แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินพิจิตร

ด้วยข้าพเจ้า **นางสาวณัฐชนัญ ชินปุษยานนท์** ตำแหน่ง **นักวิชาการเกษตรชำนาญการ** สังกัด ฝ่ายวิชาการเพื่อการพัฒนาที่ดิน สถานีพัฒนาที่ดินพิจิตร สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ หลักสูตร **การเรียนรู้ผ่านสื่อการเรียนการสอน E-learning หลักสูตร Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น** ระหว่างวันที่ ๒๒ กรกฎาคม ๒๕๖๘ ถึงวันที่ ๒๓ กรกฎาคม ๒๕๖๘ เป็นเวลารวมทั้งสิ้น ๒ วัน ณ สถานีพัฒนาที่ดินพิจิตร ซึ่งหลักสูตรดังกล่าวจัดโดย **สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy**

บัดนี้ ข้าพเจ้าได้เข้ารับพัฒนาความรู้ฯ หลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการพัฒนาความรู้ฯ เพื่อโปรดพิจารณา ดังนี้

๑. การพัฒนาความรู้ฯ ดังกล่าวมีวัตถุประสงค์เพื่อ

๑.๑ สร้างความรู้ความเข้าใจเรื่องภัยคุกคามทางไซเบอร์ในยุคดิจิทัล

๑.๒ พัฒนาทักษะพื้นฐานในการใช้งานเทคโนโลยีอย่างปลอดภัย

๑.๓ เสริมสร้างวินัยและพฤติกรรมการใช้งานเทคโนโลยีสารสนเทศที่ปลอดภัยในชีวิตประจำวัน

๒. เนื้อหาและหัวข้อวิชาของการพัฒนาความรู้ฯ มีดังนี้

๒.๑ แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Best Practices) เป็นสิ่งสำคัญที่ช่วยป้องกันข้อมูลส่วนตัว ทรัพย์สินทางดิจิทัล และระบบสารสนเทศจากภัยคุกคามในโลกออนไลน์ โดยสามารถแบ่งแนวทางออกเป็น ๓ ระดับหลัก ได้แก่ ระดับบุคคล ระดับองค์กร และระดับเทคโนโลยี

๒.๑.๑ ระดับบุคคล (Personal Cybersecurity)

- ใช้รหัสผ่านที่รัดกุม ใช้รหัสผ่านที่ยาว มีทั้งตัวอักษรพิมพ์ใหญ่-เล็ก ตัวเลข และสัญลักษณ์ หลีกเลี่ยงการใช้ข้อมูลส่วนตัว เช่น วันเกิด หรือชื่อ
- เปิดใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication - MFA) เช่น ใช้รหัส OTP หรือแอปยืนยันตัวตนร่วมกับรหัสผ่าน
- หลีกเลี่ยงการคลิกลิงก์หรือเปิดไฟล์แนบจากแหล่งที่ไม่น่าเชื่อถือ ระวังอีเมลหลอกลวง (Phishing)
- ปรับปรุงซอฟต์แวร์และแอปพลิเคชันสม่ำเสมอ เพื่อปิดช่องโหว่ที่แฮกเกอร์อาจใช้โจมตี
- สำรองข้อมูล (Backup) เป็นประจำ เช่น สำรองลง Cloud หรือ External Drive

๒.๑.๒ ระดับองค์กร (Organizational Cybersecurity)

- กำหนดนโยบายและแนวปฏิบัติด้านไซเบอร์ที่ชัดเจน เช่น นโยบายการใช้รหัสผ่าน การเข้าถึงข้อมูล

- อบรมให้พนักงานมีความรู้ด้าน Cybersecurity เพื่อลดความเสี่ยงจาก Human Error และ Social Engineering

- แยกสิทธิ์การเข้าถึงข้อมูลตามระดับความจำเป็น (Access Control) หลักการ Need to Know / Least Privilege

- มีแผนรับมือเหตุการณ์ (Incident Response Plan) พร้อมทีมรับมือกรณีถูกโจมตีทางไซเบอร์

- ทำการประเมินความเสี่ยงและทดสอบช่องโหว่สม่ำเสมอ เช่น การทำ Penetration Test หรือ Vulnerability Scan

๒.๑.๓ ระดับเทคโนโลยี (Technical Measures)

- ติดตั้งโปรแกรมป้องกันไวรัสและมัลแวร์ และตั้งค่าให้สแกนอัตโนมัติ

- ใช้ไฟร์วอลล์ (Firewall) และระบบตรวจจับภัยคุกคาม (IDS/IPS) เพื่อตรวจจับและสกัดการเข้าถึงที่ผิดปกติ

- เข้ารหัสข้อมูล (Encryption) โดยเฉพาะข้อมูลที่สำคัญหรือข้อมูลส่วนบุคคล

- ควบคุมการใช้อุปกรณ์ภายนอก เช่น USB, External Drive โดยเฉพาะในองค์กร

- จัดการและปรับปรุงสิทธิ์ผู้ใช้งานในระบบเมื่อมีการเปลี่ยนตำแหน่ง หรือออกจากงาน

๒.๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment) คือกระบวนการสำคัญในการวิเคราะห์และจัดการกับความเสี่ยงที่อาจส่งผลกระทบต่อระบบสารสนเทศและข้อมูลขององค์กร โดยมีเป้าหมายเพื่อระบุภัยคุกคาม ช่องโหว่ และผลกระทบ เพื่อกำหนดมาตรการควบคุมความเสี่ยงอย่างมีประสิทธิภาพ

๒.๒.๑ ขั้นตอนในการประเมินความเสี่ยงไซเบอร์

- ระบุทรัพย์สินสารสนเทศ (Identify Assets) เช่น ข้อมูลลูกค้า, ระบบฐานข้อมูล, เครื่องแม่ข่าย, แอปพลิเคชัน พิจารณาทรัพย์สินที่มีความสำคัญต่อภารกิจและเป้าหมายองค์กร

- ระบุภัยคุกคาม (Identify Threats) เช่น มัลแวร์, แรนซัมแวร์, การเข้าถึงโดยไม่ได้รับอนุญาต, ฟิชชิง รวมถึงภัยจากบุคคลภายใน (Insider Threat)

- ระบุช่องโหว่ (Identify Vulnerabilities) เช่น ซอฟต์แวร์ไม่ได้อัปเดต, การตั้งค่าระบบผิดพลาด, ไม่มีการเข้ารหัสข้อมูล

- วิเคราะห์ความเสี่ยง (Risk Analysis) วิเคราะห์โอกาสที่ภัยคุกคามจะใช้ช่องโหว่โจมตีสำเร็จ ประเมินผลกระทบ (Impact) หากเกิดเหตุการณ์จริง สามารถใช้ตาราง Risk Matrix: ความน่าจะเป็น × ผลกระทบ

- ประเมินระดับความเสี่ยง (Risk Evaluation) จัดลำดับความเสี่ยง (High, Medium, Low) ตัดสินใจว่าจะยอมรับ (Accept), ลด (Mitigate), โอน (Transfer) หรือหลีกเลี่ยง (Avoid)

- กำหนดมาตรการควบคุมความเสี่ยง (Risk Treatment) เช่น การติดตั้งระบบป้องกัน, ปรับปรุงนโยบาย, ฝึกอบรมผู้ใช้

- ติดตามและทบทวน (Monitor and Review) ทบทวนความเสี่ยงอย่างสม่ำเสมอ โดยเฉพาะเมื่อมีเทคโนโลยีใหม่หรือเปลี่ยนแปลงทางธุรกิจ

๒.๒.๒ เครื่องมือ/มาตรฐานที่เกี่ยวข้อง

- ISO/IEC ๒๗๐๐๕: แนวทางการบริหารความเสี่ยงด้านความมั่นคงสารสนเทศ

- NIST SP ๘๐๐-๓๐: คู่มือการประเมินความเสี่ยงระบบสารสนเทศ

- OCTAVE, FAIR, CRAMM: วิธีการประเมินความเสี่ยงแบบต่าง ๆ

๒.๓ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) คือแนวทางหรือเครื่องมือที่ถูกจัดทำขึ้นเพื่อช่วยให้องค์กรสามารถบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นระบบ มีมาตรฐาน และสามารถปฏิบัติได้จริง โดยจะครอบคลุมตั้งแต่การวางแผน ป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากเหตุการณ์ด้านไซเบอร์

กรอบมาตรฐานหลักที่นิยมใช้ทั่วโลก

๒.๓.๑ NIST Cybersecurity Framework (NIST CSF)

จัดทำโดย สถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา เวอร์ชันล่าสุด NIST CSF ๒.๐ (๒๐๒๔)

องค์ประกอบหลัก (Function ๖ ด้าน)

- Govern – การกำกับดูแล
- Identify – การระบุ
- Protect – การป้องกัน
- Detect – การตรวจจับ
- Respond – การตอบสนอง
- Recover – การฟื้นฟู

จุดเด่น

- เข้าใจง่าย เหมาะกับองค์กรทุกขนาด
- ช่วยให้เห็นภาพรวมของความเสี่ยงและระดับการควบคุม
- เป็นพื้นฐานให้หน่วยงานรัฐและเอกชนทั่วโลกนำไปปรับใช้

๒.๓.๒ ISO/IEC ๒๗๐๐๑ & ๒๗๐๐๒

จัดทำโดย International Organization for Standardization (ISO)

ISO/IEC ๒๗๐๐๑: มาตรฐานระบบบริหารจัดการความมั่นคงสารสนเทศ (ISMS)

ISO/IEC ๒๗๐๐๒: แนวทางปฏิบัติ (Code of practice) สำหรับการควบคุมต่างๆ เช่น การเข้ารหัส การควบคุมการเข้าถึง

จุดเด่น

- เป็นมาตรฐานสากลที่สามารถขอการรับรอง (Certification) ได้
- เหมาะกับองค์กรที่ต้องการความน่าเชื่อถือและความสอดคล้องกับกฎหมาย

๒.๓.๓ COBIT (Control Objectives for Information and Related Technologies)

จัดทำโดย ISACA

การบริหารจัดการไอที (IT Governance) ควบคู่กับความมั่นคงปลอดภัย

เชื่อมโยงเป้าหมายธุรกิจกับ IT และ Cybersecurity

เหมาะสำหรับ องค์กรที่ต้องการควบคุมทั้งระบบงานและเทคโนโลยีแบบองค์รวม

๒.๓.๔ CIS Controls (Center for Internet Security Controls)

จัดทำโดย Center for Internet Security

แบ่งเป็น ๑๘ Control Groups เช่น การควบคุมอุปกรณ์และซอฟต์แวร์ การตั้งค่าระบบอย่างปลอดภัย การควบคุมการเข้าถึง

จุดเด่น เป็นแนวทางที่ "นำไปใช้ได้ทันที" (Practical) มีลำดับความสำคัญของการควบคุมตามความเสี่ยงขององค์กร

๒.๓.๕. PDPA/ GDPR – กฎหมายความเป็นส่วนตัวข้อมูล

แม้ไม่ใช่ "framework" โดยตรง แต่กฎหมายเหล่านี้บังคับให้องค์กรต้องมีมาตรการด้าน Cybersecurity เพื่อคุ้มครองข้อมูลส่วนบุคคล เช่น การเข้ารหัสข้อมูล (Encryption) การจัดเก็บข้อมูลอย่างปลอดภัย การแจ้งเหตุละเมิดข้อมูล (Breach Notification)

๒.๔ การป้องกันความเสี่ยง (Protect) โดยการประเมินช่องโหว่ (Vulnerability Assessment) เป็นหนึ่งในกระบวนการสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะในเฟส "Protect" ของกรอบ NIST Cybersecurity Framework เพื่อค้นหาและลดช่องโหว่ก่อนที่แฮกเกอร์จะใช้เป็นช่องทางในการโจมตี

Vulnerability Assessment คือ การตรวจสอบ วิเคราะห์ และประเมินช่องโหว่ของระบบ เทคโนโลยี หรือกระบวนการภายในองค์กร โดยมีเป้าหมายเพื่อ ค้นหาจุดอ่อนที่อาจถูกโจมตีได้ (เช่น ซอฟต์แวร์ที่ล้าสมัย, ระบบไม่ได้ตั้งค่าความปลอดภัย) ประเมินระดับความรุนแรงของช่องโหว่ แนะนำวิธีการป้องกันหรือแก้ไข

ขั้นตอนการทำ Vulnerability Assessment

๒.๔.๑ กำหนดขอบเขต (Define Scope) ระบุว่าจะตรวจอะไร เช่น ระบบเครือข่าย, เว็บแอปพลิเคชัน, อุปกรณ์ IoT, เซิร์ฟเวอร์

๒.๔.๒ เก็บข้อมูล (Information Gathering) ตรวจสอบรายละเอียดระบบ เช่น OS, Service, Port, Software ที่ใช้งานอยู่

๒.๔.๓ สแกนหาช่องโหว่ (Vulnerability Scanning) ใช้เครื่องมือสแกนอัตโนมัติ เช่น Nessus OpenVAS Qualys Nikto (สำหรับ Web) Burp Suite (Web App)

๒.๔.๔ วิเคราะห์และประเมินผล (Analysis & Risk Rating) จัดลำดับความรุนแรง Critical, High, Medium, Low อ้างอิงจากฐานข้อมูล เช่น CVSS (Common Vulnerability Scoring System), NVD

๒.๔.๕ จัดทำรายงานผลและแนะนำแนวทางแก้ไข (Reporting & Mitigation Plan) ระบุช่องโหว่ที่ตรวจพบ แนะนำวิธีอุดช่องโหว่ เช่น Patch, ปิดพอร์ต, ปรับการตั้งค่า

๒.๔.๖ ติดตามผลและทำซ้ำ (Remediation & Re-scan) แก้ไขตามคำแนะนำและทำการประเมินซ้ำจนมั่นใจว่าปลอดภัย

ประโยชน์ของการประเมินช่องโหว่

- ลดความเสี่ยงก่อนถูกโจมตี
- ปรับปรุงมาตรการด้านความปลอดภัยให้เหมาะสม
- เป็นส่วนหนึ่งของการปฏิบัติตามมาตรฐาน เช่น ISO ๒๗๐๐๑, NIST, PDPA
- ป้องกันความเสียหายทางชื่อเสียงและการละเมิดข้อมูล

๒.๕ การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) คือกระบวนการในการตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ โดยเน้นการเฝ้าระวังและแจ้งเตือนภัยคุกคามที่อาจเกิดขึ้น เพื่อให้สามารถตอบสนองได้อย่างรวดเร็วและลดผลกระทบต่อระบบสารสนเทศขององค์กร

๒.๕.๑ จุดประสงค์ของ “Detect”

- ตรวจจับกิจกรรมหรือเหตุการณ์ที่ผิดปกติ
- เฝ้าระวังระบบอย่างต่อเนื่อง (๒๔/๗ Monitoring)
- แจ้งเตือนภัยคุกคามหรือการบุกรุก
- สนับสนุนการตอบสนองและกู้คืนระบบ

๒.๕.๒ วิธีการและเครื่องมือในการตรวจสอบและเฝ้าระวัง

- ระบบตรวจจับการบุกรุก (IDS/IPS)

IDS (Intrusion Detection System) ตรวจจับกิจกรรมที่น่าสงสัยและแจ้งเตือน

PS (Intrusion Prevention System) ตรวจจับและป้องกันโดยอัตโนมัติ เช่น บล็อก IP

- SIEM (Security Information and Event Management) ระบบรวมและวิเคราะห์ Log จากหลายแหล่ง เพื่อหาความผิดปกติ เช่น การล็อกอินผิดหลายครั้ง การเข้าถึงระบบจาก IP ต่างประเทศ การดาวน์โหลดไฟล์จำนวนมาก

ตัวอย่าง SIEM : Splunk, IBM QRadar, Microsoft Sentinel, ELK Stack (ElasticSearch, Logstash, Kibana)

- Log Monitoring & Audit Trail ตรวจสอบ Log จากระบบต่าง ๆ เช่น Firewall, Web Server, Email Server วิเคราะห์หาพฤติกรรมผิดปกติย้อนหลัง จัดทำบันทึกเพื่อรองรับการสืบสวน (Forensics)

- Threat Intelligence ใช้ฐานข้อมูลภัยคุกคามจากแหล่งภายนอก เช่น รายการ IP/Domain อันตราย Indicators of Compromise (IOC) รายงานภัยจาก CERT หรือหน่วยงานความปลอดภัย

แหล่ง Threat Intel ที่น่าเชื่อถือ VirusTotal, AlienVault OTX, MISP

- UEBA (User and Entity Behavior Analytics) ระบบที่ใช้ AI วิเคราะห์พฤติกรรมของผู้ใช้งาน เพื่อตรวจจับพฤติกรรมผิดปกติ เช่น พนักงานเข้าระบบนอกเวลาปกติ การเข้าถึงไฟล์ที่ไม่เกี่ยวข้องกับหน้าที่

๒.๕.๓ ประโยชน์ของการเฝ้าระวังและตรวจสอบภัย

- ลดเวลาในการตรวจพบการโจมตี (Mean Time to Detect - MTTD)
- ลดผลกระทบจากภัยคุกคาม
- สนับสนุนการวิเคราะห์ย้อนหลังและหลักฐานทางนิติวิทยาศาสตร์
- เสริมความน่าเชื่อถือขององค์กร

๒.๖ การเผชิญเหตุภัยคุกคาม ภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

การเผชิญเหตุและฟื้นฟูจากภัยคุกคามทางไซเบอร์ เป็นสองขั้นตอนสำคัญใน NIST Cybersecurity Framework คือ Respond (การตอบสนอง) Recover (การฟื้นฟู) โดยมีเป้าหมายเพื่อ จำกัดความเสียหาย, กู้คืนระบบ, และ เรียนรู้เพื่อป้องกันเหตุซ้ำซ้อนในอนาคต

๒.๖.๑ การเผชิญเหตุภัยคุกคามทางไซเบอร์ (Respond)

จุดประสงค์

- ตอบสนองเหตุการณ์ด้านไซเบอร์อย่างมีประสิทธิภาพ
- ลดความเสียหายจากเหตุการณ์
- สื่อสารกับผู้เกี่ยวข้องอย่างถูกต้องและทันเวลา

๒.๖.๒ การฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

จุดประสงค์

- ฟื้นฟูระบบและบริการให้กลับมาใช้งานได้อย่างปลอดภัย
- สร้างความเชื่อมั่นกลับคืน
- ปรับปรุงกระบวนการให้แข็งแกร่งขึ้น

๓. ประโยชน์ที่ได้รับจากการพัฒนาความรู้ต่อตนเอง ได้แก่

มีความรู้พื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ เข้าใจคำศัพท์และแนวคิดพื้นฐาน เช่น ฟิชชิง, มัลแวร์, รหัสผ่านปลอดภัย ตระหนักรู้ถึงภัยคุกคามรอบตัวในโลกออนไลน์ เพิ่มทักษะการป้องกันตนเองในชีวิตประจำวัน สามารถป้องกันบัญชีส่วนตัว, ข้อมูลส่วนบุคคล, และอุปกรณ์ดิจิทัล ลดความเสี่ยงจากการถูกหลอกลวง หรือโจมตีผ่านทางไซเบอร์ เข้าใจพฤติกรรมที่ปลอดภัยเมื่อใช้อีเมล โซเชียลมีเดีย และอินเทอร์เน็ต หลีกเลี่ยงการเปิดลิงก์หรือดาวน์โหลดไฟล์ที่ไม่ปลอดภัย ไม่เป็นต้นเหตุของการรั่วไหลข้อมูล เคารพสิทธิของผู้อื่นในการใช้ข้อมูลดิจิทัล

๔. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการพัฒนาความรู้ฯ ครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน มีดังนี้

ปฏิบัติตามนโยบายและข้อบังคับที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ที่กำหนดโดยหน่วยงานหรือองค์กร ส่งเสริมพฤติกรรมปลอดภัยในการใช้งานระบบสารสนเทศ รณรงค์การตั้งรหัสผ่านที่ปลอดภัย แจ้งเตือนเมื่อพบอีเมลน่าสงสัย หรือเว็บไซต์ปลอม ปฏิบัติตนเป็นแบบอย่างในการรักษาความปลอดภัยไซเบอร์ เช่น ไม่คลิกลิงก์น่าสงสัย, สำรองข้อมูลอย่างสม่ำเสมอ หลีกเลี่ยงการติดตั้งซอฟต์แวร์หรือแอปพลิเคชันที่ไม่ได้รับอนุญาต ปฏิบัติตามหลักการรักษาความลับของข้อมูลราชการและข้อมูลส่วนบุคคลอย่างเคร่งครัด

๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน

ความไม่เข้าใจหรือขาดความตระหนักของบุคลากร บางคนอาจมองว่าความปลอดภัยไซเบอร์ไม่สำคัญ มีทัศนคติว่า “เป็นเรื่องของฝ่ายไอที” เท่านั้น ไม่เห็นความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้น ขาดการสนับสนุนจากองค์กร ไม่มีนโยบายหรือแนวทางปฏิบัติที่ชัดเจน ไม่มีการจัดสรรงบประมาณหรือเวลาในการพัฒนาด้าน Cybersecurity ข้อจำกัดด้านทรัพยากร อุปกรณ์หรือซอฟต์แวร์ที่ใช้ไม่มีระบบความปลอดภัยเพียงพอ ขาดเครื่องมือสำหรับตรวจสอบหรือป้องกัน เช่น โปรแกรมสแกนมัลแวร์, ระบบสำรองข้อมูลอัตโนมัติ

๖. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล ได้แก่

ผู้บริหารส่งเสริมให้มีนโยบายหรือแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ในหน่วยงาน กำหนดให้มีแนวทางในการใช้งานระบบคอมพิวเตอร์, อีเมล, อุปกรณ์พกพา อย่างปลอดภัย สนับสนุนให้บุคลากรเข้าร่วมอบรมทั้งภายในและภายนอกองค์กร สนับสนุนด้านทรัพยากร จัดหาเครื่องมือพื้นฐานสำหรับรักษาความปลอดภัย เช่น Antivirus, ระบบสำรองข้อมูล พัฒนาโครงสร้างพื้นฐาน IT ให้รองรับมาตรฐานความปลอดภัย จัดสรรงบประมาณในส่วนที่เกี่ยวข้องกับ Cybersecurity

จึงเรียนมาเพื่อโปรดพิจารณา

(นางสาวณัฐชนัญ ชินปุษยานนท์)
นักวิชาการเกษตรชำนาญการ
ผู้เข้ารับการพัฒนาความรู้