น

สถานการณ์ความเสี่ยง Risk Assessment	ผลกระทบต่อท้องถิ่น Threat&Vulnerability Analysis	ความต้องการของท้องถิ่น User Requirements	แนวทางการพัฒนาระบบ Security Policy Design	การวิเคราะห์กลไกด้านความปลอดภัย Security Mechanism Analysis	กลไกด้านความปลอดภัย Security Mechanism Design
<u>ด้านการจัดการ</u> **(Management)** ขาดการจัดทำข้อมูลพื้นฐานที่มีความสำคัญต่อระบบความปลอดภัยทางไซเบอร์ ได้แก่ แผนผังเชื่อมโยงระบบเครือข่ายของหน่วยงานท้องถิ่น(Network Diagram)	ไม่สามารถวิเคราะห์และแก้ไขปัญหาที่เกิดขึ้น ในกรณีที่ระบบเครือข่ายคอมพิวเตอร์ในหน่วยงานมีปัญหา	จัดทำแบบแผนผังการเชื่อมโยงเครือข่าย(Network Diagram) ที่เหมาะสม เพื่อพร้อมในการพัฒนาไปสู่การติดตั้งอุปกรณ์ป้องกันภัยคุกคามทางไซเบอร์	๑.จัดทำแผนผังการเชื่อมโยงเครือข่ายการใช้งาน ๒.เสนอแนะแนวทางปรับปรุงแก้ไข ระบบเครือข่ายให้มีความเหมาะสมเพื่อรองรับการติดตั้งอุปกรณ์ป้องกันภัยคุกคามทางไซเบอร์	แสดงรายละเอียดของอุปกรณ์ที่เกี่ยวข้องในการเชื่อมต่อระบบเครือข่ายทั้งหมด/เครือข่ายการรับส่งข้อมูลทั้งภายในและภายนอกแสดง Internet Address สำหรับอุปกรณ์ที่มีการต่อเชื่อมทั้งหมดในองค์กร	แผนผังการออกแบบอุปกรณ์การเชื่อมต่อและระบบเครือข่ายทั้งหมด

สถานการณ์ความเสี่ยง Risk Assessment	ผลกระทบต่อท้องถิ่น Threat&Vulnerability Analysis	ความต้องการของท้องถิ่น User Requirements	แนวทางการพัฒนาระบบ Security Policy Design	การวิเคราะห์กลไกด้านความปลอดภัย Security Mechanism Analysis	กลไกด้านความปลอดภัย Security Mechanism Design
<u>ด้านงบประมาณและเครื่องมือ (Money&Material)</u> การขาดงบประมาณในการมุ่งเป้าไปที่ระบบความปลอดภัยทางไซเบอร์ ส่งผลกระทบต่อการส่งเสริมการใช้อุปกรณ์ระบบความปลอดภัยทางไซเบอร์ อันได้แก่ ๑.ไม่มีระบบบริหารจัดการการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ๒.ขาดการติดตั้งระบบป้องกันการบุกรุกระหว่างเครือข่ายภายในและภายนอกเช่น ระบบป้องกันไวรัส (antivirus) รวมไปถึงการอัพเดทโปรแกรมป้องกันไวรัส (antivirus) อย่างสม่ำเสมอ ระบบ Firewall เป็นต้น	๑.เกิดการหยุดชะงักของระบบสารสนเทศภายในหน่วยงานท้องถิ่น ที่เกิดจากระบบทำงานผิดพลาด ๒.อาจมีการรั่วไหลของข้อมูลสู่มิจฉาชีพหรือผู้ไม่ประสงค์ดี ๓.ขาดความมั่นคงปลอดภัยของข้อมูล	๑.ความต้องการพื้นฐานของระบบเนื่องจากหน่วยงาน อบต./เทศบาล ขนาดเล็ก ส่วนใหญ่ประสบปัญหาขาดแคลนงบประมาณใน การบำรุงรักษาระบบ ๒.เครื่องมือสำหรับการป้องกันข้อมูลสารสนเทศต่างๆ ๓.ต้องการใช้งานเครื่องมือหรือระบบสารสนเทศที่ไม่มียุ่งยากซับซ้อนจนเกินไปเน้นการใช้งานที่ง่ายและรวดเร็ว ๔.ปลอดภัยสำหรับผู้ใช้งานและข้อมูลที่ใช้รับ-ส่งในการใช้งาน ๕.มีการใช้ข้อมูลสารสนเทศเพื่อการสืบค้นและการสื่อสารที่สะดวกและรวดเร็วยิ่งขึ้น	พัฒนาอุปกรณ์ป้องกันภัยทางไซเบอร์ในรูปแบบ Appliances สามารถเก็บ Log File ตาม พรบ. คอมฯ คัดกรองเนื้อหาที่ไม่เหมาะสม วิเคราะห์ภัยคุกคามและมีระบบแจ้งเตือนภัย	๑.การบริหารจัดการฐานข้อมูลโดยควรใช้อุปกรณ์ที่สามารถเชื่อมต่อฐานข้อมูลร่วมกันได้เพื่อการบรูณาการข้อมูล ๒.อุปกรณ์เฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชนที่เหมาะสมกับการใช้งานในท้องถิ่น ทำหน้าที่ในเก็บข้อมูลจราจรการใช้งานอินเทอร์เน็ต (log file) ๓.ระบบคัดกรองเนื้อหาไม่เหมาะสมที่เผยแพร่ทางอินเทอร์เน็ตเพื่อใช้กับองค์กรท้องถิ่น	๑.อุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์(logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall,Network Devices ต่างๆ ๒.ระบบปฏิบัติการ ระบบ appliances ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย 15 อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้

		๖.ระบบในการบริหารจัดการเครือข่ายภายในองค์กร ๗.ระบบคัดกรองเนื้อหาไม่เหมาะสมที่เผยแพร่ทางอินเทอร์เน็ตเพื่อใช้กับองค์กรท้องถิ่น ได้แก่ ภัยคุกคามที่เกิดจากการนำเข้าข้อมูลที่มีเนื้อหาที่ผิดกฎหมาย			๓. สามารถจัดเก็บ log file ได้แก่ ภัยคุกคามที่เกิดจากการนำเข้าข้อมูลที่มีเนื้อหาที่ผิดกฎหมาย เช่น การนำเข้าข้อมูลที่ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย หรือการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงภาพของผู้อื่น โดยระบบควรมีคุณสมบัติอย่างน้อยดังนี้ - สามารถนำเข้าฐานข้อมูลเว็บไซต์หรือโดเมนที่ไม่เหมาะสมและป้องกันข้อมูลเว็บไซต์หรือโดเมนที่ไม่เหมาะสม - สามารถตรวจสอบกลุ่มเนื้อหาที่กระทบต่อความมั่นคงต่อประเทศ - สามารถตรวจสอบกลุ่มเนื้อหาลามกอนาจารทั้งที่มีเนื้อหาภาษาไทยและเนื้อหาภาษาอังกฤษ - สามารถตรวจสอบกลุ่มเว็บไซต์หรือโดเมนที่มีมีการโฆษณาชวนเชื่อ กลุ่มเนื้อหาที่ผิดกฎหมาย (การพนัน ยา

					เสพติด เป็นต้น) ทั้งที่มีเนื้อหาภาษาไทยและเนื้อหาภาษาอังกฤษ - สามารถแสดงการรายงานผลผ่าน Web Base GUI - สามารถแสดงการรายงานผลและสรุปสถิติจำนวนการใช้งานอินเทอร์เน็ตหรือการใช้งานแบนด์วิดธ์ที่เกิดขึ้น - สามารถแสดงการรายงานผลและสรุปสถิติจำนวนการปิดกั้น (Internet Blocked) แบบภาพรวม - สามารถแสดงผลรายงานการบันทึก Log files จากการใช้งานอินเทอร์เน็ตเพื่อเก็บบันทึกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้อย่างน้อย ๙๐ วัน - มีการเข้ารหัสผ่าน (HTTPS) และการบริหารจัดการระบบผ่าน SSH รวมถึงปิด Port Services ที่ไม่ได้ใช้ออกเพื่อความมั่นคงปลอดภัย - รองรับการใช้งาน window os, mac os, android และ ios ด้วย Cloud Server ซึ่ง

					มีค่าใช้จ่ายต่ำกว่าการลงทุนเป็น Hardware หรือServer ขนาดใหญ่ ซึ่งการกำหนดข้อมูลในการกรองข้อมูลในเบื้องต้น ควรใช้คณะทำงานผู้เชี่ยวชาญด้าน Cyber Security เป็นผู้คัดกรองข้อมูล แล้วจัดเก็บฐานข้อมูลเข้าสู่ระบบ ตัวอย่างตามภาพได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฉบับที่มีผลบังคับใช้โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐาน เช่น ต้องผ่านการรับรองมาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ.4003.1 – 2552) เป็นต้น เพื่อความแม่นยำถูกต้องสามารถใช้ยืนยันได้ในชั้นศาล

สถานการณ์ความเสี่ยง Risk Assessment	ผลกระทบต่อท้องถิ่น Threat&Vulnerability Analysis	ความต้องการของท้องถิ่น User Requirements	แนวทางการพัฒนาระบบ Security Policy Design	การวิเคราะห์กลไกด้านความปลอดภัย Security Mechanism Analysis	กลไกด้านความปลอดภัย Security Mechanism Design
๓. ขาดการติดตั้งระบบการพิสูจน์ตัวตน (Authentication)	เสี่ยงต่อการใช้เป็นช่องทางกระทำความผิด ตาม พรบ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ หรือ การกระทำผิดทางกฎหมายด้านอื่นๆ	ติดตั้งระบบแสดงตัวตน (Authentication) เพื่อแสดงตัวตนการใช้งานอินเทอร์เน็ต ใช้งานง่าย ไม่ซับซ้อน บุคลากร ที่ใช้งานมีพื้นฐานการใช้งานคอมพิวเตอร์ทั่วไปสามารถเป็น Admin ได้	ระบบแสดงตัวตน (Authentication) แสดงตัวตนการใช้งานอินเทอร์เน็ต กำหนดสิทธิในการใช้งานอินเทอร์เน็ตจาก Adminของหน่วยงาน กำหนดนโยบายระยะเวลาการใช้ User และ Password พัฒนาขึ้นมาเป็นส่วนหนึ่งของระบบป้องกันภัยคุกคามทางไซเบอร์ สอดคล้อง ตาม พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ฯ	๑. อุปกรณ์ตรวจสอบการเข้าใช้งานอินเทอร์เน็ตของหน่วยงานท้องถิ่น ๒. มีระบบจัดการสมาชิก และสามารถสร้างรหัสผ่านให้ผู้ใช้งานได้ ๓. สามารถจัดการสมาชิกแบบรายบุคคล รายกลุ่ม ๔. จัดการและจัดรูปแบบกลุ่มสมาชิก เช่น ความเร็ว ระยะเวลา	ระบบพิสูจน์ตัวตนทำหน้าในการตรวจสอบ และอนุญาตให้ ผู้ใช้บริการเข้าสู่การใช้งานอินเทอร์เน็ต โดยประกอบไปด้วย ๑. ส่วนการจำกัดการเข้าใช้บริการ ๒. ส่วนพิสูจน์ตัวตน ๓.ระบบฐานข้อมูลผู้ใช้บริการ

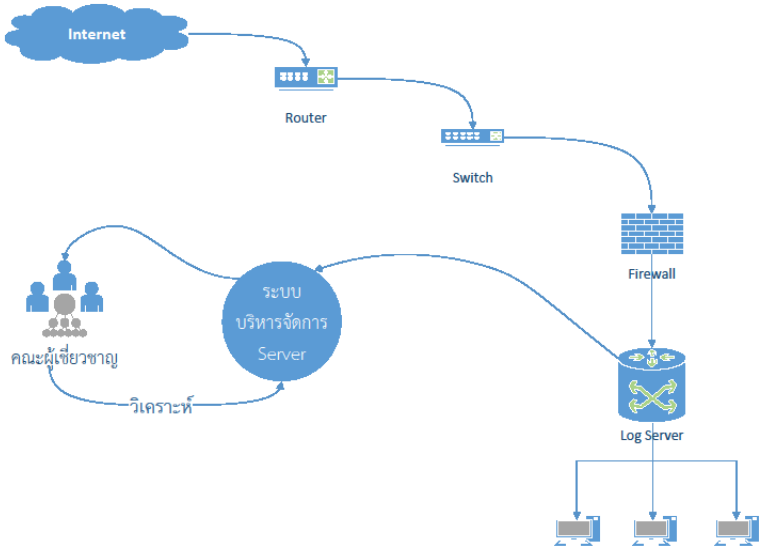
จากกระบวนการคิดวิเคราะห์ข้างต้นมีการใช้งานที่เกี่ยวข้องกับได้แก่ งานด้านรับ-ส่งข้อมูล ผ่านโปรแกรมสำเร็จรูปของหน่วยงานต้นสังกัด/ระบบบัญชีคอมพิวเตอร์e-LAAS/ระบบแผนที่ภาษีและทะเบียนทรัพย์สินและโปรแกรมประยุกต์ระบบสารสนเทศภูมิศาสตร์(Ltax3000&LtaxGis)/การให้บริการอินเทอร์เน็ตฟรีแก่ประชาชน/ใช้ระบบสำนักงานทั่วไปและบริการอื่นๆ แก่หน่วยงานภายใต้ อปท.เช่น โรงเรียน/สาธารณสุขตำบล หรือกลุ่มอาชีพ & ศูนย์การเรียนรู้ เป็นต้น ซึ่งหน่วยงานมีจำเป็นต้องใช้ระบบเครือข่ายและการป้องกันความปลอดภัยทางไซเบอร์ สังเกตได้จากการวางระบบโครงข่ายอินเทอร์เน็ต (Network Diagram) ขององค์กรแล้ว คณะผู้วิจัยพบว่า ยังขาดการบันทึกข้อมูลจราจรการใช้งานอินเทอร์เน็ต (Log file) การบันทึกการใช้งานแบนวิทต่อเดือน โดยการออกแบบต้นแบบจำลองระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น ประกอบด้วย

๑) อุปกรณ์เฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชนที่เหมาะสมกับการใช้งานในท้องถิ่น ทำหน้าที่ในเก็บข้อมูลจราจรการใช้งานอินเทอร์เน็ต (log file) และบริหารจัดการฐานข้อมูล โดยควรใช้อุปกรณ์ที่สามารถเชื่อมต่อฐานข้อมูลร่วมกันได้ เพื่อการบรูณาการข้อมูล

๒) ระบบคัดกรองเนื้อหาไม่เหมาะสมที่เผยแพร่ทางอินเทอร์เน็ตเพื่อใช้กับองค์กรท้องถิ่น ได้แก่ ภัยคุกคามที่เกิดจากการนำเข้าข้อมูลที่มีเนื้อหาที่ผิดกฎหมาย เช่น การนำเข้าข้อมูลที่ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย หรือการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงภาพของผู้อื่น โดยระบบควรมีคุณสมบัติอย่างน้อยดังนี้

- สามารถนำเข้าฐานข้อมูลเว็บไซต์หรือโดเมนที่ไม่เหมาะสมและป้องกันข้อมูลเว็บไซต์หรือโดเมนที่ไม่เหมาะสม
- สามารถตรวจสอบกลุ่มเนื้อหาที่กระทบต่อความมั่นคงต่อประเทศ
- สามารถตรวจสอบกลุ่มเนื้อหาลามกอนาจารทั้งที่มีเนื้อหาภาษาไทยและเนื้อหาภาษาอังกฤษ
- สามารถตรวจสอบกลุ่มเว็บไซต์หรือโดเมนที่มีมีการโฆษณาชวนเชื่อ กลุ่มเนื้อหาที่ผิดกฎหมาย (การพนัน ยาเสพติด เป็นต้น) ทั้งที่มีเนื้อหาภาษาไทยและเนื้อหาภาษาอังกฤษ
- สามารถตรวจสอบการดาวน์โหลด/อัพโหลดที่มีความเสี่ยงต่อการละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา
- สามารถแสดงการรายงานผลผ่าน Web Base GUI
- สามารถแสดงการรายงานผลและสรุปสถิติจำนวนการใช้งานอินเทอร์เน็ตหรือการใช้งานแบนวิทที่เกิดขึ้น
- สามารถแสดงการรายงานผลและสรุปสถิติจำนวนการปิดกั้น (Internet Blocked) แบบภาพรวม
- สามารถแสดงผลรายงานการบันทึก Log files จากการใช้งานอินเทอร์เน็ตเพื่อเก็บบันทึกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้อย่างน้อย ๙๐ วัน
- มีการเข้ารหัสผ่าน (HTTPS) และการบริหารจัดการระบบผ่าน SSH รวมถึงปิด Port Services ที่ไม่ได้ใช้ออกเพื่อความมั่นคงปลอดภัย
- รองรับการใช้งาน window os, mac os, android และ ios

ซึ่งการกำหนดข้อมูลในการกรองข้อมูลในเบื้องต้น ควรใช้คณะทำงานผู้เชี่ยวชาญด้าน Cyber Security เป็นผู้คัดกรองข้อมูล แล้วจัดเก็บฐานข้อมูลเข้าสู่ระบบ ตัวอย่างตามภาพ



ภาพต้นแบบจำลองระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกัน
ภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น

ทั้งนี้การออกแบบต้นแบบจำลองระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อเป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น คณะผู้วิจัยจะดำเนินการในขั้นตอนต่อไป โดยการรับฟังความคิดเห็นกลุ่มย่อย (Focus Group) เพื่อรวบรวมความคิดเห็นต่างๆประกอบการพัฒนาต้นแบบจำลองระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่นให้เหมาะสมมากยิ่งขึ้นและตอบสนองกับการปฏิบัติงานของผู้ปฏิบัติงานและการให้บริการด้านต่างๆแก่ประชาชนให้เกิดประโยชน์สูงสุด

ผลสรุปจากการลงพื้นที่สำรวจใช้งานระบบเทคโนโลยีระบบสารสนเทศของท้องถิ่นทั้งปัญหาภัยคุกคามทางไซเบอร์ของท้องถิ่นและการสัมภาษณ์เชิงลึกทำให้คณะผู้วิจัยรับทราบข้อมูลเชิงลึก อุปสรรคและปัญหาในด้านที่เกี่ยวของกับความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับท้องถิ่นในภูมิภาคต่างๆจึงได้ประเด็นสำคัญในข้างต้นมาทำการวิเคราะห์ได้คือ

การให้องค์ความรู้เกี่ยวกับ Cyber Security ถือเป็นปัจจัยสำคัญลำดับต้นๆ ในการพัฒนาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยถือว่าจากผลการสำรวจพบว่าบุคลากรขาดองค์ความรู้ ขาดความเข้าใจเป็นสำคัญ ส่งผลกระทบให้ไม่ทราบถึงภัยคุกคามที่มีอยู่ภายในองค์กร อาจส่งผลกระทบถึงระดับประเทศได้ เนื่องจากองค์กรระดับท้องถิ่นมีช่องโหว่ในการถูกโจมตีได้ง่าย และมีเป็นจำนวนมากยากต่อการป้องกันทั้งหมด

การขาดแคลนทรัพยากรได้แก่ ระบบการบริหารจัดการเฉพาะด้าน อาทิ เช่น ระบบป้องกันไวรัส (antivirus) รวมไปถึงการอัพเดทโปรแกรมป้องกันไวรัส (antivirus) อย่างสม่ำเสมอ ระบบบริหารจัดการการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ระบบ Firewall เป็นต้น โดยระบบต่างๆ ถือมีความจำเป็นต้องกระทำควบคู่ไปกับการเสริมสร้างองค์ความรู้ เพื่อเป็นการป้องกันอย่างรวดเร็ว เพื่อไม่ให้ส่งผลกระทบในวงกว้าง

การใช้งานคอมพิวเตอร์ของบุคลากรค่อนข้างมีความเสี่ยงพอสมควร เนื่องจากยังขาดความเข้าใจในการเข้ารหัสข้อมูลองค์กร การบริหารจัดการข้อมูลองค์กรอย่างมีประสิทธิภาพ การป้องกันข้อมูลรั่วไหลสู่มิจชีพหรือผู้ไม่ประสงค์ดีก็ตาม โดยในส่วนนี้ ควรกระทำควบคู่ไปกับการเสริมสร้างองค์ความรู้

พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีบทลงโทษทั้งจำคุกและปรับ ซึ่งบุคลากรยังขาดความรู้ความเข้าใจใน พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อยู่เป็นจำนวนมาก ทั้งนี้ รวมไปถึงประชาชนในท้องถิ่น ซึ่งถือว่ามีความเสี่ยงในกระทำความผิดต่อ พ.ร.บ. ดังกล่าวเนื่องจากขาดความรู้ความเข้าใจในการเฝ้าระวังเรื่องดังกล่าว รวมไปถึงการหาวิธีป้องกัน/เครื่องมือและบริหารจัดการการใช้งานคอมพิวเตอร์ผ่านอินเทอร์เน็ต

ดังนั้นการส่งเสริมบุคลากรในระดับท้องถิ่นและประชาชนทั่วไปให้ตระหนักรู้ เข้าใจพื้นฐานการรักษาความมั่นคงปลอดภัยไซเบอร์รวมถึงมีส่วนร่วมในการพัฒนาระบบความปลอดภัยทางไซเบอร์เพื่อนำไปใช้ได้จริงในองค์กรระดับท้องถิ่นในอนาคตจึงนำประเด็นสำคัญและผลการสำรวจเก็บรวบรวมข้อมูลไปสู่การจัดงานเสวนาแลกเปลี่ยนเรียนรู้ เผยแพร่ และสร้างความตระหนักให้รู้เท่าทันภัยคุกคามทางไซเบอร์ใน ไตรมาสที่๓ ภายใต้หัวข้อ “การเผยแพร่องค์ความรู้และสร้างความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์สำหรับองค์กรขนาดเล็กระดับชุมชนและประชาชนทั่วไป”

กิจกรรมการรับฟังความคิดเห็นจากการเสวนาแลกเปลี่ยนเรียนรู้ เผยแพร่ และสร้างความตระหนักให้รู้เท่าทันภัยคุกคามทางไซเบอร์บุคลากรท้องถิ่น / ประชาคม /ประชาชนทั่วไป ที่เกี่ยวข้องในชุมชน เพื่อการเผยแพร่ให้ความรู้เบื้องต้น โดยอาจแบ่งได้เป็น ๒ ประเด็นหลัก คือ (๑) การเผยแพร่ความรู้มุ่งเน้นการจัดเก็บข้อมูลการจราจรทางอินเทอร์เน็ต ๙๐ วัน ตาม พรบ. เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ถึงความจำเป็นในการปฏิบัติตาม พรบ. ดังกล่าว หากไม่ดำเนินการมีบทลงโทษระบุไว้ตาม พรบ. และ (๒) การรับฟังความคิดเห็นต่อร่างต้น

การจัดเสวนา ในโครงการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ สำหรับองค์กรขนาดเล็กในระดับชุมชน จัดขึ้นโดยกำหนดชื่อโครงการเสวนา “โครงการเผยแพร่ความรู้และสร้างความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์สำหรับองค์กรขนาดเล็กระดับชุมชนและประชาชนทั่วไป”ในระหว่างวันที่ ๓-๖ ตุลาคม ๒๕๖๐ โดยมีรายละเอียดการเสวนาดังต่อไปนี้

วันที่ ๑

ความเข้าใจเบื้องต้นเกี่ยวกับภัยคุกคามทางไซเบอร์ ผลกระทบต่อท้องถิ่นและประชาชน”

โดย อาจารย์สมทบ แก้วเชื้อ วิทยากร

ปัญหาเทคโนโลยีและการรักษาความปลอดภัยพื้นฐานการจัดการข้อมูลส่วนตัว เพื่อความปลอดภัยพื้นฐาน

โดย อาจารย์สมิทธินันท์ ไทยรุ่งโรจน์ วิทยากร

ปัญหาเทคโนโลยีและการรักษาความปลอดภัย พื้นฐานสื่อสังคมออนไลน์กับความปลอดภัยทางไซเบอร์

โดย อาจารย์สมทบ แก้วเชื้อ และ อาจารย์สมิทธินันท์ ไทยรุ่งโรจน์ วิทยากร

วันที่ ๒

ปัญหา เทคโนโลยีและการรักษาความปลอดภัยพื้นฐานกับธุรกรรมทางการเงินและ พาณิชย์อิเล็กทรอนิกส์

โดย อาจารย์สมิทธินันท์ ไทยรุ่งโรจน์ วิทยากร

สถานการณ์ ความเสี่ยงทางไซเบอร์ในประเทศไทย

โดย อาจารย์สมิทธินันท์ ไทยรุ่งโรจน์ วิทยากร

แนวทางการรักษาความมั่นคงปลอดภัยสำหรับท้องถิ่นและประชาชน

-มาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify)

-การปกป้องดูแลสารสนเทศ (Protect)

โดย อาจารย์สมทบ แก้วเชื้อ วิทยากร

แนวทางการรักษาความมั่นคงปลอดภัยสำหรับท้องถิ่นและประชาชน

- การรับมือภัยคุกคามทางไซเบอร์(Respond)

-การกู้คืนข้อมูลและระบบ (Recover)

โดย อาจารย์สมิทธินันท์ ไทยรุ่งโรจน์ วิทยากร

วันที่ ๓

กฎหมายพรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์

-ที่มาของพรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์

-สิทธิส่วนบุคคล (Right To Privacy) สิทธิในการรับรู้ข่าวสาร (Right To Know)

พัฒนาการ การปรับปรุง พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ จาก ปี ๒๕๕๐ ถึง ๒๕๖๐

โดย อาจารย์สมิทธินันท์ ไทยรุ่งโรจน์ วิทยากร

กฎหมายพรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์โดยอธิบายแง่มุมทางกฎหมาย ข้อบัญญัติ ตาม พรบ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ๒๕๖๐

โดย อาจารย์สมิทธินันท์ ไทยรุ่งโรจน์ วิทยากร

บทบาท หน้าที่ขององค์กรท้องถิ่นขนาดเล็ก ในการเฝ้าระวังความปลอดภัยทางไซเบอร์ ตามข้อบัญญัติ ตาม พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และ หน้าที่ในการเผยแพร่ ส่งเสริมการตระหนักรู้แก่ประชาชน

โดย อาจารย์สมิทธินันท์ ไทยรุ่งโรจน์ วิทยากร

ระดมความคิดเห็น จาก บุคลากร ท้องถิ่น เข้าร่วมสัมมนา ส่วนต่างๆ และ ส่วนงานด้านกฎหมาย เกี่ยวกับการปฏิบัติงาน พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ๒๕๕๐ และข้อจำกัด

โดย อาจารย์สมทบ แก้วเชื้อ และ อาจารย์สมิทธินันท์ ไทยรุ่งโรจน์ วิทยากร

วันที่ ๔

สภาพการณ์ทั่วไป การใช้สารสนเทศในองค์กรท้องถิ่นขนาดเล็ก ภาพรวม สถานการณ์สารสนเทศ ของ องค์กรท้องถิ่นขนาดเล็ก ปัญหา อุปสรรค์ ข้อจำกัด

โดย อาจารย์สมทบ แก้วเชื้อ วิทยากร

กรณีศึกษา การวางระบบเครือข่าย (Network) ภายใน องค์กรท้องถิ่นขนาดเล็กที่มีอยู่รูปแบบต่างๆ

โดย อาจารย์สมทบ แก้วเชื้อ วิทยากร

สภาพการณ์ทั่วไป การใช้สารสนเทศ ใน องค์กรท้องถิ่น ขนาดเล็ก

-นำเสนอผลการผลสำรวจ ปัญหา ระบบความปลอดภัยทางไซเบอร์ สำหรับองค์ท้องถิ่นขนาดเล็ก ในโครงการการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงานและพัฒนา

-เครื่องมือในการเฝ้าระวังความ มั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชน

โดย อาจารย์สมทบ แก้วเชื้อ วิทยากร

เวทีระดมความคิดเห็น ปัญหา แนวทาง และ ข้อเสนอแนะ การแก้ไขปัญหา ภัยคุกคามทางไซเบอร์

โดย อาจารย์สมทบ แก้วเชื้อ และ อาจารย์สมิทธินันท์ ไทยรุ่งโรจน์ วิทยากร

แต่เนื่องจากผู้เข้าร่วมเสวนาในโครงการส่วนใหญ่ได้แจ้งกับคณะทำงานถึงการติดภารกิจในการเตรียมงานพระราชพิธีถวายพระเพลิงพระบรมศพ พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช วันสำคัญทางศาสนาและผู้เข้าร่วมบางท่านติดภาระกิจอื่นๆไม่สามารถอยู่ร่วมงานได้จนครบตามวันเวลาที่กำหนดไว้ ทางคณะดำเนินงานจึงวางแผนและปรับการเสวนาให้เหมาะสมกับเหตุการณ์ที่เกิดขึ้นโดยจัดกิจกรรมในระหว่างวันที่ ๓-๔ ตุลาคม ๒๕๖๐ ณ ห้องประจักษ์ตราเฟิร์สคลาส ๒ โรงแรมประจักษ์ตรา ดีไซน์ โฮเทล ซึ่งได้ปรับแต่งเนื้อหาให้สั้นกระชับแต่ยังคงครอบคลุมเนื้อหาสาระสำคัญในการเสวนาเช่นกำหนดการเดิมโดยมีเนื้อหาดังนี้

วันที่ ๑

-ความเข้าใจเบื้องต้นเกี่ยวกับภัยคุกคามทางไซเบอร์ ผลกระทบ ต่อชุมชนท้องถิ่น

-ปัญหาเทคโนโลยีและการรักษาความปลอดภัย พื้นฐานการจัดการข้อมูลส่วนตัวเพื่อความปลอดภัยพื้นฐาน

-ปัญหาเทคโนโลยีและการรักษาความปลอดภัย พื้นฐานสื่อสังคมออนไลน์กับความปลอดภัยทางไซเบอร์

-สถานการณ์ ความเสี่ยงทางไซเบอร์ในประเทศไทย

-แนวทางการรักษาความมั่นคงปลอดภัยสำหรับท้องถิ่นและประชาชน

-มาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify)

-การปกป้องดูแลสารสนเทศ(Protect)

โดย คณะผู้วิจัย วิทยากร

<u>ข้อสรุปและความคิดเห็นเพิ่มเติมของผู้เข้าร่วมสัมมนาในวันที่ ๑</u>

การบรรยายในวันที่ ๑ คณะผู้วิจัย จัดเตรียมเนื้อหาทั้งเอกสารเล่ม ประกอบการบรรยายและการนำเสนอประกอบการบรรยายเพื่อให้ผู้เข้าร่วมสัมมนาเกิดความกระจ่างชัดในความหมายของภัยคุกคามทางไซเบอร์ โดยผู้เข้าร่วมสัมมนา ต่างมีมุมมองแตกต่างกันออกไป ประชาชนทั่วไป และกลุ่มอาชีพ ที่เข้าร่วม มองภัยคุกคามทางไซเบอร์เป็นเรื่องใกล้ตัว เช่น การฉ้อโกง หลอกลวงผ่านทางเฟสบุ๊ค ส่วนเจ้าหน้าที่หน่วยงาน หรือองค์กรท้องถิ่นมองว่าเป็นเรืองของการดูแลรักษาคอมพิวเตอร์และข้อมูลจากไวรัส แต่ยังไม่เข้าใจถึงผลกระทบในความเสี่ยงเท่าไหร่นัก

ระหว่างการบรรยายในเรื่องแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในวันแรก มีบุคลากรของท้องถิ่น แสดงความคิดเห็นเกี่ยวกับพันธกิจในปัจจุบัน ที่หน่วยงานท้องถิ่นต้อง ดำเนินการในการรับส่งข้อมูลด้วย

โปรแกรมฯตามนโยบายที่ทางกรมส่งเสริมการปกครองส่วนท้องถิ่นซึ่งเป็นต้นสังกัดสั่งการมาให้ดำเนินการ หน่วยงานจึงจำเป็นต้องติดตั้งอินเทอร์เน็ต เพื่อใช้ในการรับส่งข้อมูลดังกล่าว และเมื่ออินเทอร์เน็ตมาถึงหน่วยงาน หน่วยงานก้อจะเป็นสถานที่ที่ ประชาชนที่ผ่านไปมาขอใช้บริการอย่างหลีกเลี่ยงไม่ได้ ส่วนการติดตั้งอุปกรณ์ป้องกัน ส่วนใหญ่ยังไม่มีการดำเนินการ เพราะหน่วยงานจะขอให้ช่างติดตั้งที่มาติดตั้งอินเทอร์เน็ตของผู้ให้บริการแค่ติดตั้งและกระจายสัญญาณให้ใช้ได้ครอบคลุมสำนักงานเท่านั้น

กรณีการปกป้องดูแลสารสนเทศ (Protect) บุคลากรจากหน่วยที่เข้าร่วม ได้แบ่งปันประสบการณ์ การดูแลป้องกันดังนี้ เนื่องจากไม่ได้มีความรู้และงบประมาณที่จะติดตั้งระบบป้องกัน แต่เคยประสบปัญหาที่เครื่องติดไวรัส ก็มักจะส่งให้ร้านคอมพิวเตอร์ในเมือง ดำเนินการแก้ไข บางครั้งข้อมูลก้อสูญหายไปด้วย จากประสบการณ์ดังกล่าว จึงไม่อนุญาต ให้ใช้อุปกรณ์แฟลชไดรฟ์มาใช้กับเครื่องในหน่วยงาน แต่วิธีที่นิยมมากที่สุด คือ แบ่งเครื่องคอมพิวเตอร์ที่เก็บข้อมูลสำคัญแยกออกมาเฉพาะไม่ให้มีการใช้งานอื่นๆ นอกจากงานสำคัญที่มีลักษณะเฉพาะทาง เช่น เครื่องที่ใช้ส่ง e-laas จะใช้ในงานด้านนี้อย่างเดียวโดยเฉพาะ

วันที่ ๒

-กฎหมายพรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์

-อธิบายแง่มุมทางกฎหมายตามข้อบัญญัติตาม พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ๒๕๖๐

-สภาพการณ์ทั่วไป การใช้สารสนเทศ ใน องค์กรท้องถิ่น ขนาดเล็ก ภาพรวม สถานการณ์สารสนเทศขององค์กรท้องถิ่นขนาดเล็ก กรณีศึกษาปัญหา อุปสรรค์ ข้อจำกัด ได้แก่ การใช้งานคอมพิวเตอร์ อินเทอร์เน็ต และโปรแกรมสำเร็จรูปต่างๆ ของหน่วยงานในท้องถิ่น

-นำเสนอ กรณีศึกษา การวางระบบเครือข่าย(Network)ภายในองค์กรท้องถิ่นขนาดเล็ก รูปแบบต่างๆ พร้อม การวิเคราะห์ โดยวิทยากร

- ระดมความคิดเห็นเกี่ยวกับปัญหา และ ข้อเสนอแนะการแก้ไขปัญหาภัยคุกคามทางไซเบอร์

โดย คณะผู้วิจัย วิทยากร

หลังจากลงพื้นที่เพื่อเก็บรวบรวมข้อมูลจากแบบสอบถามกลุ่มตัวอย่างและคัดเลือกกลุ่มเป้าหมายเพื่อสัมภาษณ์เชิงลึกทำให้คณะผู้วิจัยประเมินสถานการณ์ระดับความเข้าใจและการรับรู้ของประชาชนและเจ้าหน้าที่หน่วยงานท้องถิ่นต่อปัญหาภัยคุกคามทางไซเบอร์ว่า ส่วนใหญ่การรับรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ มาจากข้อมูลข่าวสาร ทั่วไปที่ได้รับผ่านสื่อ และการประชาสัมพันธ์ของหน่วยงานรัฐ เกี่ยวกับเนื้อหาของพ.ร.บว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ๒๕๕๐ ซึ่งสื่อให้ความสำคัญกับการกำหนดประเด็นข่าว(Setting Agenda) ไปที่ประเด็นเรื่องการกระทำผิดที่เกี่ยวข้องกับเรื่องใกล้ตัวประชาชนทั่วไป เช่น การใช้สื่อสังคมออนไลน์ (Social Media) ในการละเมิดสิทธิผู้อื่น การกระทำต่อความมั่นคงของรัฐและความสงบสุขรวมถึงประเด็นการหลอกลวงต่างๆผ่านสื่อออนไลน์

คณะผู้วิจัยเห็นว่าหากผู้เข้าร่วมเสวนายังมีข้อจำกัดเกี่ยวกับความรู้ความเข้าใจถึงภัยคุกคามทางไซเบอร์ อาจทำให้การระดมคิดเห็นขาดซึ่งข้อมูลที่มีความครบถ้วนถูกต้องการเสวนาจึงจำเป็นที่ต้องสร้างกระบวนการถ่ายทอดความรู้เกี่ยวกับขอบเขตของภัยคุกคามทางไซเบอร์ เพื่อให้ผู้เข้าร่วมเสวนามีโอกาสขยายขอบเขตความรู้เข้าใจ ในภัยคุกคามทางไซเบอร์เพื่อให้การระดมความคิดเห็นสามารถนำไปสู่ข้อสรุปแนวทางเพื่อคลี่คลายปัญหาที่มีความลึกและตรงประเด็นมากขึ้น คณะผู้วิจัยฯจึงเล็งเห็นว่าการเสวนาจำเป็นต้องสร้างกระบวนการให้ความรู้ และกระตุ้นการมีส่วนร่วมในการเสวนาดังนี้

๑. ให้ความรู้พื้นฐาน(To Educate) ผ่านเนื้อหาการบรรยาย และเอกสารเพื่อให้เกิดพื้นความรู้ ขอบเขตของภัยคุกคามทางไซเบอร์ เป็นลำดับแรก ซึ่งคณะผู้วิจัยฯ ได้ออกแบบเนื้อหา ประกอบบรรยายเพื่อให้ผู้เข้าร่วมสัมมนาเกิดความรู้เข้าใจในเบื้องต้นเป็นลำดับแรก ก่อนเข้าสู่กระบวนการระดมความคิด

ภาพการเสวนาโครงการการศึกษาและพัฒนาบุคลากรเพื่อปรับปรุงการปฏิบัติงาน
และพัฒนาเครื่องมือในการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชน

๒. กระตุ้น (To Persuade) ให้ผู้เข้าร่วมเสวนา ร่วมแสดงความคิดเห็นให้ข้อมูล ผ่านการระดมความคิดเห็นโดยบางช่วงใช้วิธีการยกตัวอย่างกรณีศึกษาใกล้ตัวและอาจมีผลกระทบต่อผู้เข้าร่วมสัมมนาโดยตรง เพื่อให้ผู้เข้าร่วมสัมมนาเห็นความสำคัญกับ การป้องกันภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อท้องถิ่น อีกทั้งกระตุ้นให้ผู้สัมมนานำข้อมูลไปสู่การเผยแพร่แบบปากต่อปาก (Word Of Mouth) หลังเสร็จสิ้นการสัมมนา

โดยประเด็นหัวข้อที่ใช้ในการกระตุ้นและระดมความคิดของผู้เข้าร่วมเสวนา แบ่งออกเป็น ๒ ประเด็นดังนี้

ประเด็นที่ ๑ กรณีการกระทำความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ๒๕๕๐ โดยคณะวิจัยฯ ได้ ขยายความกรณีศึกษาปัญหาภัยคุกคามทางไซเบอร์อย่างง่าย

ตัวอย่างเช่น กรณีหาก หน่วยงานท้องถิ่น เก็บรวบรวมโฉนดที่ดิน ในระบบข้อมูลแผนที่ภาษี และทะเบียนทรัพย์สินไว้ในคอมพิวเตอร์สำนักงาน หากมีเจ้าหน้าที่แอบเข้าไป ลักลอบขโมยข้อมูลโฉนดที่ดินเพื่อนำไปขายให้นายทุนที่ดิน

ถือเป็นการกระทำความผิดในพ.ร.บ ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ตามมาตรา ๕ “ในการผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน มีโทษตาม พ.ร.บ ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ปี ๒๕๕๐ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกิน หนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ โดยฉบับแก้ไขเพิ่มเติมปี ๒๕๖๐ เป็นโทษจำคุกไม่เกิน ๒ ปี ปรับไม่เกิน ๔ หมื่นบาทหรือทั้งจำทั้งปรับ”

ประเด็นที่ ๒ สภาพการณ์ทั่วไป การใช้สารสนเทศ ในองค์กรท้องถิ่นขนาดเล็ก ภาพรวม สถานการณ์สารสนเทศ ขององค์กรท้องถิ่นขนาดเล็ก ปัญหา อุปสรรค์ ข้อจำกัด ได้แก่ การใช้งานคอมพิวเตอร์ อินเทอร์เน็ต และโปรแกรมสำเร็จรูปต่างๆ ของหน่วยงานในท้องถิ่น โดยคณะผู้วิจัยกระตุ้นการมีส่วนร่วมผู้เข้าร่วมสัมมนา จากผลการสำรวจ ประกอบภาพ ที่คณะผู้วิจัยฯ ได้ลงพื้นที่พบเห็น เพื่อให้ผู้เข้าร่วมสัมมนา อธิบายถึงเหตุผลที่มาปัญหาดังกล่าวและร่วมเสนอแนะแนวทางคลี่คลาย ซึ่งผู้เข้าร่วมสัมมนาเกิดความเข้าใจและเล็งเห็นปัญหาดังกล่าวหลังรับฟังการบรรยายกว่า ๒ วัน ส่วนการลงมือวางแผนเพื่อดำเนินระบบป้องกันความปลอดภัยทางไซเบอร์นั้นอยู่ที่ทัศนคติของผู้นำท้องถิ่น และแรงผลักดันของประชาชนและบุคลากรระดับหนุ่มสาวในท้องถิ่น

การกระตุ้นการมีส่วนร่วมในปัญหาจากกระบวนการระดมความคิดเห็นผ่านการเสวนานอกจากจะทำให้ผู้เข้าร่วมเสวนาเกิดความรู้เข้าใจได้แล้วหากผู้เข้าร่วมเสวนามีความสนใจและขยายผลต่อเนื่อง จะทำให้ปัญหาภัยคุกคามทางไซเบอร์กลายเป็นปัญหาสำคัญที่ต้องตระหนักอันนำไปสู่การเป็นประเด็นสาธารณะ (Public Agenda) สำคัญ ที่จะถูกขยายต่อไปในเวทีเสวนาท้องถิ่นอื่นๆ

<u>ข้อสรุปและความคิดเห็นเพิ่มเติมของผู้เข้าร่วมสัมมนาในวันที่ ๒</u>

การใช้บริการ อินเทอร์เน็ต ในภูมิภาค จำนวนมาก ผู้ให้บริการอินเทอร์เน็ต (ISP) มุ่งขยายโครงข่ายไปสู่หน่วยราชการท้องถิ่น เป็นอันดับแรก เช่น อบต. และ เทศบาล ตำบล แต่ยังไม่ขยายโครงข่ายการให้บริการไปยังที่อยู่อาศัยบ้านเรือน และ ส่วนบริการประชาชนด้านอื่นๆ เช่น โรงเรียนภายใต้สังกัด อบต. ทำให้ประชาชนและนักเรียนอาศัยอินเทอร์เน็ตของอบต.ในพื้นที่ ในการใช้งาน โดย อบต. ส่วนใหญ่ เปิดให้ใช้บริการฟรี ไม่มีเจ้าหน้าที่ผู้ดูแลระบบ และระบบป้องกันภัยคุกคามทางไซเบอร์ ซึ่งความเห็นดังกล่าวสอดคล้องกับการลงพื้นที่สำรวจของคณะวิจัย ที่พบปัญหาลักษณะเดียวกันที่ อบต.นาซาว จังหวัดน่าน ที่แม้จะเป็น อบต.ที่อยู่ในเขตอำเภอเมือง แต่บริการอินเทอร์เน็ต ยังไม่สามารถให้ได้ครอบคลุมประชาชนได้ทั้งเขตตำบล ระบบโครงข่ายของผู้ให้บริการ (ISP) ให้บริการได้เพียงรอบๆที่ทำการของอบต.เท่านั้น อบต.จึงกลายเป็นจุดบริการฟรีอินเทอร์เน็ตอย่างหลีกเลี่ยงไม่ได้ ด้วยเหตุผลของหน้าที่ในฐานะส่วนราชการท้องถิ่นที่ต้องให้การบริการประชาชนประกอบกับการเป็นเพียงหน่วยงานสุดท้ายแห่งเดียวที่ใกล้ชิดปัญหาประชาชนมากที่สุด ไม่สามารถเพิกเฉยต่อการขาดแคลนทรัพยากรได้

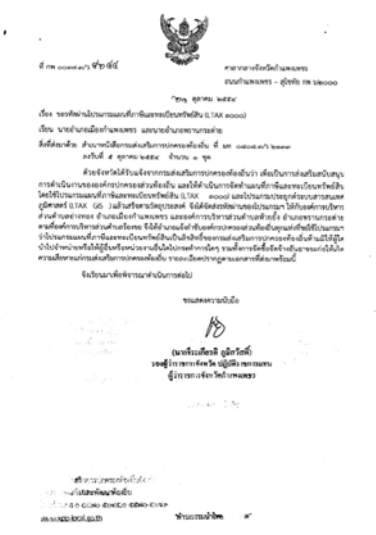
คณะผู้วิจัยเห็นว่าความไม่พร้อมด้านบุคลากร ความรู้ความเข้าใจ ในการรักษาความปลอดภัยทางไซเบอร์ ประกอบกับงบประมาณที่มีอยู่อย่างจำกัด อีกทั้งไม่ได้มีการกำหนดแผนงานและงบประมาณเพื่อดำเนินงานด้านการรรักษาความปลอดภัยทางไซเบอร์ทำให้ อบต.เป็นจุดเสียงสำคัญประการหนึ่ง

จากความคิดเห็นของผู้เข้าร่วมสัมมนาทำให้คณะผู้วิจัยได้เสนอความคิดเห็นเพิ่มเติมต่อยอดเพื่อให้ผู้เข้าร่วมสัมมนาเกิดความกระจ่าง เกี่ยวกับการพัฒนาเครื่องมืออุปกรณ์ระบบป้องกันภัยทางไซเบอร์ ที่นอกจากจะทำหน้าที่ในการเก็บ ข้อมูลการจราจรทางคอมพิวเตอร์ (Log ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐) และการปิดกั้น (Internet Blocked) ยังทำหน้าที่ในการ รายงาน (Report) การใช้งานอินเทอร์เน็ต หรือหรือการใช้งานแบนวิทที่เกิดขึ้นในรูปแบบต่างๆ โดยเฉพาะกรณีที่มีผู้เข้ามาใช้อินเทอร์เน็ตเพื่อเข้าสู่ข้อมูลที่ไม่มีประโยชน์ และมีการดาวน์โหลด ข้อมูลจำนวนมาก อันจะส่งผลกระทบต่อผู้ใช้งานท่านอื่น ซึ่ง หากหน่วยงานมีอุปกรณ์ระบบป้องกันภัยทางไซเบอร์ จะช่วยให้หน่วยงานท้องถิ่นสามารถMonitorผ่านหน้าจอที่เข้าใจได้อย่างง่ายๆ ซึ่งจะทำให้อบต. ให้บริการอินเทอร์เน็ตฟรี อย่างมีความปลอดภัย ถูกต้องตามกฎหมาย พ.ร.บ ว่าด้วยการกระทำผิด

ทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ สามารถบริหารการใช้ Bandwidth ให้เกิดประโยชน์สูงสุด ทั้งพันธกิจทางราชการและบริการประชาชน ควบคู่กันไป ซึ่งผู้เข้าร่วมสัมมนาเห็นว่าถ้ามีอุปกรณ์เกิดขึ้นจริงน่าจะช่วยลดทอนปัญหาที่เกิดขึ้นใน หน่วยงานท้องถิ่นมากพอสมควร

ภาพเด็กนักเรียน มาใช้ ฟรีอินเทอร์เน็ตที่ อบต. เปิดให้บริการใช้ฟรี(ภาพซ้าย)
และตำแหน่งการปล่อยสัญญาณอินเทอร์เน็ต (ภาพขวา)

การใช้งานโปรแกรมต่างๆที่ได้รับมอบหมายจากกรมส่งเสริมการปกครองท้องถิ่นเช่น โปรแกรมแผนที่และทะเบียนทรัพย์สินและระบบสารสนเทศภูมิศาสตร์ (Ltax3000 & LtaxGis) และโปรแกรมระบบบัญชีคอมพิวเตอร์ขององค์กรปกครองส่วนท้องถิ่น (E-Laas) เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาจากส่วนงานต่างๆ ในกรมส่งเสริมการปกครองท้องถิ่นเพื่อให้หน่วยงานท้องถิ่นนำไปปฏิบัติใช้งาน ซึ่งที่ผ่านมา ส่วนกลางจะอบรมการใช้งานของบุคลากรในท้องถิ่นและมอบหมายให้ดำเนินการใช้โปรแกรมสำเร็จรูปเหล่านี้ให้สำเร็จลุล่วงตามวัตถุประสงค์ซึ่ง ส่วนใหญ่ไม่ได้ให้ความสำคัญพูดถึงความรู้และแนวทางเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ประเด็นเรื่องความปลอดภัยทางไซเบอร์ จึงเป็นเรื่องที่ ท้องถิ่นแต่ละแห่งจะดำเนินการศึกษาและแก้ไขเอง ส่วนการตั้งรหัสความปลอดภัยของการใช้งานคอมพิวเตอร์ ผู้เข้าสัมมนาแสดงความคิดเพิ่มเติม ยอมรับว่ามักจะตั้งรหัสให้ง่าย โดยเฉพาะหากเป็นโปรแกรมที่ต้องใช้งานร่วมกันหลายคน จำเป็นที่ผู้เกี่ยวข้องหลายคนต้องเข้าใช้งานระบบด้วยรหัสเดียวกันได้ แต่ในส่วนของรหัสที่ใช้โปรแกรมสำเร็จรูปที่ใช้ในการปฏิบัติงาน บางโปรแกรมจะอนุมัติการใช้งานและรหัสจากหน่วยงานต้นสังกัด เช่น การใช้โปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สิน หน่วยงานที่จะปฏิบัติงานต้องอนุมัติรหัส โดยอธิบดีกรมส่งเสริมการปกครองส่วนท้องถิ่น เป็นผู้อนุญาตและผ่านจังหวัดไปสู่หน่วยงานปฏิบัติการณ์ดังตัวอย่าง การขออนุมัติเพื่อดำเนินการติดตั้งและรับรหัสโปรแกรมฯดังภาพ



สำเนาภาพตัวอย่าง หนังสือขอดำเนินการขอรหัสสำหรับโปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สิน
ข้อมูล: อ้างอิงจาก http://www.kpp-local.go.th/files/order/20111025153317okahb.pdf

รหัสผ่าน (License) โปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สิน (LTAX ๓๐๐๐) จังหวัดกำแพงเพชร			
ลำดับที่	อำเภอ	ชื่อ อปท.	รหัสผ่าน
๑	พรานกระต่าย	อบต.ห้วยยั้ง	เครื่องที่ 1 73454d873065934d1678464d9a2250fb
			เครื่องที่ 2 602f92b2fda20d503a0f4097b1571f75
๒	เมืองอ่างทอง	อบต.อ่างทอง	เครื่องที่ 1 4bc6be4624c62147afccf3fdaa59b26b
			เครื่องที่ 2 555d9a927058c882459d5dcf39193f5f
			เครื่องที่ 3 baf5d504634064a7685c28d28d30ed44

สำเนาภาพตัวอย่าง หนังสือขอดำเนินการขอรหัสสำหรับโปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สิน
ข้อมูล: อ้างอิงจาก http://www.kpp-local.go.th/files/order/20111025153317okahb.pdf

ในส่วนการรับรู้ พรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ๒๕๕๐ ส่วนใหญ่รับรู้ผ่านสื่อสารมวลชนต่างๆ เป็นการรับรู้ในแง่มุมของสิทธิ และการถูกละเมิดสิทธิผ่านทางสื่อสังคมออนไลน์(Social Media) เช่นการเผยแพร่ภาพลามกอนาจาร การตกแต่งดัดแปลงภาพทำให้บุคคลอื่นโดนดูหมิ่น หรือการโพสดูหมิ่นบุคคลอื่นๆ แต่ยังไม่ศึกษาเข้าใจอย่างลึกซึ้ง ถึงความเกี่ยวพันกับปัญหาที่เกิดขึ้นกับระบบคอมพิวเตอร์ของหน่วยงานท้องถิ่น เช่น กรณีการทำให้คอมพิวเตอร์ หรือชุดคำสั่งก่อให้เกิดความเสียหาย ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่ง ไปจนถึงการทำให้เกิดผลการสูญเสียข้อมูลสำคัญของท้องถิ่น

ปัญหาด้านบุคลากร หน่วยงาน อบต.ขนาดเล็กหลายอบต. ไม่มีบุคลากรด้านคอมพิวเตอร์ โดยตรงอาศัยเจ้าหน้าที่ด้านพัสดุ การคลัง ซึ่งเป็นผู้ใช้งานธรรมดา (User) เช่น เจ้าหน้าที่คลังพัสดุ นายช่างโยธา ปลัดฯ การแก้ไขปัญหา จึงอาศัย ร้านคอมพิวเตอร์ ในพื้นที่ แต่หากเกิดปัญหาที่มาจากโปรแกรมสำเร็จรูปของกรม จะประสานงานกับส่วนงานที่เกี่ยวข้องกับโปรแกรมเหล่านั้นๆ ที่ส่วนกลาง เช่น โปรแกรม แผนที่ภาษีและทะเบียนทรัพย์สิน จะติดต่อที่ส่วนงาน แผนที่ภาษีและทะเบียนทรัพย์สิน สำนักบริหารการคลังท้องถิ่น

ซึ่งกรณีปัญหาส่วนใหญ่เกิดจากเครื่องคอมพิวเตอร์ที่ใช้ในการบันทึกข้อมูลภาษีของประชาชนโดนไวรัส จนไม่สามารถใช้งานได้ จึงแก้ไขปัญหาโดยการให้ร้านคอมพิวเตอร์ มาซ่อมบำรุงอุปกรณ์ Hardware และ ลงโปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สินใหม่อีกครั้ง ซึ่งข้อมูลที่เคยจัดเก็บมักจะสูญหายไป เป็นการสร้างความสูญเสียให้กับ หน่วยงานเป็นอันมาก ประเด็นนี้สอดคล้องกับการทำสำรวจแบบสำรวจ ที่พบว่า หน่วยงานท้องถิ่น เมื่อคอมพิวเตอร์เสียหายใช้งานไม่ได้ จะส่งให้เจ้าหน้าที่ (ที่พอมีความรู้) ๕๔.๒๖% เพื่อแก้ไขเบื้องต้น หากเป็นปัญหาที่ไม่สามารถแก้ไขได้ จึงส่งไปให้ร้านคอมพิวเตอร์ในพื้นที่ซ่อมแซมให้ ขณะที่ ๒๙.๖๐% จะส่งให้ร้านคอมพิวเตอร์ในพื้นที่ซ่อม เนื่องจากไม่มีผู้รับผิดชอบ

กรณีความคิดเห็นเกี่ยวกับการเก็บ Log ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ความคิดเห็นของประชาชนที่เข้าร่วมสัมมนาเห็นว่า ในระดับประชาชน ไม่จำเป็นต้องมีอุปกรณ์ดังกล่าว จะเป็นการสร้างความยุ่งยากในการใช้เครื่องมือสื่อสาร แต่ควรให้ความสำคัญกับเรื่องของการตั้งรหัส ในโทรศัพท์มือถือ เมล์ และ โปรแกรมสำเร็จรูปแบบต่างๆ ส่วนความคิดเห็นของ หน่วยงานท้องถิ่น หลังได้ฟังจากการเสวนาเห็นว่าควรเริ่มต้นศึกษาและ หาวิธีการจัดซื้อจัดหาอุปกรณ์ Log ตาม พ.ร.บ ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ๒๕๕๐ เนื่องจากข้อมูลของหน่วยงานถือว่ามีความสำคัญ โดยอยากให้มีหน่วยงานที่มีความเชี่ยวชาญเข้ามาเป็นเสมือนพี่เลี้ยงให้ หน่วยงานท้องถิ่นจัดทำLogตามพ.ร.บ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ เนื่องจากหน่วยงานท้องถิ่นส่วนใหญ่ไม่มีบุคลากรที่มีความชำนาญเฉพาะด้านนี้ ซึ่งการแสดงความคิดเห็นดังกล่าวสอดคล้องกับแบบสำรวจของคณะวิจัยที่ลงพื้นที่สำรวจ ที่พบว่ากว่า ๖๓.๐๗ %ไม่มีความรู้ เกี่ยวกับพ.ร.บ.ข้อมูลจราจรทางคอมพิวเตอร์ ๒๕๕๐

นอกจากนี้ในส่วนของบุคลากรด้านการศึกษาของโรงเรียนในสังกัด องค์กรปกครองส่วนท้องถิ่น เสนอความเห็นให้ ผู้เกี่ยวข้องแทนที่จะมุ่งเป้าการส่งเสริมการรับรู้ไปที่หน่วยงานท้องถิ่นเพียงอย่างเดียว แต่ควรให้ประชาชน และครู ในสังกัด องค์กรปกครองส่วนท้องถิ่น ได้มีโอกาสรับรู้อีกกลุ่มหนึ่ง เนื่องจาก เนื่องจากโรงเรียนเป็นส่วนหนึ่งที่ใช้อินเทอร์เน็ตค่อนข้างมาก และ บุคลากรครูจำนวนหนึ่ง มีทักษะพื้นความรู้ด้านคอมพิวเตอร์ที่สามารถเรียนรู้ อันจะช่วยเผยแพร่ความรู้ ด้านการระวังความปลอดภัยทางไซเบอร์ให้ไปสู่ชุมชนท้องถิ่นได้อีกช่องทางหนึ่ง

จากการระดมความคิดเห็นของประชาชน ในท้องถิ่น ผ่านเวทีสัมมนาดังกล่าวทำให้คณะผู้วิจัยฯสรุปปัญหาอุปสรรค์ของสร้างระบบความปลอดภัยทางไซเบอร์ในท้องถิ่น ดังแผนภาพนี้

แผนภาพสรุป อุปสรรค์ปัญหา ของการสร้างระบบความปลอดภัยทางไซเบอร์ในท้องถิ่น

แบบจำลองระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น ซึ่งต้นแบบจำลองระบบฯ ควรยึดตามมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐาน เช่น ต้องผ่านการรับรองมาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ.๔๐๐๓.๑ – ๒๕๕๒) เป็นต้น รวมไปถึงระดับการทำงานของระบบฯ สำหรับองค์การปกครองส่วนท้องถิ่น แบ่งได้เป็น ๒ ระดับ ได้แก่ (๑) ระดับองค์การปกครองส่วนท้องถิ่นขนาดเล็ก (ลูกข่าย) การป้องกันภัยคุกคามดำเนินการ ๕ ขั้นตอน ได้แก่ การบันทึกข้อมูลจราจรคอมพิวเตอร์ (Record) การเตรียมการ (Prepare) การป้องกัน (Protection) การวิเคราะห์ (Analyze) การเตือนภัย (Response) และ (๒) ระดับองค์การปกครองส่วนท้องถิ่นหน่วยงานกลางหรือขนาดใหญ่ (แม่ข่าย) การป้องกันภัยคุกคามดำเนินการ ๕ ขั้นตอน ได้แก่ การบันทึกข้อมูลจราจรคอมพิวเตอร์ (Record) การเตรียมการ (Prepare) การป้องกัน (Protection) การวิเคราะห์ (Analyze) การเตือนภัย (Response) การสืบค้นย้อนกลับ (Traceability) การโจมตีกลับ (Offensive)

สรุปปัญหาและอุปสรรคที่เกิดขึ้นจากการดำเนินโครงการ (สาเหตุของปัญหาพร้อมด้วยวิธีแก้ไขปัญหา)**สรุปผลการรวบรวมสภาพปัญหา วิเคราะห์ความเสี่ยงและผลกระทบ**

๑. การให้องค์ความรู้เกี่ยวกับ Cyber Security ถือเป็นปัจจัยสำคัญลำดับต้นๆ ในการพัฒนาด้านการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยถือว่าจากผลการสำรวจพบว่าบุคลากรขาดองค์ความรู้ ขาดความเข้าใจเป็นสำคัญ ส่งผลกระทบให้ไม่ทราบถึงภัยคุกคามที่มีอยู่ภายในองค์กร อาจส่งผลกระทบถึงระดับประเทศได้ เนื่องจากองค์กรระดับท้องถิ่นมีช่องโหว่ในการถูกโจมตีได้ง่าย และมีเป็นจำนวนมากยากต่อการป้องกันทั้งหมด

๒. การขาดแคลนทรัพยากรได้แก่ ระบบการบริหารจัดการเฉพาะด้าน อาทิ เช่น ระบบป้องกันไวรัส (antivirus) รวมไปถึงการอัพเดทโปรแกรมป้องกันไวรัส (antivirus) อย่างสม่ำเสมอ ระบบบริหารจัดการการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ระบบ Firewall เป็นต้น โดยระบบต่างๆ ถือมีความจำเป็นต้องกระทำควบคู่ไปกับการเสริมสร้างองค์ความรู้ เพื่อเป็นการป้องกันอย่างรวดเร็ว เพื่อไม่ให้ส่งผลกระทบในวงกว้าง

๓. การใช้งานคอมพิวเตอร์ของบุคลากรค่อนข้างมีความเสี่ยงเนื่องจากยังขาดความเข้าใจในการเข้ารหัสข้อมูลองค์กร การบริหารจัดการข้อมูลองค์กรอย่างมีประสิทธิภาพ การป้องกันข้อมูลรั่วไหลสู่มิจชีพหรือผู้ไม่ประสงค์ดีก็ตาม โดยในส่วนนี้ ควรกระทำควบคู่ไปกับการเสริมสร้างองค์ความรู้

๔. พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีบทลงโทษทั้งจำคุกและปรับ ซึ่งบุคลากรยังขาดความรู้ความเข้าใจใน พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อยู่เป็นจำนวนมาก ทั้งนี้ รวมไปถึงประชาชนในท้องถิ่น ซึ่งถือว่ามีความเสี่ยงในกระทำความผิดต่อ พ.ร.บ. ดังกล่าวเนื่องจากขาดความรู้ความเข้าใจในการเฝ้าระวังเรื่องดังกล่าว รวมไปถึงการหาวิธีป้องกัน/เครื่องมือและบริหารจัดการการใช้งานคอมพิวเตอร์ผ่านอินเทอร์เน็ต

๕. การบริหารจัดการระบบสารสนเทศส่วนใหญ่สืบเนื่องมาจากบุคลากรขาดความชำนาญในการใช้งานเครื่องมือการใช้งานของระบบสารสนเทศต่างๆ มีความยุ่งยากซับซ้อนจนเกินไป เครือข่ายอินเทอร์เน็ตไม่เสถียรหรือไม่เพียงพอต่อการใช้งาน จากปัจจัยสะท้อนให้เห็นถึงปัญหาอุปสรรคหลักๆ ๓ ปัจจัย ได้แก่ บุคลากร (Human) องค์ความรู้ (Knowledge) โครงข่าย (Infra Structure) และยังพบความต้องการของผู้ใช้งาน (User) ในระดับองค์กรท้องถิ่นขนาดเล็ก มีความต้องการใช้งานเครื่องมือหรือระบบสารสนเทศที่ไม่มียุ่งยากซับซ้อนจนเกินไปเน้นการใช้งานที่ง่ายและรวดเร็ว ทั้งนี้ต้องมีความปลอดภัยสำหรับผู้ใช้งานและข้อมูลที่ใช้รับ-ส่งในการใช้งาน รวมไปถึงความต้องการด้านบุคลากรผู้เชี่ยวชาญในแต่ละด้าน ได้แก่ ด้านสารสนเทศ ด้านความปลอดภัยข้อมูลสารสนเทศ

๖. ความต้องการพื้นฐานของระบบ หน่วยงาน อบต./เทศบาล ขนาดเล็ก ส่วนใหญ่ประสบปัญหาขาดแคลนงบประมาณในการบำรุงรักษาระบบ เนื่องจากมีประชากรในพื้นที่ค่อนข้างน้อย ส่งผลให้การจัดเก็บรายได้น้อยตามไปด้วย หากระบบต้องใช้งบประมาณในการดูแลรักษาสูง อาทิ เช่น เซิฟเวอร์ในการจัดเก็บข้อมูลจราจรทางอินเทอร์เน็ตที่ต้องจัดเก็บ ๙๐ วัน ควรใช้เป็น Cloud Server ซึ่งมีค่าใช้จ่ายต่ำกว่าการลงทุนเป็น Hardware หรือ Server ขนาดใหญ่

ข้อเสนอแนะโครงการที่ควรสนับสนุนดำเนินงาน

การใช้งานคอมพิวเตอร์ในองค์กรเพื่อการสื่อสาร รับ-ส่งข้อมูลสารสนเทศสำหรับการปฏิบัติงาน เป็นสิ่งที่มีความสำคัญจำเป็นที่จะต้องได้รับการป้องกันจากภัยไซเบอร์เพื่อให้ข้อมูลสารสนเทศและเครือข่ายต่างๆ มีความปลอดภัย สามารถทำงานได้อย่างมีเสถียรภาพ ปราศจากภัยคุกคาม และลดระดับความรุนแรงที่อาจเกิดขึ้น โดยเฉพาะองค์การปกครองส่วนท้องถิ่น ถือเป็นองค์กรขนาดเล็กที่มีความเสี่ยงเกี่ยวกับภัยคุกคามทางไซเบอร์ค่อนข้างหลากหลายรูปแบบเนื่องจากเป็นหน่วยงานที่ใกล้ชิดกับประชาชนในพื้นที่ การป้องกันภัยคุกคามทางไซเบอร์ควรดำเนินการในลักษณะ sector-based คือ การเฝ้าระวัง แจ้งเตือนภัย และการดูแลความปลอดภัย ซึ่งสามารถแบ่งการพัฒนาได้เป็น ๓ ด้าน ดังนี้

๑. ด้านการพัฒนาองค์กรสู่มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

การพัฒนาองค์กรไปสู่มาตรฐานสากล ถือเป็นปัจจัยสำคัญยิ่งเพื่อทำให้องค์กรสร้างความมั่นใจในการป้องกันและรักษาข้อมูลสารสนเทศเป็นไปอย่างถูกต้องครบถ้วน ต้องมีมาตรฐานหรือแนวทางปฏิบัติที่มีประสิทธิภาพ อาทิ เช่น มาตรฐาน ISO/IEC ๒๗๐๐๑เป็นมาตรฐานขั้นพื้นฐานในการรักษาความปลอดภัยไซเบอร์ที่มีการนำไปใช้แพร่หลายทั่วโลก อย่างไรก็ตาม การพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑ ให้มีประสิทธิภาพควรอยู่บนพื้นฐานของการประเมินความเสี่ยงและจัดการความเสี่ยงในด้านต่างๆ ควบคู่กันไป ได้แก่ (๑) การรักษาความลับของข้อมูล (confidentiality) โดยการกำหนดสิทธิ์การเข้าถึงข้อมูล (๒) ความถูกต้องครบถ้วนของข้อมูล (integrity) เป็นการกำหนดมาตรการ หรือแนวทางในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลเพื่อป้องกันความผิดพลาดหรือการเข้าแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต และ (๓) ความพร้อมใช้ (availability) ผู้มีสิทธิ์ในการเข้าถึงข้อมูลในระบบต่างๆ ของหน่วยงานต้องสามารถเข้าใช้ข้อมูลได้ในกรอบเวลาที่ต้องการ

หลักการของระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems : ISMS) โดยในขั้นตอนแรกของการดำเนินการระบบ ISMS อย่างประสบผลสำเร็จ คือ การทำให้ผู้มีส่วนได้เสียที่สำคัญ (key stakeholders) ตระหนักถึงความจำเป็นของการรักษาความปลอดภัยของข้อมูล เพราะหากไม่ได้รับความร่วมมือจากผู้ที่เกี่ยวข้องทั้งหมดขององค์กร ซึ่งล้วนแต่เป็นผู้ที่ต้องปฏิบัติตาม ตรวจสอบและกำกับดูแลและคงรักษาระบบ ISMS ย่อมเป็นเรื่องยากที่จะประสบความสำเร็จในการให้ได้มาและคงรักษาไว้ซึ่งการได้รับการรับรองมาตรฐาน โดยต้องทำการวิเคราะห์ความจำเป็นด้านการรักษาความปลอดภัยสำหรับแต่ละข้อมูลสารสนเทศและนำการควบคุมที่เหมาะสมต่างๆ มาใช้เพื่อให้สามารถเก็บรักษาข้อมูลสารสนเทศดังกล่าวไว้ได้อย่างปลอดภัยจากภัยคุกคามทางข้อมูลต่างๆ อย่างเหมาะสม โดยการประยุกต์ใช้หลักการ Plan-Do-Check-Act : PDCA ซึ่งการรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑ แบ่งเป็นกระบวนการตรวจประเมินได้ ดังนี้

๑) การตรวจประเมินจะทำการทบทวนและตรวจสอบระบบ ISMS อย่างไม่เป็นทางการ การทบทวนตรวจสอบนี้ จะหมายรวมถึงการดำเนินการต่างๆ เช่น การตรวจสอบการมีอยู่ของเอกสารที่สำคัญในระบบ ISMS และตรวจสอบระบบ ISMS โดยภาพรวม เป้าหมายของการตรวจประเมินระยะที่ ๑ คือ เพื่อให้ผู้ตรวจประเมินรู้จักและคุ้นเคยกับองค์กร รวมถึงเพื่อให้องค์กรได้ทำความรู้จักกับผู้ตรวจประเมิน

๒) การตรวจประเมินติดตามผล–ระยะสุดท้ายของการรับรองมาตรฐานระบบ ISO/IEC ๒๗๐๐๑ คือการตรวจประเมินเพื่อทำให้มั่นใจว่าระบบ ISMS ของท่านได้รับการประเมินและปรับปรุงอย่างต่อเนื่อง การตรวจประเมินติดตามผลจะถูกดำเนินการอย่างน้อยที่สุดปีละหนึ่งครั้ง โดยมีจุดประสงค์เพื่อเป็นการยืนยันว่าองค์กรยังคงมีความลอดคล้องกับมาตรฐาน การตรวจประเมินติดตามผลนี้อาจถูกดำเนินการบ่อยครั้งกว่าในช่วงเริ่มต้นของการนำระบบไปปฏิบัติ

๒. ด้านการพัฒนาระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น

การพัฒนาระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์ฯ ถือเป็นเครื่องมือสำคัญประการหนึ่ง ต้องคำนึงถึงความสอดคล้องกับหลักการและมาตรฐาน ISO/IEC ๒๗๐๐๑ ซึ่งผู้วิจัยได้พัฒนาต้นแบบจำลองระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น ประกอบด้วย

๑) อุปกรณ์เฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรขนาดเล็กในระดับชุมชนที่เหมาะสมกับการใช้งานในท้องถิ่น ทำหน้าที่ในการจัดเก็บ log file และบริหารจัดการฐานข้อมูล โดยควรใช้อุปกรณ์ที่สามารถเชื่อมต่อฐานข้อมูลร่วมกันได้ และควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA 3 ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) โดยควรมีคุณสมบัติอย่างน้อยดังนี้

- เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์(logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่างๆ ระบบปฏิบัติการ ระบบ appliances ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้อย่างน้อย ๑๕ อุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้
- สามารถจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฉบับที่มีผลบังคับใช้โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐาน เช่น ต้องผ่านการรับรองมาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ.๔๐๐๓.๑ – ๒๕๕๒) เป็นต้น เพื่อความแม่นยำถูกต้อง สามารถใช้ยืนยันได้ในชั้นศาล
- มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน MD5 หรือ SHA-1 หรือดีกว่า
- สามารถเก็บ Log File ในรูปแบบ Syslog , FTP, SFTP และ Syslog Agent
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้
- สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage เป็นต้น

๒) ระบบคัดกรองเนื้อหาไม่เหมาะสมที่เผยแพร่ทางอินเทอร์เน็ตเพื่อใช้กับองค์กรท้องถิ่น ได้แก่ ภัยคุกคามที่เกิดจากการนำเข้าข้อมูลที่มีเนื้อหาที่ผิดกฎหมาย เช่น การนำเข้าข้อมูลที่ทำให้ ผู้อื่น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย หรือการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงภาพของผู้อื่น โดยระบบควรมีคุณสมบัติอย่างน้อยดังนี้

- สามารถนำเข้าฐานข้อมูลเว็บไซต์หรือโดเมนที่ไม่เหมาะสมและป้องกันข้อมูลเว็บไซต์หรือโดเมนที่ไม่เหมาะสม
- สามารถตรวจสอบกลุ่มเนื้อหาที่กระทบต่อความมั่นคงต่อประเทศ
- สามารถตรวจสอบกลุ่มเนื้อหาลามกอนาจารทั้งที่มีเนื้อหาภาษาไทยและเนื้อหาภาษาอังกฤษ
- สามารถตรวจสอบกลุ่มเว็บไซต์หรือโดเมนที่มีมีการโฆษณาชวนเชื่อ กลุ่มเนื้อหาที่ผิดกฎหมาย (การพนัน ยาเสพติด เป็นต้น) ทั้งที่มีเนื้อหาภาษาไทยและเนื้อหาภาษาอังกฤษ

- สามารถตรวจสอบการดาวน์โหลด/อัพโหลดที่มีความเสี่ยงต่อการละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา

- สามารถแสดงการรายงานผลผ่าน Web Base GUI

- สามารถแสดงการรายงานผลและสรุปสถิติจำนวนการใช้งานอินเทอร์เน็ตหรือการใช้งานแบนวิทที่เกิดขึ้น

- สามารถแสดงการรายงานผลและสรุปสถิติจำนวนการปิดกั้น (Internet Blocked) แบบภาพรวม

- สามารถแสดงผลรายงานการบันทึก Log files จากการใช้งานอินเทอร์เน็ตเพื่อเก็บบันทึกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้อย่างน้อย ๙๐ วัน

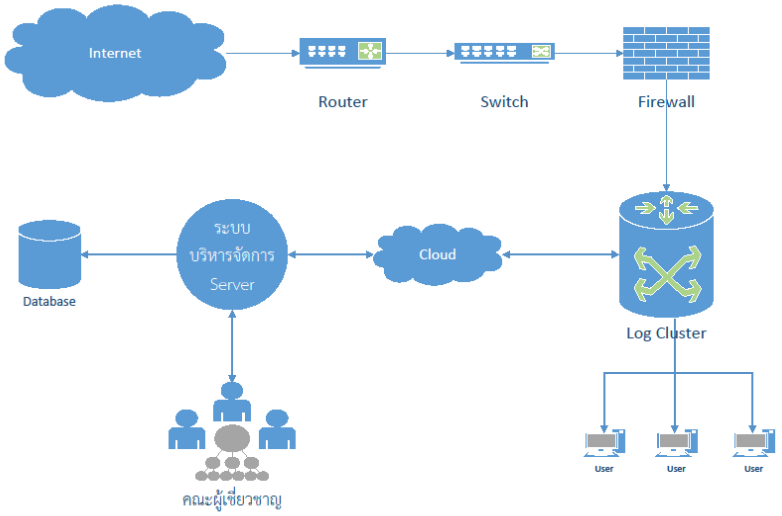
- มีการเข้ารหัสผ่าน (HTTPS) และการบริหารจัดการระบบผ่าน SSH รวมถึงปิด Port Services ที่ไม่ได้ใช้ออกเพื่อความมั่นคงปลอดภัย

- รองรับการใช้งาน window os, mac os, android และ ios

- สามารถค้นหาข้อมูลได้ในรูปแบบทั้ง AND , OR, NOT

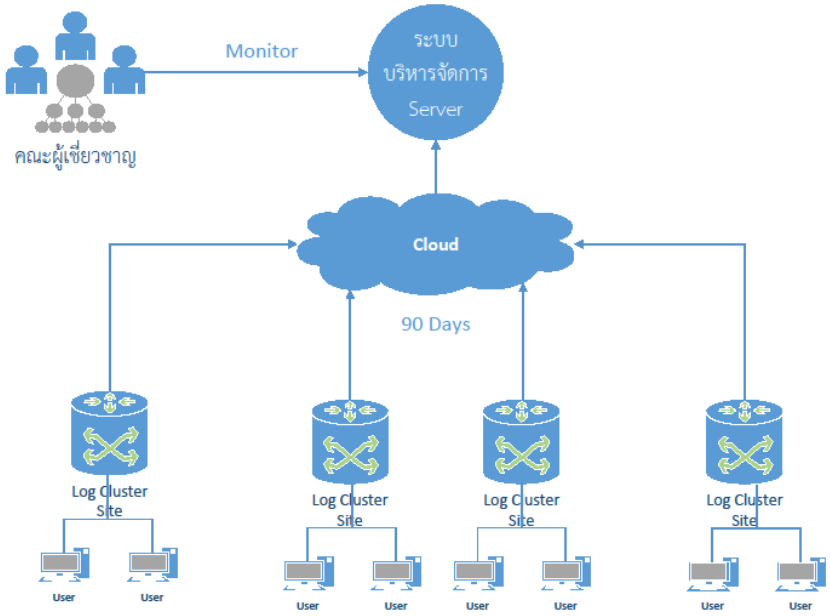
- สามารถวิเคราะห์ Log และ Use Case ที่ถูกปรับแต่งมาโดยเฉพาะ ผ่านการออกแบบโดยคณะทำงานผู้เชี่ยวชาญด้าน Cyber Security

- สามารถวิเคราะห์ภัยคุกคามแบบ Advanced Persistent Threats (APT Analysis) ซึ่งการกำหนดข้อมูลในการกรองข้อมูลเบื้องต้นควรใช้คณะทำงานผู้เชี่ยวชาญด้าน Cyber Security เป็นผู้กรองข้อมูลแล้วจัดเก็บฐานข้อมูลเข้าสู่ระบบ ตัวอย่างตามภาพ



ทั้งนี้จากภาพต้นแบบจำลองระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น โดยการพัฒนาระบบมุ่งเน้น **การบันทึกข้อมูลจราจรคอมพิวเตอร์ (Record) การเตรียมการ (Prepare) การป้องกัน (Protection) การวิเคราะห์ (Analyze) การเตือนภัย (Response)** ใช้ระยะเวลาโดยประมาณ ๒ ปี โดยปีที่ ๑ มุ่งเน้นกระบวนการจัดเก็บข้อมูลเพื่อทำการเตรียมการและวิเคราะห์ข้อมูลโดยคณะทำงานผู้เชี่ยวชาญผู้มีใบรับรองตามมาตรฐานสากล จะดำเนินการวิเคราะห์ข้อมูลแล้วจัดเก็บเป็น Database ไตรมาสละ ๑ ครั้ง และในปีที่สองระบบจะดำเนินการนำ

Database แบ่งเป็น ๒ Layer ได้แก่ (๑) Layer ทั่วไป ได้แก่ การป้องกันทั่วไป ที่มีสถิติความเสี่ยงบ่อยในระยะที่ผ่านมาเพื่อป้องกันภัยคุกคามทางไซเบอร์ และ (๒) Layer เฉพาะเจาะจง ได้แก่โดยควรแบ่ง Log Server เป็นคลัสเตอร์ โดยประมาณ ๓ จังหวัด ต่อ ๑ คลัสเตอร์ สำหรับจังหวัดขนาดเล็ก โดยทั้งประเทศอาจแบ่งได้ประมาณ ๓๐ คลัสเตอร์ รายละเอียดตามภาพ



ระยะปีที่ ๑ สามารถแบ่งออกเป็นกิจกรรมหลักๆ ได้ ๔ กิจกรรม ได้แก่

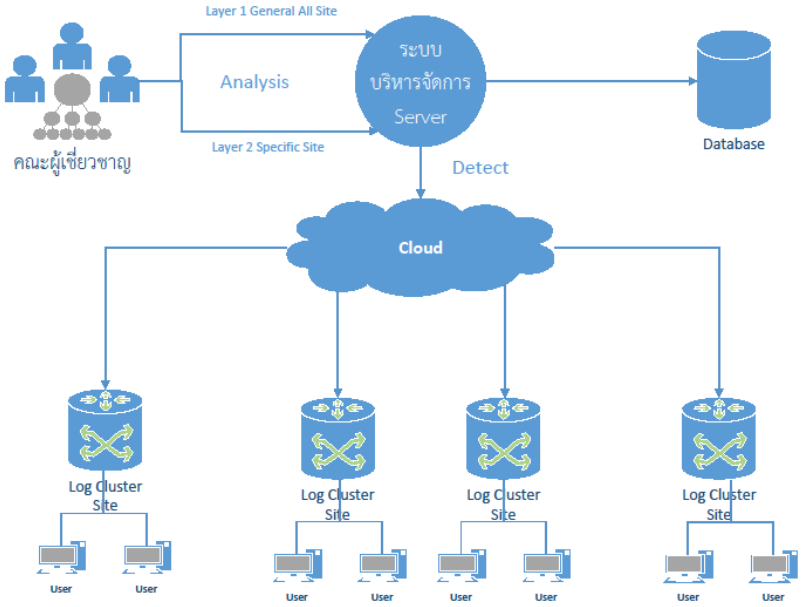
๑) สำรวจข้อมูลทางกายภาพของ อบต./เทศบาล เพื่อดำเนินการคัดเลือกติดตั้ง log Cluster จำนวนประมาณ ๓๐ แห่งทั่วประเทศ (๑ คลัสเตอร์ครอบคลุมพื้นที่โดยประมาณ ๒ – ๓ จังหวัด) โดยเน้นพื้นที่ ที่มีจำนวนประชากรประมาณไม่มากกว่า ๘,๐๐๐ คน หรือมีพื้นที่ประมาณไม่มากกว่า ๒๐๐ ตารางกิโลเมตรเป็นหลัก พร้อมดำเนินการติดตั้งอุปกรณ์ ใช้ระยะเวลาประมาณ ๒ – ๓ เดือน

๒) ประชุมสัมมนาและเผยแพร่ความรู้ พร้อมทั้งสร้างความเข้าใจในการดำเนินการป้องกันภัยคุกคามทางไซเบอร์ ให้แก่กลุ่มเป้าหมาย ใช้ระยะเวลา ประมาณ ๒ – ๓ เดือน

๓) พัฒนา และติดตั้งระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น ใช้ระยะเวลาประมาณ ๖ เดือน

๔) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตาม พรบ. คอมพิวเตอร์ให้จัดเก็บอย่างน้อย ๙๐ วัน เพื่อการเฝ้าระวังและคัดกรองข้อมูลเบื้องต้น (Monitor) โดยคณะทำงานผู้เชี่ยวชาญผู้มีใบรับรองตามมาตรฐานสากล พร้อมการวิเคราะห์ข้อมูลที่มีความเสี่ยงแล้วจัดเก็บเป็น Database อย่างน้อยไตรมาสละ ๑ ครั้ง

ทั้งนี้ ระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่นคาดว่าพร้อมใช้งานได้ภายในระยะเวลา ๖ เดือน



ระยะปีที่ ๒ สามารถแบ่งออกเป็นกิจกรรมหลักๆ ได้ ๒ กิจกรรม

๑) คณะทำงานผู้เชี่ยวชาญฯ วิเคราะห์ข้อมูล พร้อมแบ่งข้อมูลเป็น ๒ Layer ได้แก่ (๑) Layer ทั่วไป ได้แก่ การป้องกันทั่วไป ที่มีสถิติความเสี่ยงบ่อยในระยะที่ผ่านมาเพื่อป้องกันภัยคุกคามทางไซเบอร์ และ (๒) Layer เฉพาะเจาะจง ที่มีความเสี่ยงเป็นการเฉพาะพื้นที่ อาทิ เช่น จังหวัดชายแดนภาคใต้ที่อาจต้องการการป้องกันทางไซเบอร์เป็นการพิเศษ

๒) พัฒนาหลักสูตรเฝ้าระวังภัยคุกคามทางไซเบอร์ เทียบเท่ามาตรฐานสากล พร้อมทั้งพัฒนาบุคลากรขององค์กรให้มีความเชี่ยวชาญด้านป้องกันภัยคุกคามทางไซเบอร์ให้เทียบเท่ามาตรฐานสากล

๓) พัฒนาองค์กรสู่มาตรฐานด้านความปลอดภัยทางไซเบอร์ ISO/IEC ๒๗๐๐๑

ทั้งนี้ การพัฒนา**ต้นแบบจำลองระบบเครือข่ายเฝ้าระวังภัยคุกคามทางไซเบอร์เพื่อใช้เป็นเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์การปกครองส่วนท้องถิ่น** ด้านงบประมาณอาจแบ่งได้เป็นงบลงทุน (Investment Budget) ได้แก่ การพัฒนาระบบและอุปกรณ์ผู้วิจัยประเมินเบื้องต้นใช้งบประมาณไม่เกิน ๒๐ ล้านบาท โดยหน่วยงานอาจหางบประมาณสนับสนุนจากแหล่งทุนอื่น อาทิ เช่น กองทุนที่เกี่ยวข้อง และงบดำเนินการ (Operating Budget) ได้แก่ ค่าเช่า Cloud server ค่าใช้จ่ายรายเดือนอื่นๆ เห็นควรให้องค์การปกครองส่วนถิ่นร่วมรับผิดชอบ

๓. ด้านการพัฒนาบุคลากรสู่ความเป็นเลิศด้านความมั่นคงปลอดภัยทางไซเบอร์

การพัฒนาบุคลากรภายในองค์กรถือเป็นกระบวนการสำคัญยิ่งที่ต้องพัฒนาควบคู่ไปพร้อมกันระบบและองค์กร โดยการพัฒนาบุคลากรคำนึงถึงการกระตุ้นการสร้างความเข้าใจเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์ พร้อมกับการสร้างความกระตือรือล้นที่จะปฏิบัติงานด้านการแจ้งเตือนภัยและการรักษาความปลอดภัยเครือข่าย รวมไปถึงการรณรงค์เผยแพร่องค์ความรู้เบื้องต้นให้แก่ประชาชนในพื้นที่

การพัฒนาความรู้และทักษะที่จำเป็นในการดำเนินงานด้านการรักษาความปลอดภัยไซเบอร์โดยบุคลากรผู้ปฏิบัติงาน องค์การปกครองส่วนท้องถิ่นอาจจัดทำความร่วมมือร่วมกับองค์กรที่เกี่ยวข้องศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team) ฯลฯ ในการฝึกอบรมสัมมนาเพื่อพัฒนาบุคลากร โดยองค์การปกครองส่วนท้องถิ่นสามารถขอเข้ารับการอบรมเป็นหมู่คณะซึ่งในการอบรมมีทั้งการอบรมเพื่อผลิตผู้ปฏิบัติงานและการอบรมเพื่อผลิตผู้ฝึกอบรม

เนื่องจากองค์การปกครองส่วนท้องถิ่นมีบุคลากรเป็นจำนวนมาก เพื่อการพัฒนาบุคลากรด้านการรักษาความปลอดภัยไซเบอร์อย่างบูรณาการ ควรมีการจัดทำระบบฝึกอบรมออนไลน์ควบคู่ไปด้วย

จากข้อเสนอแนะที่กล่าวในข้างต้น แนวทางการศึกษาและพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในอนาคตควรมุ่งเน้นก้าวไปสู่ขั้นของการพัฒนาให้เกิดผลเป็นรูปธรรมใช้ประโยชน์ได้จริงในภูมิภาคท้องถิ่นที่มีความแตกต่างกันออกไป ซึ่งที่ผ่านมาการพัฒนานวัตกรรมของระบบสารสนเทศ ในหน่วยงานท้องถิ่นยึดมั่นกับรูปแบบการพัฒนาโดยอาศัยระบบบริหารราชการแผ่นดินส่วนกลาง อาทิ การนำเทคโนโลยีสารสนเทศมาใช้โดย มุ่งใช้กระบวนการส่งผ่านแผนปฏิบัติงาน ลักษณะของการส่งผ่านการสั่งการ (Command) จากส่วนกลางไปสู่องค์กรปกครองส่วนท้องถิ่นกว่าทั่วประเทศโดยเน้นไปที่พันธกิจเฉพาะบางด้าน เช่นการส่งเสริมระบบการจัดเก็บภาษีด้วยโปรแกรมแผนที่ภาษีและทะเบียนทรัพย์สิน จากกรมส่งเสริมการปกครองส่วนท้องถิ่น มุ่งเน้นให้บุคลากรส่วนงานด้านการจัดเก็บภาษีดำเนินการติดตั้งระบบและทำการบันทึกข้อมูล โดยยังขาดการบูรณาการเทคโนโลยีด้านความปลอดภัยทางไซเบอร์เข้าไปเป็นส่วนประกอบ อาจทำให้การพัฒนาระบบการจัดเก็บภาษีด้วยโปรแกรมแผนที่ภาษีขาดเสถียรภาพ จนถึงขั้นความสูญเสียของข้อมูล

ตัวอย่างการอบรม การจัดทำแผนที่ภาษี ณ อ.พยุหคีรี จังหวัดนครสวรรค์วันที่ 23 กันยายน 2559
ข้อมูลจากเว็บไซต์ องค์การบริหารส่วนจังหวัดนครสวรรค์
http://www.nakhonsawanpao.go.th/webboard1/index.php?topic=6814.0

การศึกษาและพัฒนาในอนาคต จึงควรมุ่งให้ความสำคัญกับการพัฒนาวิธีวิทยา (Methodology) บนข้อจำกัดของพื้นที่ทางวัฒนธรรมที่มีความแตกต่างหลากหลายความไม่เท่าเทียมกันของหน่วยงานท้องถิ่น ให้ความสำคัญกับการศึกษาโดยการแบ่งการศึกษาเป็นรายคลัสเตอร์ เพื่อเฉพาะเจาะจงให้เกิดรูปธรรมที่มีมิติชัดเจน โดยทั้งประเทศอาจแบ่งได้ประมาณ ๓๐ คลัสเตอร์

ข้อสรุปแนวทางการศึกษาการพัฒนาระบบเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ สำหรับองค์กรขนาดเล็กในระดับชุมชนได้เป็น ๓ ด้าน ตามแผนภาพ

แผนภาพแนวทางการศึกษาการพัฒนาระบบเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์

๒.๒ สถานภาพการดำเนินโครงการรายกิจกรรม

กิจกรรม	ระยะเวลา	สถานะกิจกรรม/ผลดำเนินงาน			แผนปฏิบัติการ ณ วันลงนามในสัญญา		ความก้าวหน้า โปรดทำเครื่องหมาย (✓)			กรณีล่าช้าหรือเร็วกว่าแผน	
		แล้วเสร็จ	อยู่ระหว่างดำเนินการ	ยังไม่ดำเนินการ	เริ่มต้น	สิ้นสุด	ล่าช้า	ตามแผน	เร็วกว่าแผน	เริ่มต้น	สิ้นสุด
1. นำเสนอรายงานแผนการดำเนินงาน	30 วัน	✓			20 ก.พ 60	20 มี.ค 60	-	✓			
1.1 รายงานแผนการดำเนินงาน (Project Plan)	30 วัน	✓			20 ก.พ 60	20 มี.ค 60	-	✓			
2. สำรวจการใช้งานระบบเทคโนโลยีสารสนเทศของท้องถิ่น	150 วัน			✓	23 มี.ค 60	19 ส.ค 60		✓			
2.1 กระจายแบบสำรวจให้ครอบคลุมตามระเบียบงานวิจัย	60 วัน			✓	23 มี.ค 60	31 พ.ค 60		✓			
2.2 สุ่มกลุ่มตัวอย่างสัมภาษณ์เชิงลึก	60 วัน	✓			23 มี.ค 60	31 พ.ค 60		✓			
2.3 รวบรวมแบบสอบถาม และสรุปผล	60 วัน	✓			23 มี.ค 60	31 พ.ค 60		✓			

กิจกรรม	ระยะเวลา	สถานะกิจกรรม/ผลดำเนินงาน			แผนปฏิบัติการ ณ วันลงนามในสัญญา		ความก้าวหน้า โปรดทำเครื่องหมาย (✓)			กรณีล่าช้าหรือเร็วกว่าแผน	
		แล้วเสร็จ	อยู่ระหว่างดำเนินการ	ยังไม่ดำเนินการ	เริ่มต้น	สิ้นสุด	ล่าช้า	ตามแผน	เร็วกว่าแผน	เริ่มต้น	สิ้นสุด
2.4 ศึกษาแนวทางแก้ปัญหา และศึกษาวิเคราะห์แบบจำลองระบบเครือข่ายความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน	60 วัน	✓			1 มิ.ย 60	31 ก.ค 60		✓			
2.5 นำเสนอรายงานผลการสำรวจและการศึกษาวิเคราะห์ พร้อมแนวทางการวิจัยพัฒนาระบบเครือข่ายความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน	30 วัน	✓			19 ก.ค 60	19 ส.ค 60		✓			
3. จัดเสวนาแลกเปลี่ยนเรียนรู้ เผยแพร่ และสร้างความตระหนักให้รู้เท่าทันภัยคุกคามทางไซเบอร์	60 วัน	✓			20 ส.ค 60	18 ต.ค 60		✓			
3.1 จัดทำหลักสูตร แนวทางการอบรม	10 วัน	✓			20 ส.ค 60	30 ส.ค 60		✓			
3.2 ส่งหนังสือเชิญหน่วยงานที่สนใจเข้าร่วมเสวนา/อบรม	10 วัน	✓			25 ส.ค 60	4 ก.ย 60		✓			

กิจกรรม	ระยะเวลา	สถานะกิจกรรม/ผลดำเนินงาน			แผนปฏิบัติการ ณ วันลงนามในสัญญา		ความก้าวหน้า โปรดทำเครื่องหมาย (✓)			กรณีล่าช้าหรือเร็วกว่าแผน	
		แล้วเสร็จ	อยู่ระหว่างดำเนินการ	ยังไม่ดำเนินการ	เริ่มต้น	สิ้นสุด	ล่าช้า	ตามแผน	เร็วกว่าแผน	เริ่มต้น	สิ้นสุด
3.3 จัดเตรียมความพร้อมสำหรับการอบรมและถ่ายทอดแนวทางในการสร้างมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับองค์กรให้กับผู้เข้าร่วมเสวนา/อบบรม	7 วัน	✓			4 ก.ย 60	11 ก.ย 60		✓			
3.4 อบรมและถ่ายทอดแนวทางในการสร้างมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับองค์กรให้กับผู้เข้าร่วมเสวนา/อบบรม	2 วัน	✓			12 ก.ย 60	15 ก.ย 60		✓			
3.5 ศึกษาแนวทางแก้ปัญหา และศึกษาวิเคราะห์แบบจำลองระบบเครือข่ายความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน	10 วัน	✓			16 ก.ย 60	26 ก.ย 60		✓			
3.6 จัดทำข้อเสนอแนะเชิงนโยบาย และเอกสารแนวทางในการพัฒนาอุปกรณ์ป้องกันภัยคุกคามข้อมูลสารสนเทศที่เหมาะสมกับองค์กรขนาดเล็กในระดับชุมชน	16 วัน	✓			27 ก.ย 60	12 ต.ค 60		✓			

กิจกรรม	ระยะเวลา	สถานะกิจกรรม/ผลดำเนินงาน			แผนปฏิบัติการ ณ วันลงนามในสัญญา		ความก้าวหน้า โปรดทำเครื่องหมาย (✓)			กรณีล่าช้าหรือเร็วกว่าแผน	
		แล้วเสร็จ	อยู่ระหว่างดำเนินการ	ยังไม่ดำเนินการ	เริ่มต้น	สิ้นสุด	ล่าช้า	ตามแผน	เร็วกว่าแผน	เริ่มต้น	สิ้นสุด
4. นำเสนอผลการดำเนินงานโครงการ	6 วัน	✓			13 ต.ค 60	18 ต.ค 60		✓			
4.1 สรุปผลการจัดเสวนาแลกเปลี่ยนเรียนรู้เผยแพร่ และสร้างความตระหนักรู้ภัยคุกคามทางไซเบอร์	5 วัน	✓			13 ต.ค 60	17 ต.ค 60		✓			
4.2 ข้อเสนอแนะเชิงนโยบายและผลการดำเนินโครงการ	5 วัน	✓			13 ต.ค 60	17 ต.ค 60		✓			
4.3 รายงานผลต่อ สำนักงานกสทช. และหน่วยงานที่เกี่ยวข้อง	1 วัน	✓			18 ต.ค 60	18 ต.ค 60		✓			

๒.๓ สรุปปัญหาและอุปสรรคที่เกิดขึ้นจากการดำเนินโครงการ ปัญหาและอุปสรรคที่เกิดขึ้นจากการดำเนินโครงการอาจเกิดขึ้นจากกระบวนการดำเนินงานที่ต้องอาศัยระยะเวลาในการประสานงานระหว่างหน่วยงานต่างๆ อาทิ เส้นทางเอกสารในการขอความร่วมมือเพื่อสำรวจเก็บข้อมูลและเสวนาที่ต้องใช้ระยะเวลาทำเส้นทางเพื่อส่งถึงผู้มีอำนาจในการสั่งการ วิธีแก้ไข สร้างเครือข่ายในการประสานงานในส่วนต่างๆกระจายเป็นภูมิภาคต่างๆจากประชาชนทั่วประเทศ

๒.๔ แผนการดำเนินงานในระยะต่อไป ไม่มี

๒.๕ รายงานการจัดซื้อครุภัณฑ์ในโครงการ (ถ้ามี)

๒.๕.๑ ครุภัณฑ์สำหรับการวิจัยและพัฒนาฯ

ลำดับ	รายการจัดซื้อครุภัณฑ์ (สำหรับการวิจัยและพัฒนาฯ)	วัน/เดือน/ปี	มูลค่า	เอกสารอ้างอิง
	ไม่มี			

๒.๕.๒ ครุภัณฑ์สำหรับการดำเนินโครงการ

ลำดับ	รายการจัดซื้อครุภัณฑ์ (สำหรับการวิจัยและพัฒนาฯ)	วัน/เดือน/ปี	มูลค่า	เอกสารอ้างอิง
	ไม่มี			

ส่วนที่ ๓ รายงานความก้าวหน้าทางการเงิน

๓.๑ รายงานสรุปการใช้จ่ายงบประมาณ

รายละเอียดค่าใช้จ่ายในโครงการ							
หมวดค่าใช้จ่าย	งบประมาณ	Q 1	Q 2	Q 3	รวม	คงเหลือ	ร้อยละการเบิกจ่าย
1. ค่าตอบแทนบุคลากร	1,000,000			✓	1,000,000	0	100
2. ค่าใช้สอย	1,614,300	✓	✓	✓	1,262,350	221,235	78.20
3. ค่าวัสดุ							
4. ค่าใช้จ่ายครุภัณฑ์							
5. ค่าบริหารจัดการ							
6. ค่าใช้จ่ายอื่นๆ (ขออนุมัติเบิกเงินและนำส่งเข้ามหาวิทยาลัย 5%)		✓	✓	✓	130,715	0	100
รวม	2,614,300				2,393,065	221,235	91.54

๓.๒ รายงานสรุปความก้าวหน้าทางการเงิน

จำนวนเงินทุนที่ได้รับและจำนวนเงินทุนคงเหลือ						
ประจำงวด	**มูลค่าตามสัญญา**	**วัน/เดือน/ปีที่ได้รับ**	**งบประมาณที่ได้รับจริง**	**ค่าใช้จ่าย**	**คงเหลือ**	**หมายเหตุ**
งวดที่ 1	784,290	24 พ.ค. 60	784,290	684,164.50	100,125.50	
งวดที่ 2	1,045,720	28 ก.ย. 60	1,045,720	669,686	476,159.50	
งวดที่ 3	784,290	รอการเบิกจ่าย	รอการเบิกจ่าย	1,039,214.50	221,235	รอการเบิกจ่าย
งวดที่ 4						
งวดที่ ฯลฯ						
งวดที่						
รวม	2,614,300		2,614,300	2,393,065	221,235	

(*หมายเหตุ: คณะผู้วิจัยอยู่ระหว่างการจัดทำรายงานทางการเงิน โดยผู้วิจัยจะดำเนินจัดส่งเพิ่มเติมอีกครั้งเมื่อแล้วเสร็จ

รายละเอียดการบันทึกบัญชีรับ จ่ายเงิน

แบบ กทปส.1

วันเดือนปี	เลขที่เอกสาร	รายการ	รับเงิน (บาท)	จ่ายเงิน (บาท)						เงินคงเหลือ (บาท)
				ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าครุภัณฑ์	ค่าใช้จ่ายอื่น	ค่าบริการโครงการ	
18 พ.ค. 60	เช็คเลขที่ 4173678	รับเงินจากกองทุนฯ งวดที่ 1	784,290.00							784,290.00
30 พ.ค. 60	เลขที่ วจก 1571	ขออนุมัติเบิกเงินและนำส่งเข้ามหาวิทยาลัย 5%						39,214.50		
22 ส.ค. 60	ใบเสร็จรับเงิน เลขที่ IVT17-0006	ค่าที่พักคณะทำงาน			212,650.00					
20 ก.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)	ค่าเช่าเหมารถ(นายประมาณ ศรีวิลัย)			50,000.00					
20 ก.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)	ค่าเช่าเหมารถ(นายอำนวย แสงจันทร์)			50,000.00					551,864.50
22 ก.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)	ค่าเช่าเหมารถ(นายประทีป ภิญญะโภชน์)			50,000.00					
5 ส.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)	ค่าเช่าเหมารถ(นายราเมศร์ มีสัมพันธ์)			50,000.00					
9 ส.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)	ค่าเช่าเหมารถ(นายสมภพ จุ๊สกุล)			50,000.00					
9 ส.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)	ค่าเช่าเหมารถ(นายภูริต กมลพรเกษม)			50,000.00					
										232,425.50

วันเดือนปี	เลขที่เอกสาร	รายการ	รับเงิน (บาท)	จ่ายเงิน (บาท)						เงินคงเหลือ (บาท)
				ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าครุภัณฑ์	ค่าใช้จ่ายอื่น	ค่าบริการโครงการ	
26 ก.ย. 60	เช็คเลขที่ 04173723	รับเงินจากกองทุนฯ งวดที่ 2	1,045,720.00							1,278,145.50
2 ต.ค. 60	เลขที่ วจก 2769	ขออนุมัติเบิกเงินและนำส่งเข้ามหาวิทยาลัย5%						52,286		
3 ต.ค. 60	ใบกำกับภาษี เลขที่ 7562	ค่าเช่าพื้นที่สำหรับการอบรม			21,200.00					
3 ต.ค. 60	ใบกำกับภาษี เลขที่ 7563	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,600.00					
3 ต.ค. 60	ใบกำกับภาษี เลขที่ 7564	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,600.00					
3 ต.ค. 60	ใบกำกับภาษี เลขที่ 7565	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,600.00					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 22	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 23	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 24	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 25	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 26	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 27	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 28	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 29	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 30	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 31	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 32	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 33	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 34	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 35	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 36	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 37	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 38	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 39	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 40	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 41	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					

26 ก.ย. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 42	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
2 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 43	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 22	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 23	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 24	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 25	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 26	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 27	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 28	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 29	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 30	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 31	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 32	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 33	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 34	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 35	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 36	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 37	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 38	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 39	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 40	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 41	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 42	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 43	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 44	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 45	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					

26 ก.ย. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 46	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
2 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 47	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 48	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 49	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 428 เลขที่ 50	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 1	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 2	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 3	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 4	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 5	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 6	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 7	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 8	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 9	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 10	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 11	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 12	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 13	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 14	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 15	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 16	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 17	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 18	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 19	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 20	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					
3 ต.ค. 60	ใบเสร็จรับเงิน เล่มที่ 429 เลขที่ 21	ค่าที่พักสำหรับผู้เข้าร่วมอบรม			1,200					

รายละเอียดการบันทึกบัญชีรับ จ่ายเงิน

แบบ กทปส.1

วันเดือนปี	เลขที่เอกสาร	รายการ	รับเงิน (บาท)	จ่ายเงิน (บาท)						เงินคงเหลือ (บาท)
				ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าครุภัณฑ์	ค่าใช้จ่ายอื่น	ค่าบริการโครงการ	
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)1	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)2	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)3	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)4	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)5	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)6	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)7	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)8	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)9	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)10	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)11	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)12	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)13	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)14	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)15	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)16	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)17	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)18	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)19	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)20	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)21	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)22	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)23	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)24	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					

รายละเอียดการบันทึกบัญชีรับ จ่ายเงิน

แบบ กทปส.1

วันเดือนปี	เลขที่เอกสาร	รายการ	รับเงิน (บาท)	จ่ายเงิน (บาท)						เงินคงเหลือ (บาท)
				ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าครุภัณฑ์	ค่าใช้จ่ายอื่น	ค่าบริการโครงการ	
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)25	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)26	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)27	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)28	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)29	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)30	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)31	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)32	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)33	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)34	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)35	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)36	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)37	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)38	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)33	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)34	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)35	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)36	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)37	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)38	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)39	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)40	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)41	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)42	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					

รายละเอียดการบันทึกบัญชีรับ จ่ายเงิน

แบบ กทปส.1

วันเดือนปี	เลขที่เอกสาร	รายการ	รับเงิน (บาท)	จ่ายเงิน (บาท)						เงินคงเหลือ (บาท)
				ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าครุภัณฑ์	ค่าใช้จ่ายอื่น	ค่าบริการโครงการ	
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)43	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)44	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)45	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)46	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)47	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)48	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)49	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)50	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)51	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)52	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)53	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)54	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)55	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)56	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)57	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)58	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)59	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)60	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)61	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)62	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)61	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)62	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)63	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)64	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					

รายละเอียดการบันทึกบัญชีรับ จ่ายเงิน

แบบ กทปส.1

วันเดือนปี	เลขที่เอกสาร	รายการ	รับเงิน (บาท)	จ่ายเงิน (บาท)						เงินคงเหลือ (บาท)
				ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าครุภัณฑ์	ค่าใช้จ่ายอื่น	ค่าบริการโครงการ	
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)65	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)66	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)67	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)68	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)69	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)70	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)71	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)72	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)73	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)74	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)75	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)76	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)77	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)78	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)79	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)80	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)81	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)82	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)83	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)84	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)85	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)86	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)87	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)88	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					

รายละเอียดการบันทึกบัญชีรับ จ่ายเงิน

แบบ กทปส.1

วันเดือนปี	เลขที่เอกสาร	รายการ	รับเงิน (บาท)	จ่ายเงิน (บาท)						เงินคงเหลือ (บาท)
				ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าครุภัณฑ์	ค่าใช้จ่ายอื่น	ค่าบริการโครงการ	
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)89	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)90	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)91	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)92	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)93	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)94	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)95	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)96	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)97	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)98	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)99	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)100	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)101	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)102	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)103	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)104	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)105	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)106	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)107	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)108	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)109	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)110	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)111	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)112	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					

รายละเอียดการบันทึกบัญชีรับ จ่ายเงิน

แบบ กทปส.1

วันเดือนปี	เลขที่เอกสาร	รายการ	รับเงิน (บาท)	จ่ายเงิน (บาท)						เงินคงเหลือ (บาท)
				ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าครุภัณฑ์	ค่าใช้จ่ายอื่น	ค่าบริการโครงการ	
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)113	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)114	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)115	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)116	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)117	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)118	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)119	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)120	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)121	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)122	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)123	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)124	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)125	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)126	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)127	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)128	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)129	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)130	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)131	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)132	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)133	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)134	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)135	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)136	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					

รายละเอียดการบันทึกบัญชีรับ จ่ายเงิน

แบบ กทปส.1

วันเดือนปี	เลขที่เอกสาร	รายการ	รับเงิน (บาท)	จ่ายเงิน (บาท)						เงินคงเหลือ (บาท)
				ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าครุภัณฑ์	ค่าใช้จ่ายอื่น	ค่าบริการโครงการ	
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)139	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)140	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)141	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)142	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)143	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)144	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)145	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)146	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)147	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)148	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					669,686.00
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)149	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบสำคัญรับเงิน FM-15/25(00)150	ค่าพาหนะสำหรับผู้เข้าร่วมอบรม			2,400					
3 ต.ค. 60	ใบเสร็จ เล่มที่ 09/เลขที่ 16	ค่าอาหารสำหรับผู้เข้าร่วมอบรม (200คน)			72,000.00					
3 ต.ค. 60	ใบเสร็จ เล่มที่ 09/เลขที่ 19	ค่าอาหารว่างสำหรับผู้เข้าร่วมอบรม (200คน)			28,000.00					
6 ก.ย.60	ใบเสร็จ เล่มที่ 010/เลขที่ 095	ค่าจัดทำรายงานงวดที่ 2			2,500.00					
15 ก.ย.60	ใบเสร็จ เล่มที่ 011/เลขที่ 015	ค่าจัดทำรายงานงวดที่ 2(แก้ไข)			2,500.00					
18 ก.ย.60	ใบเสร็จ เล่มที่ 011/เลขที่ 025	ค่าจัดทำรายงานงวดที่ 2(แก้ไข)			2,500.00					

รายละเอียดการบันทึกบัญชีรับ จ่ายเงิน

แบบ กทปส.1

วันเดือนปี	เลขที่เอกสาร	รายการ	รับเงิน (บาท)	จ่ายเงิน (บาท)						เงินคงเหลือ (บาท)
				ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าครุภัณฑ์	ค่าใช้จ่ายอื่น	ค่าบริการโครงการ	
18 ต.ค. 60	ใบเสร็จ เล่มที่ 011/เลขที่ 093	ค่าจัดทำรายงานงวดที่ 3			2,500.00					
7 พ.ย. 60	ใบเสร็จ เล่มที่ 012/เลขที่ 035	ค่าจัดทำรายงานงวดที่ 3(แก้ไข)			5,000.00					
4 ธ.ค. 60	ใบเสร็จ เล่มที่ 012/เลขที่ 065	ค่าจัดทำรายงานงวดที่ 3(แก้ไข)			5,000.00					
2 พ.ย. 60	ใบเสร็จ เลขที่ 002/2560	ค่าดำเนินการตรวจสอบความ			25,000.00					
		ถูกต้องของค่าใช้จ่ายของโครงการ								476,159.50
.....	เช็คเลขที่	รับเงินจากกองทุนฯ งวดที่ 3	784,290.00					39,214.50		1,260,449.50
	ใบเสร็จ เล่มที่...../เลขที่	ขออนุมัติเบิกเงินและนำส่งเข้า								
	(รอการเบิกจ่าย)	มหาวิทยาลัย 5%		240,000						
	ใบสำคัญรับเงิน FM-15/25(00)	ค่าตอบแทนหัวหน้าโครงการ		200,000						
	ใบสำคัญรับเงิน FM-15/25(00)	ค่าตอบแทนนักวิจัย		200,000						
	ใบสำคัญรับเงิน FM-15/25(00)	ค่าตอบแทนนักวิจัย		240,000						1,039,214.50
	ใบสำคัญรับเงิน FM-15/25(00)	ค่าตอบแทนผู้ช่วยนักวิจัย		120,000						
	ใบสำคัญรับเงิน FM-15/25(00)	ค่าตอบแทนผู้ประสานงาน								
		รวมหน้า 1 ถึงหน้า 9	2,614,300.00	1,000,000.00	1,262,350.00			130,715.00		221,235

ลงลายมือชื่อ.....

(นายสมทบ แก้วเชื้อ)

ตำแหน่ง หัวหน้าโครงการ

วันที่ 18 ตุลาคม 2560