ศสช
2(23)

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กพช. โทร. ๐-๒๖๑๘-๒๓๒๓ ต่อ ๑๐๑๒
ที่ นร ๐๒๐๖.๐๓/ ๗๖๒ **วันที่** ๒๒ กันยายน ๒๕๕๔
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศกรมประชาสัมพันธ์

เรียน อปส. ผ่าน รปส. (นางเตือนใจ สินธุวณิก)

ตามตัวชี้วัดที่ ๑๑ ระดับความสำเร็จของการพัฒนาคุณภาพ การบริหารจัดการภาครัฐ ประจำปีงบประมาณ พ.ศ. ๒๕๕๔ หมวด ๔ การวัด การวิเคราะห์ และการจัดการความรู้ ในรหัส IT๖ ได้กำหนดให้ส่วนราชการต้องมีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยองค์การจะต้องแสดงนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือ CEO เป็นผู้อนุมัติ ซึ่งมี ศสช.เป็นหน่วยงานรับผิดชอบประเด็นการตรวจตามตัวชี้วัดดังกล่าว นั้น

ในการนี้ ศสช. ได้ดำเนินการจัดทำเอกสารนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมประชาสัมพันธ์ ประจำปีงบประมาณ พ.ศ. ๒๕๕๔ เสร็จเรียบร้อยแล้ว (เอกสารแนบ ๑ และ ๒) ซึ่งประกอบด้วย

๑. ระเบียบปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมประชาสัมพันธ์
๒. ประกาศกรมประชาสัมพันธ์ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

จึงเรียนมาเพื่อโปรดพิจารณาลงนามอนุมัติให้ความเห็นชอบและลงนามในประกาศ หากลงนามเรียบร้อยแล้ว ศสช. จะดำเนินการเวียนแจ้งให้บุคลากรใน กปส. ถือปฏิบัติต่อไป

(นายสมโภชน์ วิสุทธิแพทย์)
อสช.

- อนุมัติ
- ลงนามแล้ว

(นายกฤษณพร เสริมพานิช)
อปส.
23 ก.ย. 2554

(นางเตือนใจ สินธุวณิก)
รปส.
22 ก.ย. 2554

รปส. (นางเตือนใจ สินธุวณิก) 1022

(นายกฤษณพร เสริมพานิช) 23 ก.ย. 2554

เรียน ผอ.สำนัก/กอง และหัวหน้าหน่วยงานต่างๆ

ศสช. ขอเวียนแจ้งระเบียบตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ กปส. พ.ศ. ๒๕๕๔ และประกาศกรมประชาสัมพันธ์ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้ทุกหน่วยงานถือปฏิบัติอย่างเคร่งครัดต่อไป โดยสามารถดาว์นโหลดข้อมูลได้จากอินทราเน็ต สื่อเผยแพร่ ศสช.

จึงเรียนมาเพื่อโปรดทราบ และเวียนแจ้งให้ข้าราชการ ลูกจ้างในสังกัดทราบและถือปฏิบัติต่อไป

(นายสมโภชน์ วิสุทธิแพทย์)

อสช.

๒๙ ก.ค. ๕๔

ประกาศกรมประชาสัมพันธ์

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

---

๑. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กรมประชาสัมพันธ์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อองค์การ ซึ่งมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตุประสงค์ ดังต่อไปนี้

๑.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์การ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ เพื่อให้การกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศมีความสอดคล้องกับมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

๑.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์การได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธิปฏิบัติ ให้บุคลากรภายในและบุคคลภายนอกตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวน ตรวจสอบและประเมินนโยบายอย่างน้อยปีละ ๑ ครั้ง

๒. องค์ประกอบของนโยบาย

๒.๑ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and environment security) มีการกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับ ผู้ใช้ และ หน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๒.๒ การควบคุมการเข้าออกห้องศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ (Computer Center Entry Control) มีการกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์การ โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์

๒.๓ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control) มีการกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ขององค์การ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การได้อย่างถูกต้อง

๒.๔ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third party access control) มีการกำหนดและควบคุมการใช้บริการจากหน่วยงานภายนอกที่อาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ ให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือกควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบ การใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

๒.๕ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer) มีการกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้จะต้องทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์การ ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

๒.๖ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Use of Notebook Computer) มีการกำหนดมาตรฐานการใช้งานเพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกองค์การ เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์การให้เกิดความปลอดภัย ผู้ใช้จึงต้องรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยนง ในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

๒.๗ การใช้งานอินเทอร์เน็ต (Use of the Internet) เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์การ ถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒.๘ การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail) มีการกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์การซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒.๙ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) มีการกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์การ โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์การซึ่งบุคลากรภายในและบุคคลภายนอกองค์การจะต้องปฏิบัติตามอย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๓ กันยายน พ.ศ. ๒๕๕๔

(นายกฤษณพร เสริมพานิช)
อธิบดีกรมประชาสัมพันธ์