



ประกาศสำนักงานธรรมาภิบาล
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสศค.

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงานเป็นไปตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชบัญญัติกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๔ เพื่อให้การปฏิบัติงานและการบริหารราชการมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล สำนักงานธรรมาภิบาล (สศค.) จึงเห็นควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสศค. เพื่อเป็นเครื่องมือให้กับผู้ให้บริการ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของสศค. โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศสำนักงานธรรมาภิบาล เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสศค.”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓. สศค.ได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสศค. ประกอบด้วยเนื้อหา ๒ ส่วน ดังนี้

๓.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาตามที่กำหนดข้อ ๔

๓.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาตามที่กำหนดข้อ ๕ – ๑๕

ข้อ ๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้มีดังนี้

๔.๑ การจัดทำนโยบายต้องมีผู้บริหาร เจ้าหน้าที่ปฏิบัติงานด้านคอมพิวเตอร์และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบาย

๔.๒ นโยบายต้องจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสศค.

๔.๓ มีการกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวไว้ชัดเจน

๔.๔ มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๔.๕ มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ การควบคุมการเข้าถึงสารสนเทศ และ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๔.๖ มีนโยบายให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๔.๗ มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

๔.๘ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๔.๙ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๔.๑๐ มีนโยบายการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔.๑๑ การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

๔.๑๒ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือจัดฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๕. การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) ประกอบด้วย

๕.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยเป็นสำคัญ

๕.๒ ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจของหน่วยงาน

๕.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ซึ่งได้รับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตประกอบด้วย

๖.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๖.๒ การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากระบบของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๖.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

๖.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๖.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๗. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมย อุปกรณ์ประมวลผลสารสนเทศ ประกอบด้วย

๗.๑ การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๗.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๗.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศเช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากกระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๗.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ

ข้อ ๘. การควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ประกอบด้วย

๘.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๘.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๘.๓ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๘.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๘.๕ การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๘.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๘.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙. การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ประกอบด้วย

๙.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๙.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๙.๓ การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๙.๔ การใช้งานโปรแกรมมอรรดประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทมอรรดประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๙.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๙.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๐. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (application and information access control) ประกอบด้วย

๑๐.๑ การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน และบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑๐.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing) และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking)

๑๐.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๐.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๑. การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

๑๑.๑ บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานต้องทำเรื่องขออนุญาตจากผู้ดูแลระบบ โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศเพื่อขออนุมัติจากผู้อนุญาตหรือผู้ที่ได้รับมอบหมาย

๑๑.๒ หน่วยงานภายนอกที่ทำงานให้กับ สรค. ไม่ว่าจะทำงานอยู่ภายในหน่วยงาน หรือนอกสถานที่จำเป็นต้องลงนามในสัญญา หรือข้อตกลงการไม่เปิดเผยข้อมูลของ สรค. โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๑๑.๓ สำหรับงานลักษณะโครงการ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของ สรค. ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๑๑.๔ ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

ข้อ ๑๒. การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ประกอบด้วย

๑๒.๑ การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๑๒.๒ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๒.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๒.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๑๒.๕ มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๑๒.๖ มีศูนย์คอมพิวเตอร์สำรองซึ่งตั้งอยู่ในสถานที่ที่ปลอดภัยพร้อมระบบคอมพิวเตอร์เพื่อสนับสนุนการปฏิบัติงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน

ข้อ ๑๓. การจัดทำแผนเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน ประกอบด้วย

๑๓.๑ ต้องมีการจัดทำแผนด้านระบบสารสนเทศ

๑๓.๒ ต้องมีการจัดทำแผนด้านระบบคอมพิวเตอร์และระบบเครือข่าย

๑๓.๓ ต้องมีการจัดทำแผนด้านบุคลากรผู้รับผิดชอบ สถานที่ในการปฏิบัติงาน เพื่อเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน

ข้อ ๑๔. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ประกอบด้วย

๑๔.๑ ต้องมีการจัดทำแผนบริหารความเสี่ยงด้านระบบสารสนเทศ

๑๔.๒ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๑๔.๓ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดย ผู้ตรวจสอบภายในของ สรค. (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้สรค. ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๕. สรค.กำหนดความรับผิดชอบ ดังนี้

๑๕.๑ ระดับนโยบายกำหนดให้ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกำหนดให้ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) เป็นผู้รับผิดชอบติดตามกำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ ให้คำปรึกษาแก่เจ้าหน้าที่ระดับปฏิบัติ

๑๕.๒ ระดับปฏิบัติ

๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศผู้รับผิดชอบ ได้แก่

๑.๑) ผู้จัดการส่วนเทคโนโลยีสารสนเทศ

๑.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๓) เจ้าหน้าที่ประจำโครงการของสำนักงาน

๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน ผู้รับผิดชอบ ได้แก่

๒.๑) ผู้จัดการส่วนเทคโนโลยีสารสนเทศ

๒.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๓) ผู้ใช้งาน

๓) การควบคุมการเข้าถึงเครือข่าย ผู้รับผิดชอบ ได้แก่

๓.๑) ผู้จัดการส่วนเทคโนโลยีสารสนเทศ

๓.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๓) ผู้ใช้งาน

๔) การควบคุมการเข้าถึงระบบปฏิบัติการ ผู้รับผิดชอบ ได้แก่

๔.๑) ผู้จัดการส่วนเทคโนโลยีสารสนเทศ

๔.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๕) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศผู้รับผิดชอบ

ได้แก่

๕.๑) ผู้จัดการส่วนเทคโนโลยีสารสนเทศ

๕.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๖) การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศผู้รับผิดชอบ ได้แก่

๖.๑) ผู้จัดการส่วนเทคโนโลยีสารสนเทศ

๖.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๖.๓) เจ้าหน้าที่ประจำโครงการของสำนักงาน

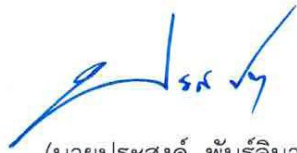
๗) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมผู้รับผิดชอบ ได้แก่

๗.๑) ผู้จัดการส่วนเทคโนโลยีสารสนเทศ

๗.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

- ๘) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่
- ๘.๑) ผู้จัดการส่วนเทคโนโลยีสารสนเทศ
 - ๘.๒) ผู้ที่ได้รับมอบหมาย
- ๙) การจัดทำแผนเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน ผู้รับผิดชอบ ได้แก่
- ๙.๑) ผู้จัดการส่วนเทคโนโลยีสารสนเทศ
 - ๙.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๑๐) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่
- ๑๐.๑) ผู้อำนวยการ
 - ๑๐.๒) ผู้ตรวจสอบภายใน (Internal Auditor) หรือ ผู้ตรวจสอบจากภายนอก (External Auditor)
 - ๑๐.๓) ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๑๑) นโยบายสร้างความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยสารสนเทศ ผู้รับผิดชอบ ได้แก่
- ๑๑.๑) ผู้จัดการส่วนเทคโนโลยีสารสนเทศ
 - ๑๑.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
 - ๑๑.๓) เจ้าหน้าที่ที่ได้รับมอบหมาย

ประกาศ ณ วันที่ ๒๑ มิถุนายน พ.ศ. ๒๕๖๔



(นายประสงค์ พันธลิมา)

ผู้อำนวยการสำนักงานธนานุเคราะห์