

แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สพข.7

รอบการประเมิน 2 (เมษายน – กันยายน 2569)

ประจำปีงบประมาณ พ.ศ. 2569

ส่วนที่ 1 ข้อมูลทั่วไป

ชื่อ.....นางสาวมยุรี.....นามสกุล.....ปละอูด.....

ตำแหน่ง.....นักวิชาการเกษตรชำนาญการพิเศษ.....กลุ่ม/ฝ่าย.....กลุ่มวิชาการเพื่อการพัฒนาที่ดิน

หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ

.....หลักสูตร ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (UNDERSTANDING AND USING DIGITAL TECHNOLOGY)

สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ

.....แพลตฟอร์มหลักสูตรการเรียนรู้ออนไลน์ด้านดิจิทัลของสถาบันพัฒนาบุคลากรด้านดิจิทัลภาครัฐ (TDGA)

ศูนย์รวมหลักสูตรกลางเพื่อการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรภาครัฐ

หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้

.....กรมพัฒนาที่ดิน

ตั้งแต่วันที่ 9 เดือน กันยายน พ.ศ. 2569 ถึงวันที่ 10 เดือน กันยายน พ.ศ. 2569

เพื่อ ☒ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ.....

ส่วนที่ 2 สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

2.1 รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/ สัมมนา/พัฒนาความรู้ฯ

วัตถุประสงค์การพัฒนาความรู้

1. เพื่อให้มีความรู้ ความเข้าใจในด้านสารสนเทศ สื่อ และเทคโนโลยีดิจิทัล

2. เพื่อให้มีความเข้าใจในการใช้สื่อดิจิทัล เพื่อสามารถวิเคราะห์ แยกแยะ สื่อดิจิทัลเพื่อเลือกใช้งาน

ได้อย่างเหมาะสม

3. เพื่อให้มีการใช้เทคโนโลยีดิจิทัลและสื่อดิจิทัล เพื่อทำงานได้อย่างถูกต้องและปลอดภัย ตลอดจนตระหนัก ถึงภัยคุกคามทางดิจิทัลและสามารถตรวจสอบการทำงานตามหลักปฏิบัติงานที่ดีได้ในเบื้องต้น

4. เพื่อให้มีความเข้าใจในการใช้เทคโนโลยีดิจิทัล และมีความรู้ในการใช้สื่อดิจิทัลเพื่อการทำงานได้อย่างมีประสิทธิภาพ

2. เนื้อหาและหัวข้อวิชาของการพัฒนาความรู้

1. จริยธรรมการใช้เทคโนโลยีสารสนเทศ หมายถึง หลักศีลธรรมจรรยาที่กำหนดขึ้นเพื่อใช้เป็นแนวทาง ปฏิบัติหรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศ หลักของความถูกต้องและความผิดที่บุคคลใช้เป็น แนวทางในการปฏิบัติ และสรุปเป็นหลักเกณฑ์ที่ประชาชนตกลงร่วมกัน เพื่อใช้เป็นแนวทางในการปฏิบัติร่วมกันในสังคม จริยธรรมในการใช้เทคโนโลยีคอมพิวเตอร์และสารสนเทศ มี 4 ประเด็น ในลักษณะตัวอย่างว่า PAPA ประกอบด้วย

1.1) ความเป็นส่วนตัว (Information Privacy) คือ สิทธิในการควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น การละเมิดความเป็นส่วนตัว เช่น การรวบรวมข้อมูลส่วนบุคคลสร้างเป็นฐานข้อมูลแล้วเอาไปขายทำธุรกิจผ่านเว็บไซต์เพื่อรวบรวมข้อมูลไปขาย และการใช้ internet ติดตามผู้ใช้เพื่อทำการส่ง e-mail ขยายสินค้า ทำให้เกิดอีมေးล์ (junk mail) ที่ผู้รับไม่ต้องการ เรียกว่า “สแปม”

1.2) ความถูกต้อง (Information Accuracy) คือ ความถูกต้องขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูล มีการตรวจสอบความถูกต้องก่อนการบันทึก เช่น ถ้าให้ลูกค้าป้อนข้อมูลเอง ต้องให้สิทธิ์ในการเข้าไปตรวจสอบความถูกต้องด้วยตนเอง และข้อมูลต้องมีความทันสมัยอยู่เสมอ

1.3) ความเป็นเจ้าของ (Intellectual Property : IP) คือ (1) กรรมสิทธิ์ในการถือครองทรัพย์สิน โดยทรัพย์สินแบ่งเป็น จำต้องได้ เช่น คอมพิวเตอร์ รถยนต์ และจำต้องไม่ได้แต่บันทึกลงในสื่อต่างๆ ได้ เช่น ทรัพย์สินทางปัญญา บทเพลง โปรแกรมคอมพิวเตอร์ (2) ได้รับความคุ้มครองสิทธิภายใต้กฎหมาย เช่น ลิขสิทธิ์ (3) สิทธิความเป็นเจ้าของ หมายถึง กรรมสิทธิ์ในการถือครองทรัพย์สินที่จำต้องได้ หรืออาจเป็นทรัพย์สินทางปัญญา และ (4) ความเป็นเจ้าของด้านเทคโนโลยีสารสนเทศ หมายถึง สิทธิซอฟต์แวร์

สิทธิของเจ้าของลิขสิทธิ์ประกอบด้วยสิทธิใหญ่ 2 ประการ คือ

1) สิทธิทางเศรษฐกิจ (Economic Rights) คือ เจ้าของลิขสิทธิ์ย่อมมีสิทธิแต่เพียงผู้เดียว ที่จะกระทำการแก่ตนเอง เช่น ทำซ้ำ โดยการคัดลอก เลียนแบบ ทำสำเนา ทำแม่พิมพ์ บันทึกเสียง เป็นต้น เผยแพร่ต่อสาธารณชน ให้เช่าต้นฉบับหรือสำเนาโปรแกรมคอมพิวเตอร์ สดทัศน์วัสดุ ภาพยนตร์และสิ่งบันทึกเสียง ให้ประโยชน์อันเกิดจากลิขสิทธิ์แก่ผู้อื่น และอนุญาตให้ผู้อื่นใช้สิทธิ โดยจะกำหนดเป็นเงื่อนไขหรือไม่ก็ได้ แต่เงื่อนไขที่กำหนดจะเป็นการจำกัดการแข่งขันโดยไม่เป็นธรรมไม่ได้

2) สิทธิทางศีลธรรม (Moral Rights) ผู้สร้างสรรค์มีสิทธิที่จะแสดงตัวว่าเป็นผู้สร้างสรรค์ และห้ามมิให้มีการบิดเบือน ตัดทอน ดัดแปลง หรือกระทำการให้เกิดความเสียหาย

1.4) การเข้าถึงข้อมูล (Data Accessibility) คือ การกำหนดสิทธิตามระดับผู้ใช้งาน เพื่อป้องกันการเข้าไปดำเนินการต่างๆ กับข้อมูลของผู้ที่ไม่เกี่ยวข้อง และต้องมีการออกแบบระบบรักษาความปลอดภัยในการเข้าถึงข้อมูลของผู้ใช้

2. การเข้าถึงสื่อดิจิทัล

2.1 สื่อดิจิทัล หมายถึง สื่อที่นำเอาข้อความ กราฟิก ภาพเคลื่อนไหว เสียง มาจัดรูปแบบ โดยอาศัยเทคโนโลยีความเจริญก้าวหน้าทางด้านคอมพิวเตอร์ และการสื่อสารมาประยุกต์ใช้ ทำให้ลดค่าใช้จ่ายและระยะเวลา ซึ่งประเภทของสื่อดิจิทัล ได้แก่ ภาพดิจิทัล เสียงดิจิทัล วิดีโอดิจิทัล ที่วีดิทัศน์ และอินเทอร์เน็ตดิจิทัล

2.2 อินเทอร์เน็ต (Internet) หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั่วโลกเข้าไว้ด้วยกัน เพื่อให้เกิดการสื่อสาร และการแลกเปลี่ยนข้อมูล ประโยชน์ของอินเทอร์เน็ต ได้แก่

- ใช้ในการสื่อสาร เช่น e-mail, chat, telephone
- ใช้ในการแลกเปลี่ยนข้อมูล เช่น ส่งไฟล์ต่าง webboard
- เป็นเครื่องมือทางธุรกิจ เช่น เว็บไซต์บริษัท ระบบธุรกรรมทางอิเล็กทรอนิกส์
- สืบค้นข้อมูล เช่น google, bing, aol, yahoo
- เพื่อความบันเทิง เช่น youtube, sanook การค้นหาข้อมูลในอินเทอร์เน็ต เป็นการค้นหาสิ่งที่ต้องการรู้ในข่ายเครือข่ายอินเทอร์เน็ต โดยการค้นหาผ่าน เว็บไซต์ต่างๆ เช่น Google Yahoo โดยมีเทคนิคการค้นหา

- การระบุค่าเป็นวลี ใช้เครื่องหมายคำพูด
- การค้นหาโดยใช้หลายค า ใช้ OR เช่น “โลกร้อน” OR “เรียนกระเจก”
- การค้นหาข้อความในเว็บนั้น site:url keyword
- การค้นหาเฉพาะประเภทไฟล์ filetype:PDF keyword

- ค้นหาที่ไม่รู้ในเวลานั้น ใช้ * เช่น A * History of Philosophy ได้ผลลัพธ์เป็น A Little History of Philosophy

- หาเว็บที่เกี่ยวข้อง related:url

- หาเฉพาะหัวเรื่อง intitle:keyword

- ค้นหาโดยใช้ภาพ หาจก <https://images.google.com> (ใช้ตรวจหาต้นฉบับภาพได้)

- การแปลงหน่วย แปลงค่าเงิน เช่น 100 USD to TH

- การค้นหาตำแหน่ง (Google Map) โดยการใส่คำที่ต้องการค้นหา สามารถดูสภาพแวดล้อมผ่านมุมมองถนน (Street View) และท่องเที่ยวกับ Google Street View

3. ความเข้าใจและสื่อสารยุคดิจิทัล

3.1 บทบาทการสื่อสาร ประกอบด้วย ผู้รับสารและผู้ส่งสาร โดยสารที่ใช้มีการแสดงข้อเท็จจริง (Fact) และ ข้อคิดเห็น (Opinion)

- ข้อเท็จจริง คือ ข้อความแห่งเหตุการณ์ที่เป็นมาหรือเป็นอยู่ตามจริง หรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จ หรือจริง สามารถพิสูจน์สนับสนุนยืนยันได้

- ข้อคิดเห็น คือ ความเห็น ความรู้สึกนึกคิดของผู้ส่งสารที่สอดแทรกอยู่ในเนื้อหา ไม่สามารถพิสูจน์สนับสนุนยืนยันได้

ลักษณะข้อเท็จจริง (Fact)	ลักษณะข้อคิดเห็น (Opinion)
1) มีความเป็นไปได้	1) เป็นข้อความที่แสดงความรู้สึก
2) มีความสมจริง	2) เป็นข้อความที่แสดงความคิดเห็น
3) มีหลักฐานเชื่อถือได้	3) เป็นข้อความที่แสดงการเปรียบเทียบอุปมาอุปไมย
4) มีความสมเหตุสมผล	4) เป็นข้อความที่เป็นข้อเสนอแนะหรือเป็นความคิดเห็นของผู้พูดเอง

3.2 ความแตกต่างระหว่างการสื่อสารด้วยวิธีต่างๆ และความเหมาะสม

1) การสื่อสารแบบประสานเวลา และต่างเวลา

- การสื่อสารแบบสมวาร (ประสานเวลา) Synchronous ปฏิสัมพันธ์ที่เกิดขึ้นในเวลาเดียวกัน สามารถสื่อสารร่วมกันเหมาะกับการแลกเปลี่ยนสารสนเทศ เครื่องมือสื่อสาร ผ่านระบบอินเทอร์เน็ต เช่น ห้องสนทนา (Chat Room) การประชุมผ่านวิดีโอทัศน์ (Video Conference) เป็นต้น

- การสื่อสารแบบอสมวาร (ไม่ประสานเวลา) Asynchronous ปฏิสัมพันธ์ที่ไม่ได้เกิดขึ้นในเวลาเดียวกัน ณ เวลาใดเวลาหนึ่งโดยผู้ส่งสารและผู้รับสารไม่ต้องรอเพื่อตอบโต้กันภายในเวลาเดียวกัน เครื่องมือสื่อสารผ่านระบบอินเทอร์เน็ต เช่น จดหมายอิเล็กทรอนิกส์ (e-mail)

2) การสื่อสารแบบตัวต่อตัว กับแบบกลุ่ม

- การสื่อสารแบบตัวต่อตัว มีผู้รับและผู้ส่งสารไม่เกิน 3 คน ครอบคลุมพื้นที่การสื่อสารระยะใกล้และไกล เห็นหน้ากันหรือไม่ก็ได้ ขึ้นอยู่กับวัตถุประสงค์ เช่น สร้างความสัมพันธ์ แจ้งข่าว ถ่ายทอดความรู้ เป็นต้น

- การสื่อสารแบบกลุ่ม ระหว่างกลุ่มบุคคลจำนวนมากที่มีความสนใจ หรือการแสดงออกในเรื่องราวเดียวกัน เช่น กลุ่มสนทนา การอภิปราย การสัมมนา การบรรยาย เป็นต้น

3) การสื่อสารแบบทางการ กับไม่ทางการ

- การสื่อสารแบบเป็นทางการ มีรูปแบบของการสื่อสารที่มีระเบียบแบบแผน มีข้อกำหนดใช้ในการติดต่อสื่อสารของหน่วยงาน เช่น e-mail

- การสื่อสารแบบไม่เป็นทางการ ไม่มีข้อกำหนดรูปแบบที่ชัดเจน ซึ่งจะเป็นการติดต่อสื่อสารระหว่างบุคคลหรือกลุ่มที่มีสัมพันธ์ของแต่ละบุคคล เช่น Chat

4. ความปลอดภัยยุคดิจิทัล

ความเป็นส่วนตัว (Privacy) ส่วนสำคัญคือ รอยเท้าดิจิทัล (Digital Footprint) ซึ่งข้อมูลต่างๆ เช่น ข้อความ รูปภาพ สิ่งต่างๆ ที่ลงไว้ใน Social Media Facebook, Twitter, Instagram, Social Cam หรือช่องทางไหนก็ตาม ข้อมูลมีโอกาสโดนทำสำเนาไปนับไม่ถ้วน และอยู่ในมือผู้ไม่หวังดี ทำให้เสียภาพพจน์ และภาพลักษณ์โดยไม่อาจแก้ไขได้เราควรจะต้องระมัดระวังในการโพสต์ในสื่อสังคมออนไลน์

4.1 การป้องกันในการเข้าถึงข้อมูลรอยเท้าดิจิทัล หรือ Digital Footprint ด้วยวิธีการตั้งรหัสผ่าน ควรเปลี่ยนแปลงรหัสผ่านบ่อยๆ คาดเดายากสำหรับบุคคลอื่นแต่่ง่ายสำหรับเรา

ลักษณะข้อเท็จจริง (Fact)	ลักษณะข้อคิดเห็น (Opinion)
1) ใช้รหัสเดียวกันหมด รู้รหัสเดียวสามารถเข้าถึงได้หมด	1) ใช้รหัสผ่านที่ยาว (อย่างน้อย 8 ตัว)
2) ไม่มีการเปลี่ยนรหัสผ่าน	2) ใช้อักษรตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก ตัวเลข รวมทั้งสัญลักษณ์ต่างๆ ประกอบกัน
3) คาดเดาง่าย เช่น 1234567	3) ใช้สัญลักษณ์อย่างน้อยหนึ่งตัวในตำแหน่ง 2-6
4) ประกอบด้วยข้อมูลบุคคล เช่น วันเกิด เบอร์โทร	4) ใช้อักษรที่แตกต่างกันอย่างน้อย 4 ตัว (อย่างใช้ตัวอักษรซ้ำกัน) ใช้ตัวเลขและตัวอักษรแบบสลับ
5) ใช้คำมีความหมาย เช่น ชื่อเล่น love happy	
6) ใช้ตัวพิมพ์ทั้งหมด ไม่มีตัวเลขหรือตัวอักษรผสมเลย	

4.2 การพิสูจน์ตัวตน การพิสูจน์ตัวบุคคลโดยใช้ 2 ปัจจัย (Two-Factor Authentication) คือ การใช้ปัจจัยที่สอง ร่วมกับการล็อกอินด้วยรหัสผ่านตามปกติ ซึ่งหลังจากการล็อกอินด้วยรหัสผ่านแล้วระบบจะถามรหัสยืนยันจากอุปกรณ์อื่น เช่น โทรศัพท์มือถือ หรือ Token เพื่อความปลอดภัยมากขึ้น อาทิ Google 2 Factor Authentication เป็นต้น

4.3 การกำหนดสิทธิ์ (Authorization) หลักการสิทธิประโยชน์ที่สุด Principle of Least Privilege สามารถใช้ปรับปรุงความปลอดภัยของระบบคอมพิวเตอร์ เป็นเรื่องพื้นฐานแต่สำคัญมากที่มักถูกมองข้ามหลักการนี้ คือผู้ใช้จะต้องมีระดับต่ำที่สุดของสิทธิตามความต้องการเพื่อการทำงานตามที่มอบหมาย

4.4 การเข้ารหัสข้อมูล HTTPS ย่อมาจาก Hypertext Transfer Protocol Secure หรือ Hypertext Transfer Protocol Over SSL (Secure Socket Layer) เป็นการทำงานเหมือนกับ HTTP ธรรมดาแต่ทำอยู่บน SSL เพื่อให้เกิดความปลอดภัย ในการส่งข้อมูลมากยิ่งขึ้น มีรูปแบบดังนี้

- การใช้งาน URL จะเข้าต้นด้วย http:// ตามด้วยชื่อของเว็บไซต์
- ทำงานที่พอร์ต (port) 443 (มาตรฐาน)
- ส่งข้อมูลเป็นแบบ Cipher text คือ มีการเข้ารหัสข้อมูลในระหว่างการส่ง (Encryption) สามารถถูกดักจับได้ แต่อ่านข้อมูลนั้นไม่รู้เรื่อง

- มีการทำ Authentication เพื่อตรวจสอบยืนยันระบุตัวตน WPA2 คือ เทคโนโลยีการรักษาความปลอดภัยที่ปกป้องเครือข่าย Wi-Fi ของคุณโดยการเข้ารหัสการจราจรบนเครือข่าย นอกจากนี้ยังทำให้ผู้เข้าที่ได้รับอนุญาตเข้าถึงเครือข่ายได้ยากขึ้น

4.5 มัลแวร์ (malware - malicious software) คือ โปรแกรมที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อเครื่องคอมพิวเตอร์และเพื่อกดขู่ข้อมูลสำคัญไปจากผู้ใช้งานคอมพิวเตอร์ เช่น WannaCry ไวรัสเรียกค่าไถ่ที่ระบาดไปทั่วโลก โดยวันแรกที่ระบาดมีเครื่องคอมพิวเตอร์ติดถึง 230,000 กว่าเครื่องใน 150 ประเทศ

4.6 การหลอกลวง (Scam) เล่ห์อุบาย แผนการร้าย คำนี้หากอยู่ในวงการออนไลน์จะใช้เรียกพฤติกรรมที่มีเจตนาหลอกลวงให้เสียทรัพย์ให้เสียข้อมูล การหลอกลวงทางอินเทอร์เน็ต เช่น Email Scams Phishing Scam เป็นต้น โดยการใช้การโจมตีแบบวิศวกรรมสังคม (Social Engineering) จากความไม่รู้เท่าทันของผู้ใช้งาน โดยใช้อีเมลหรือหน้าเว็บไซต์ปลอม เพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่นๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบ หรือสร้างความเสียหายในด้านอื่นๆ เช่น ด้านการเงิน เป็นต้น นอกจากนี้การหลอกลวง ออนไลน์ (Fraud) มีฉ้อโกงติดต่อเหยื่อ สร้างความน่าเชื่อถือ หว่านล้อมให้โอนเงิน ไม่ส่งสินค้าหรือส่งสินค้าปลอม ปิดช่องทางการสื่อสาร เปลี่ยนชื่อเริ่มวงจรใหม่

4.7 ความเป็นส่วนตัวและความปลอดภัยบนมือถือ (Mobile Security and Privacy) สร้างความปลอดภัย ดังนี้ (1) ติดตั้งโปรแกรมป้องกันไวรัสบนมือถือ (2) ติดตั้งเฉพาะโปรแกรมที่น่าเชื่อถือ (3) ปิดการใช้งาน WIFI และ Bluetooth เมื่อไม่ได้ใช้งาน (4) ปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอ (5) สำรองข้อมูลที่สำคัญ (6) ตั้งค่าให้มือถือพบบข้อมูลอัตโนมัติเพื่อสูญหาย

พฤติกรรมเสี่ยง เมื่อใช้อุปกรณ์ในที่สาธารณะ (1) เชื่อมกับไวไฟที่ไม่ได้เข้ารหัส (2) ไม่ระวังว่ามีผู้อื่นแอบฟังบทสนทนาอยู่ (3) ไม่ระวังผู้อื่นแอบหน้าจอ (4) ไม่ระวังรอบตัว

2.2 ประสพการณ์/ประโยชน์ที่ได้รับ/การประยุกต์ใช้กับหน่วยงาน

☒ ต่อตนเอง

ทำให้ได้รับความรู้และประสบการณ์เกี่ยวกับการใช้เทคโนโลยีดิจิทัลอย่างถูกต้อง เหมาะสม และปลอดภัย สามารถนำความรู้ไปใช้ในการทำงานและการดำเนินชีวิตประจำวันได้อย่างมีประสิทธิภาพมากยิ่งขึ้น โดยเฉพาะการรู้จักวิเคราะห์และแยกแยะข้อเท็จจริงกับข้อคิดเห็น รวมถึงการตรวจสอบความน่าเชื่อถือของข้อมูลก่อนนำไปใช้หรือเผยแพร่ต่อ ทั้งนี้สามารถนำความรู้ที่ได้รับมาประยุกต์ใช้ในการทำงาน โดยเลือกใช้เครื่องมือดิจิทัลให้เหมาะสมกับงาน สามารถค้นหาข้อมูลจากอินเทอร์เน็ตได้อย่างมีประสิทธิภาพ และสื่อสารผ่านช่องทางดิจิทัลได้อย่างเหมาะสม ส่งผลให้การทำงานมีความสะดวก รวดเร็ว มีประสิทธิภาพ และลดความเสี่ยงจากภัยคุกคามทางดิจิทัล นอกจากนี้ยังสามารถนำความรู้ดังกล่าวไปใช้ในการดำเนินชีวิตประจำวัน เพื่อให้สามารถใช้เทคโนโลยีดิจิทัลได้อย่างรู้เท่าทัน มีความรับผิดชอบ และปลอดภัยมากยิ่งขึ้น

☒ ต่อหน่วยงาน/การนำมาประยุกต์ใช้กับหน่วยงาน

สามารถนำความรู้ด้านสารสนเทศ สื่อ และเทคโนโลยีดิจิทัลมาประยุกต์ใช้ในการปฏิบัติงานของหน่วยงาน เพื่อเพิ่มประสิทธิภาพ ลดขั้นตอนและระยะเวลาในการทำงาน ตลอดจนสนับสนุนการสื่อสารและการประสานงานให้มีความรวดเร็วและเหมาะสม นอกจากนี้ยังสามารถนำความรู้ด้านจริยธรรมและความปลอดภัยทางดิจิทัลมาใช้ในการรักษาความเป็นส่วนตัว ความถูกต้อง และความปลอดภัยของข้อมูล การกำหนดสิทธิ์การเข้าถึงข้อมูล รวมถึงการป้องกันภัยคุกคามทางดิจิทัล โดยความรู้ที่ได้รับสามารถนำไปใช้เพื่อพัฒนาระบบการทำงานของหน่วยงานให้มีความทันสมัย มีประสิทธิภาพ และปลอดภัยมากยิ่งขึ้น ตลอดจนส่งเสริมให้บุคลากรมีความรู้เท่าทันสื่อและเทคโนโลยีดิจิทัล สามารถปฏิบัติงานได้อย่างถูกต้อง มีความ

รับผิดชอบ เพื่อให้การปฏิบัติงานของหน่วยงานเป็นไปอย่างถูกต้อง ปลอดภัย มีประสิทธิภาพ และสอดคล้อง
กับการทำงานในยุคดิจิทัล

2.3 ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้

2.4 ข้อคิดเห็นและข้อเสนอแนะ

ลงชื่อ..... 

(นางสาวมยุรี ปละอุด)

ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ

ผู้รายงาน

วันที่..... 10เดือน กันยายน พ.ศ. 2569

ลงชื่อ..... 

(นางสุนิย์รัตน์ โลหะโชติ)

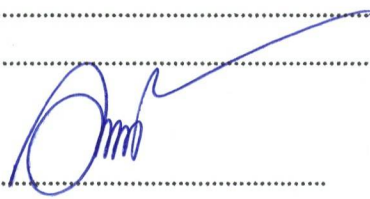
ตำแหน่ง ผู้เชี่ยวชาญด้านวางระบบการพัฒนาที่ดิน

รักษาการในตำแหน่ง ผู้อำนวยการกลุ่มวิชาการเพื่อการพัฒนาที่ดิน

วันที่..... 10เดือน กันยายน พ.ศ. 2569

ส่วนที่ 3 ความเห็นของผู้บังคับบัญชา

() ทราบ

ลงชื่อ..... 

(นายเอนก ดีพรมกุล)

ตำแหน่ง ผู้อำนวยการสำนักงานพัฒนาที่ดินเขต 7

วันที่..... 14เดือน ก.ค..... พ.ศ. 69

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

มยุรี พละอุด

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์
(Understanding Cybersecurity Risk Management)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 8 กันยายน 2569

A. L.

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

