คู่มือแนวทางการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย

กองยุทธศาสตร์และแผนงาน
กรมกิจการสตรีและสถาบันครอบครัว

คำนำ

ปัจจุบัน เทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology: ICT) มีบทบาทสำคัญอย่างยิ่งต่อการดำเนินงานของภาครัฐ โดยเฉพาะด้านการให้บริการประชาชน การจัดเก็บข้อมูล การแลกเปลี่ยนสารสนเทศ และการบริหารจัดการภารกิจภายในองค์กร กรมกิจการสตรีและสถาบันครอบครัว (สค.) ได้นำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการปฏิบัติงานในทุกระดับ เพื่อเพิ่มประสิทธิภาพ ความรวดเร็ว ความโปร่งใส และความน่าเชื่อถือในการให้บริการแก่ประชาชนและผู้มีส่วนได้ส่วนเสีย

อย่างไรก็ตาม การนำเทคโนโลยีสารสนเทศมาใช้ย่อมมาพร้อมกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risks) ทั้งจากภัยคุกคามทางไซเบอร์ (Cyber Threats) เช่น มัลแวร์ การโจมตีแบบฟิชชิง การเข้าถึงระบบโดยไม่ได้รับอนุญาต ตลอดจนความผิดพลาดจากการใช้งานของบุคลากร เช่น การเปิดเผยข้อมูลโดยไม่ตั้งใจ การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการไม่ปฏิบัติตามมาตรการควบคุมที่กำหนดไว้ เหตุการณ์ดังกล่าวอาจส่งผลกระทบต่อความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล รวมถึงสร้างความเสียหายต่อภาพลักษณ์และความน่าเชื่อถือของหน่วยงาน

เพื่อให้เกิดการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพและเป็นระบบ ตลอดจนสร้างความตระหนักรู้ให้กับบุคลากรทุกระดับ กรมกิจการสตรีและสถาบันครอบครัวจึงได้จัดทำ “คู่มือแนวทางการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย” ขึ้น เพื่อใช้เป็นเอกสารอ้างอิงและแนวปฏิบัติในการใช้งานระบบสารสนเทศ อุปกรณ์คอมพิวเตอร์ เครือข่าย และข้อมูลของหน่วยงานอย่างถูกต้อง ปลอดภัย และเป็นไปตามกรอบนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน ตลอดจนกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง ซึ่งการปฏิบัติตามคู่มือนี้จะช่วยลดความเสี่ยงจากภัยคุกคามไซเบอร์ ป้องกันการรั่วไหลของข้อมูลสำคัญและข้อมูลส่วนบุคคล สนับสนุนให้การดำเนินงานของหน่วยงานเป็นไปอย่างต่อเนื่อง ไม่หยุดชะงัก และเสริมสร้างภาพลักษณ์ขององค์กรที่โปร่งใสและน่าเชื่อถือ อันจะนำไปสู่การสร้าง “วัฒนธรรมความมั่นคงปลอดภัยสารสนเทศ” ให้เกิดขึ้นอย่างยั่งยืนภายในหน่วยงาน

กองยุทธศาสตร์และแผนงาน

กรมกิจการสตรีและสถาบันครอบครัว

สารบัญ

หน้า

คำนำ

คู่มือแนวทางการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย 1

1. วัตถุประสงค์ 1

2. ขอบเขต 1

3. บทบาทของผู้ใช้งาน 2

4. แนวทางการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย 3

4.1 การจัดการรหัสผ่าน (Password Management) 3

4.2 การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control) 4

4.3 การใช้อีเมลและอินเทอร์เน็ต (Email and Internet Usage) 5

4.4 การปกป้องข้อมูลและอุปกรณ์ (Data and Device Protection) 6

4.5 การตอบสนองเหตุผิดปกติ (Incident Response) 6

5. ข้อห้ามสำคัญ 7

6. ข้อแนะนำการปฏิบัติ 7

7.ช่องทางติดต่อ IT 8

8. บทสรุป 9

คู่มือแนวทางการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย

1. วัตถุประสงค์

เพื่อกำหนดแนวทางที่ชัดเจนในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการสตรีและสถาบันครอบครัว (สค.) อย่างถูกต้องและปลอดภัย โดยมุ่งเน้นให้บุคลากรทุกระดับ ทั้งข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ผู้บริหาร เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ ผู้พัฒนาระบบ รวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบของหน่วยงาน มีความรู้ ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ

นอกจากนี้ ยังมีวัตถุประสงค์เพื่อส่งเสริมให้บุคลากรสามารถปฏิบัติตาม นโยบาย มาตรการ และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ของหน่วยงานได้อย่างถูกต้อง เป็นระบบ และสอดคล้องกับกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง อันจะช่วยลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) และการละเมิดข้อมูล ทั้งข้อมูลภายใน ข้อมูลสำคัญของราชการ และข้อมูลส่วนบุคคล

การดำเนินการตามวัตถุประสงค์นี้ มีเป้าหมายเพื่อเพิ่มประสิทธิภาพและความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน สร้างความตระหนักรู้ (Awareness) และความรับผิดชอบร่วมกันของบุคลากรทุกระดับ ลดโอกาสในการเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจส่งผลกระทบต่อภารกิจหลักของกรมฯ และส่งเสริมให้เกิดวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Culture) อย่างยั่งยืน

2. ขอบเขต

คู่มือนี้กำหนดขอบเขตการใช้งานและการบังคับใช้สำหรับบุคลากรทุกระดับของกรมกิจการสตรีและสถาบันครอบครัว (สค.) ได้แก่ ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ผู้บริหาร เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ ผู้พัฒนาระบบ ตลอดจนบุคคลภายนอกหรือหน่วยงานที่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศของกรมฯ ไม่ว่าจะเป็นการใช้งานภายในสถานที่ราชการหรือผ่านการเชื่อมต่อจากภายนอก

ขอบเขตของคู่มือนี้ครอบคลุมถึงการใช้งานระบบและอุปกรณ์เทคโนโลยีสารสนเทศทุกประเภทที่อยู่ภายใต้ความรับผิดชอบของกรมฯ ดังต่อไปนี้

- เครื่องคอมพิวเตอร์ตั้งโต๊ะ (Desktop Computer) และเครื่องคอมพิวเตอร์แบบพกพา (Notebook / Laptop) ที่ใช้ในการปฏิบัติงานราชการ

- ระบบเครือข่ายภายใน (Intranet) และเครือข่ายภายนอก (Internet) รวมถึงการเชื่อมต่อผ่านระบบเครือข่ายไร้สาย (Wi-Fi) ของหน่วยงาน

- ระบบสารสนเทศ (Information Systems) และระบบฐานข้อมูล (Databases) ที่พัฒนาและดูแลโดยกรมฯ หรือหน่วยงานที่ได้รับมอบหมาย

- ระบบอีเมลราชการ ระบบรับ–ส่งข้อมูลอิเล็กทรอนิกส์ ระบบอินเทอร์เน็ต และช่องทางสื่อสารออนไลน์ เช่น Social Network หรือระบบประชุมทางไกล (Video Conference) ที่ใช้ในการดำเนินงานของหน่วยงาน

- อุปกรณ์เคลื่อนที่ (Mobile Devices) เช่น โทรศัพท์มือถือ แท็บเล็ต หรืออุปกรณ์อัจฉริยะอื่น ๆ ที่เชื่อมต่อกับระบบของหน่วยงาน ไม่ว่าจะเป็นของราชการหรือของบุคลากรที่ได้รับอนุญาตให้ใช้งานเพื่อวัตถุประสงค์ในการปฏิบัติงาน

นอกจากนี้ คู่มือนี้ยังครอบคลุมถึงการปฏิบัติที่เกี่ยวข้องกับการเข้าถึง การใช้งาน การเก็บรักษา และการแลกเปลี่ยนข้อมูลสารสนเทศ ทั้งในรูปแบบอิเล็กทรอนิกส์และสื่อบันทึกข้อมูลทุกประเภท เพื่อให้เกิดมาตรฐานและแนวทางเดียวกันในการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

3. บทบาทของผู้ใช้งาน

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการสตรีและสถาบันครอบครัว (สค.) ทุกระดับ มีบทบาทสำคัญในการสนับสนุนให้การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงานเป็นไปอย่างมีประสิทธิภาพและยั่งยืน การปฏิบัติตามบทบาทและความรับผิดชอบที่กำหนดไว้อย่างเคร่งครัด จะช่วยลดความเสี่ยงจากภัยคุกคามไซเบอร์ ป้องกันความเสียหายที่อาจเกิดขึ้นกับข้อมูลและระบบของหน่วยงาน และส่งเสริมให้เกิดวัฒนธรรมความมั่นคงปลอดภัยสารสนเทศร่วมกันภายในหน่วยงาน

ผู้ใช้งานมีหน้าที่และความรับผิดชอบ ดังนี้

(1) ปฏิบัติตามนโยบาย มาตรการ และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของกรมฯ อย่างเคร่งครัด รวมถึงข้อกำหนด กฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง เพื่อให้การใช้งานระบบและข้อมูลของหน่วยงานเป็นไปตามกรอบที่กำหนด

(2) ใช้งานระบบเทคโนโลยีสารสนเทศเพื่อวัตถุประสงค์ในการปฏิบัติงานตามสิทธิที่ได้รับอนุญาตเท่านั้น ห้ามใช้งานระบบในลักษณะที่อาจก่อให้เกิดความเสียหายต่อระบบ ข้อมูล หรือภาพลักษณ์ของหน่วยงาน ไม่ว่าจะโดยเจตนาหรือไม่เจตนา

(3) รักษาความลับของข้อมูลผู้ใช้งาน (Username) และรหัสผ่าน (Password) ต้องไม่เปิดเผยข้อมูลดังกล่าวให้แก่บุคคลอื่น ไม่บันทึกหรือจดรหัสผ่านในที่ที่ไม่ปลอดภัย และต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

(4) รายงานเหตุการณ์ผิดปกติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศต่อเจ้าหน้าที่ที่เกี่ยวข้องทันที เช่น การพบไวรัส มัลแวร์ การเข้าถึงระบบโดยไม่ได้รับอนุญาต การใช้งานระบบผิดปกติ หรือเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของข้อมูลและระบบ เพื่อให้สามารถดำเนินการตอบสนองและแก้ไขได้อย่างทันท่วงที

(5) ปฏิบัติตามขั้นตอนการลงทะเบียนและเพิกถอนสิทธิการใช้งานระบบสารสนเทศ ในกรณีที่มีการโยกย้าย เปลี่ยนหน้าที่การงาน ลาออก สิ้นสุดสัญญาจ้าง หรือสิ้นสุดภารกิจ เพื่อให้สิทธิการเข้าถึงระบบเป็นปัจจุบัน และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(6) มีความรับผิดชอบในการดูแลรักษาอุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับมอบหมาย เช่น เครื่องคอมพิวเตอร์ โทรศัพท์มือถือ หรือสื่อบันทึกข้อมูล ให้มีความปลอดภัยจากการสูญหาย การโจรกรรม หรือการเข้าถึงโดยบุคคลที่ไม่เกี่ยวข้อง

(7) ส่งเสริมและเป็นแบบอย่างที่ดีในการปฏิบัติตามแนวทางด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อสร้างบรรยากาศและวัฒนธรรมความมั่นคงปลอดภัยในหน่วยงาน

4. แนวทางการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการสตรีและสถาบันครอบครัว (สค.) เป็นไปอย่างปลอดภัย มีประสิทธิภาพ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ บุคลากรทุกระดับจำเป็นต้องปฏิบัติตามแนวทางการใช้งานที่ถูกต้อง ครอบคลุมทั้งการบริหารบัญชีผู้ใช้งาน การใช้อุปกรณ์ ระบบเครือข่าย และการตอบสนองเหตุการณ์ผิดปกติ ทั้งนี้เพื่อให้เป็นไปตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของกรมฯ และมาตรฐานที่เกี่ยวข้อง

4.1 การจัดการรหัสผ่าน (Password Management)

การกำหนดและดูแลรักษารหัสผ่านเป็นมาตรการพื้นฐานที่สำคัญในการป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต ผู้ใช้งานต้องปฏิบัติตามหลักเกณฑ์ดังต่อไปนี้

(1) การตั้งรหัสผ่านที่มีความปลอดภัย

- ต้องกำหนดรหัสผ่านที่มีความยาวไม่น้อยกว่า 8 ตัวอักษร
- ประกอบด้วยตัวอักษร พิมพ์ใหญ่ (A–Z) ตัวอักษร พิมพ์เล็ก (a–z) ตัวเลข (0–9) และอักขระพิเศษ (เช่น ! @ # $ % ^ & *)

- หลีกเลี่ยงการใช้รหัสผ่านที่สามารถคาดเดาได้ง่าย เช่น ชื่อ–นามสกุลของตนเองหรือบุคคลใกล้ชิด วันเดือนปีเกิด หมายเลขโทรศัพท์ หรือรหัสบัตรประชาชน คำศัพท์ทั่วไป เช่น “password” “123456” หรือรูปแบบซ้ำ ๆ เป็นต้น
- ห้ามใช้รหัสผ่านเดียวกันกับระบบส่วนตัวหรือบัญชีโซเชียลมีเดีย

(2) การเปลี่ยนรหัสผ่าน
- ต้องเปลี่ยนรหัสผ่านทุก 180 วัน หรือบ่อยกว่านั้นตามประกาศหรือนโยบายที่หน่วยงานกำหนด
- เมื่อได้รับรหัสผ่านครั้งแรกจากระบบหรือผู้ดูแลระบบ ต้องทำการเปลี่ยนรหัสผ่าน ภายใน 7 วัน
- ต้องเปลี่ยนรหัสผ่านทันที หากสงสัยว่ารหัสผ่านถูกเปิดเผยหรืออาจรั่วไหล

(3) การเก็บรักษารหัสผ่าน
- ห้ามจดบันทึกรหัสผ่านในที่เปิดเผย เช่น โพสต์อิท ใต้แป้นพิมพ์ หรือในสมุดบันทึกที่ไม่ปลอดภัย
- ห้ามส่งรหัสผ่านผ่านช่องทางที่ไม่ปลอดภัย เช่น อีเมล ข้อความ หรือแอปพลิเคชันสนทนา
- ไม่เปิดใช้ฟังก์ชัน “จำรหัสผ่านอัตโนมัติ” (Save Password/Auto Login) บนเครื่องคอมพิวเตอร์สำนักงาน

(4) การจัดการรหัสผ่านหลายระบบ
- ผู้ใช้งานที่มีสิทธิ์เข้าถึงหลายระบบต้องกำหนดรหัสผ่านที่แตกต่างกันในแต่ละระบบ เพื่อป้องกันความเสี่ยงหากรหัสผ่านระบบหนึ่งถูกเปิดเผย
- ควรจัดทำแนวทางการจำรหัสผ่านอย่างปลอดภัย เช่น การใช้ Password Manager

(5) การปฏิบัติกรณีรหัสผ่านสูญหายหรือถูกเปิดเผย
- หากลืมหรือสงสัยว่ารหัสผ่านถูกบุกรุก ต้องแจ้งเจ้าหน้าที่ผู้ดูแลระบบ (IT) โดยทันที เพื่อดำเนินการรีเซ็ตรหัสผ่านและตรวจสอบเหตุการณ์
- ห้ามพยายามเข้าถึงหรือเปลี่ยนแปลงรหัสผ่านของบุคคลอื่นโดยไม่ได้รับอนุญาต

4.2 การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

การควบคุมการเข้าถึงระบบสารสนเทศ เป็นมาตรการสำคัญเพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลหรือระบบของหน่วยงาน ผู้ใช้งานต้องปฏิบัติตามหลักเกณฑ์ ดังนี้

(1) ใช้บัญชีผู้ใช้งาน (User Account) ที่ได้รับอนุญาตเท่านั้น
- การเข้าถึงระบบสารสนเทศทุกประเภท ต้องใช้บัญชีที่ออกให้โดยหน่วยงานอย่างเป็นทางการและเป็นบัญชีเฉพาะบุคคล
- ห้ามใช้บัญชีผู้ใช้งานร่วมกัน เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารที่เกี่ยวข้องและมีกลไกการควบคุมติดตามที่ชัดเจน

(2) การจัดการสิทธิ์การเข้าถึง

- สิทธิ์การเข้าถึงระบบจะต้องสอดคล้องกับหน้าที่และความรับผิดชอบของบุคลากร (Role-based Access Control)
- ผู้ใช้งานไม่มีสิทธิ์เพิ่ม ลด หรือปรับเปลี่ยนสิทธิ์การเข้าถึงของตนเองหรือผู้อื่นโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

(3) การออกจากระบบและการล็อกหน้าจอ
- ผู้ใช้งานต้องออกจากระบบทุกครั้งเมื่อเลิกใช้งาน หรือเมื่อเปิดอุปกรณ์โดยไม่มีผู้ดูแล
- ต้องตั้งค่าล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานเกิน 15 นาที เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(4) การเข้าถึงจากภายนอก (Remote Access)
- การเข้าระบบจากภายนอกสถานที่ทำงาน ต้องดำเนินการผ่านระบบเครือข่ายส่วนตัวเสมือน (VPN) ของหน่วยงาน และต้องได้รับอนุญาตจากกลุ่มเทคโนโลยีสารสนเทศ
- ผู้ใช้งานต้องปฏิบัติตามมาตรการควบคุมด้านความปลอดภัย เช่น การพิสูจน์และยืนยันตัวตนทางดิจิทัล (DOPA-Digital ID) ผ่านแอปพลิเคชัน ThaID หรือการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) หากระบบรองรับ

(5) การเชื่อมต่ออุปกรณ์เครือข่าย
- ห้ามติดตั้งหรือเชื่อมต่ออุปกรณ์เครือข่ายใด ๆ (เช่น Access Point, Router, Switch ส่วนบุคคล) เข้ากับระบบของหน่วยงานโดยไม่ได้รับอนุญาต
- อุปกรณ์ที่นำมาเชื่อมต่อภายนอกต้องผ่านการตรวจสอบด้านความปลอดภัยจากเจ้าหน้าที่ IT ก่อนใช้งาน

4.3 การใช้อีเมลและอินเทอร์เน็ต (Email and Internet Usage)

(1) การใช้อีเมลราชการ
- ใช้อีเมลของหน่วยงานเพื่อวัตถุประสงค์ในการปฏิบัติงานเท่านั้น
- ห้ามเปิดไฟล์แนบหรือคลิกลิงก์จากอีเมลที่ไม่รู้จักหรือมีลักษณะน่าสงสัย หากพบให้แจ้งเจ้าหน้าที่ IT ทันที
- ห้ามส่งต่อข้อมูลที่เป็นความลับหรือข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

(2) การใช้งานอินเทอร์เน็ต
- ห้ามใช้ระบบของกรมฯ เพื่อกิจกรรมส่วนตัว เช่น การเล่นเกม การซื้อขายออนไลน์ หรือกิจกรรมเชิงพาณิชย์ที่ไม่เกี่ยวข้องกับภารกิจราชการ
- ห้ามเข้าถึงเว็บไซต์ที่มีความเสี่ยงต่อความปลอดภัย เช่น เว็บไซต์ผิดกฎหมาย ลามกอนาจาร การพนัน หรือเว็บที่ระบบเตือนว่าไม่ปลอดภัย

(3) การใช้โปรแกรมและบริการออนไลน์

- ห้ามติดตั้งหรือใช้งานโปรแกรม P2P หรือซอฟต์แวร์ที่มีความเสี่ยงสูง เช่น BitTorrent เว้นแต่ได้รับอนุญาตจากหัวหน้าหน่วยงาน
- หากมีความจำเป็นต้องใช้บริการออนไลน์จากภายนอก ต้องตรวจสอบความน่าเชื่อถือก่อนทุกครั้ง

4.4 การปกป้องข้อมูลและอุปกรณ์ (Data and Device Protection)

(1) การเก็บรักษาข้อมูล

- ต้องจัดเก็บเอกสาร ข้อมูลราชการ และข้อมูลสำคัญในที่ปลอดภัย และควบคุมสิทธิ์การเข้าถึงอย่างเหมาะสม
- ห้ามเก็บข้อมูลสำคัญไว้บนเครื่องส่วนบุคคล หรือบริการ Cloud ส่วนตัว เช่น Google Drive, Dropbox

(2) การสำรองข้อมูล

- ข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานต้องมีการสำรองไว้ตามรอบระยะเวลาที่กำหนด เพื่อป้องกันการสูญหาย

(3) การทำลายสื่อบันทึกข้อมูล

- ต้องทำลายสื่อบันทึกข้อมูล เช่น แผ่น CD, USB Drive, ฮาร์ดดิสก์ ตามมาตรฐานความปลอดภัย (เช่น DOD 5220.22-M) หรือวิธีที่หน่วยงานกำหนด ก่อนทิ้งหรือส่งต่อให้บุคคลอื่น

(4) การรักษาความปลอดภัยของอุปกรณ์

- ผู้ใช้งานต้องรับผิดชอบดูแลอุปกรณ์คอมพิวเตอร์ โทรศัพท์มือถือ หรืออุปกรณ์พกพาที่ได้รับมอบหมาย ไม่ให้สูญหายหรือถูกโจรกรรม
- หากอุปกรณ์สูญหาย ถูกขโมย หรือสงสัยว่ามีการเข้าถึงโดยไม่ได้รับอนุญาต ต้องแจ้งเจ้าหน้าที่ IT โดยทันที

4.5 การตอบสนองเหตุผิดปกติ (Incident Response)

(1) หยุดการใช้งานทันที

เมื่อพบเหตุการณ์ผิดปกติ เช่น เครื่องติดไวรัส ระบบทำงานผิดปกติ หรือสงสัยว่าข้อมูลรั่วไหล ให้หยุดใช้งานระบบหรืออุปกรณ์ทันทีเพื่อป้องกันความเสียหายเพิ่มเติม

(2) เก็บหลักฐานของเหตุการณ์

จัดเก็บข้อมูลหรือหลักฐานที่เกี่ยวข้อง เช่น ภาพหน้าจอ ข้อความแจ้งเตือน รายละเอียดเหตุการณ์ หรืออีเมลที่น่าสงสัย เพื่อประกอบการตรวจสอบ

(3) แจ้งหน่วยงานที่รับผิดชอบ

รีบแจ้งกลุ่มเทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบที่เกี่ยวข้องทันที เพื่อให้สามารถดำเนินการตรวจสอบ วิเคราะห์ และตอบสนองเหตุการณ์ได้อย่างทันท่วงที

(4) งดการแก้ไขปัญหาด้วยตนเอง

ห้ามดำเนินการแก้ไขระบบ ลบไฟล์ หรือติดตั้งโปรแกรมเพิ่มเติมโดยไม่ได้รับคำแนะนำจากเจ้าหน้าที่ที่มีอำนาจ เพื่อป้องกันการทำลายหลักฐานหรือทำให้สถานการณ์ซับซ้อนขึ้น

5. ข้อห้ามสำคัญ

(1) ห้ามเผยแพร่หรือทำสำเนาข้อมูลลับโดยไม่ได้รับอนุญาต

บุคลากรทุกคนต้องปฏิบัติตามนโยบายความลับขององค์กรอย่างเคร่งครัด ห้ามส่งต่อ แจกจ่าย ทำสำเนา หรือเปิดเผยข้อมูลที่จัดเป็นความลับหรือมีข้อจำกัดด้านการเข้าถึงโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

(2) ห้ามติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์

การติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์ถือเป็นการกระทำที่ผิดกฎหมายและละเมิดนโยบายความมั่นคงปลอดภัยของหน่วยงาน บุคลากรต้องติดตั้งซอฟต์แวร์ที่ได้รับอนุมัติเท่านั้น

(3) ห้ามดักจับข้อมูล เฝ้าดูเครือข่าย หรือเข้าถึงบัญชีของผู้อื่นโดยมิชอบ

การเข้าถึงข้อมูลส่วนบุคคล ข้อมูลการทำงาน หรือระบบงานของผู้อื่นโดยไม่ได้รับอนุญาตถือเป็นการละเมิดความเป็นส่วนตัวและกฎหมายที่เกี่ยวข้อง บุคลากรต้องใช้งานระบบเครือข่ายและอุปกรณ์คอมพิวเตอร์ด้วยความโปร่งใสและถูกต้องตามวัตถุประสงค์ของหน่วยงานเท่านั้น

(4) ห้ามใช้ระบบของกรมฯ เพื่อกิจกรรมที่ผิดกฎหมาย ศีลธรรม หรือขัดต่อภารกิจของหน่วยงาน

ระบบสารสนเทศและอุปกรณ์ขององค์กรต้องใช้เพื่อวัตถุประสงค์ในการปฏิบัติงานตามภารกิจของกรมฯ เท่านั้น ห้ามใช้เพื่อกิจกรรมที่ผิดกฎหมาย ละเมิดศีลธรรม หรือไม่สอดคล้องกับเป้าหมายและนโยบายขององค์กร

6. ข้อแนะนำการปฏิบัติ

(1) สำรองข้อมูลเป็นประจำ

- เก็บสำรองข้อมูลในแฟลชไดรฟ์, SD Card หรือพื้นที่จัดเก็บที่ปลอดภัย
- ตรวจสอบสำเนาสำรองอย่างสม่ำเสมอ เพื่อให้ข้อมูลพร้อมใช้งานเมื่อจำเป็น

(2) อัปเดตซอฟต์แวร์และระบบปฏิบัติการ
- ติดตั้งอัปเดตล่าสุดของซอฟต์แวร์และระบบปฏิบัติการ
- ป้องกันช่องโหว่ที่อาจถูกโจมตี

(3) เครือข่ายอย่างปลอดภัย
- หลีกเลี่ยงการเชื่อมต่อ Wi-Fi สาธารณะ
- หากจำเป็น ให้เชื่อมต่อผ่าน VPN เพื่อเข้ารหัสข้อมูล

(4) ระมัดระวังสภาพแวดล้อมรอบตัว
- สังเกตพฤติกรรมและท่าทีของคนรอบข้าง
- ป้องกันการสอดแนมหรือขโมยข้อมูล

(5) เข้ารหัสข้อมูลและตั้งรหัสผ่านปลอดภัย
- เข้ารหัสไฟล์และอุปกรณ์ที่สำคัญ
- ใช้รหัสผ่านที่คาดเดายาก และไม่เปิดเผยให้ผู้อื่น

(6) เข้าถึงเว็บไซต์อย่างปลอดภัย
- ตรวจสอบให้เว็บไซต์ใช้ HTTPS
- เปิดใช้งานการยืนยันตัวตนแบบสองขั้นตอน (2FA) เมื่อเป็นไปได้

(7) ดูแลอุปกรณ์อย่างใกล้ชิด
- ห้ามทิ้งคอมพิวเตอร์หรืออุปกรณ์พกพาโดยไม่มีผู้ดูแล
- ป้องกันการโจรกรรมหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(8) ป้องกันการสอดแนมทางสายตา
- ใช้เทปปิดกล้องเว็บแคมหรือฟิล์มกรองแสงหน้าจอ
- ป้องกันการแอบมองข้อมูลจากบุคคลภายนอก

(9) ใช้อุปกรณ์ชั่วคราวอย่างระมัดระวัง
- เก็บเฉพาะข้อมูลสำคัญที่จำเป็นต่อการทำงาน
- ลบข้อมูลทันทีหลังเสร็จสิ้นการใช้งาน

7.ช่องทางติดต่อ IT

กลุ่มเทคโนโลยีสารสนเทศ (กทส.)

โทรศัพท์: 0 2659 6790

อีเมล: ict@dwf.go.th

8. บทสรุป

บุคลากรทุกคนถือเป็นส่วนสำคัญในการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของกรมฯ การปฏิบัติตามคู่มือการใช้งานระบบสารสนเทศนี้ไม่เพียงแต่ช่วยปกป้องข้อมูลสำคัญและข้อมูลส่วนบุคคลของประชาชน แต่ยังส่งเสริมให้ภารกิจของกรมกิจการสตรีและสถาบันครอบครัวดำเนินไปอย่างมั่นคงปลอดภัย มีความต่อเนื่อง และน่าเชื่อถือ นอกจากนี้ การยึดมั่นในมาตรฐานความปลอดภัยและแนวทางปฏิบัติที่กำหนดยังช่วยสร้างวัฒนธรรมความมั่นคงปลอดภัยด้านสารสนเทศภายในหน่วยงานอย่างยั่งยืน

****