กองนโยบายและแผนการใช้ที่ดิน
เลขที่รับ [illegible]
วันที่ ๑๒ ก.พ. ๖๙
เวลา ๑๕.๐๐ น.

บันทึกข้อความ

ส่วนราชการ กลุ่มเศรษฐกิจที่ดินทางการเกษตร กองนโยบายและแผนการใช้ที่ดิน โทร. ๒๒๒๐

ที่ กษ ๐๘๓๗.๐๗/ ๑๑๓ **วันที่** ๑๒ กุมภาพันธ์ ๒๕๖๙

เรื่อง รายงานการสรุปการอบรม สัมมนา และการพัฒนาความรู้ผ่านระบบ OCSC-Learning

เรียน ผู้อำนวยการกลุ่มเศรษฐกิจที่ดินทางการเกษตร

ตามที่กองการเจ้าหน้าที่กำหนดตัวชี้วัดกลางรายบุคคลด้านการพัฒนาบุคลากร รอบการประเมินที่ ๑ (๑ ตุลาคม ๒๕๖๘ – ๓๑ มีนาคม ๒๕๖๙) ระดับความสำเร็จของการพัฒนาความรู้ โดยมีการพัฒนาความรู้ ๒ เรื่อง (ผ่านระบบ e-learning ของสำนักงาน ก.พ. ๒ เรื่อง) รวมทั้งให้มีการสรุปบทเรียน ๑ เรื่อง นั้น

ในการนี้ ข้าพเจ้าได้เข้ารับพัฒนาความรู้ จำนวน ๒ เรื่อง ได้แก่ ๑) หลักสูตร AI skills for All เพื่อใช้ AI ในการแก้ปัญหาสังคมและชีวิตประจำวัน ของสำนักงาน ก.พ. และ ๒) หลักสูตร การบริหารความเสี่ยงดิจิทัล (Digital Risk managemaent) เพื่อป้องกันและลดผลกระทบจากภัยคุกคามดิจิทัล ทั้งนี้ได้สรุปบทเรียนการพัฒนาความรู้ผ่านระบบ OCSC-Learning ของสำนักงาน ก.พ. จำนวน ๑ เรื่อง ได้แก่ หลักสูตร การบริหารความเสี่ยงดิจิทัล (Digital Risk managemaent) เพื่อป้องกันและลดผลกระทบจากภัยคุกคามดิจิทัล เสร็จเรียบร้อยแล้ว (รายละเอียดตามที่แนบ)

จึงเรียนมาเพื่อโปรดพิจารณา นำเรียน ผอ.กนผ. เพื่อทราบต่อไป

(นายณรงค์กรณ์ การินทร์)
เศรษฐกร

เรียน ผอ.กนผ.
เพื่อโปรดพิจารณาลงนามในรายงานสรุปอบรม/พัฒนาความรู้

(นายธนกฤต ผลเกลี้ยง)
ผู้อำนวยการกลุ่มเศรษฐกิจที่ดินทางการเกษตร

- ผอ. ลงนามแล้ว
- [illegible]

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

****

ส่วนที่ ๑ ข้อมูลทั่วไป

ชื่อ-นามสกุล นายณรงค์กรณ์ การินทร์
ตำแหน่ง เศรษฐกร **กลุ่ม** เศรษฐกิจที่ดินทางการเกษตร
หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ :
การบริหารความเสี่ยงดิจิทัล
สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ :
ศึกษาในระบบ OCSC-Learning ของสำนักงาน ก.พ.
หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ :
สำนักงาน ก.พ.
ตั้งแต่วันที่ ๑๐ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙ **ถึงวันที่** ๑๐ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙
เพื่อ ☑ อบรม ☐ สัมมนา ☐ อื่น ๆ ระบุ.....

ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

๒.๑ รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/ สัมมนา/พัฒนาความรู้ฯ

ในยุคดิจิทัล องค์กรทุกประเภทต้องเผชิญกับความเสี่ยงที่ซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว ไม่ว่าจะเป็นภัยคุกคามทางไซเบอร์ การจัดการข้อมูลส่วนบุคคล ความเสี่ยงจากการใช้เทคโนโลยีใหม่ เช่น AI หรือ Cloud Computing รวมถึงความเสี่ยงด้านกฎระเบียบและชื่อเสียง การบริหารความเสี่ยงดิจิทัลจึงเป็นหัวใจสำคัญในการสร้างความมั่นคงและความยั่งยืนขององค์กร

ความหมายและความสำคัญของการบริหารความเสี่ยงดิจิทัล

ความหมาย การบริหารความเสี่ยงดิจิทัลคือกระบวนการระบุ ประเมิน และจัดการความเสี่ยงที่เกิดจากการใช้เทคโนโลยีดิจิทัลและข้อมูลในองค์กร

ความสำคัญ ป้องกันการสูญเสียทางการเงินและชื่อเสียง
สร้างความเชื่อมั่นให้กับผู้ใช้บริการและผู้มีส่วนได้ส่วนเสีย
สนับสนุนการดำเนินงานและการเปลี่ยนแปลงเชิงดิจิทัลอย่างปลอดภัย

ประเภทของความเสี่ยงดิจิทัล

๑. ความเสี่ยงด้านไซเบอร์ (Cybersecurity Risk)• การโจมตีทางไซเบอร์ เช่น Malware, Ransomware, Phishing
• การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
๒. ความเสี่ยงด้านข้อมูล (Data Risk)• การรั่วไหลของข้อมูลส่วนบุคคล
• การจัดเก็บและใช้ข้อมูลไม่เป็นไปตามกฎหมาย เช่น GDPR หรือ PDPA
๓. ความเสี่ยงด้านเทคโนโลยี (Technology Risk)• ความล้มเหลวของระบบ IT
• การพึ่งพาเทคโนโลยีใหม่ที่ยังไม่มั่นคง เช่น AI, IoT
๔. ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk)• การไม่ปฏิบัติตามข้อกำหนดทางกฎหมายและมาตรฐานสากล

๕. ความเสี่ยงด้านชื่อเสียง (Reputation Risk)

• การจัดการเหตุการณ์ผิดพลาดที่ส่งผลต่อภาพลักษณ์องค์กร

กระบวนการบริหารความเสี่ยงดิจิทัล

๑. การระบุความเสี่ยง (Risk Identification)

• วิเคราะห์ระบบ กระบวนการ และข้อมูลที่เกี่ยวข้อง

๒. การประเมินความเสี่ยง (Risk Assessment)

• ประเมินความรุนแรงและความน่าจะเป็นของความเสี่ยง

๓. การวางแผนและจัดการความเสี่ยง (Risk Mitigation)

• กำหนดมาตรการป้องกัน เช่น Firewall, Encryption, Training

• จัดทำแผนตอบสนองเมื่อเกิดเหตุการณ์ (Incident Response Plan)

๔. การติดตามและทบทวน (Monitoring & Review)• ตรวจสอบและปรับปรุงมาตรการอย่างต่อเนื่อง

• ใช้เครื่องมือดิจิทัล เช่น AI และ Big Data ในการตรวจจับความเสี่ยง

แนวทางปฏิบัติที่ดี (Best Practices)

• บูรณาการการบริหารความเสี่ยงดิจิทัลเข้ากับ Enterprise Risk Management (ERM)

• สร้างวัฒนธรรมความปลอดภัยไซเบอร์ในองค์กร โดยการอบรมและสร้างความตระหนักรู้

• ลงทุนในเทคโนโลยีป้องกันและตรวจจับภัยคุกคาม เช่น SIEM, Threat Intelligence

• กำหนดนโยบายการจัดการข้อมูลที่ชัดเจน ครอบคลุมการเก็บ ใช้ และทำลายข้อมูล

• สร้างความร่วมมือกับพันธมิตรและหน่วยงานกำกับดูแล เพื่อแลกเปลี่ยนข้อมูลและแนวทางป้องกัน

ความท้าทายและโอกาส

• ความท้าทาย: ภัยคุกคามที่ซับซ้อนขึ้น การขาดบุคลากรที่มีทักษะด้านความปลอดภัยไซเบอร์ และการเปลี่ยนแปลงกฎระเบียบที่รวดเร็ว

• โอกาส: การใช้ AI และ Machine Learning ในการตรวจจับและตอบสนองต่อภัยคุกคาม การสร้างความเชื่อมั่นให้กับลูกค้า และการเพิ่มขีดความสามารถในการแข่งขันขององค์กร

กรณีศึกษาและบทเรียนจากองค์กรจริง

๑. กรณีการโจมตี Ransomware ในองค์กรภาครัฐ• หลายหน่วยงานถูกโจมตีด้วย Ransomware ทำให้ข้อมูลสำคัญถูกเข้ารหัสและไม่สามารถใช้งานได้

• บทเรียน: ต้องมี ระบบสำรองข้อมูล (Backup) ที่ปลอดภัยและทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ

๒. กรณีการรั่วไหลของข้อมูลลูกค้าในภาคเอกชน• บริษัทที่ให้บริการออนไลน์ถูกโจมตีจนข้อมูลลูกค้าหลายล้านรายรั่วไหล

• บทเรียน: ต้องมี มาตรการเข้ารหัสข้อมูล (Encryption) และ การควบคุมสิทธิ์การเข้าถึง (Access Control) ที่เข้มงวด

๓. กรณีการเปลี่ยนแปลงกฎระเบียบด้านข้อมูลส่วนบุคคล (PDPA)• องค์กรที่ไม่ปรับตัวให้ทันต่อกฎหมายใหม่ เสี่ยงต่อการถูกปรับและเสียชื่อเสียง

• บทเรียน: ต้องมี ทีมกำกับดูแลด้าน Compliance ที่ติดตามกฎหมายและปรับปรุงนโยบายอย่างต่อเนื่อง

กลยุทธ์การบริหารความเสี่ยงดิจิทัลในองค์กร

• เชิงป้องกัน (Preventive Strategy)• ลงทุนในระบบรักษาความปลอดภัย เช่น Firewall, IDS/IPS, Endpoint Security

• จัดอบรมบุคลากรให้มีความรู้ด้าน Cyber Hygiene

• เชิงตรวจจับ (Detective Strategy)• ใช้ระบบ SIEM (Security Information and Event Management) เพื่อตรวจจับเหตุการณ์ผิดปกติ

• ใช้ AI และ Machine Learning วิเคราะห์พฤติกรรมการใช้งานที่ผิดปกติ

• เชิงตอบสนอง (Responsive Strategy)• จัดทำ Incident Response Plan ที่ชัดเจน

• มีทีม CERT (Computer Emergency Response Team) พร้อมปฏิบัติการ

• เชิงฟื้นฟู (Recovery Strategy)• มีระบบ Disaster Recovery Plan (DRP) และ Business Continuity Plan (BCP)

• ทดสอบการฟื้นฟูระบบอย่างสม่ำเสมอ

บทบาทของบุคลากรและวัฒนธรรมองค์กร

• ผู้บริหารระดับสูง (Executives) ⟶ ต้องกำหนดนโยบายและสนับสนุนทรัพยากร

• ฝ่าย IT และ Security ⟶ เป็นผู้ดำเนินการและตรวจสอบระบบ

• พนักงานทุกคน ⟶ ต้องมีความตระหนักรู้และปฏิบัติตามมาตรการความปลอดภัย

• วัฒนธรรมองค์กร ⟶ ต้องสร้างบรรยากาศที่ให้ความสำคัญกับความปลอดภัยไซเบอร์ เช่น การแจ้งเหตุผิดปกติทันที

แนวโน้มอนาคตของการบริหารความเสี่ยงดิจิทัล

• การใช้ AI และ Automation ⟶ ตรวจจับภัยคุกคามแบบ Real-time

• Zero Trust Architecture ⟶ แนวคิดที่ไม่เชื่อถือใครโดยอัตโนมัติ ต้องตรวจสอบทุกการเข้าถึง

• การจัดการความเสี่ยงด้าน Cloud และ Multi-Cloud ⟶ เน้นการควบคุมข้อมูลที่กระจายอยู่หลายแพลตฟอร์ม

• Cyber Insurance ⟶ การทำประกันภัยไซเบอร์เพื่อรองรับความเสียหายที่อาจเกิดขึ้น

ข้อเสนอแนะเชิงกลยุทธ์สำหรับองค์กรไทย

๑. สร้างศูนย์กลางการบริหารความเสี่ยงดิจิทัล (Digital Risk Center)• ทำหน้าที่รวบรวม วิเคราะห์ และตอบสนองต่อภัยคุกคาม

๒. พัฒนาบุคลากรด้าน Cybersecurity อย่างต่อเนื่อง• ผ่านการอบรม การสอบใบรับรอง เช่น CISSP, CISM

๓. บูรณาการความเสี่ยงดิจิทัลเข้ากับกลยุทธ์องค์กร• ไม่ใช่เพียงเรื่อง IT แต่เป็นเรื่องของการบริหารองค์กรโดยรวม

๔. สร้างความร่วมมือกับภาครัฐและเอกชน• แลกเปลี่ยนข้อมูลภัยคุกคามและแนวทางป้องกัน

สรุป

การบริหารความเสี่ยงดิจิทัลเป็นเรื่องที่ต้องดำเนินการอย่างต่อเนื่องและครอบคลุมทุกระดับขององค์กร ตั้งแต่ผู้บริหารจนถึงพนักงานทุกคน การมีระบบป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูที่ครบวงจร จะช่วยให้องค์กรสามารถรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ พร้อมทั้งใช้โอกาสจากเทคโนโลยีใหม่ ๆ เพื่อสร้างความได้เปรียบในการแข่งขัน

๒.๒ ประสบการณ์/ประโยชน์ที่ได้รับ /การประยุกต์ใช้กับหน่วยงาน

☑ต่อตนเองเพื่อเพิ่มพูนความรู้

ได้เรียนรู้การปฏิบัติตนให้เป็นผู้ที่มีความเป็นภาวะผู้นำที่ดี

☑ต่อหน่วยงาน / การนำมาประยุกต์ใช้กับหน่วยงาน

เพื่อนำสิ่งที่ได้อบรมมาช่วยสนับสนุนการทำงานของตนเองร่วมกับผู้อื่นได้

๒.๓ ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้ฯ

-

๒.๔ ข้อคิดเห็นและข้อเสนอแนะ

-

ลงชื่อ.....

(นายณรงค์กรณ์ การินทร์)

ตำแหน่ง เศรษฐกร

ผู้รายงาน

วันที่ ๑๐ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙

ส่วนที่ ๓ ความเห็นของผู้บังคับบัญชา

(✓) ทราบ

.....

.....

.....

ลงชื่อ.....

((นายนันทพล หนองหารพิทักษ์))

ตำแหน่งผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่.....๑๒ กพ ๒๕๖๙.....เดือน.....พ.ศ. .....

Microsoft

สำนักงานคณะกรรมการข้าราชการพลเรือน

ร่วมกับ

บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด

ขอมอบประกาศนียบัตรฉบับนี้ให้เพื่อแสดงว่า

นายณรงค์กรณ์ การินทร์

ได้ผ่านการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์

วิชา AI Skills for All

(รวมระยะเวลาทั้งสิ้น 2 ชั่วโมง)

ให้ไว้ ณ วันที่ 9 กุมภาพันธ์ พ.ศ. 2569

(นายปิยวัฒน์ ศิวรักษ์)

เลขาธิการคณะกรรมการข้าราชการพลเรือน

OCSC

สำเนาถูกต้อง

สำนักงาน ก.พ.
Office of the Civil Service Commission

สำนักงานคณะกรรมการข้าราชการพลเรือน

ขอมอบประกาศนียบัตรฉบับนี้ให้เพื่อแสดงว่า

นายณรงค์กรณ์ การินทร์

ได้ผ่านการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์

วิชา การบริหารความเสี่ยงดิจิทัล (Digital Risk Management)

(รวมระยะเวลาทั้งสิ้น 3 ชั่วโมง)

ให้ไว้ ณ วันที่ 10 กุมภาพันธ์ พ.ศ. 2569

(นายปิยวัฒน์ ศิวรักษ์)
เลขาธิการคณะกรรมการข้าราชการพลเรือน