



บันทึกข้อความ

สปร. สุวพ. 42
เลขที่รับ ๕๗
วันที่ ๒๒ ก.ย. ๒๕๖๕
เวลา ๑๐.๒๕ น.

ส่วนราชการ กลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๔ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน โทร ๑๒๘๓ ต่อ ๑๐๖

ที่ กษ ๐๘๐๔.๐๙/๕๖๖

วันที่ ๒ กันยายน ๒๕๖๕

เรื่อง รายงานผลการเรียนรู้ด้วยตัวเองผ่าน Digital Government Learning Platform

เรียน ผอ.สวพ. ผ่าน ผอ.กพฐ๔

ตามแบบกำหนดและประเมินตัวชี้วัดด้านผลสัมฤทธิ์ของประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ของสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน ให้ข้าราชการอบรมศึกษาการพัฒนาความรู้ผ่านระบบ Digital Government Learning Platform สถาบันพัฒนาบุคลากรภาครัฐดิจิทัล โดยพัฒนาครบถ้วนตามเงื่อนไขของหลักสูตร อย่างน้อย ๒ เรื่อง และมีการสรุปบทเรียน ๑ เรื่อง ส่งให้ผู้บังคับบัญชา นั้น

ข้าพเจ้า นายธนดล บุญสุข ตำแหน่ง วิศวกรโยธาปฏิบัติการ สังกัดกลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๔ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน ได้ผ่านการพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านระบบ Digital Government Learning Platform สถาบันพัฒนาบุคลากรภาครัฐดิจิทัล จำนวน ๒ หลักสูตร ได้แก่

๑. จริยธรรมสารสนเทศสำหรับพลเมืองดิจิทัล
๒. การรักษาความปลอดภัยไซเบอร์สำหรับผู้ปฏิบัติงานด้านเทคโนโลยี

จึงขอสรุปบทเรียนที่ได้รับการพัฒนาความรู้ในรอบการประเมินที่ ๒/๒๕๖๕ จำนวน ๑ หลักสูตร ได้แก่ เรื่อง จริยธรรมสารสนเทศสำหรับพลเมืองดิจิทัล รายละเอียดปรากฏตามรายงานสรุปบทเรียน และได้แนบสำเนาใบประกาศนียบัตร จำนวน ๒ หลักสูตร มาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณา

ธนดล

(นายธนดล บุญสุข)
วิศวกรโยธาปฏิบัติการ

นางสาวอุดมลักษณ์ อินทรกำแหง
ผู้อำนวยการกลุ่มพัฒนาโครงสร้างพื้นฐานที่

- ทราบ

- ผอ.ร. (พัสดุ) (คุณกตพร) ทราบ

(นายจักรกฤษณ์ มีโย)

ผู้อำนวยการสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน

ชื่อเรื่อง : จริยธรรมสารสนเทศสำหรับพลเมืองดิจิทัล

(โดย นายธนดล บุญสุข วิศวกรโยธาปฏิบัติการ)

๑. วัตถุประสงค์

เพื่อให้ผู้เรียนเข้าใจความหมายและความสำคัญของจริยธรรมสารสนเทศ สามารถใช้ข้อมูลและเทคโนโลยีดิจิทัลได้อย่างถูกต้อง เหมาะสม และมีความรับผิดชอบ รวมทั้งตระหนักถึงสิทธิส่วนบุคคล การคุ้มครองข้อมูล ลิขสิทธิ์ ทรัพย์สินทางปัญญา และการอ้างอิงผลงานอย่างถูกต้อง

นอกจากนี้ยังมุ่งให้ผู้เรียนรู้เท่าทันสื่อและภัยคุกคามทางไซเบอร์ สามารถป้องกันความเสี่ยงจากการใช้เทคโนโลยี และนำความรู้ด้านจริยธรรมสารสนเทศและความมั่นคงปลอดภัยไปประยุกต์ใช้ในการทำงานภายในองค์กร รวมถึงพัฒนางานวิศวกรรมโยธาของกรมพัฒนาที่ดินให้มีความถูกต้อง โปร่งใส ปลอดภัย และสามารถตรวจสอบย้อนหลังได้ง่ายขึ้น

๒. บทนำ

ปัจจุบันการเปลี่ยนแปลงเข้าสู่ยุคดิจิทัลทำให้ข้อมูลและสารสนเทศกลายเป็นทรัพยากรที่มีความสำคัญอย่างยิ่งต่อบุคคล องค์กร และหน่วยงานภาครัฐ การปฏิบัติงานไม่ได้เกี่ยวข้องเพียงกับการใช้คอมพิวเตอร์หรืออินเทอร์เน็ตเท่านั้น แต่ครอบคลุมตั้งแต่การสร้างข้อมูล การรวบรวม การจัดเก็บ การประมวลผล การแลกเปลี่ยนข้อมูล ตลอดจนการเผยแพร่และนำข้อมูลไปใช้เพื่อประกอบการตัดสินใจ

การใช้สารสนเทศจึงจำเป็นต้องอยู่บนพื้นฐานของความถูกต้อง ความรับผิดชอบ ความเป็นธรรม การเคารพสิทธิของผู้อื่น และการรักษาความมั่นคงปลอดภัยของข้อมูล แม้เทคโนโลยีจะช่วยเพิ่มความรวดเร็วและประสิทธิภาพในการปฏิบัติงาน แต่หากไม่มีหลักจริยธรรมกำกับก็อาจก่อให้เกิดปัญหา เช่น การละเมิดข้อมูลส่วนบุคคล การคัดลอกผลงาน การละเมิดลิขสิทธิ์ การเผยแพร่ข้อมูลที่ไม่ถูกต้อง การนำข้อมูลไปใช้เกินวัตถุประสงค์ หรือการเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์

แนวคิดเรื่อง Information Ethics for Digital Citizenship จึงเป็นการเชื่อมโยงระหว่างจริยธรรมสารสนเทศ เทคโนโลยี กฎหมาย และความรับผิดชอบต่อบุคคลในสังคมดิจิทัล เพื่อให้สามารถใช้ข้อมูลและเทคโนโลยีได้อย่างมีประสิทธิภาพควบคู่กับการเคารพสิทธิของบุคคลและผลประโยชน์ของส่วนรวม

๓. เนื้อหา

๓.๑ ความรู้พื้นฐานเกี่ยวกับจริยธรรมสารสนเทศ

จริยธรรมสารสนเทศหมายถึงหลักหรือแนวทางที่ใช้พิจารณาความถูกต้องและความเหมาะสมของพฤติกรรมที่เกี่ยวข้องกับสารสนเทศ ตั้งแต่การสร้าง การรวบรวม การจัดเก็บ การจัดระบบ การประมวลผล การเผยแพร่

และการนำสารสนเทศไปใช้ โดยมุ่งให้ผู้ใช้อ้างอิงข้อมูลตระหนักถึงสิทธิของตนเองและผู้อื่น รวมถึงผลกระทบที่อาจเกิดขึ้นจากการใช้ข้อมูล

จริยธรรมมีความแตกต่างจากกฎหมายในด้านสภาพบังคับ กฎหมายมีข้อกำหนดและบทลงโทษที่ชัดเจน ในขณะที่จริยธรรมเป็นหลักในการกำกับพฤติกรรมโดยอาศัยความรับผิดชอบและค่านิยมที่เหมาะสม อย่างไรก็ตาม จริยธรรมและกฎหมายมีความสัมพันธ์กันในหลายกรณี เช่น การนำข้อมูลส่วนบุคคลของผู้อื่นไปเผยแพร่โดยไม่ได้รับอนุญาต อาจถือเป็นทั้งการกระทำที่ไม่เหมาะสมทางจริยธรรมและอาจเป็นการกระทำที่ขัดต่อกฎหมาย

๓.๒ จริยธรรมสารสนเทศกับความเป็นพลเมืองดิจิทัล

พลเมืองดิจิทัลหมายถึงบุคคลที่สามารถใช้เทคโนโลยีสารสนเทศ อินเทอร์เน็ต และสื่อดิจิทัลได้อย่างมีความรู้ มีวิจารณญาณ และมีความรับผิดชอบต่อผลที่เกิดขึ้นจากการกระทำของตนเอง ทักษะความฉลาดทางดิจิทัล ประกอบด้วยการรักษาอัตลักษณ์ที่ดีของตนเอง การจัดสรรเวลาหน้าจอ การรับมือกับการคุกคามทางออนไลน์ การรักษาความปลอดภัยของข้อมูล การปกป้องข้อมูลส่วนบุคคล การคิดวิเคราะห์และตรวจสอบข้อมูล การจัดการร่องรอยดิจิทัล และการมีความเห็นอกเห็นใจต่อผู้อื่นในโลกออนไลน์

หลักการสำคัญของการเป็นพลเมืองดิจิทัลคือการคิดก่อนโพสต์ ตรวจสอบก่อนแชร์ เคารพสิทธิของผู้อื่น ไม่สร้างความเสียหายแก่บุคคลอื่น และรับผิดชอบต่อข้อความ ภาพ หรือข้อมูลที่ตนเองนำเข้าสู่อินเทอร์เน็ต

๓.๓ จริยธรรมในการผลิต จัดเก็บ และเผยแพร่สารสนเทศ

การผลิตและจัดเก็บสารสนเทศที่ดีต้องคำนึงถึงความถูกต้อง ความครบถ้วน ความน่าเชื่อถือ และความสามารถในการตรวจสอบย้อนกลับ ข้อมูลควรได้รับการบริหารจัดการตั้งแต่ขั้นตอนการสร้าง การรวบรวม การจัดเก็บ การประมวลผล การนำไปใช้ การเผยแพร่ ตลอดจนการเก็บรักษาหรือทำลายเมื่อหมดความจำเป็น

การนำระบบคอมพิวเตอร์เข้ามาช่วยในการจัดการสารสนเทศสามารถเพิ่มประสิทธิภาพและลดระยะเวลาการดำเนินงาน แต่ในขณะเดียวกันต้องมีมาตรการควบคุมเพื่อป้องกันข้อมูลสูญหาย ถูกเปลี่ยนแปลง หรือถูกเข้าถึงโดยผู้ที่ไม่มีความเหมาะสม องค์กรจึงควรมีกรอบการกำกับดูแลข้อมูล หรือ Data Governance เพื่อกำหนดผู้รับผิดชอบข้อมูล มาตรฐานการจัดเก็บ สิทธิการเข้าถึง กระบวนการตรวจสอบ และแนวทางในการนำข้อมูลไปใช้

๓.๔ ทรัพย์สินทางปัญญา ลิขสิทธิ์ และสัญญาอนุญาต

ทรัพย์สินทางปัญญาเป็นสิทธิที่เกี่ยวข้องกับผลงานที่เกิดจากความคิดและการสร้างสรรค์ของบุคคล เช่น ลิขสิทธิ์ สิทธิบัตร เครื่องหมายการค้า โปรแกรมคอมพิวเตอร์ งานเขียน เอกสารวิชาการ และผลงานประเภท

อื่น การนำผลงานของบุคคลอื่นมาใช้จึงต้องพิจารณาทั้งเรื่องสิทธิของเจ้าของผลงาน การอ้างอิงแหล่งที่มา และเงื่อนไขในการนำผลงานไปใช้

Creative Commons เป็นรูปแบบสัญญาอนุญาตที่เจ้าของผลงานสามารถกำหนดเงื่อนไขในการนำผลงานไปใช้ได้ โดย BY หมายถึงต้องระบุที่มา NC หมายถึงไม่อนุญาตให้นำไปใช้เพื่อการค้า SA หมายถึงหากมีการดัดแปลงต้องเผยแพร่ผลงานใหม่ภายใต้สัญญาอนุญาตแบบเดียวกัน และ ND หมายถึงไม่อนุญาตให้ดัดแปลงผลงาน

๓.๕ สิทธิส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคล

สิทธิส่วนบุคคลเป็นสิทธิของบุคคลในการกำหนดว่าข้อมูลเกี่ยวกับตนเองจะถูกเปิดเผยให้บุคคลใด เมื่อใด ในลักษณะใด และมากน้อยเพียงใด การเก็บรวบรวม ใช้ ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลจึงต้องมีวัตถุประสงค์ที่ชัดเจน มีฐานในการดำเนินการที่เหมาะสม และคำนึงถึงสิทธิของเจ้าของข้อมูล

แนวคิด PAPA เป็นกรอบสำคัญในการพิจารณาจริยธรรมสารสนเทศ โดยประกอบด้วย Privacy หมายถึงความเป็นส่วนตัว Accuracy หมายถึงความถูกต้องของข้อมูล Property หมายถึงความเป็นเจ้าของข้อมูล และ Accessibility หมายถึงการเข้าถึงข้อมูลอย่างเหมาะสม หลักทั้งสี่ประการช่วยให้องค์กรและบุคคลสามารถพิจารณาการใช้ข้อมูลได้อย่างรอบด้าน

๓.๖ จริยธรรมทางวิชาการและการคัดลอกผลงาน

การจัดทำรายงาน งานวิจัย แบบก่อสร้าง คู่มือ รายการคำนวณ หรือเอกสารทางวิชาการ จำเป็นต้องคำนึงถึงความถูกต้องและการอ้างอิงแหล่งที่มาของข้อมูล การนำข้อความ แนวคิด ตาราง รูปภาพ แบบก่อสร้าง หรือผลการศึกษาของผู้อื่นมาใช้โดยไม่อ้างอิงแหล่งที่มาอาจถือเป็นการคัดลอกผลงาน หรือ Plagiarism ซึ่งขัดต่อจริยธรรมทางวิชาการ

การจัดทำผลงานที่ถูกต้องจึงควรสร้างผลงานด้วยตนเอง ใช้ข้อมูลจากแหล่งที่เชื่อถือได้ มีการอ้างอิงแหล่งที่มาอย่างเหมาะสม ไม่บิดเบือนข้อมูล และไม่นำผลงานของผู้อื่นมาแสดงว่าเป็นผลงานของตนเอง

๓.๗ ความมั่นคงปลอดภัยของสารสนเทศ

หลักพื้นฐานด้านความมั่นคงปลอดภัยของสารสนเทศที่สำคัญคือ CIA Triad ซึ่งประกอบด้วย Confidentiality หรือการรักษาความลับของข้อมูล Integrity หรือการรักษาความถูกต้องครบถ้วนของข้อมูลไม่ให้ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และ Availability หรือการทำให้ระบบและข้อมูลพร้อมใช้งานเมื่อผู้มีส่วนเกี่ยวข้องต้องการใช้งาน

มาตรการที่สามารถใช้ในการรักษาความมั่นคงปลอดภัย ได้แก่ การเข้ารหัสข้อมูล การใช้ Hashing การใช้ Virtual Private Network การใช้ Firewall การใช้ Intrusion Detection System การใช้ Intrusion Prevention System การป้องกันข้อมูลรั่วไหล การรวบรวมและวิเคราะห์ Log การสำรองข้อมูล การบริหารจัดการ Patch และการแบ่งเครือข่ายออกเป็นส่วนย่อย

๓.๘ ภัยคุกคามทางไซเบอร์

ภัยคุกคามด้านความมั่นคงปลอดภัยมีหลายประเภท Virus เป็นมัลแวร์ที่อาศัยไฟล์หรือโปรแกรมอื่นในการแพร่กระจาย Worm สามารถแพร่กระจายตัวเองผ่านระบบเครือข่ายได้โดยอัตโนมัติ Trojan Horse แฝงตัวมากับซอฟต์แวร์หรือไฟล์ที่ดูน่าเชื่อถือและอาจเปิดช่องทางให้ผู้ไม่หวังดีควบคุมเครื่อง Ransomware มุ่งเข้ารหัสข้อมูลของเหยื่อและเรียกค่าไถ่เพื่อแลกกับการถอดรหัส และ Spyware ใช้สำหรับแอบติดตามหรือรวบรวมข้อมูลของผู้ใช้

นอกจากนี้ยังมีการโจมตีที่อาศัยการหลอกลวงบุคคล เช่น Phishing ซึ่งหลอกให้ผู้ใช้เปิดเผยข้อมูลสำคัญ Spear Phishing เป็นการหลอกลวงที่เจาะจงบุคคลหรือกลุ่มเป้าหมาย Social Engineering เป็นการใช้เทคนิคทางจิตวิทยาเพื่อหลอกให้บุคคลเปิดเผยข้อมูลหรือกระทำการที่เป็นประโยชน์ต่อผู้โจมตี และ Zero Day Exploit เป็นการโจมตีโดยอาศัยช่องโหว่ที่เพิ่งถูกค้นพบและยังไม่มี Patch สำหรับแก้ไข

๓.๙ การบริหารความเสี่ยงและการตอบสนองต่อเหตุการณ์

Threat หมายถึงสิ่งที่มีศักยภาพในการก่อให้เกิดอันตรายต่อระบบ Vulnerability หมายถึงจุดอ่อนหรือช่องโหว่ของระบบที่เปิดโอกาสให้ภัยคุกคามเข้ามาโจมตีได้ ส่วน Risk หมายถึงความเป็นไปได้ที่จะเกิดเหตุการณ์และผลกระทบที่เกิดขึ้นเมื่อภัยคุกคามสามารถใช้ประโยชน์จากช่องโหว่ได้สำเร็จ

การลดความเสี่ยงจึงต้องดำเนินการทั้งในด้านเทคนิคและด้านการบริหาร เช่น การตั้งค่าระบบอย่างปลอดภัย การปิด Port และ Service ที่ไม่จำเป็น การเปลี่ยนรหัสผ่านเริ่มต้น การจำกัดสิทธิ์ Administrator การบริหารจัดการ Patch การสำรองข้อมูล การแบ่งเครือข่าย การจัดทำนโยบายการใช้ทรัพยากรสารสนเทศ และการจัดทำ Incident Response Plan สำหรับใช้เป็นแนวทางเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

๔. ประโยชน์ที่ได้รับ

๑) ทำให้มีความรู้และความเข้าใจเกี่ยวกับความหมาย ความสำคัญ และหลักพื้นฐานของจริยธรรมสารสนเทศ สามารถพิจารณาความเหมาะสมในการสร้าง จัดเก็บ ใช้ และเผยแพร่ข้อมูลได้อย่างมีหลักการ

๒) ทำให้ตระหนักถึงสิทธิส่วนบุคคลและความสำคัญของการคุ้มครองข้อมูล สามารถพิจารณาได้ว่า ข้อมูลประเภทใดควรเปิดเผย ข้อมูลประเภทใดควรจำกัดการเข้าถึง และควรมีมาตรการป้องกันข้อมูลอย่างไร

๓) ทำให้มีความเข้าใจเกี่ยวกับทรัพย์สินทางปัญญา ลิขสิทธิ์ การอ้างอิงแหล่งข้อมูล และการป้องกันการคัดลอกผลงาน ซึ่งสามารถนำไปใช้กับการจัดทำเอกสารทางวิชาการและเอกสารประกอบการปฏิบัติงานได้

๔) ทำให้สามารถใช้เทคโนโลยีและสื่อออนไลน์ได้อย่างมีวิจารณญาณ ตรวจสอบข้อมูลก่อนนำไปใช้ หรือเผยแพร่ และตระหนักถึงผลกระทบที่อาจเกิดขึ้นจากการกระทำในโลกดิจิทัล

๕) ทำให้เข้าใจหลักพื้นฐานด้าน Cybersecurity สามารถจำแนกภัยคุกคาม ช่องโหว่ และความเสี่ยง รวมทั้งเข้าใจมาตรการรักษาความมั่นคงปลอดภัย เช่น การสำรองข้อมูล การเข้ารหัส การอัปเดต Patch การตรวจจับและป้องกันการบุกรุก และการบริหารสิทธิของผู้ใช้

๖) ทำให้สามารถนำหลักจริยธรรมและหลักความมั่นคงปลอดภัยมาประยุกต์ใช้ในการกำหนดนโยบาย และแนวปฏิบัติภายในองค์กร ส่งผลให้การบริหารจัดการข้อมูลมีความถูกต้อง โปร่งใส และสามารถตรวจสอบได้

๕. แนวคิดการนำไปใช้ปรับใช้ในการพัฒนาวิศวกรรมโยธาในกรมพัฒนาที่ดิน ✓

๑) จัดเก็บข้อมูลโครงการให้เป็นระบบ โดยรวมข้อมูลสำรวจ แบบก่อสร้าง BOQ รายการคำนวณ ภาพถ่ายหน้างาน และเอกสารตรวจรับไว้ในระบบเดียวกัน เพื่อให้ค้นหาง่าย ลดข้อมูลซ้ำ และตรวจสอบย้อนหลังได้

๒) ควบคุมแบบและเอกสารให้ใช้ฉบับล่าสุดเสมอ โดยกำหนดเลข Revision หรือวันที่แก้ไขให้ชัดเจน เพื่อป้องกันการนำแบบเก่าหรือ BOQ คนละฉบับไปใช้ก่อสร้าง

๓) ตรวจสอบความถูกต้องของข้อมูลก่อนนำไปใช้ เช่น ค่าพิภักดิ์ ค่าระดับ ปริมาณงาน ราคาวัสดุ และสูตรคำนวณ เพื่อช่วยลดความผิดพลาดในการออกแบบและประมาณราคา

๔) กำหนดสิทธิการเข้าถึงข้อมูลให้เหมาะสม โดยให้เจ้าหน้าที่แต่ละคนเข้าถึงหรือแก้ไขเฉพาะข้อมูลที่เกี่ยวข้องกับหน้าที่ของตน เพื่อป้องกันข้อมูลสูญหาย ถูกแก้ไข หรือเผยแพร่โดยไม่ได้รับอนุญาต

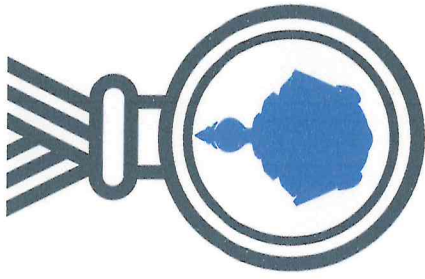
๕) สำรองข้อมูลสำคัญอย่างสม่ำเสมอ เช่น แบบก่อสร้าง BOQ ข้อมูลสำรวจ และรายงานควบคุมงาน เพื่อป้องกันความเสียหายจากเครื่องคอมพิวเตอร์ขัดข้อง ไวรัส หรือ Ransomware

๖) ใช้ซอฟต์แวร์และข้อมูลอย่างถูกต้องตามลิขสิทธิ์ โดยใช้โปรแกรมที่ได้รับอนุญาต อ้างอิงแหล่งที่มาของแบบ มาตรฐาน แผนที่ และข้อมูลที่น่ามาใช้ เพื่อให้การทำงานถูกต้องตามกฎหมายและจริยธรรม

๗) เพิ่มความปลอดภัยให้ระบบคอมพิวเตอร์ เช่น ตั้งรหัสผ่านที่ปลอดภัย อัปเดตระบบและโปรแกรมสม่ำเสมอ ใช้โปรแกรมป้องกันไวรัส และหลีกเลี่ยงการติดตั้งโปรแกรมที่ไม่ทราบแหล่งที่มา

๘) พัฒนาระบบงานวิศวกรรมแบบดิจิทัลให้เชื่อมโยงกันตั้งแต่การสำรวจ ออกแบบ ประมาณราคา ก่อสร้าง ควบคุมงาน ตรวจรับ และเก็บข้อมูลหลังการก่อสร้าง เพื่อให้ทุกขั้นตอนใช้ข้อมูลชุดเดียวกันและลดการทำงานซ้ำ

สรุป คือควรพัฒนางานวิศวกรรมโยธาให้เป็นระบบที่ ข้อมูลถูกต้อง เอกสารไม่สับสน ปลอดภัย ตรวจสอบย้อนหลังได้ และนำข้อมูลเดิมกลับมาใช้ต่อยอดได้ ซึ่งจะช่วยให้งานของกรมพัฒนาที่ดินมีประสิทธิภาพและโปร่งใสมากขึ้น



CERTIFICATE OF COMPLETION

THAI MOOC

Thailand Massive Open Online Course

ประกาศนียบัตรฉบับนี้ให้เพื่อแสดงว่า

ธนดล บุญสุข

ได้ผ่านเกณฑ์หลักสูตรออนไลน์จนได้รับใบประกาศนียบัตรในรายวิชา

จริยธรรมสารสนเทศสำหรับพลเมืองดิจิทัล (7 ชั่วโมง)

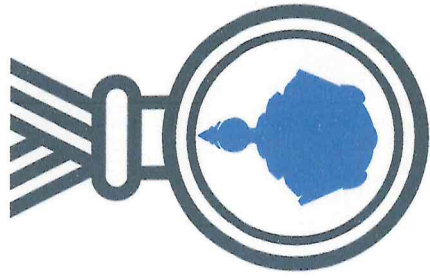
โดย มหาวิทยาลัยวลัยลักษณ์ ให้ไว้ ณ วันที่ 01 กันยายน 2569



d91a8ba6

Signed by สำนักงานคณะกรรมการการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
Ministry of Higher Education, Science, Research and Innovation
Date: 2026-09-01T23:41:18.523653+07:00
Reason: Thai MOOC Certificate of Completion

ศาสตราจารย์ ดร. จินตวิทย์ คล้ายสังข์
ผู้อำนวยการโครงการมหาวิทยาลัยไซเบอร์ไทย (TCU)
กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม



CERTIFICATE OF COMPLETION THAI MOOC

Thailand Massive Open Online Course

THIS CERTIFICATE IS AWARDED TO

Thanadon Boonsuk

for the completion and fulfillment of the online course

Information Ethics for Digital Citizenship (7 Hours)

Awarded by Walailak University on 01 September 2026

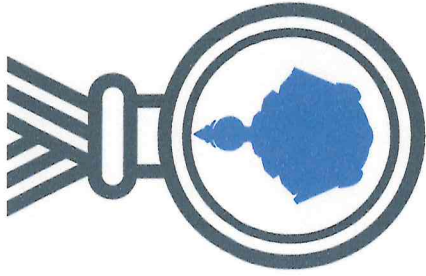
Professor Dr. Jintavee Khlaisang

Director of Thailand Cyber University Project (TCU)
Ministry of Higher Education, Science, Research and Innovation



d91a8ba6

Signed by สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
Ministry of Higher Education, Science, Research and Innovation
Date: 2026-09-01T23:41:18.523653+07:00
Reason: Thai MOOC Certificate of Completion



CERTIFICATE OF COMPLETION THAI MOOC

Thailand Massive Open Online Course

ประกาศนียบัตรฉบับนี้ให้ไว้เพื่อแสดงว่า

ธนดล บุญสุข

ได้ผ่านเกณฑ์หลักสูตรออนไลน์จนได้รับใบประกาศนียบัตรในรายวิชา

การรักความปลอดภัยไซเบอร์สำหรับผู้ปฏิบัติงานด้านเทคโนโลยี (3 ชั่วโมง)

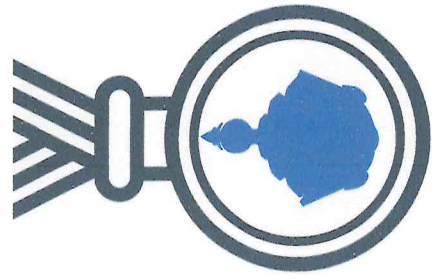
โดย สำนักงานคณะกรรมการการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ให้ไว้ ณ วันที่ 01 กันยายน 2569



6892bc6e

Signed by สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
Ministry of Higher Education, Science, Research and Innovation
Date: 2026-09-01T23:58:43.582573+07:00
Reason: Thai MOOC Certificate of Completion

ศาสตราจารย์ ดร.จินตวีร์ คล้ายสังข์
ผู้อำนวยการโครงการมหาวิทยาลัยไซเบอร์ไทย (TCU)
กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม



CERTIFICATE OF COMPLETION THAI MOOC

Thailand Massive Open Online Course

THIS CERTIFICATE IS AWARDED TO

Thanadon Boonsuk

for the completion and fulfillment of the online course

Cybersecurity Principle for Technology Practitioners (3 Hours)

Awarded by The National Board of Digital Economy and Society Office on 01 September 2026



6892bc6e

Signed by สำนักงานคณะกรรมการการอุดมศึกษา วิทยาเขตวิจัยและนวัตกรรม
Ministry of Higher Education, Science, Research and Innovation
Date: 2026-09-01T23:58:43.582573+07:00
Reason: Thai MOOC certificate of Completion

Professor Dr. Jintavee Khlaisang
Director of Thailand Cyber University Project (TCU)
Ministry of Higher Education, Science, Research and Innovation