ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่

พ.ศ. ๒๕๖๔

เพื่อให้การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีความชัดเจนและเป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๑๙ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๒/๒๕๖๔ เมื่อวันที่ ๔ ตุลาคม ๒๕๖๔ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“รัฐมนตรี” หมายความว่า นายกรัฐมนตรี

ข้อ ๔ พนักงานเจ้าหน้าที่ต้องมีคุณสมบัติ ดังต่อไปนี้

(๑) มีคุณสมบัติอย่างหนึ่งอย่างใด ดังต่อไปนี้

(๑.๑) รับราชการ หรือเคยรับราชการ หรือเป็นบุคคลที่ทำงานเกี่ยวกับการสืบสวนสอบสวนหรือวิเคราะห์ข้อมูล (Data Analyst) ไม่น้อยกว่า ๒ (สอง) ปี ในตำแหน่งที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security) ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ด้านการบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) หรือด้านการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) หรือ

(๑.๒) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรี หรือเทียบเท่าทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ รัฐประศาสนศาสตร์ หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้

ก. สำเร็จการศึกษาตาม (๑.๒) ในระดับปริญญาตรี หรือเทียบเท่าและมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่า ๔ (สี่) ปี

ข. สำเร็จการศึกษาตาม (๑.๒) ในระดับปริญญาโทและมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่า ๓ (สาม) ปี

ค. สำเร็จการศึกษาตาม (๑.๒) ในระดับปริญญาเอกและมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่า ๒ (สอง) ปี

(๒) มีความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) ผ่านการอบรมด้านจริยธรรม สืบสวน สอบสวน ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) การบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) หรือการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) ตามภาคผนวกท้ายประกาศนี้

ข้อ ๕ ในกรณีที่มีเหตุผลความจำเป็น รัฐมนตรีอาจยกเว้นคุณสมบัติตามข้อ ๔ ไม่ว่าทั้งหมดหรือบางส่วนก็ได้ ทั้งนี้ ในการยกเว้นคุณสมบัติดังกล่าว ให้สำนักงานแสดงเหตุผลความจำเป็นเสนอรัฐมนตรีเพื่อใช้ประกอบการพิจารณาแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่เป็นการเฉพาะก็ได้

ทั้งนี้ บุคคลที่ได้รับการยกเว้นคุณสมบัติตามวรรคหนึ่ง ต้องผ่านการอบรมหลักสูตรเร่งรัด (Intensive Courses) ตามภาคผนวกท้ายประกาศนี้ด้วย

ข้อ ๖ พนักงานเจ้าหน้าที่ต้องมีสัญชาติไทยและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) เป็นบุคคลล้มละลาย หรือเคยเป็นบุคคลล้มละลายทุจริต

(๒) เป็นคนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ

(๓) เคยต้องคำพิพากษาถึงที่สุดให้จำคุกไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๔) เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หรือออกจากงานจากหน่วยงานที่เคยปฏิบัติหน้าที่เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง

(๕) เคยถูกถอดถอนออกจากตำแหน่งตามกฎหมาย

(๖) เป็นผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่นหรือผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งซึ่งรับผิดชอบการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ของพรรคการเมือง

ข้อ ๗ การแต่งตั้งบุคคลหนึ่งบุคคลใดเป็นพนักงานเจ้าหน้าที่ ให้แต่งตั้งจากบุคคลซึ่งมีคุณสมบัติตามข้อ ๔ หรือข้อ ๕ และไม่มีลักษณะต้องห้ามตามข้อ ๖

การแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ดำรงตำแหน่งคราวละ ๔ (สี่) ปี

การแต่งตั้งและการพ้นจากตำแหน่งของพนักงานเจ้าหน้าที่ ให้ประกาศในราชกิจจานุเบกษา

ข้อ ๘ พนักงานเจ้าหน้าที่พ้นจากตำแหน่ง เมื่อ

(๑) ตาย

(๒) ลาออก

(๓) มีลักษณะต้องห้ามตามข้อ ๖

(๔) คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีมติให้ออกเพราะบกพร่องหรือทุจริตต่อหน้าที่ มีความประพฤติเสื่อมเสีย

(๕) ครบวาระการดำรงตำแหน่ง

ประกาศ ณ วันที่ ๑๙ พฤศจิกายน พ.ศ. ๒๕๖๔
พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ภาคผนวก

ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่

พ.ศ. ๒๕๖๔

ผู้ที่จะได้รับการแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จะต้องผ่านการอบรมด้านจริยธรรม สืบสวน สอบสวน ที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security) ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ด้านการบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) หรือด้านการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) แล้วแต่กรณี ดังต่อไปนี้

๑. หลักสูตรมาตรฐานสากล (International Standard Courses)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดอบรมให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีทั่วไป (หลักสูตรเต็มเวลาประมาณ ๑ เดือน) ทั้งภาคทฤษฎีและปฏิบัติ

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่เป็นพนักงานเจ้าหน้าที่

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวน เพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร
๑	กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
๒	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๔	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๕	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๖	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยานหลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษา พยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๗	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security)

ลำดับ	เนื้อหาหลักสูตร
๑	General security concepts and Management
๒	Treats, Attacks and Vulnerabilities
๓	Network Components and Protocol
๔	System Architecture and topology
๕	Secure System Design and Secure Application Development
๖	Identity and Access Management
๗	Risk Management
๘	Cryptography

ด้านที่สี่ การบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling)

ลำดับ	เนื้อหาหลักสูตร
๑	Fundamentals of Incident Management
๒	Incident Handling and Response Program Planning
๓	Anti-forensics Techniques
๔	Malware Incident Handling and Response
๕	Email Security Incident Handling and Response
๖	Network Security Incident Handling and Response
๗	Web Security Incident Handling and
๘	Response Cloud Security Incident Handling and Response
๙	Insider Threat-related Incident Handling and Response

ด้านที่ห้า การพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

ลำดับ	เนื้อหาหลักสูตร
๑	Fundamentals of Computer Forensics and Forensic Readiness
๒	Computer Forensics Investigation Process - Obtain Search Warrant - Evaluate and Secure the Scene - Collect the Evidence - Secure the Evidence and Chain of Custody - Acquire Data and Analyze Data - Assess Evidence and Case - Testify as Expert Witness
๓	Defeating Anti-Forensics Techniques
๔	Operating System Forensics
๕	Network Forensics
๖	Web Attack Forensics
๗	Database Forensics
๘	Cloud Forensics
๙	Wireless Forensics
๑๐	Malware Forensics
๑๑	Email-Crime Forensics
๑๒	Mobile Forensics
๑๓	Application Password Cracker
๑๔	Investigative Reports

๒. หลักสูตรเร่งรัด (Intensive Courses) (๕ วัน)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดอบรมให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีพิเศษ ซึ่งได้รับการยกเว้นตามหลักเกณฑ์ในการกำหนดคุณสมบัติเป็นพนักงานทั่วไป ให้สามารถบริหารจัดการภัยคุกคามไซเบอร์เบื้องต้นได้

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่เป็นพนักงานเจ้าหน้าที่

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร
๑	กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
๒	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๔	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๕	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๖	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยานหลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษา พยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๗	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม การบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) และการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

ลำดับ	เนื้อหาหลักสูตร
๑	Fundamentals of Incident Management
๒	Incident Handling and Response Program Planning
๓	Anti-forensics Techniques
๔	Malware Incident Handling and Response
๕	Email Security Incident Handling and Response
๖	Network Security Incident Handling and Response
๗	Web Security Incident Handling and Response
๘	Cloud Security Incident Handling and Response
๙	Insider Threat-related Incident Handling and Response
๑๐	Fundamentals of Computer Forensics
๑๑	Computer Forensics Investigation Process
๑๒	Investigative Reports
