



รายงานการศึกษาส่วนบุคคล  
(Individual Study)

เรื่อง การยกระดับการรักษาความมั่นคงปลอดภัย  
ด้านสารสนเทศขององค์กร

จัดทำโดย นางสาวสิริกานต์ มหาสิทธิ์ระกุล  
รหัส 89018

รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม  
หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 89  
วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.  
ประจำปี 2562  
ลิขสิทธิ์ของสำนักงาน ก.พ.



รายงานการศึกษาส่วนบุคคล  
(Individual Study)

เรื่อง การยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ  
ขององค์กร

จัดทำโดย นางสาวสิริกานต์ มหาสิทธิ์ระกูล  
รหัส 89018

หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 89  
วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.  
ประจำปี 2562

รายงานนี้เป็นความคิดเห็นเฉพาะบุคคลของผู้ศึกษา



(หน้าอนุมัติ)  
สำนักงาน ก.พ.

เอกสารรายงานการศึกษาส่วนบุคคลนี้ อนุมัติให้เป็นส่วนหนึ่งของการฝึกอบรม  
หลักสูตรนักรับบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรมของสำนักงาน ก.พ.

ลงชื่อ .....  
( ..... )  
อาจารย์ที่ปรึกษา

ลงชื่อ .....  
( ..... )  
อาจารย์ที่ปรึกษา

ลงชื่อ .....  
( ..... )  
อาจารย์ที่ปรึกษา

ลงชื่อ .....  
( ..... )  
อาจารย์ที่ปรึกษา

## บทสรุปสำหรับผู้บริหาร

ทิศทางการพัฒนาประเทศไทยตามวิสัยทัศน์ คือ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามปรัชญาของเศรษฐกิจพอเพียง” และเพื่อให้บรรลุวิสัยทัศน์ดังกล่าว รัฐบาลจึงมีนโยบายที่จะใช้โมเดลขับเคลื่อนเศรษฐกิจด้วยนวัตกรรมเพื่อพัฒนาประเทศไปสู่การเป็นประเทศไทย 4.0 ดังนั้น รัฐบาลจึงต้องมีการเปลี่ยนแปลงขนานใหญ่ ให้สอดคล้องกับบริบทไปสู่การเป็นประเทศไทย 4.0 ที่สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรต่างๆ โดยมุ่งเน้นการพัฒนาระยะยาวที่สอดคล้องกับการจัดทำยุทธศาสตร์ชาติ ระยะ 20 ปี แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 โดยได้กำหนดแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2560 – 2564 เพื่อยกระดับภาครัฐสู่การเป็นรัฐบาลดิจิทัลที่มีการบูรณาการระหว่างหน่วยงาน มีการทำงานแบบอัจฉริยะ และขับเคลื่อนให้เกิดการเปลี่ยนแปลงได้อย่างแท้จริง โดยการนำเทคโนโลยีดิจิทัลมาบริหารจัดการให้เข้าสู่ระบบราชการ 4.0 (Government 4.0 หรือ Gov. 4.0) ซึ่งเป็นฟันเฟืองและเสาหลักที่สำคัญในการขับเคลื่อนนโยบายของรัฐบาลให้สามารถปฏิบัติงานได้อย่างสอดคล้องกับทิศทางการบริหารงานของประเทศให้ก้าวสู่การเป็นประเทศที่พัฒนาแล้ว เพื่อส่งผลให้ระบบราชการมีการพัฒนาและปรับตัวต่อความท้าทายใหม่ๆ อีกทั้งเป็นการเพิ่มศักยภาพในการแข่งขันกับนานาประเทศ และยังเป็นการยกระดับสมรรถนะของหน่วยงานภาครัฐให้มีประสิทธิภาพมากยิ่งขึ้น โดยทุกส่วนราชการมีการจัดทำแผนยุทธศาสตร์รองรับนโยบายดังกล่าว

อย่างไรก็ตาม ความก้าวหน้าด้านเทคโนโลยียังมีจุดอ่อนเรื่องปัญหาความมั่นคงปลอดภัยของระบบสารสนเทศที่มีความสำคัญและต้องตระหนักถึงอย่างยิ่ง อีกทั้งจุดอ่อนเหล่านี้มีแนวโน้มที่จะส่งผลกระทบต่อการดำเนินงานในรูปของข้อมูลอิเล็กทรอนิกส์เพิ่มมากขึ้นอย่างต่อเนื่อง ทั้งนี้ การดำเนินการตามยุทธศาสตร์ชาติ ระยะ 20 ปี ด้านความมั่นคง ได้กำหนดให้มีการแก้ไขปัญหาความมั่นคงในปัจจุบัน เพื่อให้ปัญหาเดิมที่มีอยู่ได้รับการแก้ไขอย่างจริงจัง จนยุติลง หรือไม่ส่งผลกระทบต่อประเทศชาติ รวมทั้งให้การบริหารและการพัฒนาบ้านเมืองเดินไปด้วยกันอย่างมีประสิทธิภาพ โดยผลักดันการวิเคราะห์สาเหตุที่แท้จริงของปัญหาทุกภาคส่วนในทุกประเด็นอย่างเป็นระบบด้วยการผนึกกำลังคน และทรัพยากรให้มีส่วนร่วมแบบบูรณาการอย่างแท้จริงในการส่งเสริม หรือ วางแผน และยกระดับวิธีการแก้ไขปัญหา รวมถึงการเสริมสร้างความร่วมมือกันระหว่างหน่วยงานหลักและรองในการป้องกันและแก้ไขปัญหาจากภัยคุกคามรวมทั้งปัญหาที่ส่งผลกระทบต่อความมั่นคงต่างๆ เช่น อาชญากรรมทางไซเบอร์ เป็นต้น ที่จะส่งผลกระทบต่อความมั่นคงของชาติ และส่งผลกระทบต่อในการดำเนินการตามนโยบาย ยุทธศาสตร์ระดับต่างๆ รวมทั้งโครงการสำคัญของประเทศเพื่อให้บรรลุผลสำเร็จตามเป้าหมายที่กำหนดอย่างมีประสิทธิภาพ

ในขณะที่เทคโนโลยีสารสนเทศมีความก้าวหน้าอย่างรวดเร็ว และเป็นที่สนใจใช้งานจากทั่วทุกสาขาและทุกมุมโลก จึงมีมีจอาชีพที่จ้องฉวยโอกาสลักลอบนำข้อมูลสารสนเทศต่างๆ มาใช้ประโยชน์ส่วนตน ดังนั้น ระบบเทคโนโลยีสารสนเทศทุกระบบของภาครัฐจึงจำเป็นต้องมีการรักษาความปลอดภัยอย่างเข้มงวด รวมทั้งการรับ-ส่งข้อมูลในระบบสารสนเทศของกระทรวงการคลังที่มีภารกิจหลักที่สำคัญอย่างยิ่งในการหารายได้ให้รัฐบาลเพื่อนำมาบริหารประเทศ และสำนักงานปลัดกระทรวงการคลังซึ่งเป็นส่วนราชการในสังกัดของกระทรวงการคลังที่มีภารกิจหลักในการเป็นศูนย์กลางการบริหารงานของกระทรวงการคลัง และปัจจุบันยังมีการสื่อสารข้อมูลราชการทั้งการใช้บริการจดหมายอิเล็กทรอนิกส์ที่ให้บริการโดยไม่เรียกเก็บค่าธรรมเนียม (Free e-mail) และในเครือข่ายสังคมออนไลน์ (Social Network) ที่จัดทำขึ้น

โดยบริษัทเอกชนของต่างประเทศ ซึ่งมีผลเสียหายต่อประเทศไทยหากบริษัทเอกชนเหล่านั้นนำข้อมูลทางจรรยาบรรณของการสื่อสารกันมาวิเคราะห์เพื่อวัตถุประสงค์อื่นๆ ในด้านที่มีขอบ รวมถึงการสอดแนมเอกสารที่ทางราชการใช้ดำเนินงานภายในหน่วยงานทั้งหลาย และที่ยังอยู่ในฐานะปกปิดจนกว่าจะได้รับอนุมัติตลอดจนเอกสารที่ต้องปิดเป็นความลับ เช่น การปรับอัตราภาษี การยกเว้นภาษี หรือเอกสารเกี่ยวกับการจัดซื้อจัดจ้าง เป็นต้น ดังนั้น จึงเป็นความท้าทายที่ต้องดำเนินการพัฒนาและบริหารจัดการทรัพยากรที่มีอยู่ กฎหมายหลักเกณฑ์การปฏิบัติที่เกี่ยวข้อง และบุคลากรผู้นำไปปฏิบัติอย่างเคร่งครัด ทั้งในส่วนที่ต้องกระทำและงดเว้นการกระทำให้เกิดประโยชน์สูงสุดเพื่อขจัดปัญหาเหล่านี้ให้เป็นที่ยุติ ซึ่งผู้จัดทำรายงานได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการใช้งานคอมพิวเตอร์และใช้งานอินเทอร์เน็ตในส่วนที่เกี่ยวข้องกับการรับ-ส่งข้อมูลอิเล็กทรอนิกส์และในเครือข่ายสังคมออนไลน์ของหน่วยงานของทุกส่วนราชการในสังกัดกระทรวงการคลัง จึงมีความมุ่งมั่นในการแก้ไขปัญหาและพัฒนาการดำเนินการด้านการสื่อสารในระบบเทคโนโลยีสารสนเทศพร้อมทั้งขอเสนอแนวทางการดำเนินการเรื่อง “การยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร” เพื่อให้เอกสารราชการในระบบสารสนเทศมีความมั่นคงปลอดภัยสูงสุด เป็นไปตามกฎหมาย แนวนโยบาย และแนวปฏิบัติที่เกี่ยวข้องโดยใช้กรอบความคิดของทฤษฎีการบริหาร 4 M ในการวิเคราะห์เพื่อให้เกิดผลสำเร็จในการดำเนินการ ประกอบด้วย 1) Material : ช่องทางการรับ-ส่งข้อมูลสารสนเทศของทางราชการ 2) Man : เจ้าหน้าที่ของรัฐ 3) Money : งบประมาณ และ 4) Management : วิธีบริหารจัดการสามารถสรุปแนวทางในการแก้ไขปัญหาหรือพัฒนางาน ได้ดังนี้

**แนวทางในการแก้ไขปัญหาหรือพัฒนางานเรื่อง “การยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร”**

**1. Material : แนวทางการแก้ไขปัญหาหรือการพัฒนาช่องทางการรับ-ส่งข้อมูลสารสนเทศของหน่วยงานภาครัฐ** ประกอบด้วย 2 ช่องทาง ดังนี้

### **1.1 การรับ-ส่งข้อมูลราชการทางระบบอิเล็กทรอนิกส์**

#### **1.1.1 การใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ (e-mail)**

การรับ-ส่งข้อมูลทางระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นเรื่องพื้นฐานที่ทุกคนสามารถดำเนินการได้อย่างคล่องแคล่วและเป็นปกติทั้งในรูปแบบส่วนบุคคลและงานราชการ และเนื่องจากทุกส่วนราชการในประเทศไทยมีเว็บไซต์ของส่วนราชการอยู่แล้ว ซึ่งแต่ละเว็บไซต์จะมีระบบจดหมายอิเล็กทรอนิกส์ให้บริการแก่บุคลากรในสังกัด โดยการติดต่อขอลงทะเบียนใช้งานได้ที่หน่วยงานที่ทำหน้าที่เป็นศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของแต่ละส่วนราชการ ทั้งนี้ ผู้ขอใช้จดหมายอิเล็กทรอนิกส์จะต้องให้ความยินยอมตามเงื่อนไขการรักษาความมั่นคงปลอดภัยในการสื่อสารด้วยระบบสารสนเทศตามที่หน่วยงานกำหนด หรืออาจขอให้ผู้ดูแลระบบของหน่วยงานประสานขอใช้บริการระบบจดหมายอิเล็กทรอนิกส์กลาง mail.go.th ได้จากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)

#### **1.1.2 การใช้โปรแกรม IP Messenger (IPMsg)**

โปรแกรม IP Messenger เป็นโปรแกรมที่ใช้กับเครื่องคอมพิวเตอร์ผ่านหมายเลขประจำเครื่องคอมพิวเตอร์ที่ระบุตัวตนของเครื่องคอมพิวเตอร์แต่ละเครื่องที่เชื่อมต่ออยู่บนเครือข่ายหรือที่เรียกว่า IP Address (Internet Protocol Address) ซึ่งบุคลากรในสังกัดสำนักงานปลัดกระทรวงการคลังมีเครื่องคอมพิวเตอร์ใช้ประจำทุกคน โปรแกรม IP Messenger สามารถดาวน์โหลดได้จากอินเทอร์เน็ตโดยไม่มีค่าใช้จ่ายใดๆ (Free Download) รวมทั้งสามารถรับ-ส่งไฟล์และโพลเดอร์ได้ด้วย

ระบบ LAN แบบ Pop up และตัวโปรแกรมไม่ต้องอาศัยแม่ข่าย (Server) เป็นตัวกลาง นอกจากนี้ยังใช้เป็นโปรแกรมสนทนา (Chat) ได้ต่อกันกับปลายทางในระบบ LAN หรือเครือข่ายส่วนตัวได้อีกช่องทางหนึ่งอย่างสะดวก รวดเร็ว เนื่องจากโปรแกรมมีขนาดเล็ก กะทัดรัด เบาล่งต่อการใช้งาน และไม่ต้องการเบราว์เซอร์ (Browser) รวมทั้งสามารถเข้ารหัสข้อความ (Encryption) เพื่อป้องกันข้อมูลหรือข้อความตั้งต้นที่ต้องการส่งไปถึงผู้รับได้อีกด้วย

ในส่วนของผู้ดูแลระบบคอมพิวเตอร์ จะใช้โปรแกรม IP Messenger ในการสื่อสารหรือทดสอบการทำงานของคอมพิวเตอร์ว่าสามารถสื่อสารถึงกันได้หรือไม่ รวมทั้งประยุกต์การใช้งานสื่อสารกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร ซึ่งสามารถควบคุมจำนวนอุปกรณ์คอมพิวเตอร์ และการเปลี่ยนค่า IP Address ได้อย่างแม่นยำ

## 1.2 การสื่อสารในเครือข่ายสังคมออนไลน์ (Social Network)

แอปพลิเคชัน G-Chat เป็นช่องทางการสื่อสารในเครือข่ายสังคมออนไลน์ภาครัฐที่มีความปลอดภัยสูงสุดในระดับสากล จัดทำโดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ที่ได้พัฒนา G-Chat ขึ้นเพื่อใช้เป็นระบบติดต่อสื่อสารแบบออนไลน์สำหรับหน่วยงานภาครัฐผ่านอุปกรณ์สื่อสารแบบเคลื่อนที่ เพื่อความมั่นคงปลอดภัยของข้อมูล ซึ่งมีความคล้ายคลึงกับแอปพลิเคชัน LINE ใช้งานง่าย แทบจะไม่ต้องเรียนรู้อะไรใหม่ จึงแนะนำให้ทุกหน่วยงานในภาครัฐใช้ G-Chat แทนแอปพลิเคชัน LINE หรือแอปพลิเคชันสนทนาอื่นๆ (chat) โดยแยกการสนทนาเรื่องส่วนตัวกับเรื่องงานที่มีความสำคัญออกจากกันเพื่อให้มั่นใจว่าข้อมูลที่สนทนาหรือส่งไฟล์ราชการถึงกันมีความปลอดภัย ซึ่งปัจจุบัน สพร. อยู่ระหว่างพัฒนาแอปพลิเคชันจาก version 1 เป็น version 2 โดยเมื่อดำเนินการแล้วเสร็จจะได้มีหนังสือเชิญชวนหน่วยงานราชการต่างๆ เพื่อให้สื่อสารในเครือข่ายสังคมออนไลน์ด้วยแอปพลิเคชันดังกล่าวต่อไป

## 2. Man : แนวทางการแก้ปัญหาหรือพัฒนาบุคลากรด้านการสื่อสารในระบบเทคโนโลยีสารสนเทศ

ในส่วนของ การวิเคราะห์ SWOT Analysis ด้านจุดอ่อน พบว่าในภาพรวมบุคลากรของสำนักงานปลัดกระทรวงการคลังยังมีความคิดริเริ่มสร้างสรรค์ การทำงานในเชิงรุก การประสานงาน และการถ่ายทอดความรู้ รวมทั้งการประชาสัมพันธ์บทบาทหน้าที่และงานขององค์กรไม่เพียงพอ ดังนั้น ในส่วนของ การสื่อสารในระบบเทคโนโลยีสารสนเทศจึงต้องมีการแก้ไขปัญหาเหล่านี้โดยการพัฒนาองค์ความรู้ของบุคลากรเพื่อให้มีความตระหนักรู้เท่าทันภัยคุกคามจากการใช้ระบบสารสนเทศและอินเทอร์เน็ต รวมทั้งมีความรู้ความเข้าใจและดำเนินการป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ ทั้งในส่วนที่ต้องกระทำและงดเว้นการกระทำ ซึ่งในปีงบประมาณ พ.ศ. 2562 สำนักงานปลัดกระทรวงการคลัง ได้จัดให้มีการฝึกอบรมในทักษะด้านความเข้าใจและการใช้เทคโนโลยีดิจิทัลของบุคลากรภาครัฐ ตามที่สำนักงานคณะกรรมการข้าราชการพลเรือน (สำนักงาน ก.พ.) ได้มีแนวทางพัฒนาทักษะด้านดิจิทัลของข้าราชการและบุคลากรภาครัฐในมิติที่ 1 รู้เท่าทันและใช้เทคโนโลยีเป็น (Digital Literacy) อย่างไรก็ตาม ในรายละเอียดหลักสูตรยังมิได้บรรจุเรื่อง การใช้งานเพื่อความปลอดภัย และการใช้ดิจิทัลเพื่อความปลอดภัยไว้แต่ประการใด ซึ่งในเบื้องต้นผู้จัดทำรายงานจะได้ประสานหน่วยงานรับผิดชอบหลักสูตร ให้บรรจุเรื่องดังกล่าวไว้ในหลักสูตรต่อไป

## 3. Money : งบประมาณ

การใช้เครื่องมือดังกล่าวตามข้อ 1 ไม่ต้องใช้เงินงบประมาณแต่ประการใด

#### 4. Management : แนวทางการแก้ปัญหาหรือพัฒนานโยบายด้านกฎหมาย ระเบียบ และแนวทางการปฏิบัติที่เกี่ยวข้อง

สืบเนื่องจากได้มีประกาศสำนักงานปลัดกระทรวงการคลัง เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง พ.ศ. 2559 ซึ่งมีข้อกำหนดเกี่ยวกับแนวทางการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจนแล้ว อย่างไรก็ตามในการนำแนวนโยบายดังกล่าวไปปฏิบัติยังสร้างความตระหนักแก่ผู้ใช้งานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (information security awareness) ไม่เข้มข้นและจริงจังเท่าที่ควรตามที่ได้กำหนดไว้ในประกาศฯ ดังนั้น ผู้บริหารระดับสูง และหน่วยงานรับผิดชอบจึงควรมีการบังคับใช้ประกาศฯ ดังกล่าวอย่างเคร่งครัด และต่อเนื่อง เพื่อมิให้การใช้งานระบบสารสนเทศทั้งในระดับนโยบายและระดับปฏิบัติในการควบคุมการใช้งานระบบคอมพิวเตอร์และสินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ เป็นต้น อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

#### ปัจจัยที่อาจมีผลกระทบต่อความสำเร็จของการดำเนินการตามข้อเสนอ และแนวทางการบริหารจัดการที่เป็นรูปธรรม

จากการนำเสนอแนวทางในการแก้ไขปัญหาหรือพัฒนานโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศดังกล่าวข้างต้น มีปัจจัยด้านบุคลากร (Man) ที่มีความเสี่ยงเพียงด้านเดียวที่อาจเกิดผลกระทบจากความรู้เท่าไม่ถึงการณ์ของบุคลากรในการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยเห็นว่าเป็นเรื่องไม่สำคัญ จึงไม่ให้ความร่วมมือในการดำเนินการเท่าที่ควร

ดังนั้น ผู้บริหารระดับสูงจึงควรมีการบริหารจัดการที่เป็นรูปธรรมเพื่อขจัดปัญหาดังกล่าวให้เป็นที่ยุติโดยเร็ว โดยดำเนินการมอบนโยบายและกำกับให้บุคลากรในสังกัดรวมทั้งหน่วยงานรับผิดชอบให้ดำเนินการเป็นกลไกในการบังคับใช้กฎหมาย และแนวนโยบายต่างๆ อย่างเคร่งครัด รวมถึงตลอดถึงผู้ใช้งานเพื่อให้เข้ารับการฝึกอบรมด้านคอมพิวเตอร์ และจะต้องศึกษาแนวนโยบายตามประกาศสำนักงานปลัดกระทรวงการคลัง เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง พ.ศ. 2559 จนเกิดความเข้าใจสามารถนำไปปฏิบัติเป็นเรื่องปกติได้อย่างขึ้นใจ และจริงจัง โดยต้องมีการวัดผลการเรียนการสอนเป็นระยะๆ อย่างต่อเนื่อง จนสามารถตระหนักถึงคุณค่าและความสำคัญและจำเป็นที่จะต้องมีการใช้เครื่องมือต่างๆ ของภาครัฐในการสื่อสารด้วยระบบสารสนเทศ ซึ่งเป็นการส่งเสริมและพัฒนาระบบราชการให้มีการปรับตัวต่อความท้าทายใหม่ๆ โดยใช้เทคโนโลยีสารสนเทศเป็นหลัก รวมทั้งให้คนและทรัพยากรมีส่วนร่วมแบบบูรณาการอย่างแท้จริงในการยกระดับวิธีการแก้ไขปัญหา

การดำเนินการที่กล่าวข้างต้น อยู่ในความรับผิดชอบของผู้ช่วยปลัดกระทรวงการคลังในการช่วยปลัดกระทรวงการคลังแปลงนโยบายชาติและนโยบายรัฐบาล ความคาดหวัง และเป้าหมายความสำเร็จในระดับประเทศที่เน้นการมีส่วนร่วมในการวางแผน บริหารจัดการและบูรณาการร่วมมือกับบุคลากรในสังกัดสำนักงานปลัดกระทรวงการคลัง โดยการปรับปรุงแนวทาง มาตรฐาน ระบบงาน หลักเกณฑ์และวิธีปฏิบัติต่างๆ เพื่อการยกระดับการรักษาความมั่นคงปลอดภัยของการสื่อสารในระบบสารสนเทศได้อย่างมีศักยภาพ ซึ่งเป็นการ “ทำน้อยได้มาก” เนื่องจากเป็นการบริหารจัดการทรัพยากรที่มีอยู่แล้วให้เกิดประโยชน์สูงสุดโดยไม่มีค่าใช้จ่ายแต่ประการใด ทั้งนี้ เพื่อให้การปฏิบัติราชการที่มีประสิทธิภาพและประสิทธิผลทันต่อการเปลี่ยนแปลง และเมื่อประสบความสำเร็จแล้ว จะขยายขอบเขตการบริหารจัดการไปยังส่วนราชการในสังกัดกระทรวงการคลังทุกแห่ง รวมทั้งรัฐวิสาหกิจในกำกับ ซึ่งกระทรวงการคลังจะเป็นองค์กรต้นแบบการสร้างการเปลี่ยนแปลงให้กับหน่วยงานทั้งประเทศต่อไป

## กิตติกรรมประกาศ

รายงานการศึกษาส่วนบุคคล เรื่อง การยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร เป็นส่วนหนึ่งของการฝึกอบรมหลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 89 วิทยาลัยนักบริหาร สำนักงานคณะกรรมการข้าราชการพลเรือน (สำนักงาน ก.พ.) ประจำปี 2562 เพื่อให้ผู้เข้ารับการอบรมได้นำประสบการณ์จากการปฏิบัติงานจริงมาศึกษาวิเคราะห์ประกอบแนวคิด ทฤษฎีการบริหารในการพัฒนาองค์กร โดยให้ผู้เข้ารับการอบรมมีโอกาสพัฒนาความรู้ ความสามารถ ทักษะ และต่อยอดประสบการณ์การแลกเปลี่ยนเรียนรู้จากคณาจารย์ผู้ทรงคุณวุฒิ เพื่อให้เป็นผู้บริหารที่มีวิสัยทัศน์และคุณธรรม

รายงานการศึกษาส่วนบุคคลนี้สำเร็จสมบูรณ์ได้ด้วยดีโดยได้รับความกรุณาในการให้คำแนะนำทางวิชาการ และชี้แนะแนวทางการจัดทำรายงานจากท่านอาจารย์ที่ปรึกษา ดร.วิฑูรย์ สิมะโชคดี อดีตปลัดกระทรวงอุตสาหกรรม คณาจารย์ผู้ทรงคุณวุฒิ รวมทั้งการสนับสนุนข้อมูลด้านนวัตกรรมจาก นายกิตติพงษ์ อภิชัยชาญกิจ รองผู้อำนวยการการประปานครหลวง (ด้านเทคโนโลยีสารสนเทศ) นายมานิต ปานเอม ผู้เชี่ยวชาญการประปานครหลวง ซึ่งเป็นผู้เข้ารับการอบรมในหลักสูตรนี้ และนายบรรพต จันทร์หอม ผู้อำนวยการกองบริหารเครือข่ายสื่อสารและความมั่นคงสารสนเทศ การประปานครหลวง ณ โอกาสนี้ จึงขอขอบพระคุณท่านอาจารย์ที่ปรึกษา คณาจารย์ผู้ทรงคุณวุฒิ และผู้ให้การสนับสนุนด้านวิชาการทุกท่าน ที่ทำให้รายงานฉบับนี้มีความสมบูรณ์ยิ่งขึ้นจนสามารถนำไปใช้ในการแก้ไขปัญหาและพัฒนางานด้านเทคโนโลยีและสารสนเทศภาครัฐให้เกิดประโยชน์ต่อไป รวมทั้งขอขอบคุณผู้เข้ารับการอบรมที่ให้ความสนใจและมีเมตตาริจิตที่ดีต่อกันตลอดระยะเวลาการอบรมครั้งนี้ ตลอดจนเจ้าหน้าที่ของสำนักงาน ก.พ. และสถาบันบัณฑิตพัฒนบริหารศาสตร์ ที่ได้อำนวยความสะดวกด้านต่างๆ ในหลักสูตรนี้

สิริกานต์ มหาสิทธิ์ระกูล

พฤษภาคม 2562



## สารบัญ

บทสรุปสำหรับผู้บริหาร	ก
กิตติกรรมประกาศ	จ
สารบัญ	ฉ
สารบัญตาราง	ช
สารบัญภาพ	ซ
1. วิสัยทัศน์ของตำแหน่งเป้าหมาย	1
1.1 การวิเคราะห์บริบทและทิศทางเชิงยุทธศาสตร์ของส่วนราชการ	1
1.2 ตำแหน่งผู้ช่วยปลัดกระทรวงที่เป็นเป้าหมาย	2
1.3 กำหนดวิสัยทัศน์ของตำแหน่งเป้าหมาย	4
2. ข้อเสนอโครงการพัฒนางาน	6
2.1 การกำหนดประเด็นการศึกษา	6
2.2 การกำหนดข้อเสนอเชิงนโยบาย	10
2.3 ภาวะผู้นำเพื่อการขับเคลื่อนข้อเสนอ	30
3. แผนพัฒนาตนเอง	32
3.1 การวิเคราะห์ตนเอง	32
3.2 การวางแผนพัฒนาตนเอง	33
บรรณานุกรม	43
ประวัติผู้เขียนรายงานการศึกษาส่วนบุคคล	44

## สารบัญตาราง

ตารางที่ 1	การเชื่อมโยงประเด็นตามกรอบยุทธศาสตร์ชาติ ระยะ 20 ปี แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 กับยุทธศาสตร์กระทรวงการคลัง และยุทธศาสตร์สำนักงานปลัดกระทรวงการคลัง ในส่วนที่เกี่ยวข้องกับรายงานการศึกษาส่วนบุคคล	1
ตารางที่ 2	ชื่อเว็บไซต์และชื่อจดหมายอิเล็กทรอนิกส์แยกตามประเภทขององค์กรในประเทศไทย	11
ตารางที่ 3	ข้อมูลที่น่ามาวิเคราะห์สถานการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง	13
ตารางที่ 4	ข้อดีและข้อจำกัดของจดหมายอิเล็กทรอนิกส์ (e-mail)	17
ตารางที่ 5	ขั้นตอนการตรวจสอบ IP Address	18
ตารางที่ 6	ขั้นตอนการใช้งานโปรแกรม IP Messenger (IPMsg) ผ่าน IP Address	21
ตารางที่ 7	ความเป็นมาและการใช้งานแอปพลิเคชัน G-Chat	24
ตารางที่ 8	หลักสูตรการฝึกอบรมวิชาการด้าน Digital Literacy ประจำปีงบประมาณ พ.ศ. 2562 ของกระทรวงการคลัง	27
ตารางที่ 9	การวิเคราะห์ผลกระทบต่อความสำเร็จของการดำเนินการตามข้อเสนอแนะและแนวทางการจัดการที่เป็นรูปธรรม	29
ตารางที่ 10	สมรรถนะที่จำเป็นต้องใช้ในการปฏิบัติหน้าที่ในตำแหน่งผู้ช่วยปลัดกระทรวงการคลังในการดำเนินการตามรายงานผลการศึกษาและที่ต้องปรับปรุงตามรายงานผลการประเมินสมรรถนะ และประเด็นที่ต้องการพัฒนาหรือจำเป็นต้องพัฒนาในช่วงระยะเวลาไม่เกิน 2 ปี	32

## สารบัญภาพ

ภาพที่ 1	แสดงสัญลักษณ์ของโปรแกรม IP Messenger (IPMsg)	20
ภาพที่ 2	แสดงสัญลักษณ์ของแอปพลิเคชัน G-Chat	24

1. วิสัยทัศน์ของตำแหน่งเป้าหมาย

(ข้อมูลส่วนบุคคล ไม่เผยแพร่)

## 2. ข้อเสนอโครงการพัฒนางาน การยกระดับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

### 2.1 การกำหนดประเด็นการศึกษา

#### 2.1.1 ปัญหา ความท้าทาย หรือการพัฒนา ที่เลือกศึกษา

ตามที่กล่าวไว้แล้วในข้อ 1 ว่า วิสัยทัศน์ประเทศไทย คือ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามปรัชญาของเศรษฐกิจพอเพียง” โดยมีฐานคิดหลัก คือ เปลี่ยนจากการผลิตสินค้าโภคภัณฑ์ไปสู่สินค้าเชิงนวัตกรรม เปลี่ยนจากการขับเคลื่อนประเทศด้วยภาคอุตสาหกรรมไปสู่การขับเคลื่อนด้วยเทคโนโลยี ความคิดสร้างสรรค์ และนวัตกรรม และเปลี่ยนจากการเน้นภาคการผลิตสินค้าไปสู่การเน้นภาคบริการมากขึ้น

เพื่อให้บรรลุวิสัยทัศน์ดังกล่าว รัฐบาลจึงมีนโยบายที่จะใช้โมเดลขับเคลื่อนเศรษฐกิจด้วยนวัตกรรมเพื่อพัฒนาประเทศไทยไปสู่การเป็นประเทศไทย 4.0 ดังนั้น ระบบราชการจึงต้องมีการเปลี่ยนแปลงขนานใหญ่ ให้สอดคล้องกับบริบทที่จะเป็นประเทศไทย 4.0 ซึ่งระบบราชการจะต้องทำงานโดยยึดหลักธรรมาภิบาลเพื่อประโยชน์สุขของประชาชนเป็นหลัก (Better Governance, Happier Citizens) ให้เป็นที่ไว้วางใจและเป็นพึ่งของประชาชนได้อย่างแท้จริง กล่าวคือภาครัฐต้องปรับตัวและขับเคลื่อนเข้าสู่ยุคดิจิทัลเพื่อยกระดับประสิทธิภาพของภาครัฐสู่สังคมดิจิทัลที่มีการเปลี่ยนแปลงอย่างรวดเร็วและไม่สามารถคาดเดาได้ เพื่อตอบสนองความต้องการของประชาชนและอำนวยความสะดวกในการดำเนินกิจกรรมทางเศรษฐกิจและสังคมในยุคดิจิทัล ทั้งนี้ ภาครัฐต้องมุ่งเน้นความคล่องตัวเพื่อขับเคลื่อนภารกิจพิเศษ (Agenda-based) โดยการนำเทคโนโลยีดิจิทัลมาบริหารจัดการให้เข้าสู่ระบบราชการ 4.0 (Government 4.0 หรือ Gov. 4.0) ซึ่งเป็นฟันเฟืองและเสาหลักที่สำคัญในการขับเคลื่อนนโยบายของรัฐบาลให้สามารถปฏิบัติงานได้อย่างสอดคล้องกับทิศทางการบริหารงานของประเทศให้ก้าวสู่การเป็นประเทศที่พัฒนาแล้ว ซึ่งจะส่งผลให้กลไกการพัฒนาระบบราชการมีการปรับตัวต่อความท้าทายใหม่ๆ อีกทั้งเป็นการเพิ่มศักยภาพในการแข่งขันกับนานาประเทศ และยังเป็นการยกระดับสมรรถนะของหน่วยงานภาครัฐให้มีประสิทธิภาพมากยิ่งขึ้น

อย่างไรก็ตาม ความก้าวหน้าด้านเทคโนโลยียังมีจุดอ่อนเรื่องปัญหาความมั่นคงปลอดภัยของระบบสารสนเทศที่มีความสำคัญและต้องตระหนักถึงอย่างยิ่ง อีกทั้งจุดอ่อนเหล่านี้มีแนวโน้มที่จะส่งผลกระทบต่อการทำงานในรูปแบบของข้อมูลอิเล็กทรอนิกส์เพิ่มมากขึ้นอย่างต่อเนื่อง ทั้งนี้ การดำเนินการตามยุทธศาสตร์ชาติ ระยะ 20 ปี ด้านความมั่นคง ได้กำหนดให้มีการแก้ไขปัญหาความมั่นคงในปัจจุบัน เพื่อให้ปัญหาเดิมที่มีอยู่ได้รับการแก้ไขอย่างจริงจัง จนยุติลง หรือไม่ส่งผลกระทบต่อประเทศชาติ รวมทั้งให้การบริหารและการพัฒนาบ้านเมืองเดินหน้าไปได้อย่างต่อเนื่องอย่างมีประสิทธิภาพ โดยผลักดันการวิเคราะห์หาสาเหตุที่แท้จริงของปัญหาทุกภาคส่วนในทุกประเด็นอย่างเป็นระบบด้วยการผึกกำลังคนและทรัพยากรให้มีส่วนร่วมแบบบูรณาการอย่างแท้จริงในการส่งเสริม หรือ วางแผน และยกระดับวิธีการแก้ไขปัญหา รวมตลอดถึงการเสริมสร้างร่วมมือกันระหว่างหน่วยงานหลักและรองในการป้องกันและแก้ไขปัญหาจากภัยคุกคามรวมทั้งปัญหาที่ส่งผลกระทบต่อความมั่นคงต่างๆ เช่น อาชญากรรมทางไซเบอร์ เป็นต้น ที่จะส่งผลกระทบต่อความมั่นคงของชาติ และส่งผลกระทบต่อการทำงานตาม

นโยบาย ยุทธศาสตร์ระดับต่างๆ รวมทั้งโครงการสำคัญของประเทศเพื่อให้บรรลุผลสำเร็จตามเป้าหมายที่กำหนดอย่างมีประสิทธิภาพ

ในส่วนของกระทรวงการคลังมีภารกิจหลักที่สำคัญอย่างยิ่งคือ การหารายได้ให้รัฐบาลเพื่อนำมาบริหารประเทศ และสำนักงานปลัดกระทรวงการคลังมีภารกิจหลักในการเป็นศูนย์กลางการบริหารงานของกระทรวงการคลัง ซึ่งในปัจจุบันยังมีการสื่อสารข้อมูลราชการทั้งการใช้บริการจดหมายอิเล็กทรอนิกส์ที่ให้บริการโดยไม่เรียกเก็บค่าธรรมเนียม (Free e-mail) และในเครือข่ายสังคมออนไลน์ (Social Network) ที่จัดทำขึ้นโดยบริษัทเอกชนของต่างประเทศ ซึ่งมีผลเสียหายต่อประเทศไทยหากบริษัทเอกชนเหล่านั้นนำข้อมูลมาวิเคราะห์เพื่อวัตถุประสงค์อื่นๆ รวมทั้งการนำข้อมูลทางจรรยาของการสื่อสารกันไปใช้ในด้านที่มีขอบ อัจฉวมถึงการสอดแนมเอกสารที่ทางราชการใช้ดำเนินงานภายในและยังอยู่ในฐานะปกปิดจนกว่าจะได้รับอนุมัติ ตลอดจนเอกสารที่ต้องปิดเป็นความลับ เช่น การปรับอัตราภาษี การยกเว้นภาษี หรือเอกสารการจัดซื้อจัดจ้าง เป็นต้น รวมตลอดถึงเอกสารภายในหน่วยงานทั้งหลาย ดังนั้น จึงเป็นความท้าทายที่ต้องดำเนินการพัฒนาและบริหารจัดการเครื่องมือที่มีอยู่ในปัจจุบัน กฎหมายหลักเกณฑ์การปฏิบัติที่เกี่ยวข้อง และบุคลากรผู้นำไปปฏิบัติอย่างเคร่งครัด ให้เกิดประโยชน์สูงสุดเพื่อขจัดปัญหาเหล่านี้ให้เป็นที่ยุติ

### 2.1.2 อธิบายให้เห็นถึงความจำเป็นในการดำเนินการแก้ไขปัญหาหรือพัฒนา

การปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของภาครัฐที่เกี่ยวข้องกับรายงานการศึกษาส่วนบุคคล มีมติคณะรัฐมนตรีและกฎหมายกำหนดหลักเกณฑ์ในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศภาครัฐ ดังนี้

#### 1) การรับ-ส่งข้อมูลราชการด้วยจดหมายอิเล็กทรอนิกส์ (e-mail)

คณะรัฐมนตรีได้มีการประชุมเมื่อวันที่ 18 ธันวาคม 2550 เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ ซึ่งเสนอโดยสำนักงานคณะกรรมการพัฒนาระบบราชการ (สำนักงาน ก.พ.ร.) รับทราบประเด็นปัญหาภาครัฐใช้บริการจดหมายอิเล็กทรอนิกส์ที่ให้บริการโดยไม่เรียกเก็บค่าธรรมเนียม (Free e-mail) ที่จัดทำขึ้นโดยบริษัทเอกชนของต่างประเทศ โดยถือเป็นนโยบายด้านความมั่นคงปลอดภัยของข่าวสารภาครัฐ รวมทั้งให้ข้าราชการและพนักงานของรัฐยุติการใช้จดหมายอิเล็กทรอนิกส์ฟรีของเอกชน โดยเฉพาะของต่างประเทศภายใน 1 ปี ทั้งนี้ ให้ข้าราชการระดับผู้อำนวยการกองหรือเทียบเท่าขึ้นไปต้องใช้ระบบของตนเองหรือภาครัฐภายใน 3 เดือน นอกจากนี้ ได้กำหนดให้สำนักงาน ก.พ.ร. เป็นหน่วยงานกลางร่วมกับสำนักข่าวกรองแห่งชาติ สำนักงานปลัดสำนักนายกรัฐมนตรี สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ และหน่วยงานที่เกี่ยวข้อง รวมทั้งนำความเห็นของคณะรัฐมนตรีไปพิจารณาด้วยว่าการรักษาความมั่นคงปลอดภัยของข่าวสารภาครัฐอาจพิจารณาดำเนินการโดยใช้ช่องทางอื่นที่มีความสามารถเท่าเทียมกันแทนการลงทุนในระบบฮาร์ดแวร์ (Hardware) ซึ่งต้องเสียค่าใช้จ่ายสูงได้ เช่น การใช้โปรแกรมซอฟต์แวร์เข้ารหัสลับ (software scrambling) เป็นต้น และในระยะต้นควรเร่งพัฒนาให้ระบบจดหมายอิเล็กทรอนิกส์และเว็บไซต์ของหน่วยงานภาครัฐมีความมั่นคงปลอดภัยและน่าเชื่อถือ ก่อนที่จะเปิดให้บริการจดหมายอิเล็กทรอนิกส์กลาง

## 2) การรับส่งข้อมูลราชการในเครือข่ายสังคมออนไลน์ (Social Network)

ตามมาตรา 5 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาคี พ.ศ. 2549 กำหนดให้หน่วยงานภาครัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ (1) เข้าถึงหรือควบคุมการใช้งานสารสนเทศ... ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล ซึ่งการกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศดังกล่าว เป็นไปเพื่อเป็นเครื่องมือให้กับผู้ให้บริการ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคนของทุกหน่วยงานภาครัฐใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศร่วมกัน โดยมาตรา 7 กำหนดให้หน่วยงานของรัฐจัดทำเป็นประกาศและต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้ และมาตรา 8 กำหนดให้มีคณะกรรมการขึ้นคณะหนึ่งซึ่งต่อมาได้มีการแต่งตั้งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เพื่อดำเนินการตามพระราชกฤษฎีกาฉบับนี้

ทั้งนี้ การรับ-ส่งข้อมูลของทางราชการในระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของสำนักงานปลัดกระทรวงการคลังและกระทรวงการคลัง ตามที่กล่าวในข้อ 2.1.1 ยังคงมีการรับ-ส่งผ่านช่องทางให้บริการของเอกชนโดยเฉพาะของแต่ละประเทศ เช่น gmail.com, hotmail.com และ yahoo.com เป็นต้น รวมทั้งในเครือข่ายสังคมออนไลน์ (Social Network) ของบริษัทเอกชนในต่างประเทศ เช่น แอปพลิเคชัน Facebook, LINE และ Instagram เป็นต้น ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่บุคลากรของสำนักงานปลัดกระทรวงการคลังและกระทรวงการคลังจะต้องร่วมมือกันในการแก้ไขปัญหาความมั่นคงปลอดภัยด้านนี้อย่างจริงจัง จนยุติลง ด้วยการนำระบบการสื่อสารด้านสารสนเทศที่มีความมั่นคงปลอดภัยสูงมาดำเนินการในองค์กรเพื่อให้ระบบการสื่อสารในระบบสารสนเทศของสำนักงานปลัดกระทรวงการคลังและกระทรวงการคลังมีความปลอดภัย ซึ่งจะเป็นการส่งเสริมและพัฒนาระบบราชการให้มีการปรับตัวต่อความท้าทายใหม่ๆ โดยใช้เทคโนโลยีสารสนเทศเป็นหลัก รวมทั้งให้คนและทรัพยากรมีส่วนร่วมแบบบูรณาการอย่างแท้จริงในการยกระดับวิธีการแก้ไขปัญหา รวมถึงถึงการเสริมสร้างความร่วมมือกันระหว่างกระทรวงการคลังซึ่งเป็นหน่วยงานหลักและส่วนราชการในสังกัด ซึ่งเป็นหน่วยงานรองในการป้องกันและแก้ไขปัญหาจากภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของระบบราชการควบคู่กันไปกับการขับเคลื่อนนโยบายของรัฐบาล

### 2.1.3 สภาพของปัญหาที่ผ่านมาและแนวโน้มของปัญหาในอนาคต และผลกระทบที่เกิดขึ้น

#### 1) สภาพของปัญหาที่ผ่านมา

ในส่วนของสำนักงานปลัดกระทรวงการคลังได้ดำเนินการตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาคี พ.ศ. 2549 โดยการออกประกาศสำนักงานปลัดกระทรวงการคลัง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง พ.ศ. 2559 เพื่อเป็นเครื่องมือให้กับผู้ให้บริการ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแล

รักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงการคลัง ซึ่งมีข้อกำหนดเรื่องหนึ่งคือ “การใช้งานระบบสารสนเทศทั้งในระดับนโยบายและระดับปฏิบัติ เพื่อควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ เป็นต้น อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ”

อย่างไรก็ตาม ในการนำนโยบายตามประกาศฯ ดังกล่าวไปปฏิบัติยังสร้างความตระหนักรู้แก่ผู้ใช้งานในการรักษาความมั่นคงปลอดภัยสารสนเทศ (information security awareness) ไม่เข้มข้น และจริงจังเท่าที่ควรตามที่ได้กำหนดไว้ในประกาศฯ “ข้อ 6 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และเพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ข้อ 6.1 สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม” ซึ่งในภาพรวมหน่วยงานในกำกับและผู้ใช้งานส่วนใหญ่ยังไม่ให้ความสำคัญและละเลยในการปฏิบัติให้เป็นไปตามประกาศฯ ดังกล่าว

## 2) แนวโน้มของปัญหาในอนาคต

ในสถานการณ์ปัจจุบันและในอนาคต เทคโนโลยีสารสนเทศมีความก้าวหน้าอย่างรวดเร็ว และเป็นที่น่าสนใจของคนทุกสาขาทุกมุมโลก จึงเป็นที่แพร่หลายและนำมาใช้ในการปฏิบัติงานภาคราชการ ภาคเอกชน และภาคประชาชน เพื่อยกระดับให้มีความทันสมัย ความคล่องตัว ประหยัดเวลา และสะดวกสบายมากยิ่งขึ้น ซึ่งระบบเทคโนโลยีสารสนเทศของภาครัฐทุกระบบมีความจำเป็นอย่างยิ่งที่จะต้องยกระดับการรักษาความมั่นคงปลอดภัยเพื่อป้องกันภัยคุกคามที่จะเกิดขึ้นอย่างมีประสิทธิภาพสูงสุด เนื่องจากมีจรรยาบรรณจะฉวยโอกาสลักลอบนำข้อมูลต่างๆ ของบุคลากรผู้ใช้คอมพิวเตอร์ทั้งภาครัฐและภาคเอกชนโดยไม่รู้ตัวเพื่อไปใช้ประโยชน์ส่วนตนโดยอาศัยช่องโหว่ของระบบปฏิบัติการ ความรู้เท่าไม่ถึงการณ์ การละเลยในการศึกษาข้อแนะนำต่างๆ ที่องค์กรกำหนดและนำไปปฏิบัติ

ดังนั้น การที่จะทำให้ระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงการคลัง และกระทรวงการคลังมีความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ และมีประสิทธิภาพสูงสุด ผู้ที่เกี่ยวข้องกับการบริหารจัดการระบบคอมพิวเตอร์และผู้ใช้คอมพิวเตอร์ทุกคนจึงควรเรียนรู้วิธีให้เท่าทันและตระหนักในการปฏิบัติตามประกาศสำนักงานปลัดกระทรวงการคลัง เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง พ.ศ. 2559 และมติคณะรัฐมนตรีเมื่อวันที่ 18 ธันวาคม 2550 อย่างเคร่งครัดและเป็นระบบ ด้วยการให้ความร่วมมือ ผนึกกำลังคนและทรัพยากรให้มีส่วนร่วมแบบบูรณาการอย่างแท้จริงในการส่งเสริม ผลักดัน ให้เกิดการสร้างนวัตกรรมและบริหารการเปลี่ยนแปลงโดยการยกระดับวิธีการแก้ไขปัญหา รวมตลอดถึงการเสริมสร้างความร่วมมือกันระหว่างหน่วยงานหลักและรองในการป้องกันและแก้ไขปัญหาจากภัยคุกคามรวมทั้งปัญหาที่ส่งผลต่อความมั่นคงต่างๆ ดังกล่าว ที่จะผลกระทบต่อความมั่นคงของชาติทั้งในปัจจุบันและอนาคต



### 3) ผลกระทบที่เกิดขึ้น

หากผู้ใช้งานคอมพิวเตอร์และใช้งานอินเทอร์เน็ตในการรับ-ส่งข้อมูลของหน่วยงานภาครัฐละเลย ไม่ตระหนักรู้ ไม่เห็นความจำเป็นในการศึกษาแนวทาง ข้อกำหนด และนำไปปฏิบัติอย่างเคร่งครัดตามที่องค์กรกำหนด ข้อมูลสารสนเทศขององค์กรจะถูกผู้ไม่ประสงค์ดีนำไปใช้ประโยชน์ส่วนตนโดยอาศัยช่องโหว่ของระบบปฏิบัติการ และความรู้เท่าไม่ถึงการณ์ของผู้ใช้คอมพิวเตอร์โดยไม่รู้ตัว ซึ่งจะส่งผลกระทบให้เกิดผลเสียหายต่อราชการและความมั่นคงของประเทศทั้งในส่วนที่ต้องกระทำและในส่วนที่ต้องงดเว้นการกระทำเพื่อมิให้เกิดภัยต่างๆ เช่น

3.1) ภัยจากการขโมยข้อมูล (Unauthorized Logical & Physical Access) เช่น การคัดลอกข้อมูลการปรับอัตราภาษี การลบลายชื่อลูกค้าภาษี และการลบลายชื่อผู้ใช้งานในระบบ เป็นต้น

3.2) ภัยที่เกิดจากการใช้อินเทอร์เน็ต (Social Engineering, Identity Theft, Phishing, and Pharming Tactics, etc.) เป็นภัยที่สร้างความเสียหายแก่ทรัพย์สินมากที่สุด เช่น การส่งจดหมายอิเล็กทรอนิกส์ (e-mail) หลอกหลวงให้โอนเงินไปให้ก่อน หรือส่ง e-mail เพื่อเข้าสู่เว็บไซต์หน่วยงานราชการหรือธนาคารต่างๆ ที่ลวงขึ้นมาเพื่อให้ผู้ใช้ e-mail กรอกรหัสสมาชิกและรหัสผ่าน ก่อนนำข้อมูลไปทำธุรกรรมต่างๆ รวมถึงการโทรศัพท์ลวงถามข้อมูลบัตรเครดิตเพื่อนำไปทำบัตรเครดิตปลอม เป็นต้น

3.3) ภัยจาก Web Application Hacking เป็นภัยจากแฮ็กเกอร์ (Hacker คือ ผู้ที่มีความรู้ความเข้าใจในระบบคอมพิวเตอร์อย่างสูง ไม่ว่าจะเป็นเรื่องเครือข่าย ระบบปฏิบัติการ จนสามารถเข้าใจว่าระบบมีช่องโหว่ตรงไหน หรือสามารถไปค้นหาช่องโหว่ได้จากตรงไหนบ้าง) ที่เข้ามาเปลี่ยนหน้าเว็บไซต์ให้ไม่สามารถใช้งานได้ และเปลี่ยนรูปแบบหน้าแรกของเว็บไซต์มาเป็นหน้าเว็บไซต์ด้านในเพื่อฝังตัวและรอจังหวะโจรกรรมข้อมูลความลับจากองค์กรนั้นๆ โดยเฉพาะข่าวสารความลับความมั่นคงด้านต่างๆ อาจถูกกลุ่มแฮ็กเกอร์เฝ้ามองเป็นพิเศษ

3.4) โปรแกรมความโหดที่เจาะระบบเพื่อโจมตีระบบสาธารณูปโภคพื้นฐาน (Cyber Terrorist/Critical Infrastructure Attack (SCADA attack) เป็นต้น

## 2.2 การกำหนดข้อเสนอเชิงนโยบาย

### 2.2.1 หลักการ แนวคิด ที่ใช้เป็นกรอบหรือแนวทางในการจัดทำข้อเสนอ

#### 1) หลักการ แนวคิดในการจัดทำข้อเสนอ

ผู้จัดทำรายงานได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการใช้งานคอมพิวเตอร์และใช้งานอินเทอร์เน็ตในส่วนที่เกี่ยวข้องกับการรับ-ส่งข้อมูลของหน่วยงานของทุกส่วนราชการในสังกัดกระทรวงการคลัง จึงมีความมุ่งมั่นที่จะพัฒนางานเรื่อง “การยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร” ด้วยการดำเนินการต่อไปนี้

#### 1.1) การรับ-ส่งข้อมูลราชการทางระบบอิเล็กทรอนิกส์ แบ่งเป็น 2 ช่องทาง ได้แก่

##### 1.1.1) การใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ (e-mail)

จดหมายอิเล็กทรอนิกส์ (e-mail) คือ การส่งข้อความหรือข่าวสารจากบุคคลหนึ่งไปยังบุคคลอื่นๆ ผ่านทางคอมพิวเตอร์และระบบเครือข่ายในรูปแบบของสัญญาณข้อมูลที่เป็นอิเล็กทรอนิกส์ในช่องสัญญาณรูปแบบต่างๆ ที่เชื่อมต่อระหว่างเครือข่ายคอมพิวเตอร์ ซึ่งจะตรงเข้ามาสู่ Mail Box ที่ถูกจัดสรรในแม่ข่าย (Server) ของผู้รับปลายทางทันที การใช้งาน e-mail จำเป็นต้องมีที่อยู่ทางอินเทอร์เน็ตของแต่ละคนทั้งผู้รับและผู้ส่งเพื่อใช้ในการอ้างอิงการส่งและรับจดหมาย

หรือเรียกว่า e-mail address มักจะแทนด้วยชื่อหรือรหัสที่ใช้แทนตัว แล้วตามด้วยชื่อของ Mail Server ที่ให้บริการ เช่น sirikan.m@mof.go.th หรือ sirikan.m@vayupak.net เป็นต้น โดยทั่วไป e-mail address จะประกอบด้วย

- User ID ใช้เป็นชื่อหรือรหัสประจำตัวของผู้ใช้บริการแต่ละคน
- เครื่องหมาย @Domain Name ของ Mail Server ที่ใช้บริการ

จดหมายหรือข้อความที่ส่งถึงกันผ่านระบบเครือข่าย สามารถส่งให้ผู้รับ ซึ่งเป็นสมาชิกของระบบอินเทอร์เน็ตได้โดยไม่จำกัดสถานที่ เวลา และอย่างรวดเร็วภายในระยะเวลาไม่กี่วินาที หรืออาจจะส่งจดหมายฉบับเดียวไปถึงผู้รับหลายคนในเวลาเดียวกันก็ได้ ซึ่งชื่อเว็บไซต์ รวมถึงชื่อจดหมายอิเล็กทรอนิกส์ขององค์กรแต่ละประเภทจะแตกต่างกัน ดังนี้

ตารางที่ 2 : ชื่อเว็บไซต์และชื่อจดหมายอิเล็กทรอนิกส์แยกตามประเภทขององค์กรในประเทศไทย

ประเภทองค์กร	ชื่อเว็บไซต์/ ชื่อจดหมายอิเล็กทรอนิกส์ (e-mail) ลงท้ายด้วย	ตัวอย่าง		
		ชื่อองค์กร	ชื่อเว็บไซต์	ชื่อจดหมายอิเล็กทรอนิกส์ (e-mail)
ภาคราชการ	.go.th	กระทรวงการคลัง	www.mof.go.th	ชื่อบุคลากร@mof.go.th
		กรมธนารักษ์	www.treasury.go.th	ชื่อบุคลากร@treasury.go.th
		ศูนย์กลางความรู้แห่งชาติ	www.tkc.go.th	ชื่อบุคลากร@tkc.go.th
รัฐวิสาหกิจ	.co.th	การประปานครหลวง	www.mwa.co.th	ชื่อบุคลากร@mwa.co.th
		การไฟฟ้าส่วนภูมิภาค	www.pea.co.th	ชื่อบุคลากร@pea.co.th
		ธนาคารออมสิน	www.gsb.co.th	ชื่อบุคลากร@gsb.co.th
ผู้ให้บริการเครือข่าย	.net	เครือข่ายวายุกักซ์ กระทรวงการคลัง	www.vayupak.net	ชื่อบุคลากร@vayupak.net
องค์กรศึกษา	.ac.th	มหาวิทยาลัยขอนแก่น	www.kku.ac.th	ชื่อบุคลากร@kku.ac.th
		มหาวิทยาลัยบูรพา	www.buu.ac.th	ชื่อบุคลากร@buu.ac.th
องค์กรที่ไม่หวังผลกำไร	.or.th/org.th	ธนาคารแห่งประเทศไทย	www.bot.or.th	ชื่อบุคลากร@bot.or.th
		มูลนิธิกระจกเงา	www.mirror.or.th	ชื่อบุคลากร@mirror.or.th
		มูลนิธิไทยรักษ์ป่า	www.thairakpa.org	ชื่อบุคลากร@thairakpa.org
ภาคเอกชน (องค์กรทั่วไป บริษัท ห้าง ร้าน เว็บไซต์ ส่วนตัว)	.com	บริษัท ปตท จำกัด (มหาชน)	http://www.pttplc.com	ชื่อบุคลากร@pttplc.com
		บริษัทปูนซิเมนต์ไทย จำกัด (มหาชน)	www.scg.com	ชื่อบุคลากร@scg.com

### 1.1.2) การใช้โปรแกรม IP Messenger (IPMsg)

โปรแกรม IP Messenger เป็นโปรแกรมที่สามารถติดตั้งได้เองโดยไม่มีค่าใช้จ่าย (Free Download) ที่ใช้กับเครื่องคอมพิวเตอร์ผ่านหมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องหรือที่เรียกว่า IP Address (Internet Protocol Address) สำหรับระบุตัวตนของเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่บนเครือข่าย ซึ่งบุคลากรในสังกัดสำนักงานปลัดกระทรวงการคลังมีเครื่องคอมพิวเตอร์ใช้ประจำทุกคน

### 1.2) การสื่อสารในเครือข่ายสังคมออนไลน์ (Social Network)

แอปพลิเคชัน G-Chat เป็นช่องทางการสื่อสารในเครือข่ายสังคมออนไลน์ภาครัฐที่มีความปลอดภัยสูงสุด จัดทำโดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) หรือ Digital Government Development Agency : DGA (Public Organization) เป็นระบบที่มีความคล้ายคลึงกับระบบสนทนาในแอปพลิเคชัน LINE

ทั้งนี้ ผู้จัดทำรายงานขอเสนอให้นำช่องทางการสื่อสารข้อมูลภาครัฐในรูปแบบเอกสารอิเล็กทรอนิกส์มาใช้ในราชการของสำนักงานปลัดกระทรวงการคลังและกระทรวงการคลัง ทั้ง 3 ช่องทางในการรับ-ส่งข้อมูลอิเล็กทรอนิกส์และในเครือข่ายสังคมออนไลน์ เพื่อให้เอกสารราชการในระบบสารสนเทศมีความมั่นคงปลอดภัยสูงสุด เป็นไปตามกฎหมาย นโยบาย และแนวปฏิบัติที่เกี่ยวข้อง

## 2) กรอบหรือแนวทางในการจัดทำข้อเสนอ

กรอบแนวคิดที่ 1 เว็บไซต์ของทุกส่วนราชการมีระบบการรับ-ส่งจดหมายอิเล็กทรอนิกส์ (e-mail ภาครัฐ) อยู่แล้ว และบุคลากรภาครัฐทุกคนต้องนำมาใช้ให้เกิดประโยชน์ต่อราชการอย่างมีประสิทธิภาพสูงสุด (Material)

กรอบแนวคิดที่ 2 โปรแกรม IP Messenger (IPMsg) เป็นโปรแกรมการสื่อสารข้อมูลอิเล็กทรอนิกส์ที่สามารถรักษาความปลอดภัยของข้อมูลราชการได้ ร้อยละ 100 เนื่องจากการส่งข้อมูลผ่านหมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องหรือที่เรียกว่า IP Address (Internet Protocol Address) ในระบบเครือข่ายที่ใช้โปรโตคอลแบบ TCP/IP สำหรับระบุตัวตนของเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่บนเครือข่าย ประกอบด้วยตัวเลข 4 ชุด ที่ไม่ซ้ำกันในแต่ละเครื่องและอยู่ในระบบ LAN เดียวกัน ซึ่งจะสามารถทราบตำแหน่งของเครื่องที่ส่งข้อมูลไปได้อย่างแม่นยำ (Material)

กรอบแนวคิดที่ 3 แอปพลิเคชัน G-Chat มีความสามารถเพียงพอกับการใช้สนทนาภายในหน่วยงานของรัฐ การใช้งานคล้ายกับแอปพลิเคชัน LINE เพื่อแยกการสนทนาเรื่องส่วนตัวกับเรื่องงานราชการออกจากกันโดยสิ้นเชิง โดยสามารถมั่นใจได้ว่าข้อมูลที่เป็นความลับของทางราชการจะอยู่ในระบบที่ปลอดภัย (Material)

กรอบแนวคิดที่ 4 การพัฒนาการสื่อสารในระบบอิเล็กทรอนิกส์ให้มีความปลอดภัยเพื่อป้องกันความลับของทางราชการต้องไม่ใช้งบประมาณในการดำเนินการแต่อย่างใด (Money)

กรอบแนวคิดที่ 5 การส่งเสริมให้บุคลากรของสำนักงานปลัดกระทรวงการคลังเก่งและดี มีคุณธรรมในการปฏิบัติงานด้วยความโปร่งใสตามหลักธรรมาภิบาล มีส่วนร่วมในการบริหารทรัพยากรแบบบูรณาการอย่างแท้จริงเพื่อยกระดับวิธีการแก้ไขปัญหา รวมตลอดถึงการรับผิดชอบในการสร้างนวัตกรรมการเปลี่ยนแปลงการปฏิบัติงานโดยเสริมสร้างความร่วมมือกันระหว่างกระทรวงการคลัง

และส่วนราชการในสังกัดให้เป็นไปตามแนวทางเดียวกัน เพื่อป้องกันและแก้ไขปัญหาจากภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของระบบราชการควบคู่กันไปกับการขับเคลื่อนนโยบายของรัฐบาล (Man และ Management)

จากกรอบความคิดทั้ง 5 ข้อข้างต้น สอดคล้องกับวิธีการบริหารแบบ 4 M ซึ่งสามารถแบ่งออกเป็น 4 ประเภท ได้แก่ วัสดุและเครื่องมือ (Material) เพื่อการดำเนินงาน รวมถึงบุคลากรในองค์กร (Man) ที่ต้องให้ความร่วมมืออย่างจริงจัง และทรัพยากรในการบริหารงาน (Money) รวมทั้งความสามารถในการจัดการ (Management) ในทุกขั้นตอนกระบวนการเพื่อให้บรรลุผลสำเร็จ

## 2.2.2 การวิเคราะห์ข้อมูลที่เกี่ยวข้องเพื่อประกอบการจัดทำข้อเสนอ

การวิเคราะห์ข้อมูลที่เกี่ยวข้องเพื่อประกอบการจัดทำข้อเสนอเรื่อง “การยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร” ได้ดำเนินการโดยนำข้อมูลที่ใช้ในการจัดทำแผนยุทธศาสตร์ของสำนักงานปลัดกระทรวงการคลังมาวิเคราะห์ โดยคัดเลือกนำเสนอเฉพาะประเด็นที่สำคัญดังปรากฏตามตารางที่ 3 ต่อไปนี้

ตารางที่ 3 : ข้อมูลที่นำมาวิเคราะห์สถานการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง

ลำดับที่	ข้อมูลที่นำมาวิเคราะห์	ความสอดคล้องกับรายงานการศึกษาส่วนบุคคล
<u>ยุทธศาสตร์การบริหารการเปลี่ยนแปลงกระทรวงการคลัง พ.ศ. 2560 – 2564</u>		
1	ยุทธศาสตร์สร้างเครือข่ายการเปลี่ยนแปลง กลยุทธ์ที่ 1.1 สร้างความเข้มแข็งของเครือข่าย บริหารการเปลี่ยนแปลง กลยุทธ์ที่ 1.2 บูรณาการข้อมูลอัจฉริยะ	-การดำเนินการเพื่อยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลังและกระทรวงการคลังก่อให้เกิดการเปลี่ยนแปลงในการสร้างความเข้มแข็งของเครือข่ายภายในองค์กรที่ร่วมกันเป็นการพัฒนาการบริหารและบูรณาการข้อมูลสารสนเทศอย่างอัจฉริยะเป็นมาตรฐานเดียวกันโดยใช้เครื่องมือเดียวกัน และจะเป็นแรงบันดาลใจให้บุคลากรในสังกัดได้คิดริเริ่มการใช้นวัตกรรมในการดำเนินการเรื่องใหม่ๆ ตามวิถีคนคลังต่อไป ซึ่งเป็นการสร้างภาพลักษณ์การเปลี่ยนแปลงให้องค์กร ดังนั้น เรื่องที่ศึกษาจึงสอดคล้องกับยุทธศาสตร์การบริหารการเปลี่ยนแปลงกระทรวงการคลัง พ.ศ. 2560 – 2564
2	ยุทธศาสตร์สร้างสรรค์นวัตกรรม กลยุทธ์ที่ 2.1 พัฒนาสมรรถนะทีมบริหารการเปลี่ยนแปลง กลยุทธ์ที่ 2.2 สร้างแรงบันดาลใจสู่นวัตกรรม	
3	ยุทธศาสตร์สร้างวัฒนธรรม กลยุทธ์ที่ 3.1 สร้างภาพลักษณ์การเปลี่ยนแปลง กลยุทธ์ที่ 3.2 สร้างวิถีคนคลัง	
<u>ภารกิจตามกฎหมาย (Legal Mandate) และหน่วยงานที่รับผิดชอบ (เฉพาะในส่วนที่เกี่ยวข้อง)</u>		
1	ทุกหน่วยงานในสังกัด : เสนอความเห็นและคำแนะนำในการกำหนดนโยบาย เป้าหมาย และผลสัมฤทธิ์ของงานในกระทรวงการคลัง	-การจัดทำรายงานการศึกษาส่วนบุคคลนี้ เป็นการเสนอความเห็นและคำแนะนำในการกำหนดนโยบาย เป้าหมาย และผลสัมฤทธิ์ของงานใน

ลำดับ ที่	ข้อมูลที่น่าสนใจวิเคราะห์	ความสอดคล้องกับรายงานการศึกษาส่วนบุคคล
2	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร : เป็นศูนย์ข้อมูลสารสนเทศของกระทรวงตลอดจนให้คำแนะนำเกี่ยวกับนโยบายและแผนการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารรวมทั้งการใช้ประโยชน์ของข้อมูลของหน่วยงานในสังกัดกระทรวงการคลัง	สำนักงานปลัดกระทรวงการคลัง โดยสามารถนำไปบูรณาการการรับ-ส่งข้อมูลราชการของส่วนราชการในสังกัดกระทรวงการคลังให้เป็นมาตรฐานเดียวกันเพื่อใช้ประโยชน์ได้อย่างมีประสิทธิภาพสูงสุด
<u>สภาพแวดล้อมของสำนักงานปลัดกระทรวงการคลัง</u> (วิเคราะห์โดยใช้หลักการ SWOT Analysis – เฉพาะในส่วนที่เกี่ยวข้อง)		
1	<u>จุดแข็ง (Strength)</u> -ผู้บริหารมีวิสัยทัศน์ มีความเป็นผู้นำ มีความคิดริเริ่มสร้างสรรค์ในการพัฒนาองค์กร และให้การสนับสนุนแนวทางการดำเนินงาน -ใกล้ชิดกับข้อมูล และมีระบบเครือข่ายข้อมูลข่าวสารที่เชื่อมโยงกับทุกหน่วยงานในสังกัด -มีสภาพแวดล้อมที่ดี และระบบเทคโนโลยีสารสนเทศที่ทันสมัย เพียงพอต่อการทำงาน -กฎกระทรวงมอบอำนาจให้สำนักงานปลัดกระทรวงการคลัง ปฏิบัติภารกิจทั้งในระดับกระทรวงและในระดับกรม	<u>การบริหารจัดการภายใน</u> -สำนักงานปลัดกระทรวงการคลังมีจุดแข็งที่สามารถส่งเสริมให้สามารถนำรายงานการศึกษาส่วนบุคคลไปปฏิบัติได้อย่างมีประสิทธิภาพเพื่อขจัดปัญหาอุปสรรคภัยคุกคามด้านความมั่นคงปลอดภัยจากการใช้ระบบสารสนเทศและการสื่อสาร -จุดอ่อนทั้งหมด เป็นปัญหาอุปสรรคที่เป็นแรงบันดาลใจให้ผู้จัดทำรายงานคิดค้นนวัตกรรมที่จะทำให้เกิดการเปลี่ยนแปลงบทบาท หน้าที่ในการดำเนินการในทิศทางเดียวกันเพื่อให้เกิดการยกระดับในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสาร ซึ่งจะต้องให้ความสำคัญกับการประชาสัมพันธ์ที่เพียงพอ เพื่อสร้างความรู้ ความเข้าใจในการนำกฎหมาย ระเบียบ และนโยบายไปปฏิบัติทั่วทั้งองค์กร
2	<u>จุดอ่อน (Weakness)</u> -ถนัดงานประจำ ขาดการทำงานในเชิงรุก และขาดความคิดริเริ่มสร้างสรรค์ในการทำงาน -ขาดการประสานงานและการถ่ายทอดความรู้ระหว่างกันภายในองค์กร -การประชาสัมพันธ์บทบาท หน้าที่ และงานขององค์กรไม่เพียงพอ -การสื่อสารและสร้างความเข้าใจเกี่ยวกับกฎระเบียบ นโยบาย การดำเนินงาน และผลการดำเนินงานไม่ทั่วถึงทั้งองค์กร	
3	<u>โอกาส (Opportunity)</u> -องค์ความรู้และระบบเทคโนโลยีสารสนเทศสมัยใหม่ สามารถนำมาประยุกต์ใช้ในการปฏิบัติงานให้มีประสิทธิภาพมากยิ่งขึ้น -การบริหารจัดการภาครัฐให้การสนับสนุนหน่วยงานนำความรู้ไปเป็นเครื่องมือในการยกระดับคุณภาพการปฏิบัติงาน	<u>การบริหารจัดการภายนอก</u> -รายงานการศึกษาส่วนบุคคลนี้สามารถตอบสนองโอกาสของสำนักงานปลัดกระทรวงการคลังซึ่งส่วนหนึ่งเป็นการนำนวัตกรรมในรูปแบบที่ยังไม่เคยนำมาใช้กับการปฏิบัติงานภายในสำนักงานปลัดกระทรวงการคลัง ทั้งนี้ ภาครัฐได้มีกฎหมายมติคณะรัฐมนตรีให้การสนับสนุนหน่วยงาน

ลำดับ ที่	ข้อมูลที่น่ามาวิเคราะห์	ความสอดคล้องกับรายงานการศึกษาส่วนบุคคล
	-นโยบายรัฐบาลที่สนับสนุน และกำหนดทิศทาง การบริหารงานไว้อย่างชัดเจน	เพื่อให้นำความรู้ไปเป็นเครื่องมือในการยกระดับ คุณภาพการปฏิบัติงาน
4	ภัยคุกคาม (Threat) -การได้รับงบประมาณที่ไม่เพียงพอต่อการ ดำเนินงาน -อาชญากรรมทางอิเล็กทรอนิกส์ที่พยายาม เข้าถึงฐานข้อมูลของกระทรวงการคลัง	-ในส่วนของภัยคุกคาม การดำเนินการตาม รายงานการศึกษาส่วนบุคคลจะสามารถป้องกัน อาชญากรรมทางอิเล็กทรอนิกส์ที่พยายาม เข้าถึงฐานข้อมูลของกระทรวงการคลังได้ อย่างมีประสิทธิภาพ โดยไม่ต้องรับการจัดสรร งบประมาณแต่อย่างใด
<u>ความคิดเห็น/ความคาดหวังของผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย</u>		
1	การเปลี่ยนแปลงในอนาคตเป็นสิ่งสำคัญที่ต้อง ตระหนัก เรียนรู้และยอมรับ ควรมีการจัดทำ แผนงานที่ใช้บริหารการเปลี่ยนแปลงของ สำนักงานปลัดกระทรวงการคลังและกระทรวง การคลัง เพื่อให้ทุกหน่วยงานในสังกัดมีการ ดำเนินงานไปในทิศทางเดียวกัน และควรเพิ่ม บทบาทหน้าที่ด้านนวัตกรรมและการบริหาร การเปลี่ยนแปลง	-การนำโปรแกรม IP Messenger และแอปพลิเคชัน G-Chat ตามรายงานการศึกษาส่วนบุคคลนี้ เป็นการนำนวัตกรรมมาใช้ในการบริหารการ เปลี่ยนแปลงเพื่อยกระดับการสื่อสารข้อมูล ราชการด้วยระบบอิเล็กทรอนิกส์ของสำนักงาน ปลัดกระทรวงการคลัง ซึ่งเมื่อดำเนินการจน เกิดความคล่องตัวและเป็นมาตรฐานเดียวกัน แล้ว จะขยายขอบเขตการดำเนินการไปยังทุก ส่วนราชการในสังกัดกระทรวงการคลังต่อไป
2	ควรบูรณาการข้อมูลระหว่างหน่วยงานให้ทั่วถึง และครอบคลุมมากขึ้น เน้นการมีส่วนร่วมใน การทำงาน และในฐานะที่สำนักงานปลัดกระทรวง การคลังเป็นหน่วยงานกลางที่บริหารงานของ กระทรวงการคลัง ในอนาคตควรเพิ่มบทบาท ในการบริหารการจัดการงานบางส่วนของ ส่วนราชการที่อยู่ในสังกัดกระทรวงการคลัง เพื่อเพิ่มประสิทธิภาพขององค์กร	เพื่อให้มีระบบการรักษาความมั่นคงปลอดภัย ด้านระบบสารสนเทศและการสื่อสารที่มี ประสิทธิภาพสูงสุด มีความทันสมัย และมี ส่วนร่วมดำเนินการในทิศทางเดียวกัน ซึ่งจะ เป็นช่องทางการติดต่อสื่อสารให้ทันต่อ เทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็วมาก ยิ่งขึ้น
3	พัฒนาระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน และชัดเจน เพื่อรองรับประชาคมเศรษฐกิจ อาเซียนที่จะเกิดขึ้นในอนาคต เช่น ข้อมูลสถิติ ต่างๆ ผลการดำเนินงาน และเนื่องจากสำนักงาน ปลัดกระทรวงการคลังเป็นหน่วยงานสนับสนุน กำกับดูแลและตรวจสอบการปฏิบัติงานของ ส่วนราชการและรัฐวิสาหกิจในสังกัดกระทรวง การคลัง ควรปรับปรุงช่องทางการติดต่อสื่อสาร ให้ทันต่อเทคโนโลยีมากขึ้น	

### 2.2.3 แนวทางในการแก้ปัญหาหรือพัฒนานโยบายที่สอดคล้องกับการวิเคราะห์

จากผลการวิเคราะห์ข้อมูลสถานการณ์การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง ในข้อ 2.2.2 เพื่อประกอบการจัดทำข้อเสนอเรื่อง “การยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร” สรุปได้ว่ามีปัจจัยที่จะส่งเสริมและผลักดันให้ข้อเสนอเรื่องดังกล่าว สามารถนำไปสู่การปฏิบัติเพื่อบริหารการเปลี่ยนแปลงองค์กรให้มีมาตรฐานเป็นที่ยอมรับในระดับสากลในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังต่อไปนี้

(ก) Material : การรับ-ส่งข้อมูลอิเล็กทรอนิกส์ในระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่ต้องมีการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยอย่างต่อเนื่องและเคร่งครัดเพื่อให้มีประสิทธิภาพสูงสุด

(ข) Man : บุคลากรของสำนักงานปลัดกระทรวงการคลัง ที่ต้องพัฒนาองค์ความรู้ของตนเอง และตระหนักรู้เท่าทันภัยคุกคามจากการใช้ระบบสารสนเทศและอินเทอร์เน็ต รวมทั้งมีความรู้ความเข้าใจ และดำเนินการป้องกันได้อย่างมีประสิทธิภาพเพื่อให้ข้อมูลราชการถูกนำไปใช้หาประโยชน์ส่วนตน ซึ่งจะก่อให้เกิดผลเสียหายต่อราชการและความมั่นคงของประเทศทั้งในส่วนที่ต้องกระทำและงดเว้นการกระทำ

(ค) Management : กฎหมาย ระเบียบ และแนวทางการปฏิบัติ ที่เกี่ยวข้อง ที่ต้องนำมาบังคับใช้อย่างจริงจัง เคร่งครัด และต่อเนื่อง

#### 1) แนวทางในการแก้ปัญหาหรือพัฒนานโยบายด้านการสื่อสารในระบบเทคโนโลยีสารสนเทศ

จากที่กล่าวข้างต้นในข้อ 2.2.1 1) ซึ่งได้อธิบายถึงช่องทางในการรับ-ส่งข้อมูลราชการทางเทคโนโลยีสารสนเทศ โดยแบ่งออกเป็น 3 ช่องทางแล้วนั้น ทั้งนี้ ผู้จัดทำรายงานได้ตระหนักถึงการรักษาความมั่นคงปลอดภัยของสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ให้ไม่อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ เพื่อให้มีการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยภาครัฐอย่างต่อเนื่อง เคร่งครัด และมีประสิทธิภาพสูงสุด จึงขอเสนอแนวทางในการแก้ไขและพัฒนาการรักษาความมั่นคงปลอดภัยของการสื่อสารในระบบเทคโนโลยีสารสนเทศให้มีความปลอดภัยได้อย่างมั่นคงและยั่งยืน ซึ่งการทำงานในการรับ-ส่งข้อมูลดังกล่าว มีรายละเอียดโดยสังเขปดังต่อไปนี้

##### 1.1) การใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ (e-mail)

การรับ-ส่งข้อมูลทางระบบจดหมายอิเล็กทรอนิกส์ภาครัฐ (e-mail) เป็นเรื่องพื้นฐานที่ทุกคนสามารถดำเนินการได้อย่างคล่องแคล่วและเป็นปกติทั้งในรูปแบบส่วนบุคคลและงานราชการ จึงจะขออธิบายโดยสังเขปเฉพาะในส่วนที่เกี่ยวข้องกับการปฏิบัติราชการเท่านั้น ดังต่อไปนี้

เนื่องจากทุกส่วนราชการในประเทศไทยมีเว็บไซต์ของส่วนราชการอยู่แล้ว เช่น เว็บไซต์กระทรวงการคลัง ([www.mof.go.th](http://www.mof.go.th)) เว็บไซต์กรมบัญชีกลาง ([www.cgd.go.th](http://www.cgd.go.th)) เว็บไซต์กรมสรรพากร ([www.rd.go.th](http://www.rd.go.th)) เป็นต้น ซึ่งแต่ละเว็บไซต์จะมีระบบจดหมายอิเล็กทรอนิกส์ให้บริการแก่บุคลากรในสังกัด โดยการติดต่อขอลงทะเบียนใช้งานได้ที่หน่วยงานที่ทำหน้าที่เป็นศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของแต่ละส่วนราชการ ทั้งนี้ ผู้ขอใช้จดหมายอิเล็กทรอนิกส์จะต้องให้ความยินยอมตามเงื่อนไขการรักษาความมั่นคงปลอดภัยในการสื่อสารด้วยระบบสารสนเทศตามที่หน่วยงานกำหนด หรืออาจให้ผู้ดูแลระบบของหน่วยงานประสานขอใช้บริการระบบจดหมายอิเล็กทรอนิกส์กลาง

mail.go.th จากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ก็ได้ ซึ่งในปัจจุบันการรับ-ส่ง ข้อมูลของทางราชการในระบบอิเล็กทรอนิกส์ของสำนักงานปลัดกระทรวงการคลัง อยู่ในความรับผิดชอบ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และยังคงมีการรับ-ส่ง e-mail ผ่านช่องทางการให้บริการ ของเอกชนในต่างประเทศ เช่น gmail.com, hotmail.com และ yahoo.com เป็นต้น ทั้งนี้ ในการ รับ-ส่งข้อมูลราชการทุกครั้ง จะต้องถือปฏิบัติตามมติคณะรัฐมนตรีเมื่อวันที่ 18 ธันวาคม 2550 และ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ข้อ 7 (3) กำหนดเรื่องการ ควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน อย่างเคร่งครัดและต่อเนื่อง เพื่อมิให้เอกสารราชการถูกนำไปใช้ประโยชน์ จากผู้ที่ไม่มีความเกี่ยวข้อง ซึ่งระบบจดหมายอิเล็กทรอนิกส์ (e-mail) มีข้อดีและข้อจำกัด ดังนี้

ตารางที่ 4 : ข้อดีและข้อจำกัดของจดหมายอิเล็กทรอนิกส์ (e-mail)

ข้อดีของจดหมายอิเล็กทรอนิกส์	ข้อจำกัดของจดหมายอิเล็กทรอนิกส์
- ประหยัดเวลา และเงิน	- ไม่สามารถเข้าถึงบุคคลได้ทุกคน
- สามารถส่งในรูปแบบมัลติมีเดียได้	- อาจมีไวรัสมาพร้อมกับเอกสารที่ส่งมา
- สามารถแนบไฟล์ที่เป็นเอกสารส่งได้	- ถ้าเครือข่ายล่ม ทำให้การส่งหรือรับข้อมูลล้มเหลว
- สามารถส่งต่อข้อมูลหรือที่เรียกว่า forward ได้	- ถ้าข้อมูลใน mail box เต็ม จะไม่สามารถรับข้อมูล อื่นได้

## 1.2) การใช้โปรแกรม IP Messenger (IPMsg)

เป็นการใช้งานโปรแกรมผ่าน IP Address หรือหมายเลขประจำเครื่องคอมพิวเตอร์ ที่ถูกกำหนดไว้แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอลแบบ TCP/IP ที่ไม่ซ้ำกัน

### 1.2.1) ความหมายของ IP Address

IP Address หรือชื่อเต็มว่า Internet Protocol Address คือ หมายเลข ประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอลแบบ TCP/IP สำหรับระบุตัวตน ของเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่บนเครือข่าย ประกอบด้วยตัวเลข 4 ชุด ที่ไม่ซ้ำกันในแต่ละเครื่อง เช่น 192.168.100.1 หรือ 172.16.10.1 เป็นต้น ซึ่งตัวเลข 4 ชุด คือ Network ID กับ Host ID จะบอก ให้รู้ว่าเครื่องคอมพิวเตอร์อยู่ใน Network ไหน และเป็นเครื่องไหนใน network นั้น

ในระบบเครือข่ายจำเป็นจะต้องมีหมายเลข IP Address กำหนดไว้ให้กับ คอมพิวเตอร์และอุปกรณ์อื่นๆ ที่ต้องการ IP Address โดยเมื่อมีการโอนย้ายข้อมูล หรือสั่งงานใดๆ จะสามารถทราบตำแหน่งของเครื่องที่เราต้องการส่งข้อมูลไปเพื่อจะได้ไม่ผิดพลาดเวลาส่งข้อมูล โดย IP Address ที่ใช้กันอยู่ในปัจจุบัน อยู่ในมาตรฐานของ version 4 หรือที่รู้จักกันในนาม IPv4

การบริหารจัดการ IP Address มีการแบ่ง IP Address ออกเป็นหมวดหมู่ เรียกว่า “class” เพื่อให้เกิดความเป็นระเบียบ



### 1.2.2) ตัวอย่าง IP Address


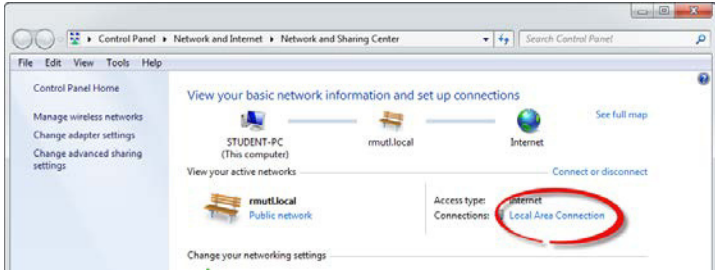
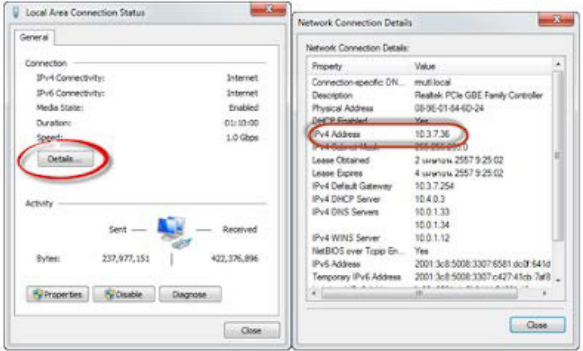
- Class A ตั้งแต่ 10.xxx.xxx.xxx
- Class B ตั้งแต่ 172.16.xxx.xxx ถึง 172.31.xxx.xxx
- Class C ตั้งแต่ 192.168.0.xxx ถึง 192.168.255.xxx

จาก IP Address จะสามารถบอกได้คร่าวๆ ว่าคอมพิวเตอร์ 2 เครื่องอยู่ใน network วงเดียวกันหรือไม่โดยการเปรียบเทียบ Network ID ของ IP Address ถ้ามี Network ID ตรงกัน แสดงว่าอยู่ใน network วงเดียวกัน เช่น คอมพิวเตอร์เครื่องหนึ่งมี IP Address 1.2.3.4 จะอยู่ใน network วงเดียวกับอีกเครื่องหนึ่งซึ่งมี IP Address 1.100.150.200 เนื่องจากมี Network ID ตรงกันคือ 1 (class A ใช้ Network ID 1 byte) เป็นต้น

### 1.2.3) วิธีตรวจสอบ IP Address

ขั้นตอนการตรวจสอบ IP Address มีดังต่อไปนี้

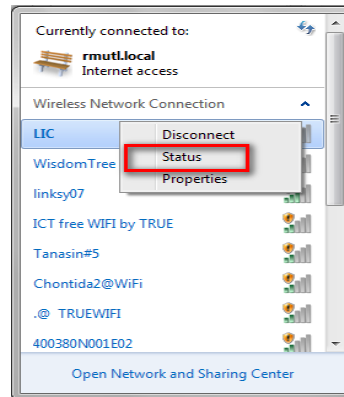
ตารางที่ 5 : ขั้นตอนการตรวจสอบ IP Address

ขั้นตอนการตรวจสอบ IP Address	
<p><b>กรณีใช้สาย LAN</b></p> <p>1. สังเกตสัญลักษณ์ไอคอนรูปการเชื่อมต่ออินเทอร์เน็ต มุมขวาล่าง และคลิกที่ไอคอนการเชื่อมต่อ Internet แล้วเลือก “Open Network and Sharing Center”</p>	
<p>2. คลิกที่ “Local Area Connection”</p>	
<p>3. คลิกที่ “Details” ให้สังเกตที่ IPV4 Address : 10.3.7.36 นั่นคือหมายเลข IP Address เครื่องคอมพิวเตอร์ที่กำลังใช้งาน</p>	

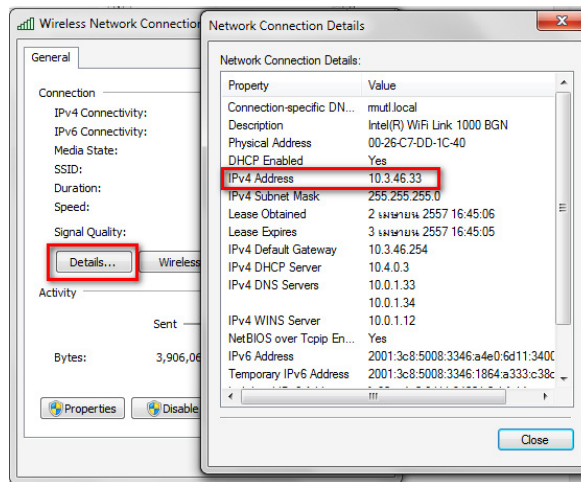
ขั้นตอนการตรวจสอบ IP Address

กรณีใช้ Wireless หรือ Wi-Fi

1. สังเกตสัญลักษณ์ไอคอนรูปการเชื่อมต่ออินเทอร์เน็ตมุมขวาล่าง จากนั้นคลิกขวาที่ไอคอนการเชื่อมต่ออินเทอร์เน็ตเลือกสัญญาณที่ได้ทำการเชื่อมต่อไว้แล้ว และคลิกขวาที่ชื่อสัญญาณ "Status"

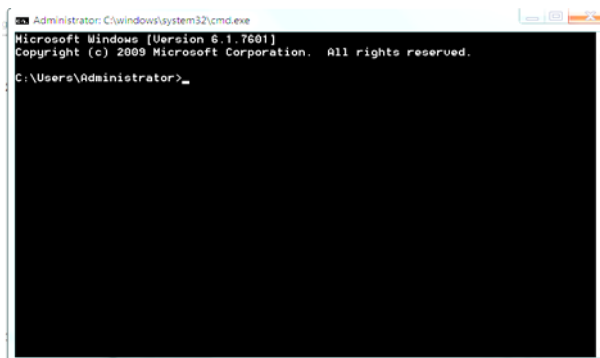


2. คลิกที่ "Details" จะมีหน้าต่างแสดงข้อมูล ให้ดูที่ IPv4 Address : 10.3.46.33 คือ หมายเลข IP Address ของเครื่องคอมพิวเตอร์ที่กำลังใช้งาน

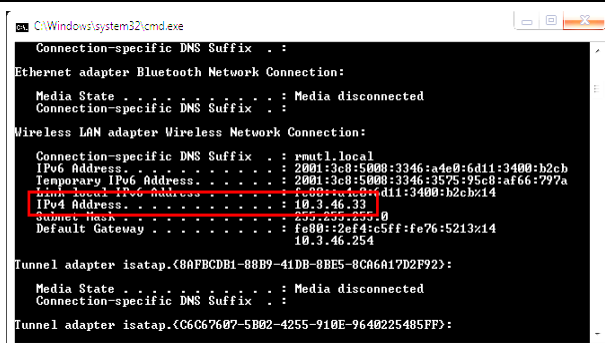


กรณีใช้ปุ่ม Start ที่หน้า Desktop โดยใช้ Command prom

1. เรียก Command prompt ขึ้นมาโดยเข้าไปที่ Start -> ตรงช่องค้นหาให้พิมพ์ "cmd" จากนั้นกด Enter หรือ กดปุ่ม Windows+R พิมพ์ "cmd" แล้วกด Run จะปรากฏหน้าต่างสีดำ



2. พิมพ์คำว่า ipconfig กด enter จะเห็นกลุ่มหมายเลข IP Address ซึ่งจะระบุในส่วนของ IPv4 Address : 10.3.46.33 คือ หมายเลข IP Address ของเครื่องคอมพิวเตอร์ที่กำลังใช้งาน



### 1.2.4) การรับ-ส่งข้อมูลอิเล็กทรอนิกส์โดยใช้โปรแกรม IP Messenger (IPMsg)

#### ผ่าน IP Address

เป็นการรับ-ส่งข้อมูลอิเล็กทรอนิกส์ (Files, Folders) ด้วยโปรแกรม IP Messenger (IPMsg) ซึ่งสามารถดาวน์โหลดโปรแกรมได้จากอินเทอร์เน็ตโดยไม่มีค่าใช้จ่ายใดๆ (Free Download) สามารถรับ-ส่งไฟล์และโฟลเดอร์ได้ด้วยระบบ LAN แบบ Pop up ที่รองรับหลากหลายแพลตฟอร์ม (Platform คือ ฐานงานที่รองรับระบบปฏิบัติการ) โดยใช้โปรโตคอลแบบ TCP/IP และตัวโปรแกรมไม่ต้องอาศัยแม่ข่าย (Server) เป็นตัวกลาง นอกจากนี้ยังใช้เป็นโปรแกรมสนทนา (Chat) โต้ตอบกันกับปลายทางในระบบ LAN หรือเครือข่ายส่วนตัวได้อีกช่องทางหนึ่ง โดยใช้ความสามารถของ TCP/IP (UDP) ในการสนทนาอย่างสะดวก รวดเร็ว เนื่องจากโปรแกรมมีขนาดเล็ก กะทัดรัด เบา ง่ายต่อการใช้งาน และไม่ต้องการเบราว์เซอร์ รวมทั้งใช้ในการเข้ารหัสข้อความ (Encryption) เพื่อป้องกันข้อมูลหรือข้อความตั้งต้นที่ต้องการส่งไปถึงผู้รับได้อีกด้วย

ในส่วนของผู้ดูแลระบบคอมพิวเตอร์ จะใช้โปรแกรม IP Messenger (IPMsg) ในการสื่อสาร หรือทดสอบการทำงานของคอมพิวเตอร์ว่าสามารถสื่อสารถึงกันได้หรือไม่ รวมทั้งการประยุกต์ใช้งานในการสื่อสารกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร ซึ่งสามารถควบคุมจำนวนอุปกรณ์คอมพิวเตอร์ และการเปลี่ยนค่า IP Address ได้อย่างแม่นยำ

#### (1) ขั้นตอนการรับ-ส่งข้อมูลอิเล็กทรอนิกส์ด้วยโปรแกรม IP Messenger (IPMsg) ผ่าน IP Address

(1.1) เชื่อมโยงจำนวนเครื่องคอมพิวเตอร์ตามต้องการด้วยระบบ LAN และ Hub

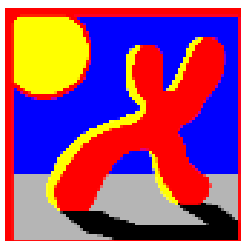
(1.2) ตั้งชื่อเครื่องคอมพิวเตอร์แต่ละเครื่องไม่ให้ซ้ำกัน

(1.3) ตั้งค่า IP address ของทุกเครื่องคอมพิวเตอร์ให้อยู่ในกลุ่มเดียวกัน

(1.4) ติดตั้งโปรแกรม IP Messenger (IPMsg) โดยการดาวน์โหลดโปรแกรม

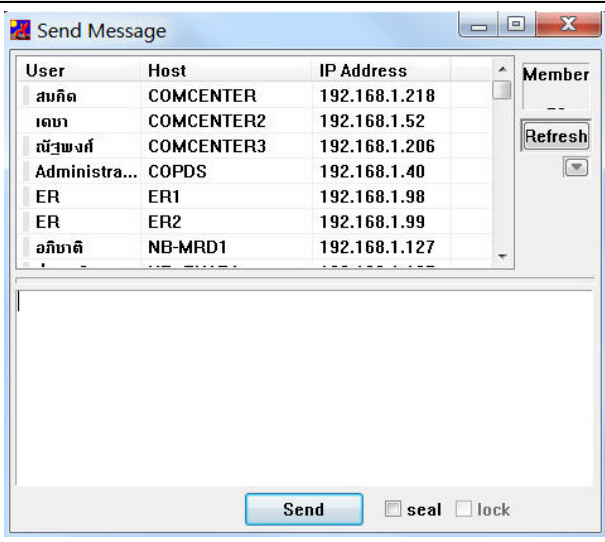
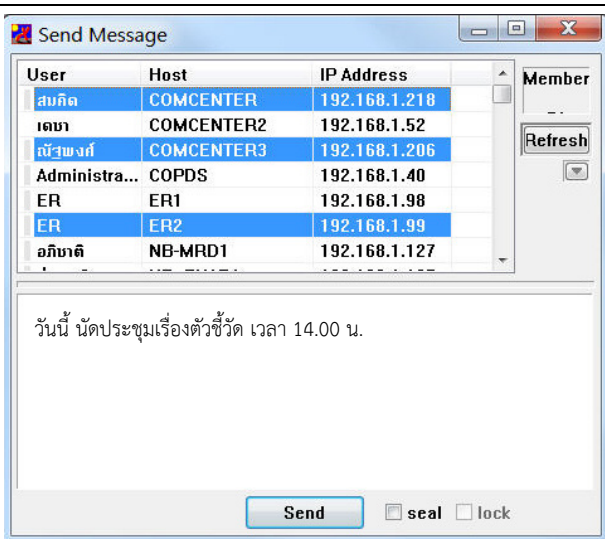
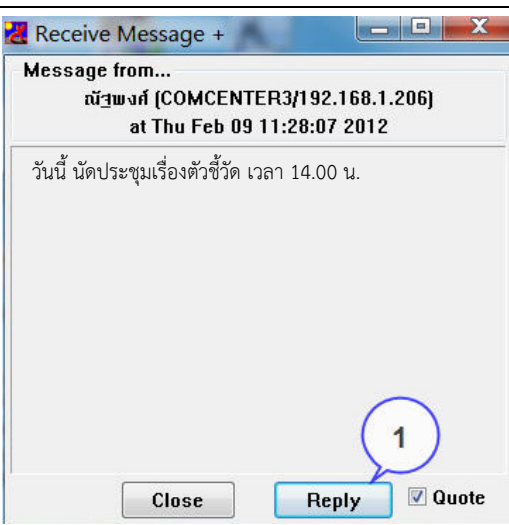
(1.5) รับ-ส่งข้อมูลอิเล็กทรอนิกส์ (Files, Folders) ด้วยโปรแกรม IP Messenger (IPMsg)

สามารถแสดงการใช้งานโปรแกรม IP Messenger (IPMsg) ผ่าน IP Address ได้ดังนี้



ภาพที่ 1 แสดงสัญลักษณ์ของโปรแกรม IP Messenger (IPMsg)

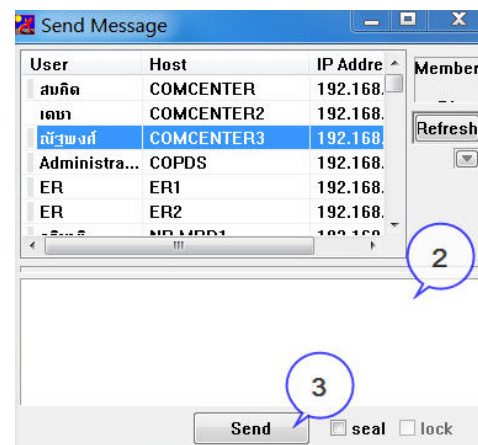
ตารางที่ 6 : ขั้นตอนการใช้งานโปรแกรม IP Messenger (IPMsg) ผ่าน IP Address

ขั้นตอนการใช้งานโปรแกรม IP Messenger (IPMsg) ผ่าน IP Address																																	
<p>1. เมื่อเริ่มเปิดการใช้งานโปรแกรมครั้งแรก โปรแกรมจะแสดงชื่อ User และ IP Address ของเครื่องคอมพิวเตอร์ทั้งหมดที่กำลังออนไลน์ใช้งานอยู่</p>	 <table border="1"> <thead> <tr> <th>User</th> <th>Host</th> <th>IP Address</th> <th>Member</th> </tr> </thead> <tbody> <tr> <td>สมคิด</td> <td>COMCENTER</td> <td>192.168.1.218</td> <td>--</td> </tr> <tr> <td>เดชา</td> <td>COMCENTER2</td> <td>192.168.1.52</td> <td></td> </tr> <tr> <td>ณัฐพงษ์</td> <td>COMCENTER3</td> <td>192.168.1.206</td> <td></td> </tr> <tr> <td>Administra...</td> <td>COPDS</td> <td>192.168.1.40</td> <td></td> </tr> <tr> <td>ER</td> <td>ER1</td> <td>192.168.1.98</td> <td></td> </tr> <tr> <td>ER</td> <td>ER2</td> <td>192.168.1.99</td> <td></td> </tr> <tr> <td>อภิชาติ</td> <td>NB-MRD1</td> <td>192.168.1.127</td> <td></td> </tr> </tbody> </table>	User	Host	IP Address	Member	สมคิด	COMCENTER	192.168.1.218	--	เดชา	COMCENTER2	192.168.1.52		ณัฐพงษ์	COMCENTER3	192.168.1.206		Administra...	COPDS	192.168.1.40		ER	ER1	192.168.1.98		ER	ER2	192.168.1.99		อภิชาติ	NB-MRD1	192.168.1.127	
User	Host	IP Address	Member																														
สมคิด	COMCENTER	192.168.1.218	--																														
เดชา	COMCENTER2	192.168.1.52																															
ณัฐพงษ์	COMCENTER3	192.168.1.206																															
Administra...	COPDS	192.168.1.40																															
ER	ER1	192.168.1.98																															
ER	ER2	192.168.1.99																															
อภิชาติ	NB-MRD1	192.168.1.127																															
<p>2. การส่งข้อความ คลิกที่ User ที่ต้องการจะส่งข้อความ -&gt; พิมพ์ข้อความที่ต้องการส่งลงในช่องดังกล่าว -&gt; คลิกปุ่ม Send</p>	 <p>วันนี้ นัดประชุมเรื่องตัวชี้วัด เวลา 14.00 น.</p>																																
<p>3. เครื่องปลายทางจะปรากฏข้อความดังกล่าว ถ้าต้องการตอบกลับให้กด -&gt; Reply</p>	 <p>Message from... ณัฐพงษ์ (COMCENTER3/192.168.1.206) at Thu Feb 09 11:28:07 2012</p> <p>วันนี้ นัดประชุมเรื่องตัวชี้วัด เวลา 14.00 น.</p> <p>1</p>																																

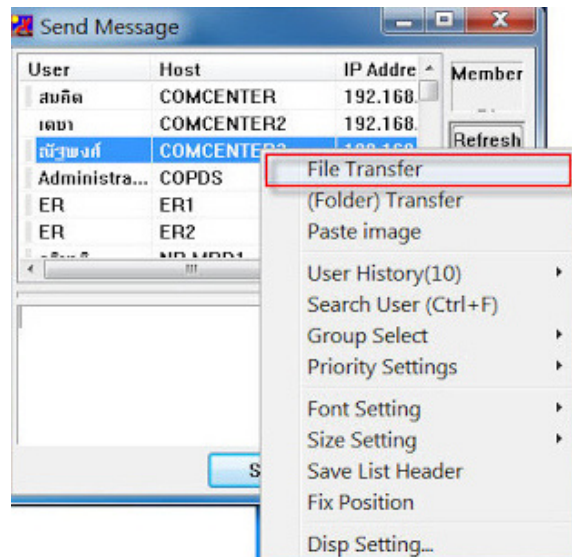
### ขั้นตอนการใช้งานโปรแกรม IP Messenger (IPMsg) ผ่าน IP Address

#### 4. การส่งไฟล์

คลิกที่ User ที่ต้องการจะส่ง -> คลิกปุ่ม  
Attach file -> เลือกไฟล์ -> Send

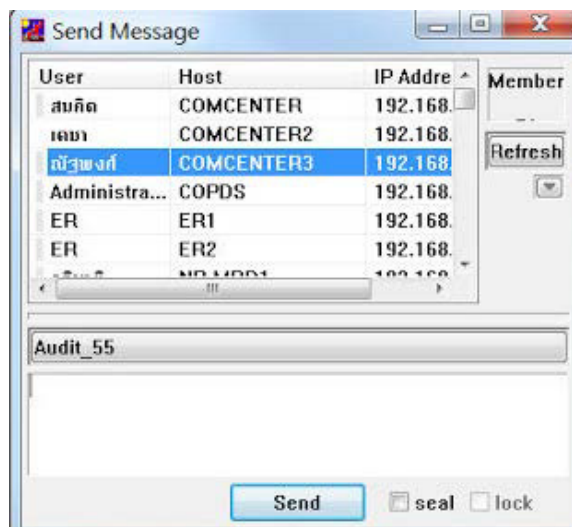


#### 5. แสดงขั้นตอนการแนบไฟล์เอกสารเพื่อ ส่งไฟล์



#### 6. การส่งโฟลเดอร์

คลิกที่ User ที่ต้องการจะส่ง -> คลิกปุ่ม  
Attach Folder -> เลือกโฟลเดอร์ที่  
ต้องการส่ง -> Send



## (2) ประโยชน์ของโปรแกรม IP Messenger (IPMsg)

- รวดเร็ว
- (2.1) สามารถใช้ติดต่อสื่อสารในระบบ LAN ด้วยข้อความได้อย่างรวดเร็ว
  - (2.2) สามารถโอนถ่ายข้อมูลขนาดใหญ่ได้ด้วยเวลาที่รวดเร็ว
  - (2.3) สามารถส่งรูปได้
  - (2.4) สามารถสนทนา (Chat) กับปลายทางในระบบ LAN หรือเครือข่ายส่วนตัว โดยใช้ความสามารถของ IP Address
  - (2.5) ขนาดกะทัดรัด เบา และ ง่ายต่อการใช้งาน

## (3) ข้อดีของโปรแกรม IP Messenger (IPMsg)

- (3.1) ไม่จำเป็นต้องมีเครื่องแม่ข่าย (Server) สำหรับการสื่อสารระหว่างคอมพิวเตอร์ตั้งแต่ 2 เครื่อง ขึ้นไป
- (3.2) สามารถถ่ายโอนไฟล์และโพลเดอร์ขนาดใหญ่ได้ทันทีบนเครือข่ายท้องถิ่น (Local Network)
- (3.3) สามารถควบคุมการรับ-ส่งข้อมูลอิเล็กทรอนิกส์ให้อยู่ในองค์กรไม่รั่วไหลไปสู่ภายนอกได้ร้อยละ 100
- (3.4) ไม่ต้องทำการ Auto Refresh เมื่อมีผู้ใช้คนใหม่เข้า/ออกจากระบบ (คือ การสั่งให้จอภาพแสดงภาพใหม่ตามข้อสนเทศที่ได้รับหลังสุด เช่น สั่งให้แสดงรายชื่อแฟ้มข้อมูลในงานบันทึกใหม่)
- (3.5) ไม่ต้องใช้งบประมาณในการติดตั้งโปรแกรม IP Messenger (IPMsg) ในการรับ-ส่งข้อมูลอิเล็กทรอนิกส์ระหว่างกัน

## (4) ข้อจำกัดของโปรแกรม IP Messenger (IPMsg)

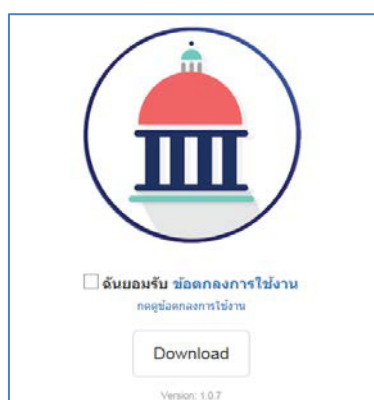
- (4.1) ไม่สามารถโอนไฟล์เป็นโพลเดอร์ได้
- (4.2) ไม่สามารถโอนไฟล์ผ่าน LAN อื่นๆ ได้
- (4.3) ไม่มีระบบความช่วยเหลือ
- (4.4) ไม่แสดงแถบแสดงผลการถ่ายโอนข้อมูลไปยังผู้รับ

### 1.3) การใช้แอปพลิเคชัน G-Chat ในสังคมออนไลน์ (Social Network)

G-Chat คือ แอปพลิเคชันความปลอดภัยสูงสุดสำหรับภาครัฐ ซึ่งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) หรือ DGA ได้พัฒนา G-Chat เพื่อใช้ภายในหน่วยงานภาครัฐเท่านั้น โดยสามารถสร้างห้องสนทนา รับ-ส่งข้อความ ประสานงาน ระดมความคิด ประชุมทางไกล และพูดคุยด้วยการโทรผ่านแอปพลิเคชันหรือวิดีโอคอลล์ที่มีประสิทธิภาพ และมีความปลอดภัยระดับสากล จึงแนะนำให้ทุกหน่วยงานในภาครัฐใช้ G-Chat แทนแอปพลิเคชัน LINE หรือแอปพลิเคชันสนทนาอื่นๆ (chat) เพื่อความปลอดภัยของข้อความที่สนทนาหรือส่งไฟล์ราชการถึงกัน เพื่อแยกการสนทนาเรื่องส่วนตัวกับเรื่องงานออกจากกัน

G-Chat เป็นแอปพลิเคชันที่ได้รับการพัฒนาขึ้นเพื่อใช้เป็นระบบติดต่อสื่อสารแบบออนไลน์สำหรับหน่วยงานภาครัฐผ่านอุปกรณ์สื่อสารแบบเคลื่อนที่ เพื่อความมั่นคงปลอดภัยของ

ข้อมูล เนื่องจากแอปพลิเคชันต่างๆ ที่ใช้สนทนาบนอุปกรณ์พกพานั้น มีความเสี่ยงสูงต่อการถูกลักลอบใช้ข้อมูลและความลับทางราชการ อีกทั้งมีโอกาสเกิดการทุจริต ส่งผลต่อความเสียหายของทางราชการ และอาจกระทบต่อความมั่นคงของประเทศ นอกจากนี้ G-Chat มีการจัดการผู้ใช้ตามโครงสร้างของหน่วยงาน มีความเป็นส่วนตัว และมีความปลอดภัยของข้อมูล ซึ่งเป็นการปรับกระบวนการทำงานราชการสู่ยุครัฐบาลดิจิทัล รวมทั้งมีเมนูต่างๆ ใกล้เคียงกับแอปพลิเคชัน LINE ที่คุ้นเคยกันอย่างมาก สามารถใช้งานง่าย แทบจะไม่ต้องเรียนรู้อะไรใหม่ ซึ่งปัจจุบัน สพร. อยู่ระหว่างพัฒนาแอปพลิเคชันจาก version 1 เป็น version 2 โดยเมื่อดำเนินการแล้วเสร็จจะได้มีหนังสือเชิญชวนหน่วยงานราชการต่างๆ เพื่อให้สื่อสารในเครือข่ายสังคมออนไลน์ด้วยแอปพลิเคชันดังกล่าวต่อไป



ภาพที่ 2 แสดงสัญลักษณ์ของแอปพลิเคชัน G-Chat

#### ตารางที่ 7 : ความเป็นมาและการใช้งานแอปพลิเคชัน G-Chat

ความเป็นมาและการใช้งานแอปพลิเคชัน G-Chat	
<p>1. รัฐบาลได้มีสาธิตแอปพลิเคชัน G-Chat ในงาน eGovDay 2015 ให้ประชาชนได้ทดลองใช้งาน เห็นว่าการสื่อสารระหว่างหน่วยงานรัฐ ก็สามารถใช้แอปพลิเคชันนี้แทนแอปพลิเคชัน LINE ได้ และมีกลิ่นเม็ดเด่นๆ มากมาย คล้ายคลึงกัน</p>	
<p>2. การเปิดตัวของ G-Chat ในงาน eGovDay 2015</p>	

ความเป็นมาและการใช้งานแอปพลิเคชัน G-Chat	
<p>3. แสดงสติ๊กเกอร์ พร้อมวัน-เวลาที่ส่งข้อความถึงกัน มีให้เลือกใช้มากมาย ตามสถานการณ์โดยไม่ต้องพิมพ์ สามารถกดส่งได้ทันทีด้วยสติ๊กเกอร์ ข้อความที่คุ้นเคย รวมถึงสติ๊กเกอร์ คำนิยม 12 ประการด้วย</p>	
<p>4. แสดงการแชร์สถานที่ที่อยู่ปัจจุบัน</p> <p>5. แสดงการสนทนาในกลุ่ม (Group Chat) มีเวลาบอกละเอียด รวมทั้งแสดงให้เห็นด้วยว่าในกลุ่มได้อ่านแล้วกี่คน</p>	
<p>6. แสดงการตั้งค่าเบื้องต้นที่จำเป็น เช่น ขนาดตัวอักษร และการแจ้งเตือน เป็นต้น</p>	

### ความสามารถและคุณสมบัติของ G-Chat

1. บริหารจัดการ เลือกรูปแบบการใช้งาน และปรับแต่งตามความต้องการของหน่วยงาน โดยผู้ดูแลระบบของแต่ละหน่วยงาน
2. สร้างห้องสนทนาเฉพาะกลุ่ม โดยกำหนดเลือกเจ้าหน้าที่ต่างแผนกให้เป็นสมาชิกในห้องเดียวกันได้ หรือเชิญให้เข้าเป็นสมาชิกตามความสมัครใจ โดยไม่จำกัดจำนวนสมาชิก



3. สร้างห้องสนทนาที่กำหนดให้มีการระบุพิกัดตำแหน่ง (Location Sharing) ของสมาชิกทุกคนเมื่อส่งข้อความ
4. สืบค้นข้อความได้
5. สมาชิกใหม่ในห้องสนทนาสามารถเห็นข้อความที่โพสต์ไว้ตั้งแต่เริ่มสร้างห้องได้
6. ผู้ส่งข้อความสามารถตรวจสอบรายชื่อผู้อ่านข้อความแล้วได้
7. กำหนดให้สื่อสารข้ามหน่วยงานได้
8. ใช้งานได้จากอุปกรณ์สื่อสารเคลื่อนที่และคอมพิวเตอร์ส่วนบุคคล

## 2) แนวทางในการแก้ปัญหาหรือพัฒนาบุคลากรของสำนักงานปลัดกระทรวงการคลังด้านการสื่อสารในระบบเทคโนโลยีสารสนเทศ

เนื่องจากบุคลากรของทุกหน่วยงานเป็นปัจจัยหลักสำคัญที่ทำให้องค์กรประสบความสำเร็จในการดำเนินการด้านต่างๆ จึงต้องมีการพัฒนาเสริมสร้างองค์ความรู้อย่างต่อเนื่อง โดยเฉพาะด้านการสื่อสารในระบบเทคโนโลยีสารสนเทศซึ่งมีการเปลี่ยนแปลงอย่างรวดเร็ว เพื่อให้ตระหนักรู้ เท่าทันเหตุการณ์ต่างๆ และสามารถป้องกันภัยที่เกิดขึ้นได้อย่างมีประสิทธิภาพ มีข้อมูลราชการถูกนำไปใช้หาประโยชน์ส่วนตนซึ่งจะก่อให้เกิดผลเสียหายต่อความมั่นคงของประเทศ ทั้งนี้ ในส่วนของการวิเคราะห์ SWOT Analysis “ข้อ 2.2.2 ตารางที่ 3 ข้อมูลที่นำมาวิเคราะห์สถานการณ์การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง” ด้านจุดอ่อน ปรากฏว่าในภาพรวมบุคลากรของสำนักงานปลัดกระทรวงการคลังยังมีความคิดริเริ่มสร้างสรรค์ การทำงานในเชิงรุก การประสานงาน และถ่ายทอดความรู้ รวมทั้งการประชาสัมพันธ์บทบาทหน้าที่และงานขององค์กรไม่เพียงพอ ดังนั้น จึงต้องมีการแก้ไขปัญหาโดยบุคลากรทุกคนต้องพัฒนาองค์ความรู้ของตนเองและตระหนักรู้เท่าทันภัยคุกคามจากการใช้ระบบสารสนเทศและอินเทอร์เน็ต รวมทั้งมีความรู้ความเข้าใจและดำเนินการป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพทั้งในส่วนที่ต้องกระทำและงดเว้นการกระทำ

ในส่วนของการพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงการคลังมีการจัดทำโครงการตามแผนพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสารให้แก่บุคลากรในสังกัดกระทรวงการคลังโดยใช้เงินกองทุนพัฒนาบุคลากรของกระทรวงการคลังเป็นประจำทุกปี เพื่อพัฒนาบุคลากรของกระทรวงการคลังให้มีสมรรถนะด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศพร้อมรองรับการเปลี่ยนแปลงที่เกิดขึ้นอย่างรวดเร็วในยุคเศรษฐกิจดิจิทัล และเพื่อเรียนรู้การสร้างสัมพันธภาพที่ดี รวมทั้งการสร้างเครือข่ายที่เข้มแข็งสามารถพึ่งพาติดต่อประสานงานระหว่างกันได้ ทั้งนี้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เป็นผู้รับผิดชอบโครงการฝึกอบรมที่เกี่ยวกับการพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยการกำหนดหลักสูตร การเรียนการสอน การฝึกทดสอบ การปฏิบัติงานจริง ให้สอดคล้องกับนโยบายของกระทรวงการคลัง ประกอบกับสำนักงานคณะกรรมการข้าราชการพลเรือน (ก.พ.) ได้มีแนวทางพัฒนาทักษะด้านดิจิทัลของข้าราชการและบุคลากรภาครัฐ เพื่อการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล ในทักษะด้านดิจิทัลของข้าราชการและบุคลากรภาครัฐ ในมิติที่ 1 รู้เท่าทันและใช้เทคโนโลยีเป็น (Digital Literacy) ซึ่งได้ให้ความหมายของ Digital Literacy คือ ทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล หรือ Digital Literacy หมายถึง ทักษะในการนำเครื่องมือ อุปกรณ์ และเทคโนโลยีดิจิทัลที่มีอยู่ในปัจจุบัน อาทิ คอมพิวเตอร์ โทรศัพท์ แท็บเล็ต โปรแกรมคอมพิวเตอร์ และสื่อออนไลน์ มาใช้ให้เกิดประโยชน์สูงสุด

ในการสื่อสาร การปฏิบัติงาน และการทำงานร่วมกัน หรือใช้เพื่อพัฒนากระบวนการทำงาน หรือระบบงาน ในองค์กรให้มีความทันสมัยและมีประสิทธิภาพ ครอบคลุมความสามารถ 4 มิติ ได้แก่ 1) การใช้ (Use) 2) เข้าใจ (Understand) 3) การสร้าง (Create) 4) เข้าถึง (Access) เทคโนโลยีดิจิทัล ได้อย่างมีประสิทธิภาพ นอกจากนี้ได้แบ่งประเภทของทักษะความเข้าใจและการใช้เทคโนโลยีดิจิทัลไว้ 9 ด้าน ได้แก่ 1) การใช้งานคอมพิวเตอร์ 2) การใช้โปรแกรมประมวลคำ 3) การใช้โปรแกรมสร้างสื่อดิจิทัล 4) การใช้งานอินเทอร์เน็ต 5) การใช้โปรแกรมตารางคำนวณ 6) การทำงานร่วมกันแบบออนไลน์ 7) การใช้งานเพื่อความมั่นคงปลอดภัย 8) การใช้โปรแกรมการนำเสนอผลงาน และ 9) การใช้ดิจิทัลเพื่อความมั่นคงปลอดภัย เพื่อให้ทุกส่วนราชการ หน่วยงานของรัฐ องค์กรกลางบริหารงานบุคคล และหน่วยงานที่เกี่ยวข้อง นำแนวทางการพัฒนาทักษะด้านดิจิทัลดังกล่าวไปปรับใช้ในการพัฒนาและเสริมสร้างกำลังคนในสังกัดทันต่อการเปลี่ยนแปลงที่สำคัญ รวมทั้งใช้เป็นกลไกสำคัญในการพัฒนาและเสริมสร้างศักยภาพกำลังคนภาครัฐ ในการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล โดยให้ข้าราชการและบุคลากรภาครัฐเร่งพัฒนาตนเองและสนับสนุนการพัฒนาผู้อื่นอย่างต่อเนื่อง

ในการนี้ กระทรวงการคลังมีนโยบายที่จะพัฒนาบุคลากรของกระทรวงการคลังทุกระดับ ให้มีความรู้ความสามารถด้าน Digital Literacy ให้สามารถใช้ปฏิบัติงานในทุกส่วนราชการในสังกัดได้อย่างมีประสิทธิภาพ ซึ่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง ในฐานะเป็นศูนย์พัฒนาบุคลากรของกระทรวงการคลังด้าน Digital Literacy ได้จัดให้มีการฝึกอบรมวิชาการด้าน Digital Literacy ประจำปีงบประมาณ พ.ศ. 2562 แก่เจ้าหน้าที่ของกระทรวงการคลัง จำนวน 10 หลักสูตร ดังต่อไปนี้

ตารางที่ 8 : หลักสูตรการฝึกอบรมวิชาการด้าน Digital Literacy ประจำปีงบประมาณ พ.ศ. 2562 ของกระทรวงการคลัง

ลำดับ ที่	ชื่อหลักสูตร	วันที่
1	การสร้าง Infographic ในยุค Digital Content	18-22 มีนาคม 2562
2	การออกแบบและจัดการฐานข้อมูลด้วย Microsoft Access	25-29 มีนาคม 2562
3	การใช้งานโปรแกรม Office ด้วย Google Drive (Google Docs)	1 เมษายน 2562
4	การใช้งานโปรแกรม Microsoft Office 2016	22-26 เมษายน 2562
5	เรียนรู้การใช้งานโปรแกรม PowToon	22-24 พฤษภาคม 2562
6	การสร้างเว็บไซต์แบบมีอาชีพด้วย WordPress	27-29 พฤษภาคม 2562
7	การสร้างแบบสำรวจอัจฉริยะ ด้วย Google Form	30 พฤษภาคม 2562
8	Microsoft PowerPoint 2016	11-13 มิถุนายน 2562
9	Functional & Data Analytics Using Microsoft Excel	24-25 มิถุนายน 2562
10	การเขียนโปรแกรมด้วย Excel VBA	26-28 มิถุนายน 2562

จากการพิจารณาหลักสูตรด้าน Digital Literacy ดังกล่าว ปรากฏว่ายังไม่ได้จัดให้มีการฝึกอบรมเรื่องการพัฒนาทักษะความเข้าใจและการใช้งานเพื่อความมั่นคงปลอดภัย รวมทั้งการใช้ดิจิทัลเพื่อความมั่นคงปลอดภัย ตามที่สำนักงาน กพ. กำหนด ทั้งนี้ การบริหารจัดการบุคลากรในสังกัด

สำนักงานปลัดกระทรวงการคลังด้าน Digital Literacy จะต้องนำภูมิหลังที่ได้มีการวิเคราะห์ SWOT Analysis ดังกล่าวข้างต้นมาประกอบการจัดทำหลักสูตรด้วย พร้อมทั้งกำหนดตัวชี้วัดเพื่อใช้วัดสถานะ ความรู้ความเข้าใจของผู้เข้ารับการฝึกอบรมให้สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ

อย่างไรก็ตาม ในเบื้องต้นผู้จัดทำรายงานจะได้ประสานหน่วยงานรับผิดชอบหลักสูตร เพื่อให้เห็นความสำคัญของการถ่ายทอดองค์ความรู้ให้ผู้เข้ารับการฝึกอบรมมีความตระหนักรู้เท่าทัน เหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่างๆ ที่เกิดขึ้นอย่างรวดเร็ว และสามารถป้องกันภัย ที่เกิดขึ้นได้อย่างมีประสิทธิภาพเพื่อมิให้ข้อมูลราชการถูกนำไปใช้หาประโยชน์ส่วนตนซึ่งจะก่อให้เกิด ผลเสียหายต่อราชการและความมั่นคงของประเทศต่อไป

### 3) แนวทางการแก้ปัญหาหรือพัฒนานโยบายด้านกฎหมาย ระเบียบ และแนวทางการปฏิบัติที่เกี่ยวข้อง

สืบเนื่องจากได้มีประกาศสำนักงานปลัดกระทรวงการคลัง เรื่อง แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง พ.ศ. 2559 ซึ่งมีข้อกำหนดเกี่ยวกับแนวทางการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจนแล้ว อย่างไรก็ตาม ในการนำแนวนโยบายดังกล่าวไปปฏิบัติยังสร้างความตระหนักรู้แก่ผู้ใช้งานในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ (information security awareness) ไม่เข้มข้นและจริงจัง เท่าที่ควรตามที่ได้กำหนดไว้ในประกาศฯ “ข้อ 6 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และเพื่อป้องกันการ เข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ข้อ 6.1 สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม” ดังนั้น จึงควรมีการบังคับใช้ประกาศฯ ดังกล่าว อย่างเคร่งครัด และต่อเนื่อง รวมทั้งนำไปใช้ในการฝึกอบรมบุคลากรด้าน Digital Literacy เพื่อสร้างความรู้ความเข้าใจตามข้อ 2 ต่อไป เพื่อมิให้การใช้งานระบบสารสนเทศทั้งในระดับนโยบาย และระดับปฏิบัติในการควบคุมการใช้งานระบบคอมพิวเตอร์และสินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ เป็นต้น อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

จากการนำเสนอแนวทางการแก้ไขปัญหาคือพัฒนานโยบายเกี่ยวกับการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศดังกล่าวข้างต้นนั้น จะสามารถดำเนินการได้ทั้งระบบอย่างเข้มข้น จริงจัง และต่อเนื่อง หากผู้จัดทำรายงานได้รับการแต่งตั้งให้ดำรงตำแหน่งผู้ช่วยปลัดกระทรวงการคลัง เนื่องจากเป็นตำแหน่งที่มีขอบเขตความรับผิดชอบในการช่วยปลัดกระทรวงการคลังในการปฏิบัติงาน เทคโนโลยีสารสนเทศและการสื่อสาร การวางแผน บริหารจัดการและบูรณาการร่วมมือกับหน่วยงาน ในสังกัดกระทรวงการคลัง และหน่วยงานต่างๆ ที่เกี่ยวข้อง เพื่อเสริมสร้างศักยภาพและสนับสนุน ทุกภาคส่วนให้เป็นพลังร่วมในการพัฒนางานในกระทรวงการคลัง รวมตลอดถึงการบริหารความเสี่ยง และวางแผนเพื่อกำหนดแนวทางการดำเนินงานในสำนักงานปลัดกระทรวงการคลังให้สอดคล้องกับ ทิศทาง นโยบาย ยุทธศาสตร์สำนักงานปลัดกระทรวงการคลัง แผนปฏิบัติราชการให้ตรงตามเป้าหมาย ความสำเร็จ โดยเชื่อมโยงกับพันธกิจของสำนักงานปลัดกระทรวงการคลังและกระทรวงการคลัง ในการ ปรับปรุงแนวทาง มาตรฐาน ระบบงาน กฎหมาย กฎ ระเบียบ ข้อบังคับ หลักเกณฑ์และวิธีปฏิบัติในเรื่อง ต่างๆ ในสำนักงานปลัดกระทรวงการคลัง เพื่อการปฏิบัติราชการที่มีประสิทธิภาพและประสิทธิผล ทันท่วง

การเปลี่ยนแปลง และตอบสนองความต้องการของประชาชน ซึ่งเมื่อการดำเนินการยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลังสำเร็จแล้ว จะขยายไปยังทุกส่วนราชการในสังกัดกระทรวงการคลัง เมื่อสำเร็จแล้วจะเป็นองค์กระต้นแบบของหน่วยงานภาครัฐทั่วประเทศต่อไป

#### 2.2.4 ปัจจัยที่อาจมีผลกระทบต่อความสำเร็จของการดำเนินการตามข้อเสนอ และแนวทางการบริหารจัดการที่เป็นรูปธรรม

การดำเนินการด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลังและกระทรวงการคลัง มีปัจจัยความสำเร็จรวม 4 เรื่อง ตามหลักการบริหาร 4 M ดังนี้

ตารางที่ 9 : การวิเคราะห์ผลกระทบต่อความสำเร็จของการดำเนินการตามข้อเสนอ และแนวทางการบริหารจัดการที่เป็นรูปธรรม

ลำดับที่	ปัจจัยความสำเร็จตามหลักการบริหาร 4 M	ผลกระทบ	แนวทางการบริหารจัดการที่เป็นรูปธรรม
1	Material ได้แก่ เครื่องมือในการดำเนินการ คือ ระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของกระทรวงการคลัง โปรแกรม IP Messenger และแอปพลิเคชัน G-Chat ซึ่งเป็นเครื่องมือที่สามารถนำมาใช้ได้ทันที	ไม่มี	-
2	Money ในการใช้เครื่องมือดังกล่าวตามข้อ 1 ไม่ต้องใช้เงินงบประมาณแต่ประการใด	ไม่มี	-
3	Man ปัจจัยแห่งความสำเร็จขึ้นอยู่กับบุคลากรที่เป็นจุดอ่อนจากการวิเคราะห์ SWOT Analysis	อาจเกิดผลกระทบจากความรู้เท่าไม่ถึงการณ์ของบุคลากรในการใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสาร โดยเห็นว่าเป็นเรื่องไม่สำคัญ จึงไม่ให้ความร่วมมือในการป้องกันภัยคุกคามในการสื่อสารด้วยระบบเทคโนโลยีสารสนเทศ	ผู้บริหารระดับสูงมอบนโยบายและกำชับให้บุคลากรในสังกัดทั้งหน่วยงานรับผิดชอบดำเนินการเป็นกลไกในการบังคับใช้กฎหมาย และแนวนโยบายต่างๆ อย่างเคร่งครัด รวมถึงตลอดถึงผู้ใช้งานเพื่อให้เข้ารับการฝึกอบรมด้านคอมพิวเตอร์ และศึกษาแนวนโยบายตามประกาศสำนักงานปลัดกระทรวงการคลังฯ จนเกิดความเข้าใจและนำไปปฏิบัติ

ลำดับ ที่	ปัจจัยความสำเร็จ ตามหลักการบริหาร 4 M	ผลกระทบ	แนวทางบริหารจัดการ ที่เป็นรูปธรรม
			ได้อย่างจริงจัง โดยต้องมีการ วัดผลการเรียนการสอนเป็น ระยะๆ อย่างต่อเนื่อง จน สามารถตระหนักรู้เท่าทัน และจำขึ้นใจถึงความสำคัญ และจำเป็นที่จะต้องมีการ ใช้เครื่องมือต่างๆ ของภาครัฐ ในการสื่อสารด้วยระบบ เทคโนโลยีสารสนเทศ
4	Management ในการบริหารจัดการเพื่อให้สามารถ ดำเนินการด้านการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของสำนักงาน ปลัดกระทรวงการคลังและกระทรวงการคลัง อย่างจริงจังและต่อเนื่อง ได้มีประกาศ สำนักงานปลัดกระทรวงการคลังกำหนด แนวนโยบายในการดำเนินงานไว้ด้วยแล้ว จึงสามารถบังคับใช้อย่างเคร่งครัดได้ทันที	ไม่มี	-

### 2.3 ภาวะผู้นำเพื่อการขับเคลื่อนข้อเสนอ

การดำเนินการด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง และกระทรวงการคลัง จะสามารถขับเคลื่อนให้เกิดเป็นรูปธรรมจนประสบความสำเร็จได้ด้วยผู้นำที่มีคุณลักษณะที่สำคัญ ดังนี้

#### 2.3.1 ความรู้ (Knowledge)

1) มีความรู้ความเข้าใจนโยบายรัฐบาล ยุทธศาสตร์ และกลยุทธ์ในระดับต่างๆ ที่เกี่ยวข้องกับ  
กับภารกิจของสำนักงานปลัดกระทรวงการคลัง

2) มีความรู้ความเข้าใจเรื่องในอนาคตเกี่ยวกับภารกิจของสำนักงานปลัดกระทรวงการคลัง  
และกระทรวงการคลังภายใต้ยุทธศาสตร์ชาติ ระยะ 20 ปี

3) มีความรู้ความเข้าใจบริบทที่เปลี่ยนแปลงไปของสำนักงานปลัดกระทรวงการคลังและ  
กระทรวงการคลัง สามารถวิเคราะห์ยุทธศาสตร์ รวมทั้งปรับบทบาทและภารกิจของส่วนราชการ  
ในสังกัดให้มีความเหมาะสม สอดรับในทิศทางเดียวกันได้อย่างชัดเจน

4) มีความรู้ความเข้าใจกระบวนการของงานสนับสนุนการดำเนินการกิจของสำนักงาน  
ปลัดกระทรวงการคลังและกระทรวงการคลัง เช่น งานเทคโนโลยีสารสนเทศและการสื่อสาร และงาน  
พัฒนาระบบบริหารทั้งหมด เป็นต้น

5) มีความรอบรู้ด้านการบริหารคน ด้านการบริหาร การบริหารแบบมีอาชีพ และการบริหารแบบมุ่งผลสัมฤทธิ์

### 2.3.2 ทักษะ (Skills)

- 1) ทักษะในการวางแผน และการแก้ปัญหาเชิงกลยุทธ์
- 2) ทักษะด้านความเป็นผู้นำการเปลี่ยนแปลง
- 3) ทักษะด้านการตัดสินใจ
- 4) ทักษะด้านการปรับตัวและความยืดหยุ่น
- 5) ทักษะด้านความคิดที่แปลกใหม่และความคิดเชิงกลยุทธ์
- 6) ทักษะด้านความคิดเชิงประมวลผล
- 7) ทักษะด้านความเข้าใจในสื่อยุคใหม่
- 8) ทักษะด้านการปรับเปลี่ยนภาครัฐให้เป็นรัฐบาลดิจิทัล
- 9) ทักษะด้านเทคโนโลยีและคอมพิวเตอร์

### 2.3.3 ความสามารถ (Ability)

- 1) การใช้อุปกรณ์ด้านเทคโนโลยีสารสนเทศได้อย่างครบวงจร
- 2) การออกแบบงานเชิงนวัตกรรม และการส่งเสริมให้เกิดนวัตกรรม และการคิดสร้างสรรค์
- 3) การประยุกต์ความรู้หลากหลายด้าน
- 4) ความสามารถและทักษะในการสื่อสาร
- 5) การประสานสัมพันธ์
- 6) การบริหารทรัพยากร

### 2.3.4 คุณลักษณะอื่นที่จำเป็น (Other Characteristic)

- 1) การมีจิตมุ่งบริการ
- 2) การทำงานเป็นทีม
- 3) การทำงานให้บรรลุผลสัมฤทธิ์
- 4) ความรับผิดชอบตรวจสอบได้
- 5) การประยุกต์ใช้ปรัชญาของเศรษฐกิจพอเพียง

### 3.แผนพัฒนาตนเอง

(ข้อมูลส่วนบุคคล ไม่เผยแพร่)

## บรรณานุกรม

- โรงพยาบาลสมเด็จพระยุพราชด่านซ้าย. (2555). คู่มือการใช้งานโปรแกรม IP Messenger. สืบค้นเมื่อวันที่ 27 มีนาคม 2562. จาก <http://imt-dansai.blogspot.com/2012/02/ip-messenger-messenger-open-source-hiroaki.html>
- สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (2550). พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549. สืบค้นเมื่อวันที่ 20 มีนาคม 2562. จาก [http://www.etcommission.go.th/files/law/saft\\_etc\\_public.pdf](http://www.etcommission.go.th/files/law/saft_etc_public.pdf)
- สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2558). บริการ G-Chat. สืบค้นเมื่อวันที่ 27 มีนาคม 2562. จาก <https://www.dga.or.th/th/profile/978/>
- สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2561). ข้อกำหนดและเงื่อนไขการให้บริการ (Service Level Agreement) ระบบจดหมายอิเล็กทรอนิกส์กลาง เพื่อการสื่อสารของหน่วยงานภาครัฐ (MailGoThai). สืบค้นเมื่อวันที่ 30 มีนาคม 2562. จาก [https://onlinereport.mail.go.th/Document/SLA\\_Mail\\_Mailgothai.pdf](https://onlinereport.mail.go.th/Document/SLA_Mail_Mailgothai.pdf)
- สำนักงานคณะกรรมการพัฒนาระบบราชการ. (2550). มติคณะรัฐมนตรี เมื่อวันที่ 18 ธันวาคม 2550. สืบค้นเมื่อวันที่ 27 มีนาคม 2562. จาก <https://www.it.chula.ac.th/sites/default/files/doc/mail-cabinet-501218.pdf>
- สำนักงานปลัดกระทรวงการคลัง. (2559). ประกาศ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง พ.ศ. 2559. สืบค้นเมื่อวันที่ 20 มีนาคม 2562. จาก [https://www.mof.go.th/home/eco/230359\\_ICT\\_I\\_Security\\_Policy\\_ICTMOF.pdf](https://www.mof.go.th/home/eco/230359_ICT_I_Security_Policy_ICTMOF.pdf)
- สำนักงานปลัดกระทรวงการคลัง. (2560). แผนยุทธศาสตร์สำนักงานปลัดกระทรวงการคลัง ปีงบประมาณ พ.ศ. 2560 – 2564. สืบค้นเมื่อวันที่ 20 มีนาคม 2562. จาก <http://mof.go.th/home/plan/STRBOOK60-64.pdf>
- สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. (2561). ประกาศ เรื่อง ยุทธศาสตร์ชาติ (พ.ศ. 2561 – 2580). สืบค้นเมื่อ 20 มีนาคม 2562. จาก [http://www.ratchakittha.soc.go.th/DATA/PDF/2561/A/082/T\\_0001.PDF](http://www.ratchakittha.soc.go.th/DATA/PDF/2561/A/082/T_0001.PDF)



## ประวัติผู้เขียนรายงานการศึกษาส่วนบุคคล

ชื่อ - สกุล นางสาวสิริกานต์ มหาสิทธิ์ระกุล

### ประวัติการศึกษา

ปริญญาตรี	บริหารธุรกิจบัณฑิต (การบัญชี)	มหาวิทยาลัยรามคำแหง	ปี พ.ศ. 2526
	นิติศาสตรบัณฑิต	มหาวิทยาลัยสุโขทัย ธรรมมาธิราช	ปี พ.ศ. 2554
ปริญญาโท	ศิลปศาสตรมหาบัณฑิต (รัฐศาสตร์สำหรับนักบริหาร)	มหาวิทยาลัยสุโขทัย ธรรมมาธิราช	ปี พ.ศ. 2544

### ประสบการณ์การรับราชการ

วัน เดือน ปี	ตำแหน่ง	สังกัด
17 มีนาคม 2529	เจ้าหน้าที่ตรวจสอบภาษี 3	กรมสรรพสามิต
21 กรกฎาคม 2543	เจ้าหน้าที่ตรวจสอบภายใน 7 ว	กรมสรรพสามิต
1 กรกฎาคม 2547	เจ้าหน้าที่ตรวจสอบภายใน 7 ว	สำนักงานปลัดกระทรวงการคลัง
18 พฤศจิกายน 2547	เจ้าหน้าที่ตรวจสอบภายใน 8 ว	สำนักงานปลัดกระทรวงการคลัง
11 ธันวาคม 2551	นักวิชาการตรวจสอบภายใน ชำนาญการพิเศษ	สำนักงานปลัดกระทรวงการคลัง
21 เมษายน 2559	ผู้ตรวจสอบภายในกระทรวง	สำนักงานปลัดกระทรวงการคลัง

### ผลงานทางวิชาการ

1. กรณีศึกษาการสอบทานกรณีพิเศษ เพื่อสนับสนุนการปฏิบัติงานของคณะกรรมการตรวจสอบและประเมินผลประจำกระทรวงการคลัง
2. รายงานผลการตรวจสอบโครงการวิจัย เรื่อง การประเมินผลโครงการด้านโครงสร้างพื้นฐานจากผลิตภาพและความสามารถในการแข่งขันของประเทศ เพื่อการบริหารหนี้สาธารณะอย่างยั่งยืน

### รางวัลหรือทุนการศึกษา

-

### ตำแหน่งหน้าที่ปัจจุบันและสถานที่ทำงาน

ปัจจุบันดำรงตำแหน่ง ผู้ตรวจสอบภายในกระทรวง สำนักงานปลัดกระทรวงการคลัง