**สรุปบทเรียน**

**หลักสูตร พัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity Series)**

**ตุลาคม ๒๕๖๘ – มีนาคม ๒๕๖๙**

**การฝึกอบรมการเรียนรู้ผ่านสื่อออนไลน์ ระบบ e-learning ของสถาบันพัฒนาบุคคลากรภาครัฐด้านดิจิทัล**

**โดย นางสาวจิรัฐติกาล สารีบุตร ตำแหน่ง เจ้าพนักงานการเกษตรปฏิบัติงาน**

---

**CyberSecurity** หรือ ความมั่นคงปลอดภัยทางไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึง วิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย, โครงสร้างพื้นฐานทางสารสนเทศ, ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจาก เป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

**พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์**

**Confidentiality** หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุด ข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

• ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น

• เบอร์โทรของพนักงานในบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

**Integrity** หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

• ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร

• ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

**Availability** หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

• ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร

• ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment) ในแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นั้น ผู้ปฏิบัติไม่ใช่เพียงแต่มีมาตรการป้องกัน ภัยคุกคาม แต่ยังต้องมีมุมมองให้เห็นภาพรวมในด้านอื่น ๆ ด้วย โดยเฉพาะเรื่องความเสี่ยงด้านไซเบอร์ และความเสี่ยงของหน่วยงาน

**๑.๑. การประเมินความเสี่ยง (Risk Assessment)** การประเมินความเสี่ยงประกอบไปด้วย ๓ ขั้นตอน ดังนี้

**๑.๑.๑. การระบุความเสี่ยง (Risk Identification)** ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยง จากภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

**๑.๑.๒. การวิเคราะห์ความเสี่ยง (Risk Analysis)** ต้องเข้าใจ และวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

**๑.๑.๓. การประเมินค่าความเสี่ยง (Risk Evaluation)** ต้องประเมินถึงผลของการวิเคราะห์ความเสี่ยงว่าความเสี่ยงที่ระบุไว้นั้น อยู่ในระดับที่ยอมรับได้หรือไม่ หรือมีผลกระทบต่อหน่วยงานมากน้อยเพียงใด โอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการปฏิบัติงาน และการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

**๑.๒. การจัดการความเสี่ยง (Risk Treatment)** ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยง และผลประโยชน์ที่คาดว่าจะได้รับ นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงานเพื่อใช้ติดตาม และทบทวนความเสี่ยง

**๑.๓. การติดตาม และทบทวนความเสี่ยง (Risk Monitoring and Review)** ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

**๑.๔. การรายงานความเสี่ยง (Risk Reporting)** ต้องรายงานระดับความเสี่ยง และผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงาน หรือผู้บริหารที่ได้รับมอบหมาย ทั้งนี้ต้องทบทวนระเบียบวิธีปฏิบัติ และกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

# ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

## คุณ จิรัฐติกาล สารีบุตร

**ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน**

Basic Cybersecurity Series :

หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

**จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 19 กุมภาพันธ์ 2569

**( นางไอรดา เหลืองวิไล )**

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-19T21:49:04.105+07:00

341575c3

# ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

## คุณ จิรัฐติกาล สารีบุตร

**ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน**

หลักสูตรทักษะเอไอระดับพื้นฐาน (AI Basics)

**จำนวนชั่วโมงการเรียนรู้ 2:30 ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 18 กุมภาพันธ์ 2569

**( นางไอรดา เหลืองวิไล )**

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-19T20:07:02.258+07:00
f1cd26ae