นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์

กรมกิจการเด็กและเยาวชน (ดย.) ปี 2566

1. หลักการ

กรมกิจการเด็กและเยาวชน ได้มีข้อกำหนดสำหรับการใช้งาน การดูแลรักษา และการป้องกันให้เหมาะสมกับลักษณะการดำเนินกิจการ ซึ่งการดูแลรักษาและการป้องกันมุ่งหมายไปในทางความมั่นคงปลอดภัย โดยมีหลักการสำคัญคือการธำรงไว้ซึ่ง การรักษาความลับของข้อมูล ความถูกต้องครบถ้วน และความสมบูรณ์พร้อมใช้ ดังนี้

1.1 การรักษาความลับ (Confidentiality) หมายถึง การป้องกันไม่ให้สินทรัพย์สามารถถูกเข้าถึงได้จากผู้ไม่มีสิทธิ โดยการเข้าถึงยังรวมถึงการถูกเปิดเผยและการจำแนกแจกจ่ายซึ่งสินทรัพย์นั้นด้วย ดังนั้น ในการรักษาความลับจำเป็นจะต้องมีการควบคุมทั้ง ทางกายภาพและทางเทคนิค โดยผู้ที่ไม่มีสิทธิจะต้องไม่สามารถเข้าถึงสินทรัพย์นั้นได้และสินทรัพย์จำเป็นจะต้องมีการจำแนก และกำหนดระดับความต้องการในการป้องกันไว้อย่างชัดเจน เพื่อให้ผู้ที่ถือครองสินทรัพย์ปฏิบัติได้ถูกต้องเหมาะสมกับระดับความต้องการนั้น

2.2 ความถูกต้องครบถ้วน (Integrity) หมายถึง การป้องกันไม่ให้สินทรัพย์ถูกเปลี่ยนแปลงแก้ไขทั้งที่มีเจตนาหรือไม่ก็ตามจากผู้ไม่มีสิทธิที่จะแก้ไขสินทรัพย์เหล่านั้น ดังนั้นการควบคุมและป้องกันจึงต้องประกอบด้วยการกำหนดสิทธิในการแก้ไข กำหนดสิทธิในการเข้าถึง และจำเป็นต้องอาศัยการตรวจสอบทั้งจากการทำรายการบัญชีสินทรัพย์และทางเทคนิคประกอบด้วย

2.3 ความสมบูรณ์พร้อมใช้ (Availability) หมายถึง การที่ผู้มีสิทธิสามารถเข้าใช้งานสินทรัพย์นั้นได้เมื่อยามต้องการใช้งาน ซึ่งมีทั้งในทางกายภาพและทางเทคโนโลยี ได้แก่ การให้บริการระบบจดหมายอิเล็กทรอนิกส์ที่จำเป็นจะต้องให้บริการตลอดเวลา ดังนั้น เมื่อผู้ใช้ต้องการจะรับหรือส่ง ระบบจำเป็นที่จะต้องสามารถให้บริการได้ตลอดเวลา เป็นต้น

2. นโยบายการปฏิบัติ

2.1 กรมกิจการเด็กและเยาวชน จัดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยการประเมินความเสี่ยงดังกล่าวพิจารณาถึงบริบทภายใน (Internal Context) บริบทภายนอก (External Context) ผู้ที่มีส่วนได้ส่วนเสีย (Interested Party) วิสัยทัศน์ พันธกิจ การเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ

2.2 กรมกิจการเด็กและเยาวชน มีการกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้และความเสี่ยงที่ยอมรับไม่ได้ เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงที่เกิดขึ้นในการประเมินความเสี่ยงที่เกิดขึ้น

2.3 กรมกิจการเด็กและเยาวชน จัดให้มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

2.4 กรมกิจการเด็กและเยาวชน มีการกำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อรับมือตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

2.5 กรมกิจการเด็กและเยาวชน มีการประเมินผลสัมฤทธิ์ของนโยบายที่ประกาศใช้ เพื่อนำมาปรับปรุงนโยบาย แผนกลยุทธ์ให้สอดคล้องกับภัยคุกคามในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต

2.6 กรมกิจการเด็กและเยาวชน จัดให้มีทรัพยากร ด้านงบประมาณ ทรัพยากรบุคคล การบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการด้านความมั่นคงปลอดภัยของสำนักงาน

3. โครงสร้างทางด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับกรมกิจการเด็กและเยาวชน

กรมกิจการเด็กและเยาวชน กำหนดมาตรการควบคุม กำกับและติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับส่วนงานต่าง ๆ ภายในกรม และเพื่อเป็นแนวทางการควบคุมอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอกให้เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ (Information and Cyber Security Policy) แบ่งเป็น 2 ส่วน คือ

1. การจัดโครงสร้างภายในองค์กร (Internal Organization)

กรมกิจการเด็กและเยาวชน มีกำหนดบทบาทหน้าที่ ความรับผิดชอบในการใช้ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม และมีความมั่นคงปลอดภัยทางไซเบอร์

2. นโยบายการควบคุมอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอก (Computing Device and Teleworking Policy)

เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับอุปกรณ์สารสนเทศและการปฏิบัติงานจากภายนอกกรมกิจการเด็กและเยาวชน

4. นโยบายความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล

กรมกิจการเด็กและเยาวชน มีกระบวนการในการคัดเลือกบุคลากร การฝึกอบรมและการควบคุมการปฏิบัติงานของบุคลากรในกรมอย่างเหมาะสมตลอดระยะเวลาการจ้างงาน และเพื่อให้เข้าใจถึงหน้าที่ความรับผิดชอบของตนในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศของกรม โดยคำนึงถึงก่อนการจ้างงาน , ระหว่างการจ้างงาน , การเปลี่ยนตำแหน่ง หรือการสิ้นสุดการจ้างงาน

5. การบริหารจัดการสินทรัพย์

กรมกิจการเด็กและเยาวชน มีการระบุสินทรัพย์ที่สำคัญของกรมและกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์จากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจเกิดขึ้นอย่างเหมาะสม โดยประกอบด้วย

1. นโยบายการบริหารจัดการสินทรัพย์ (Asset Management Policy)

กรมกิจการเด็กและเยาวชน มีการระบุสินทรัพย์ที่สำคัญของสำนักงานและกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์อย่างเหมาะสม

2. นโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy)

เพื่อให้สารสนเทศได้รับการปกป้องที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้น ๆ ที่มีต่อกรมกิจการเด็กและเยาวชน

3. นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล

เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายสินทรัพย์สารสนเทศโดยไม่ได้รับอนุญาต

6. การควบคุมการเข้าถึงระบบสารสนเทศ

กรมกิจการเด็กและเยาวชน มีนโยบายควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์สารสนเทศ สร้างความมั่นคงปลอดภัยให้กับการดำเนินงานของกรม ประกอบด้วย

1. นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

กรมกิจการเด็กและเยาวชน กำหนดกฎเกณฑ์และควบคุมการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศของสำนักงาน, ปกป้องข้อมูลและสารสนเทศจากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

2. นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control Policy)

เพื่อรักษาความมั่นคงปลอดภัยและป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

3. นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control Policy)

กรมกิจการเด็กและเยาวชน กำหนดกฎเกณฑ์ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศของกรมจากผู้ที่ไม่ได้รับอนุญาต

7. การเข้ารหัสลับของข้อมูล

กรมกิจการเด็กและเยาวชน มีนโยบายกำหนดแนวทางการเข้ารหัสลับข้อมูลและทำให้ระบบสารสนเทศรักษาไว้ซึ่งความลับของข้อมูล การพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและ เหมาะสม

8. นโยบายความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

กรมกิจการเด็กและเยาวชน กำหนดเป็นมาตรการควบคุมและป้องกัน และเป็นมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ พื้นที่ใช้งานระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบสารสนเทศ ข้อมูลซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับกับผู้ใช้งานและผู้ให้บริการภายนอก