ประกาศสำนักงานนโยบายและยุทธศาสตร์การค้า

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของ สำนักงานนโยบายและยุทธศาสตร์การค้า เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความลับ ความถูกต้อง และสภาพพร้อมใช้ของสารสนเทศ รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ สำนักงานนโยบายและยุทธศาสตร์การค้า จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ อย่างเป็นรูปธรรม ดังนั้น โดยความเห็นชอบของคณะกรรมการบริหารจัดการธรรมาภิบาลข้อมูลและคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานนโยบายและยุทธศาสตร์การค้า เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ขอบเขตการบังคับใช้นโยบาย มีผลบังคับใช้กับพื้นที่ที่สามารถเข้าถึงสารสนเทศและเครือข่ายสารสนเทศของสำนักงานนโยบายและยุทธศาสตร์การค้า รวมถึงการเข้าถึงจากระยะไกลและการเชื่อมโยงจากองค์กรภายนอก การอนุญาตและมอบสิทธิในการเข้าถึงทุกระบบ

ข้อ ๔ ในประกาศนี้

“สำนักงาน” หมายความว่า สำนักงานนโยบายและยุทธศาสตร์การค้า

“นโยบาย” หมายความว่า นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

“ผู้ใช้งาน” หมายความว่า ข้าราชการ พนักงานราชการ หรือลูกจ้างของสำนักงานนโยบายและยุทธศาสตร์การค้า ผู้รับจ้างทำของและพนักงานหรือลูกจ้างที่รับทำการงานให้กับสำนักงานนโยบายและยุทธศาสตร์การค้า และผู้ใช้บริการที่ใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานนโยบายและยุทธศาสตร์การค้า

“สารสนเทศ” หมายความว่า ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

“ระบบงาน” หมายความว่า การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้

“ระบบเครือข่าย” หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ของสำนักงานนโยบายและยุทธศาสตร์การค้า

“ความมั่นคงปลอดภัยของสารสนเทศ” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง (Integrity) สภาพพร้อมใช้งาน (Availability) ของสารสนเทศ

"ความลับ" (Confidentiality) หมายความว่า การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะเข้าถึงข้อมูลเหล่านั้นได้

"ความถูกต้อง" (Integrity) หมายความว่า การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลง หรือแก้ไขโดยผู้ไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

"สภาพพร้อมใช้งาน" (Availability) หมายความว่า การรับรองว่าข้อมูล หรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

"การเข้ารหัส" (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

"เจ้าหน้าที่" หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างหรือบุคลากรที่ได้รับมอบหมายหน้าที่จากสำนักงานนโยบายและยุทธศาสตร์การค้า

"ผู้ดูแลระบบ" หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการ ระบบคอมพิวเตอร์ลูกข่าย ระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และระบบสารสนเทศของสำนักงานนโยบายและยุทธศาสตร์การค้า

"ผู้พัฒนาระบบ" หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาและปรับปรุงระบบงานสารสนเทศของสำนักงานนโยบายและยุทธศาสตร์การค้า

"บัญชีผู้ใช้งาน" หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบสารสนเทศระบบปฏิบัติการ ระบบเครือข่าย รวมถึงโปรแกรมประยุกต์และสารสนเทศของสำนักงานนโยบายและยุทธศาสตร์การค้า

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิในการเข้าถึงระบบสารสนเทศ สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับโปรแกรมประยุกต์และสารสนเทศของสำนักงานนโยบายและยุทธศาสตร์การค้า

"ผู้ให้บริการภายนอก" หมายความว่า หน่วยงานภายนอกหรือบุคคลของหน่วยงานภายนอกที่รับจ้างปฏิบัติงานตามความต้องการของสำนักงานนโยบายและยุทธศาสตร์การค้า โดยจะได้รับสิทธิในการเข้าถึงหรือใช้งานระบบ ซึ่งเป็นไปตามที่สำนักงานนโยบายและยุทธศาสตร์การค้ากำหนดหน้าที่และต้องรับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากการปฏิบัติงาน

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

ข้อ ๕ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศจัดแบ่งสาระสำคัญออกเป็น ๑๔ หมวด มีดังนี้

๕.๑) นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

มีคณะกรรมการบริหารจัดการธรรมาภิบาลข้อมูลและคุ้มครองข้อมูลส่วนบุคคลทำหน้าที่กำกับดูแลนโยบาย และรับผิดชอบในการตรวจสอบการดำเนินงานตามนโยบายอย่างสม่ำเสมอและทันเหตุการณ์ โดยให้มีการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์เปลี่ยนแปลงที่สำคัญเพื่อความเหมาะสมและปกป้องผลประโยชน์ของสำนักงาน

๕.๒) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

ภาระความรับผิดชอบสำหรับผู้บริหารระดับสูงและผู้บริหารของทุกกองภายใต้สังกัดสำนักงานต้องกำกับดูแลให้บุคลากรได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศและปฏิบัติตามนโยบายและแนวปฏิบัติของสำนักงาน

ภาระความรับผิดชอบสำหรับผู้ใช้งานทุกคนต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของสำนักงาน และต้องรายงานต่อผู้บังคับบัญชา หากพบปัญหาหรือช่องโหว่ที่เกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศ ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของสำนักงาน ใช้งานตามสิทธิที่ได้รับอนุญาต และต้องรับผิดชอบในการไม่เปิดเผยความลับของสำนักงานโดยมิได้รับอนุญาต

ภาระความรับผิดชอบผู้พัฒนาและผู้ดูแลระบบที่เกี่ยวกับสารสนเทศทุกระบบของสำนักงาน ต้องตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ โดยมาตรการความมั่นคงปลอดภัยของระบบต้องผ่านการพิจารณาและได้รับคำแนะนำจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และต้องมีภาระงานในเรื่องความมั่นคงปลอดภัยของสารสนเทศ ทั้งด้านเทคนิค การตรวจสอบ การเฝ้าระวัง การประเมินและรายงานความเสี่ยงต่อสำนักงาน

มีการรักษาความมั่นคงปลอดภัยของการปฏิบัติงานด้วยอุปกรณ์สื่อสารพกพาและการปฏิบัติงานระยะไกล โดยต้องมีการกำหนดมาตรการบริหารจัดการและแนวปฏิบัติของสำนักงาน

๕.๓) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

บุคลากรของสำนักงาน หรือผู้ได้รับจ้างต้องปฏิบัติตามนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยของสำนักงาน โดยต้องมีการให้ความรู้และฝึกอบรมด้านความมั่นคงปลอดภัยแก่บุคลากร ในกรณีที่กระทำความผิดต้องมีกระบวนการสอบสวนและลงโทษตามระเบียบของสำนักงาน

เมื่อสิ้นสุดการเป็นบุคลากรหรือมีการโยกย้ายสับเปลี่ยนหน้าที่ความรับผิดชอบหรือการเปลี่ยนสัญญาการจ้างงานต้องมีการคืนทรัพย์สินของสำนักงาน และถอดถอนหรือมอบสิทธิที่เหมาะสมในการเข้าถึงระบบสารสนเทศของบุคลากรนั้น

๕.๔) การจัดหมวดหมู่และการควบคุมสินทรัพย์ขององค์กร (Asset Management)

มีกระบวนการในการจัดหมวดหมู่ของสินทรัพย์สารสนเทศตามระดับชั้นความลับ ทั้งนี้เพื่อให้สามารถกำหนดวิธีการในการป้องกันได้อย่างเหมาะสม รวมทั้งจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการสินทรัพย์สารสนเทศตามหมวดหมู่ที่กำหนดไว้

มีการป้องกันในการนำส่งหรือการขนย้าย หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูลอย่างมั่นคงปลอดภัยเมื่อหมดความต้องการในการใช้งาน

๕.๕) การควบคุมการเข้าถึง (Access Control)

มีการกำหนดมาตรการและแนวปฏิบัติอย่างเป็นระบบเพื่อใช้ในการจัดการสิทธิในการเข้าใช้ระบบสารสนเทศ รวมถึงการทบทวนสิทธิการเข้าถึงของผู้ใช้ โดยกำหนดรหัสบัญชีผู้ใช้งานที่มีคุณภาพยากต่อการคาดเดา และไม่ใช้คำศัพท์ที่ปรากฏในพจนานุกรม มีความยาวไม่น้อยกว่า ๘ ตัวอักขระ โดยต้องประกอบด้วยลักษณะอย่างน้อย ๓ ใน ๔ ดังนี้ (กรณีระบบรองรับ)

ตัวอักษรพิมพ์ใหญ่ (A-Z)

ตัวอักษรพิมพ์เล็ก (a-z)

ตัวเลข (๐-๙)

ตัวอักขระพิเศษ (สัญลักษณ์อื่นใด) เช่น ! @ # $ % & * ( ) [ ] { }

การเข้าถึงระบบภายในสำนักงานหรือการเชื่อมต่อจากภายนอกต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิตามขั้นตอนอย่างมีประสิทธิภาพ โดยระบบต้องยอมให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตผ่านเข้าสู่เครือข่าย และใช้บริการได้ตามสิทธิที่กำหนดให้เท่านั้น

๕.๖) การเข้ารหัสข้อมูล (Cryptography)

การเข้ารหัสมีการพิจารณาถึงการควบคุมการเข้ารหัส ผลของการประเมินความเสี่ยงเพื่อระบุระดับการป้องกัน

การบริหารจัดการการเข้ารหัส (key management) และมาตรฐานอื่นๆ ที่มีประสิทธิภาพ การใช้งาน การป้องกัน และอายุการใช้งานของกุญแจ ต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ

๕.๗) ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

มีระบบป้องกันการเสียหายและการควบคุมการเข้าออกในการรักษาความมั่นคงปลอดภัย เช่น ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ของสำนักงานต้องมีระบบรักษาความปลอดภัยและมีการควบคุมการเข้าถึงอย่างเข้มงวด

มีผู้รับผิดชอบโดยตรง และผู้รับผิดชอบเท่านั้นที่ได้รับสิทธิในการเข้าถึงอุปกรณ์ โดยมีระบบสำหรับจัดเก็บข้อมูลการเข้าถึงเพื่อใช้เป็นหลักฐานในการตรวจสอบ

อุปกรณ์สำคัญที่ถูกจัดเก็บในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ ต้องมีการจัดวางอย่างถูกต้อง มีป้ายเพื่อบ่งบอกถึงตำแหน่งในการเชื่อมต่ออุปกรณ์ และมีการกำหนดแผนการบำรุงรักษาอุปกรณ์อย่างชัดเจนและต่อเนื่อง

การนำอุปกรณ์ทุกชิ้นออกนอกหน่วยงาน ต้องปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยของสำนักงานและต้องจัดให้มีการตรวจสอบอย่างเคร่งครัด

๕.๘) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

มีการเปลี่ยนแปลงข้อมูล หรือการปรับเปลี่ยนเวอร์ชันของระบบ หรือโปรแกรมภายในต้องมีการบันทึกการจัดการกับปัญหาที่อาจเกิดขึ้นจากการเปลี่ยนแปลงนั้นได้ และสามารถกลับคืนสู่สถานะเดิมได้หากแก้ไขไม่สำเร็จ มีการบริหารขีดความสามารถของโครงสร้างพื้นฐานและระบบสารสนเทศ

มีการติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดี รวมทั้งโปรแกรมเพื่อป้องกันช่องโหว่ของระบบปฏิบัติการสำหรับระบบงานหรืออุปกรณ์หลักของสำนักงาน และกำหนดให้มีระเบียบและขั้นตอนวิธีปฏิบัติที่เหมาะสม และสนับสนุนให้หน่วยงานภายในที่มีการใช้งานผ่านระบบเครือข่ายของสำนักงานได้ยึดถือและปฏิบัติตาม

มีการสำรองข้อมูลที่สำคัญโดยต้องกำหนดรูปแบบและวิธีปฏิบัติ รวมทั้งแผนการสำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของหน่วยงานภายในสำนักงาน เพื่อป้องกันการสูญหายอันจะเกิดขึ้นจากภาวะคุกคามหรือจากการเกิดภัยพิบัติโดยต้องกำหนดให้มีผู้รับผิดชอบในการสำรองและกู้คืนข้อมูลตามรูปแบบและแผนการดำเนินการที่กำหนดไว้และจัดให้มีการทดสอบการกู้คืนตามรอบระยะเวลา

มีการเฝ้าระวังระบบที่มีความสำคัญเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ

ต้องให้มีการจัดเก็บข้อมูลจราจรบนเครือข่ายที่สอดคล้องกับข้อกำหนดตามพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์และต้องกำหนดขั้นตอนวิธีปฏิบัติในการตั้งเวลาของระบบคอมพิวเตอร์กลางให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องที่ช่วยในการตรวจสอบช่วงเวลาในกรณีเกิดเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ของสำนักงาน

มีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบรารี่ ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานโดยก่อนการติดตั้งในระบบต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดีไม่ก่อให้เกิดปัญหากับระบบ

มีปรับปรุงช่องโหว่ซอฟต์แวร์ในระบบต่างๆ โดยการประเมินความเสี่ยงของช่องโหว่เหล่านั้นตามระยะเวลาที่กำหนดอย่างน้อยปีละ ๑ ครั้ง

๕.๙) ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security)

มีการติดตามสภาพการใช้งานและวิเคราะห์ขีดความสามารถตรวจจับทรัพยากรสารสนเทศตามหลักเกณฑ์ที่สำนักงานประกาศใช้ และทดสอบการทำงานของทรัพยากรสารสนเทศนั้นเพื่อให้สามารถใช้งานได้ตามข้อกำหนด และมีการบำรุงรักษาระบบให้ใช้งานได้ดีอยู่เสมอ

กรณีการถ่ายโอนหรือแลกเปลี่ยนสารสนเทศ จากหน่วยงานภายนอกต้องมีการตรวจสอบและบันทึกการปฏิบัติงาน มีการเฝ้าระวังและจัดทำรายงานผลการดำเนินงานที่เกิดขึ้นอย่างสม่เสมอ รวมถึงกำหนดแนวทางการบริหารจัดการในกรณีที่มีการเปลี่ยนแปลงซึ่งอาจจะมีผลกระทบต่อสำนักงาน

๕.๑๐) การจัดหา พัฒนา และการบำรุงรักษาระบบ (Systems Acquisition, Development and Maintenance)

การพัฒนาระบบสารสนเทศต้องมีความมั่นคงปลอดภัยมีการออกแบบและดำเนินการตลอดวงจรชีวิตของการพัฒนา โดยการกำหนดขั้นตอนวิธีปฏิบัติอย่างเป็นทางการ เพื่อใช้ควบคุมการเปลี่ยนแปลงหรือแก้ไข และต้องมีการตรวจสอบการทำงานหลังการเปลี่ยนแปลงนั้นๆ

มีมาตรการควบคุมการใช้ข้อมูลสำหรับการทดสอบระบบและการป้องกันข้อมูลรั่วไหล เมื่อใช้งานเสร็จต้องลบข้อมูลจริงออกจากระบบทดสอบทันที

๕.๑๑) ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

มีการตรวจสอบและบันทึกการปฏิบัติงานการรับบริการจากหน่วยงานภายนอก รวมถึงการเฝ้าระวังและจัดทำรายงานผลการดำเนินงานที่เกิดขึ้นอย่างสม่ำเสมอรวมถึงกำหนดแนวทางการบริหารจัดการในกรณีที่มีการเปลี่ยนแปลงซึ่งอาจจะมีผลกระทบต่อสำนักงาน

มีการติดตามสภาพการใช้งานและวิเคราะห์ขีดความสามารถของการให้บริการโดยผู้ให้บริการภายนอกโดยตรวจรับทรัพยากรสารสนเทศและทดสอบการทำงานของทรัพยากรสารสนเทศนั้นเพื่อให้สามารถใช้งานได้ตามข้อกำหนด

๕.๑๒) การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

การแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ จุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศให้รับทราบโดยเป็นวิธีที่สอดคล้องและได้ผลสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๕.๑๓) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องในการดำเนินงานขององค์กร (Information Security Aspects of Business Continuity Management)

มีการเตรียมความพร้อมด้านความมั่นคงปลอดภัยสารสนเทศและด้านความต่อเนื่องในสถานการณ์ที่อาจส่งผลต่อความต่อเนื่องในการดำเนินงานขององค์กร เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติ จัดทำเป็นลายลักษณ์อักษร โดยซักซ้อมแผนเตรียมความพร้อมด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง และจัดเตรียมอุปกรณ์ให้พร้อมสำหรับใช้ประมวลผลสารสนเทศอย่างเพียงพอเพื่อให้ตรงตามความต้องการที่สำนักงานกำหนดไว้

๕.๑๔) การปฏิบัติตามข้อกำหนด (Compliance)

มีการศึกษา กฎ ระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เพื่อให้บุคลากรได้รับทราบทำความเข้าใจ และปฏิบัติตามได้อย่างเคร่งครัด

มีการทบทวน มาตรการ นโยบาย กระบวนการ ขั้นตอนปฏิบัติเพื่อความมั่นคงปลอดภัยสารสนเทศ อย่างอิสระตามรอบระยะเวลาที่กำหนดไว้ โดยเทียบกับนโยบายมาตรฐาน ด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง

ประกาศ ณ วันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๕

(นายรณรงค์ พูลพิพัฒน์)
ผู้อำนวยการสำนักงานนโยบายและยุทธศาสตร์การค้า