แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินพิจิตร

ด้วย ข้าพเจ้า นางสาวณัฐชนัญ ชินปุษยานนท์ ตำแหน่ง นักวิชาการเกษตรชำนาญการ สังกัด สถานีพัฒนาที่ดินพิจิตร สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ หลักสูตร **ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล** ระหว่างวันที่ ๗ สิงหาคม ๒๕๖๗ ถึงวันที่ ๒๓ สิงหาคม ๒๕๖๗ เป็นเวลารวมทั้งสิ้น ๑๗ วัน ณ สถานีพัฒนาที่ดินพิจิตร ซึ่งหลักสูตรดังกล่าวจัดโดยสำนักงานคณะกรรมการข้าราชการพลเรือน (สำนักงาน ก.พ.)

บัดนี้ ข้าพเจ้าได้เข้ารับพัฒนาความรู้ฯ หลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการพัฒนาความรู้ฯ เพื่อโปรดพิจารณา ดังนี้

๑. การพัฒนาความรู้ฯ ดังกล่าวมีวัตถุประสงค์เพื่อ

๑.๑ เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเตอร์เน็ตและการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นในยุคดิจิทัล

๑.๒ เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวังเพื่อให้ปลอดภัยจากภัยคุกคาม

๑.๓ เพื่อให้สามารถยกตัวอย่างภัยคุกคามต่างๆ ได้

๑.๔ เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันตรวจสอบความปลอดภัยด้วยตนเอง

๒. เนื้อหาและหัวข้อวิชาของการพัฒนาความรู้ฯ มีดังนี้

ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการในยุคดิจิทัลเป็นเรื่องสำคัญที่ต้องให้ความสนใจอย่างยิ่ง เนื่องจากข้าราชการมักจะมีการเข้าถึงข้อมูลที่สำคัญและละเอียดอ่อน ซึ่งจำเป็นต้องมีการป้องกันและรักษาความปลอดภัยเพื่อไม่ให้ข้อมูลเหล่านี้ตกไปอยู่ในมือของบุคคลที่ไม่ประสงค์ดี

๒.๑ แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทยมีการเปลี่ยนแปลงและพัฒนาอย่างรวดเร็วในช่วงหลายปีที่ผ่านมา และคาดว่าจะมีแนวโน้มที่น่าสนใจในอนาคต

๑) การเติบโตของผู้ใช้ จำนวนผู้ใช้บริการอินเทอร์เน็ตในประเทศไทยยังคงเพิ่มขึ้นเรื่อยๆ โดยมีการขยายไปยังพื้นที่ชนบทและพื้นที่ห่างไกลมากขึ้น ความครอบคลุมของเครือข่าย ๔G และ ๕G ช่วยกระตุ้นการเข้าถึงอินเทอร์เน็ตในพื้นที่ที่เคยเข้าถึงได้ยาก

๒) การใช้งานผ่านมือถือ การใช้งานอินเทอร์เน็ตผ่านอุปกรณ์มือถือ เช่น สมาร์ตโฟนและแท็บเล็ต มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ซึ่งเป็นผลมาจากความสะดวกในการเข้าถึงข้อมูลและการใช้บริการออนไลน์

๓) การพัฒนาเครือข่าย ๕G: การขยายเครือข่าย ๕G จะส่งผลให้การเชื่อมต่ออินเทอร์เน็ตมีความเร็วสูงขึ้นและมีความเสถียรมากขึ้น ซึ่งสามารถสนับสนุนเทคโนโลยีใหม่ๆ เช่น IoT (Internet of Things), AR/VR และการสตรีมมิ่งวิดีโอความละเอียดสูง

๔) การเพิ่มขึ้นของการซื้อขายออนไลน์ การทำธุรกรรมออนไลน์ เช่น การช้อปปิ้งออนไลน์และการชำระเงินผ่านมือถือกำลังเป็นที่นิยมมากขึ้น เนื่องจากความสะดวกและปลอดภัย

๕) การเติบโตของโซเชียลมีเดีย โซเชียลมีเดียยังคงเป็นส่วนสำคัญของการใช้งานอินเทอร์เน็ตในประเทศไทย โดยเฉพาะในแพลตฟอร์มต่างๆ เช่น Facebook, Instagram และ TikTok

๖) การให้ความสำคัญกับความปลอดภัยทางไซเบอร์ ด้วยการเพิ่มขึ้นของการใช้งานออนไลน์ ความปลอดภัยทางไซเบอร์จะได้รับความสนใจมากขึ้น ทั้งจากบุคคลและองค์กร เพื่อป้องกันข้อมูลส่วนบุคคลและการโจมตีทางไซเบอร์

๗) การเติบโตของเนื้อหาและบริการที่ใช้ AI การพัฒนาเทคโนโลยีปัญญาประดิษฐ์ (AI) และการเรียนรู้ของเครื่อง (Machine Learning) มีแนวโน้มที่จะเปลี่ยนแปลงวิธีที่เราสร้างและบริโภคเนื้อหาบนอินเทอร์เน็ต

แนวโน้มเหล่านี้ชี้ให้เห็นว่าการใช้งานอินเทอร์เน็ตในประเทศไทยกำลังพัฒนาไปในทิศทางที่ทันสมัยและเชื่อมต่อมากขึ้น ซึ่งส่งผลให้เกิดโอกาสใหม่ๆ และความท้าทายต่างๆ ในการจัดการและใช้เทคโนโลยีให้เกิดประโยชน์สูงสุด

การกระทำความผิดทางคอมพิวเตอร์มีรูปแบบและลักษณะหลากหลาย ซึ่งสามารถแบ่งออกได้เป็นหลายประเภทตามวิธีการและเป้าหมายที่เกี่ยวข้อง

๒.๒ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์

๑) การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access)

(๑) การแฮ็ก (Hacking) การเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายโดยไม่ได้รับอนุญาตเพื่อขโมยข้อมูลหรือทำลายระบบ

(๒) การบุกรุก (Intrusion) การเจาะระบบหรือเครือข่ายเพื่อเข้าถึงข้อมูลหรือทรัพยากรที่มีการป้องกัน

๒) การโจรกรรมข้อมูล (Data Theft)

(๑) การขโมยข้อมูลส่วนบุคคล เช่น ข้อมูลบัตรเครดิต, ข้อมูลทางการเงิน หรือข้อมูลส่วนตัวอื่นๆ

(๒) การขโมยข้อมูลทางธุรกิจ ข้อมูลลับทางการค้า หรือข้อมูลสำคัญขององค์กร

๓) การฉ้อโกงออนไลน์ (Online Fraud)

(๑) การฟิชชิง (Phishing) การหลอกลวงให้ผู้ใช้เปิดเผยข้อมูลส่วนตัวผ่านอีเมลหรือเว็บไซต์ปลอม

(๒) การหลอกลวงทางการเงิน (Financial Fraud) การหลอกลวงให้ทำธุรกรรมทางการเงินโดยใช้ข้อมูลปลอม

๔) การแพร่กระจายของมัลแวร์ (Malware Distribution)

(๑) ไวรัส (Virus) โปรแกรมที่สามารถแพร่กระจายและทำลายข้อมูลหรือระบบ

(๒) โทรจัน (Trojan) โปรแกรมที่ปลอมตัวเป็นสิ่งที่มีประโยชน์เพื่อแทรกซึมและทำลายระบบ

๕) การโจมตีเครือข่าย (Network Attacks)

(๑) การโจมตีแบบ Distributed Denial of Service (DDoS) การส่งคำขอจำนวนมากไปยังเซิร์ฟเวอร์เพื่อทำให้ไม่สามารถให้บริการได้

(๒) การโจมตีแบบ Man-in-the-Middle (MitM) การดักจับและแทรกแซงข้อมูลที่ส่งผ่านเครือข่าย

๖) การปลอมแปลงข้อมูล (Data Tampering)

(๑) การปลอมแปลงเอกสารดิจิทัล การแก้ไขข้อมูลหรือเอกสารเพื่อหลอกลวงหรือสร้างความเสียหาย

(๒) การแก้ไขข้อมูลในฐานข้อมูล การเปลี่ยนแปลงข้อมูลที่จัดเก็บในฐานข้อมูลเพื่อประโยชน์ส่วนตัว

๗) การละเมิดสิทธิ์การใช้งาน (License Violations)

(๑) การละเมิดลิขสิทธิ์ซอฟต์แวร์ การใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาตหรือใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์

(๒) การแจกจ่ายซอฟต์แวร์ละเมิดลิขสิทธิ์ การเผยแพร่หรือขายซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

๘) การสร้างความเสียหาย (Vandalism)

(๑) การทำลายเว็บไซต์ การแฮ็กหรือทำลายเนื้อหาเว็บไซต์

(๒) การเปลี่ยนแปลงข้อมูลในเว็บไซต์ การแก้ไขหรือเพิ่มข้อมูลที่เป็นอันตรายในเว็บไซต์

การกระทำความผิดทางคอมพิวเตอร์เป็นปัญหาที่ต้องการความเข้าใจและการป้องกันที่ดีเพื่อให้สามารถรับมือและป้องกันการกระทำเหล่านี้ได้อย่างมีประสิทธิภาพ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (พ.ร.บ. คอมพิวเตอร์) ของประเทศไทยคือ **พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐** (และมีการแก้ไขเพิ่มเติมในปี ๒๕๖๐) โดยมีวัตถุประสงค์หลักเพื่อป้องกันและปราบปรามการกระทำความผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ รวมถึงการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย พระราชบัญญัตินี้มีความสำคัญในการรักษาความปลอดภัยทางไซเบอร์และการป้องกันการกระทำความผิดทางคอมพิวเตอร์ เพื่อให้สอดคล้องกับการพัฒนาเทคโนโลยีและปัญหาที่เกิดขึ้นใหม่ๆ ในยุคดิจิทัล

๒.๓ สรุปสาระสำคัญของพระราชบัญญัตินี้มีดังนี้

๑) ความผิดทางคอมพิวเตอร์

(๑) การเข้าถึงโดยไม่ได้รับอนุญาต การเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

(๒) การทำลายหรือแก้ไขข้อมูล การทำลายหรือแก้ไขข้อมูลในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

(๓) การขโมยข้อมูล การขโมยข้อมูลหรือข้อมูลส่วนบุคคลจากระบบคอมพิวเตอร์

๒) ความผิดเกี่ยวกับเนื้อหา

(๑) การเผยแพร่เนื้อหาที่ผิดกฎหมาย การเผยแพร่ข้อมูลที่มีเนื้อหาผิดกฎหมาย เช่น เนื้อหาที่ลามกอนาจาร, โฆษณาสิ่งผิดกฎหมาย หรือข้อมูลที่เป็นอันตราย

(๒) การหลอกลวงและฉ้อโกงออนไลน์ การใช้เทคโนโลยีในการหลอกลวงหรือฉ้อโก

๓) การป้องกันและการบังคับใช้

(๑) การจัดตั้งหน่วยงาน การจัดตั้งหน่วยงานที่มีหน้าที่บังคับใช้กฎหมายและตรวจสอบการกระทำความผิด

(๒) การรวบรวมและเก็บหลักฐาน การมีอำนาจในการรวบรวมข้อมูลและหลักฐานทางคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิด

๔) โทษและการลงโทษ

การลงโทษ การกำหนดโทษสำหรับผู้กระทำความผิด ซึ่งอาจรวมถึงการจำคุกและการปรับเงิน ขึ้นอยู่กับความร้ายแรงของการกระทำความผิด

๕) มาตรการรักษาความปลอดภัย

(๑) การคุ้มครองข้อมูล การกำหนดมาตรการในการป้องกันและคุ้มครองข้อมูลส่วนบุคคลจากการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) การป้องกันการกระทำความผิด การส่งเสริมการใช้เทคโนโลยีที่ช่วยป้องกันการกระทำความผิด

๖) การแก้ไขและเพิ่มเติม

การแก้ไขเพิ่มเติม มีการปรับปรุงและเพิ่มเติมกฎหมายตามความเปลี่ยนแปลงของเทคโนโลยีและสถานการณ์การกระทำความผิดที่เกิดขึ้น

การปฏิบัติตามหลักการและข้อปฏิบัติดังต่อไปนี้ จะช่วยลดความเสี่ยงในการถูกโจมตีทางไซเบอร์และปกป้องข้อมูลสำคัญจากการถูกเข้าถึงหรือใช้โดยไม่ได้รับอนุญาต

๒.๔ หลักการและข้อปฏิบัติที่สำคัญความมั่นคงปลอดภัยบนอินเทอร์เน็ต

๑) การป้องกันข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลและข้อมูลราชการต้องได้รับการป้องกันอย่างเคร่งครัด ไม่ควรเปิดเผยข้อมูลสำคัญออกสู่สาธารณะหรือผ่านช่องทางที่ไม่ปลอดภัย เช่น โซเชียลมีเดีย หรืออีเมลที่ไม่ได้เข้ารหัส

๒) การใช้รหัสผ่านที่แข็งแรง รหัสผ่านควรเป็นการรวมกันของตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และอักขระพิเศษ และควรเปลี่ยนรหัสผ่านเป็นประจำเพื่อลดความเสี่ยงจากการถูกโจมตี

๓) การตรวจสอบสิทธิ์การเข้าถึง ตรวจสอบสิทธิ์การเข้าถึงข้อมูลและระบบอย่างสม่ำเสมอเพื่อให้แน่ใจว่าผู้ที่มีสิทธิ์เข้าถึงข้อมูลเป็นผู้ที่ได้รับอนุญาตจริงๆ

๔) การอัปเดตและแพตช์ระบบ อัปเดตซอฟต์แวร์และระบบปฏิบัติการอย่างสม่ำเสมอเพื่อปิดช่องโหว่ด้านความปลอดภัย

๕) การระวังภัยจากอีเมลฟิชชิ่งและมัลแวร์ ระมัดระวังในการเปิดอีเมลหรือคลิกลิงก์จากแหล่งที่ไม่น่าเชื่อถือ และไม่ดาวน์โหลดไฟล์จากแหล่งที่ไม่รู้จัก

๖) การใช้การเข้ารหัสข้อมูล ข้อมูลที่ถูกส่งผ่านเครือข่ายควรถูกเข้ารหัสเพื่อป้องกันการดักจับข้อมูลจากบุคคลที่ไม่ประสงค์ดี

๓. ประโยชน์ที่ได้รับจากการพัฒนาความรู้ต่อตนเอง ได้แก่

ได้เรียนรู้ เข้าใจ และเล็งเห็นความสำคัญของความมั่นคงปลอดภัยบนอินเทอร์เน็ต และการศึกษาข้อมูลเกี่ยวกับความปลอดภัยไซเบอร์ เพื่อให้เข้าใจถึงวิธีการป้องกันภัยและวิธีการตอบสนองเมื่อเกิดปัญหา

๔. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการพัฒนาความรู้ฯ ครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน มีดังนี้

ปฏิบัติตามนโยบายและข้อบังคับที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ที่กำหนดโดยหน่วยงานหรือองค์กร รายงานเหตุการณ์หรือข้อสงสัยเกี่ยวกับความปลอดภัยให้แก่หน่วยงานที่เกี่ยวข้องทันทีเพื่อให้สามารถดำเนินการแก้ไขได้อย่างรวดเร็ว การใช้เครื่องมือและโปรแกรมที่ได้รับการอนุมัติจากหน่วยงานและหลีกเลี่ยงการติดตั้งซอฟต์แวร์หรือแอปพลิเคชันที่ไม่ได้รับอนุญาต ปฏิบัติตามหลักการรักษาความลับของข้อมูลราชการและข้อมูลส่วนบุคคลอย่างเคร่งครัด

๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน

การลงทุนในเทคโนโลยีความปลอดภัย เช่น ระบบป้องกันไวรัส, การเข้ารหัสข้อมูล หรือการตรวจสอบความปลอดภัยอาจมีค่าใช้จ่ายสูง ระบบและเทคโนโลยีที่ซับซ้อนอาจทำให้การรักษาความปลอดภัยและการจัดการความเสี่ยงเป็นเรื่องที่ยุ่งยาก การขาดการอัพเดตระบบความปลอดภัยและการพัฒนาระบบเพื่อป้องกันภัยคุกคามใหม่ๆ

๖. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล ได้แก่

ผู้บริหารเข้าใจและตระหนักถึงความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้น ส่งเสริมให้บุคลากรได้รับการฝึกอบรมความรู้เกี่ยวกับแนวทางปฏิบัติในการรักษาความปลอดภัยของข้อมูลและเทคโนโลยี ความรู้ด้านความปลอดภัยไซเบอร์หรือการป้องกันการโจมตีทางเทคโนโลยี และการลงทุนในเทคโนโลยีความปลอดภัยที่อาจมีค่าใช้จ่ายสูง

จึงเรียนมาเพื่อโปรดพิจารณา

(ลงชื่อ) ณัฐชนัญ ชินปุษยานนท์

(นางสาวณัฐชนัญ ชินปุษยานนท์)

ผู้เข้ารับการพัฒนาความรู้