แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต 8

เรียน ผู้อำนวยการกลุ่มวางแผนการใช้ที่ดิน

ด้วยข้าพเจ้า นางทรายแก้ว อนากาศ ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ สังกัดกลุ่มวางแผนการใช้ที่ดิน สำนักงานพัฒนาที่ดินเขต 8 กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ หลักสูตร “ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล” ระหว่างวันที่ 6 มกราคม 2564 ถึงวันที่ 19 มกราคม 2564 เป็นเวลารวมทั้งสิ้น 3 ชั่วโมง ณ สำนักงานพัฒนาที่ดินเขต 8 (การพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์ HRD: e-Learning) ซึ่งหลักสูตรดังกล่าวจัดโดย ศูนย์พัฒนาการเรียนรู้ทางไกล สถาบันพัฒนาข้าราชการพลเรือน สำนักงานคณะกรรมการข้าราชการพลเรือน

บัดนี้ ข้าพเจ้าได้เข้ารับพัฒนาความรู้ฯ หลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการพัฒนาความรู้ฯ ดังนี้

1. การพัฒนาความรู้ฯ ดังกล่าวมีวัตถุประสงค์เพื่อ

1.1 เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเทอร์เน็ตได้

1.2 เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวังได้อย่างถูกต้อง

1.3 เพื่อให้สามารถอธิบายและยกตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

1.4 เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันและตรวจสอบความปลอดภัยได้ด้วยตนเอง

2. เนื้อหาและหัวข้อวิชาของการพัฒนาความรู้ฯ มีดังนี้

<u>2.1 สถานการณ์การใช้งานอินเทอร์เน็ต และการเปลี่ยนแปลงต่าง</u> ๆ

1) แนวโน้มการใช้งานอินเทอร์เน็ต

ในช่วงระยะเวลา 10 ปี ตั้งแต่ปี ค.ศ. 2000 ถึงปี ค.ศ. 2010 ปริมาณผู้ใช้งานอินเทอร์เน็ตมีแนวโน้มการใช้งานเพิ่มสูงขึ้นแบบก้าวกระโดด โดยเกือบ 50 เปอร์เซ็นต์ของประชากรโลก สามารถเข้าถึงอินเทอร์เน็ตได้ ทำให้อินเทอร์เน็ตมีบทบาทสำคัญต่อการดำรงชีวิตประจำวัน เช่น การติดต่อสื่อสาร ส่งข้อความ ข่าวสาร รูปภาพ วีดิโอคอนเฟอเรนซ์ (video conference) ปัจจุบันแนวโน้มการใช้งานอินเทอร์เน็ตส่วนใหญ่จะเป็นรูปแบบสื่อสังคมออนไลน์ (Social Media) ผู้ไม่ประสงค์ดีหรืออาชญากรก็มีแนวโน้มที่จะเปลี่ยนแปลงตัวเองให้ปรับตัวเข้ากับสถานการณ์หรือการใช้งานอินเทอร์เน็ตที่เป็นปัจจุบัน โดยเปลี่ยนรูปแบบการก่อเหตุให้มาเกิดขึ้นบนอินเทอร์เน็ตมากขึ้นและรุนแรงขึ้น เช่น การหลอกลวงผ่านเครือข่ายอินเทอร์เน็ต

/มีต่อหน้า 2

2) สถิติการใช้งานของประเทศไทย

กลุ่มเป้าหมายที่ใช้งานอินเทอร์เน็ตค่อนข้างสูง คือ ประชากรอายุ 20 – 30 ปี โดยมีปริมาณ 60 – 70 เปอร์เซ็นต์ ซึ่งเป็นวัยที่กำลังอยากรู้อยากเห็น เรียนรู้โลก ทำให้ประชากรเหล่านี้มีโอกาสสุ่มเสี่ยงที่จะเผชิญโลกของอาชญากรรมหรือภัยคุกคามบนเครือข่ายอินเทอร์เน็ตค่อนข้างสูง อาจตกเป็นเหยื่อของกลุ่มมิจฉาชีพหรือผู้ไม่ประสงค์ดี นอกจากนี้ยังมีกลุ่มเป้าหมายอื่น ๆ ที่อาจตกเป็นเหยื่อได้ คือ กลุ่มผู้สูงวัย หลังวัยเกษียณ ถูกมิจฉาชีพหลอกลวง เช่น แก๊งคอลเซ็นเตอร์หลอกโอนเงิน สำหรับสถิติช่วงเวลาที่มีการใช้งานอินเทอร์เน็ตส่วนใหญ่ คือ ช่วงเวลาทำงาน ทำให้มีความสุ่มเสี่ยงไม่เฉพาะต่อผู้ใช้งานเอง ยังมีความสุ่มเสี่ยงต่อหน่วยงาน องค์กร บริษัทต่าง ๆ และหน่วยงานราชการด้วยเช่นกัน เนื่องจากเป็นสถานที่ทำงาน ที่มีผู้ใช้งานอินเทอร์เน็ตจำนวนมาก หากผู้ใช้งานนำไวรัสหรือมัลแวร์ จากที่บ้านหรือที่อื่นมาเผยแพร่ในที่ทำงาน ก็จะทำให้ที่ทำงานเป็นแหล่งเผยแพร่ กระจายไวรัสหรือมัลแวร์ หรือสิ่งที่ไม่เหมาะสมนั้นได้

3) ความสัมพันธ์และการกระจายตัวของข้อมูล

ปัจจุบันเป็นโลกของสังคมออนไลน์หรือ social media ความสัมพันธ์หรือความเชื่อมโยงของข้อมูลที่เกิดขึ้น เช่น ข้อมูลเดิม ๆ ที่เราเคยได้รับในสื่อโซเชียลมาก่อน เราอาจจะยังได้รับข้อมูลเดิม ๆ นั้นอยู่อีก ซึ่งหากเป็นข้อมูลที่ไม่เหมาะสม เป็นเท็จ หรือหลอกลวง เช่น การเปิดรับบริจาคเงินเพื่อรักษาผู้ป่วยที่ผ่านมาหลายปี แต่ข้อมูลการเปิดรับบริจาคนั้น ยังมีการเผยแพร่หรือแชร์ต่อไปอย่างต่อเนื่องอยู่ ซึ่งปัจจุบันผู้ป่วยนั้นอาจจะได้รับการรักษาจนหายดีแล้ว ไม่ได้เปิดรับบริจาคแล้ว แต่ยังมีการโอนเงินเข้าบัญชีนั้นหรือบัญชีที่มีการปลอมแปลง ซึ่งไม่เกี่ยวข้องกับสถานการณ์หรือเหตุการณ์ที่เกิดขึ้น ทำให้หน่วยงานที่รับบริจาคหรือผู้เกี่ยวข้องมีปัญหาได้

ส่วนการกระจายตัวของข้อมูลในปัจจุบันนั้นมีแนวโน้มรวดเร็วและรุนแรงมากขึ้น เนื่องจากเป็น social media เพียงแค่กด Like กด Share ไปสู่เพื่อน และเพื่อนของเพื่อน แค่เวลาไม่ถึงชั่วโมง ข้อมูลนั้นอาจจะ Share ไปให้กับคนนับล้านคน ซึ่งถ้าข้อมูลนั้นเป็นข้อมูลที่ผิดกฎหมาย เป็นเท็จ ไม่เหมาะสม เป็นไวรัสหรือมัลแวร์ถูก Share ต่อไป ข้อมูลนั้นก็จะกระจายตัวต่อไปอีกทั่วประเทศหรือทั่วโลกในเวลาไม่กี่ชั่วโมง

4) วิวัฒนาการของเว็บไซต์

- ยุค Web 1.0 การให้บริการเว็บไซต์ในรูปแบบการสื่อสารทางเดียว (One Way Communication) เป็นเว็บในยุคเริ่มแรกและอาจยังพบบ้างในปัจจุบัน ทำหน้าที่ให้ข้อมูลสื่อสารในทิศทางเดียว โดยที่ผู้เข้าชมสามารถเข้าชมได้เพียงอย่างเดียว ไม่สามารถมีส่วนร่วมกับเว็บไซต์ได้ ส่วนผู้ที่กำหนดเนื้อหาและข้อมูล คือ Webmaster หรือเจ้าของเว็บไซต์เท่านั้น

- ยุค Web 2.0 การใช้งานผ่านเครือข่ายอินเทอร์เน็ตในรูปแบบสองทาง (Two Way Communication) ยุคนี้มีการพัฒนาขึ้น ให้ผู้เข้าชมมีส่วนร่วมต่อเว็บไซต์มากขึ้น โดยที่สามารถสร้างเนื้อหา และนำเสนอข้อมูลต่าง ๆ เช่น เว็บบอร์ด เว็บบล็อก แชร์รูปภาพ และการแสดงความคิดเห็น

- ยุค Web 3.0 ยุคปัจจุบัน เป็นยุครอยต่อจากยุค Web 2.0 เป็นการนำข้อมูล Big Data มาประมวลผลผ่านแพลตฟอร์มต่าง ๆ ทำให้แพลตฟอร์มฉลาดขึ้น ยุคนี้ระบบคอมพิวเตอร์รู้จักการแก้ปัญหาเอง สามารถวิเคราะห์ข้อมูลด้วยตนเอง ประมวลผลได้อย่างสมเหตุผล หรือที่เราเรียกว่า หลักการของปัญญาประดิษฐ์

/มีต่อหน้า 3

ซึ่งสามารถช่วยคาดเดาพฤติกรรม รวมทั้งวิเคราะห์ความต้องการของมนุษย์ โดยผู้ใช้สามารถอ่าน เขียน จัดการ หรือเพิ่มข้อมูลได้อย่างอิสระมากขึ้น อีกทั้งยังเข้าถึงเนื้อหาของเว็บได้ดีและตรงกับความต้องการ เช่น ผู้ใช้ค้นหาข้อมูลใน Google แค่พิมพ์ตัวอักษรเดียว เว็บไซต์ Google ก็จะประมวลผลข้อมูลตัวอักษรที่ผู้ใช้กำลังพิมพ์ และแสดงข้อมูลที่สอดคล้องกับตัวอักษรที่ผู้ใช้กำลังค้นหาได้ ทำให้ผู้ใช้งานสะดวกมากขึ้น

- ยุค Web 4.0 เว็บในอนาคตอันใกล้ เรียกว่า “A Symbiotic web” เป็นเว็บที่ทำงานแบบ Artificial Intelligence (AI) ที่ฉลาดมากยิ่งขึ้น คอมพิวเตอร์สามารถคิดได้ มีความฉลาดมากขึ้น ในการอ่านทั้งเนื้อหา ข้อความ รูปภาพ และวีดีโอ สามารถตอบสนองหรือตัดสินใจได้ว่าจะ load ข้อมูลอะไร จากไหน จึงจะให้ประสิทธิภาพดีที่สุดมาให้ผู้ใช้งาน นอกจากนี้ยังมีรูปแบบการนำมาแสดงที่รวดเร็ว WEB 4.0 จะทำให้เว็บ หรือข้อมูลต่าง ๆ สามารถทำงานได้แทบจะทุกอุปกรณ์หรืออาจจะช่วยระบุตัวตนที่แท้จริงของผู้ใช้ได้

2.2 การกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง

1) รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์

ประเภทของผู้กระทำความผิด ได้แก่

- แฮคเกอร์ (Hacker) คือ บุคคลที่มีความสนใจ ศึกษา ค้นคว้าเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ พยายามที่จะเจาะเข้าระบบโดยไม่ได้รับอนุญาต มีการแชร์ข้อมูลที่ค้นพบหรือรับทราบไม่ได้มีแนวคิดที่จะทำลาย หรือก่อความเสียหายเบื้องต้น

- แคร็คเกอร์ (Cracker) คือ บุคคลที่มีความรู้ความชำนาญด้านคอมพิวเตอร์พยายามที่จะเจาะเข้าระบบโดยไม่ได้รับอนุญาต และอาศัยช่องโหว่หรือจุดอ่อนเพื่อทำลายระบบ นำมาแสวงหาผลประโยชน์ต่อตนเอง

- สคริปต์คิดดี้ส์ (Script kiddy) คือ แฮคเกอร์ (Hacker) ประเภทหนึ่ง มีจำนวนมากในสังคม เป็นกลุ่มบุคคลที่มีความอยากรู้อยากเห็น อยากลอง แต่ยังไม่มีความชำนาญ ไม่สามารถเขียนโปรแกรมในการเจาะระบบได้เอง อาศัย Download จากอินเทอร์เน็ต เช่น มีการแจกจ่ายโปรแกรมที่สามารถโจมตีเว็บไซต์หน่วยงานราชการ บุคคลที่อยากรู้อยากเห็น Download โปรแกรมนั้นมาลองใช้งาน แล้วโจมตีหน่วยงานราชการ ทำความเสียหายต่อเวบไซต์และหน่วยงานราชการได้

- สายลับทางคอมพิวเตอร์ (Spy) คือ บุคคลที่ถูกจ้างเพื่อเจาะระบบและขโมยข้อมูล โดยพยายามไม่ให้ผู้ถูกโจมตีรู้ตัว

- พนักงาน (Employee) คือ พนักงานภายในองค์กร หรือเป็นบุคคลภายในระบบที่สามารถเข้าถึงและโจมตีระบบได้ง่าย เพราะอยู่ภายในระบบ มีการนำข้อมูลสำคัญขององค์กรไปเผยแพร่ต่อผู้อื่น โดยไม่ได้เจตนา ทำให้ผู้ได้รับข้อมูลเข้ามาโจมตีระบบขององค์กรได้

- ผู้ก่อการร้าย (Terrorist) คือ กลุ่มบุคคลหรือบุคคลที่มีความประสงค์ที่จะก่อให้เกิดความวุ่นวาย ความไม่สงบต่าง ๆ ในระบบคอมพิวเตอร์ เช่น ผู้ที่โจมตีเว็บไซต์หน่วยงานภาครัฐ หรือผู้ให้บริการทางการเงินออนไลน์ ทำให้ไม่สามารถใช้งานได้

/มีต่อหน้า 4

รูปแบบของการกระทำความผิด ได้แก่

- Social Engineering เป็นปฏิบัติการทางจิตวิทยา หลอกล่อให้เหยื่อติดกับ โดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์ เช่น

- Password Guessing การเดา Password เพื่อเข้าสู่ระบบ

- Denial of Service (DOS) การโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและการร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ

- Decryption การถอดข้อมูลที่มีการเข้ารหัสอยู่

- Birthday Attacks สุ่มคีย์ขึ้นมาและอาจจะตรงกับคีย์ที่เราเข้ารหัสไว้ จนสามารถเข้าสู่ระบบได้

- Man in the middle Attacks การพยายามที่จะทำตัวเป็นคนกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

2) สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต

- การโจมตีด้วยไวรัสหรือมัลแวร์ ผ่านอีเมล์หรือสื่อสังคมออนไลน์ต่าง ๆ โดยการหลอกให้ผู้ใช้เลือกหรือดาวน์โหลดไฟล์ต่าง ๆ

- กลลวงทางสังคม เช่น การส่งอีเมล์หลอกลวงผู้อื่นเพื่อให้เข้าเวบไซต์ปลอม หลอกลวงให้กรอกข้อมูลส่วนตัวของผู้ใช้ ซึ่งสามารถนำข้อมูลนั้นไปแสวงหาผลประโยชน์ต่อไปได้

3) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ปัจจุบันใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับ พ.ศ.2550 และ พ.ศ.2560 ที่แก้ไขเพิ่มเติม เพื่อป้องกันและควบคุมการกระทำความผิดที่จะเกิดขึ้นจากการใช้คอมพิวเตอร์ หากมีผู้กระทำความผิดตามที่ระบุไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือ พรบ.คอม ก็จะได้รับโทษตามที่กำหนด เช่น หากมีผู้ใดเข้าถึงคอมพิวเตอร์ของผู้อื่นที่มีการกำหนดรหัสผ่านไว้ ถือว่ามีความผิดทันที แม้ว่ารหัสผ่านจะถูกต้องหรือไม่ก็ตาม แต่หากคอมพิวเตอร์เครื่องนั้นไม่มีการกำหนดรหัสผ่านไว้ แล้วมีบุคคลอื่นมาเข้าถึงคอมพิวเตอร์ ถือว่าผู้นั้นไม่มีความผิด เพราะคอมพิวเตอร์เครื่องนั้นไม่มีการกำหนดรหัสผ่านไว้ ถือว่าไม่มีการกำหนดมาตรการป้องกันการเข้าถึง

<u>2.3 ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์</u>

1) การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด

- การใช้โปรแกรมในการแก้ไขคำในเกมส์ออนไลน์ เพื่ออำนวยความสะดวกในการเล่นเกมส์ ให้ผ่านหรือชนะง่ายขึ้น ทำให้เป็นการก่อกวนระบบเวบไซต์ของเกมส์นั้น

- การเผยแพร่ตัวอย่างที่ไม่ดีแก่เด็กและเยาวชน เช่น การเสพสารเสพติด การทำร้ายตัวเองผ่านอินเทอร์เน็ต

- การบริโภคข้อมูลโดยขาดความยั้งคิด เช่น ภาพเห็ดรักษามะเร็ง ซึ่งความจริงแล้วเห็ดนั้นเป็นเห็ดมีพิษ หากผู้บริโภคเชื่อข้อมูลตามภาพนั้นอาจก่อให้เกิดผลต่อชีวิต

/มีต่อหน้า 5

2) ตัวอย่าง Hacking Wi-Fi User และ Euro Grabber

- เหยื่อมักตั้งให้อุปกรณ์จดจำการเข้าสัญญาณ Wi-Fi และเข้าสู่ระบบอัตโนมัติ
- อุปกรณ์ Wi-Fi ที่มีผู้ผลิตเดียวกัน มักจะตั้งค่าเริ่มต้นเหมือนกัน
- เหยื่อมักไม่เคยเปลี่ยนชื่อ Wi-Fi ที่บ้าน
- Wi-Fi ในที่สาธารณะมักใช้ชื่อเดียวกันทั้งหมด
- เหยื่อมักเข้าสู่ระบบอินเทอร์เน็ตไร้สายสาธารณะ ที่ให้บริการแบบฟรี ไม่ต้องลงทะเบียน โดยขาดความรอบคอบ
- ผู้ไม่ประสงค์ดีจะทำการปลอมแปลงชื่อตัวกระจายสัญญาณและเหยื่อมักคุ้นเคยกับชื่อดังกล่าว และทำการเชื่อมต่อเข้าสู่ระบบ
- ผู้ไม่ประสงค์ดีทำการปล่อยสัญญาณอินเทอร์เน็ตให้ใช้บริการฟรี
- ผู้ไม่ประสงค์ดีทำการดักรับข้อมูลโดยที่เหยื่อไม่รู้ตัว

3) ตัวอย่าง Web Defacement ไวรัสเรียกค่าไถ่ และตัวอย่าง Hot Hot

- ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานราชการไทย เรียกว่า Web Defacement เช่น การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลที่เผยแพร่หน้าเว็บ ซึ่งผู้โจมตีมักจะปรับเปลี่ยนหน้าแรกของเว็บไซต์เป้าหมาย หรือทั้งเว็บไซต์ ไปเป็นหน้าเว็บไซต์ใหม่ เพื่อทำลายความน่าเชื่อถือของหน่วยงานเจ้าของเว็บไซต์
- ไวรัสเรียกค่าไถ่ เช่น ไวรัส Crypt0L0cker ระบาดในไทย ยังไม่สามารถทำการแก้ไขได้ เป็นการเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ที่ซับซ้อน มีการเรียกเงินหลักหมื่นขึ้นไป ยิ่งนานการเรียกค่าไถ่จะมีราคาสูงขึ้น ซึ่งไม่มีการรับประกันว่าเมื่อจ่ายเงินเรียกค่าไถ่แล้วจะได้ไฟล์คืน ตอนนี้ระบาดตามบริษัท และหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน โดยสามารถป้องกันได้ง่าย ๆ คือ ระมัดระวังการรับอีเมล์แปลก ๆ ที่มีไฟล์แนบมา การเข้าเวบไซต์อ่านให้ละเอียด หากเข้าแล้วมีการทำการโหลดไฟล์ ขอให้ลบอย่าเปิดไฟล์เป็นอันขาด ลง Antivirus ที่มีการ update สำรองข้อมูลเป็นประจำ และอย่าเสียบอุปกรณ์สำรองข้อมูลค้างเพราะจะลามถึงกันได้
- ตัวอย่าง Hot Hot เช่น การสวมรอย Facebook แจ้งเตือนจากเพื่อน การแฮกค์ไลน์ (LINE) หลอกให้ซื้อสินค้า

<u>2.4 วิธีป้องกันและตรวจสอบความปลอดภัยด้วยตนเอง</u> เช่น

1) การป้องกันความปลอดภัยใน Facebook

- การตั้งรหัสผ่าน ไม่ควรตั้งเป็น หมายเลขโทรศัพท์ วันเกิดของตนเองหรือคนใกล้ชิด ชื่อตัวเองหรือชื่อเล่น หรือชื่อที่ใช้สำหรับทำ User และไม่ควรเป็นชุดตัวเลขหรือตัวอักษรที่เดาได้ง่าย เช่น 1234 abcd
- การ Lock in ระบบสองชั้น โดยการใช้ password ควบคู่กับ code อีกตัวที่ส่งทาง SMS
- การแจ้งเตือนการ Lock in

2) การป้องกันความปลอดภัยใน Gmail

- การตรวจหาไวรัสหรือมัลแวร์ในเครื่องคอมพิวเตอร์ของเรา ด้วยโปรแกรม Antivirus เป็นประจำ
- การตรวจสอบความปลอดภัยของบัญชี
- การ Lock in ระบบสองชั้น

/มีต่อหน้า 6

3) การป้องกันความปลอดภัยใน Line

- การตั้งค่า ปิดการค้นหา Line ID
- การตั้งค่า การปฏิเสธข้อความจากบุคคลที่ไม่ใช่เพื่อน
- การ Block บุคคลที่เราไม่ต้องการคุยด้วย
- การตั้งค่า ไม่อนุญาตให้บุคคลอื่นเพิ่มเพื่อนด้วยหมายเลขโทรศัพท์

3. ประโยชน์ที่ได้รับจากการพัฒนาความรู้ต่อตนเอง ได้แก่

การใช้คอมพิวเตอร์และอินเทอร์เน็ต อย่างระมัดระวัง มีแนวทางการป้องกัน และแก้ปัญหาที่อาจเกิดจากเว็บหลอกลวง เว็บที่ไม่เหมาะสม โดยไม่ตกเป็นเหยื่อในการกระทำความผิดโดยไม่รู้ตัว และสามารถปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับ พ.ศ.2550 และ พ.ศ.2560 ที่แก้ไขเพิ่มเติมได้อย่างถูกต้อง

4. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการพัฒนาความรู้ฯ ครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน มีดังนี้

การใช้คอมพิวเตอร์และอินเทอร์เน็ตในที่ทำงาน อย่างระมัดระวัง การตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลก่อนนำมาเผยแพร่หรือใช้งานต่อ และระมัดระวังไวรัสหรือมัลแวร์ ที่อาจแฝงมากับเว็บไซต์หรือโปรแกรมที่เราดาวน์โหลด อาจทำให้เครื่องคอมพิวเตอร์อื่น ๆ ในสำนักงานติดไวรัสหรือมัลแวร์จากคอมพิวเตอร์ของเรา และสามารถแนะนำให้ผู้ร่วมงานใช้คอมพิวเตอร์และอินเทอร์เน็ตโดยปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับ พ.ศ.2550 และ พ.ศ.2560 ที่แก้ไขเพิ่มเติม

5. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน

การไม่ทันต่อเหตุการณ์ ความรู้ และทักษะไม่เพียงพอ เช่น ผู้ไม่ประสงค์ดีหรืออาชญากรอาจมีการใช้เทคโนโลยีที่ล้ำสมัย โดยเปลี่ยนรูปแบบการก่อเหตุในรูปแบบที่เราไม่สามารถรับมือหรือแก้ไขปัญหาได้

6. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล ได้แก่

การจัดอบรมภายในหน่วยงาน ให้กับบุคลากรที่เกี่ยวข้องกับการใช้งานคอมพิวเตอร์และอินเทอร์เน็ต โดยเชิญผู้บรรยายที่มีความรู้ความเข้าใจและมีประสบการณ์โดยตรงเกี่ยวกับความมั่นคงปลอดภัยบนอินเทอร์เน็ต และการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล และมีตัวอย่างกรณีศึกษาที่ทันต่อเหตุการณ์หรือสถานการณ์ปัจจุบัน

จึงเรียนมาเพื่อโปรดทราบ

(ลงชื่อ).....

(นางทรายแก้ว อนากาศ)

ผู้เข้ารับการพัฒนาความรู้

วันที่ 11 มีนาคม 2564