

เครื่องข่ายศูนย์เทคโนโลยีสารสนเทศ

ประกาศ

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 26 กำหนดให้ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ไว้ไม่น้อยกว่า 90 วัน นับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ฯลฯ รวมทั้งผู้ให้บริการจะต้องเก็บรักษาข้อมูล ของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มให้บริการและต้อง เก็บรักษาไว้เป็นเวลาไม่น้อยกว่า 90 วันนับตั้งแต่การให้บริการสิ้นสุดลง เพื่อให้สอดคล้องกับพระราชบัญญัติดังกล่าว ผู้ใช้บริการอินเทอร์เน็ต ในเครื่องข่ายศูนย์เทคโนโลยีสารสนเทศ จะต้องดำเนินการ login ก่อนเข้าใช้บริการ

หมายเหตุ

ที่ช่อง Username:

ในกรณีที่ใช้ e-mail somchai@health.moph.go.th ให้ใส่ somchai.health

ในกรณีที่ใช้ e-mail somchai@health2.moph.go.th ให้ใส่ somchai.health2

ในกรณีที่ใช้ e-mail somchai@health3.moph.go.th ให้ใส่ somchai.health3

ถ้ามีหน้าต่าง ถามต้องการให้ระบบจำ Password หรือไม่ ให้ตอบ **No**

Login

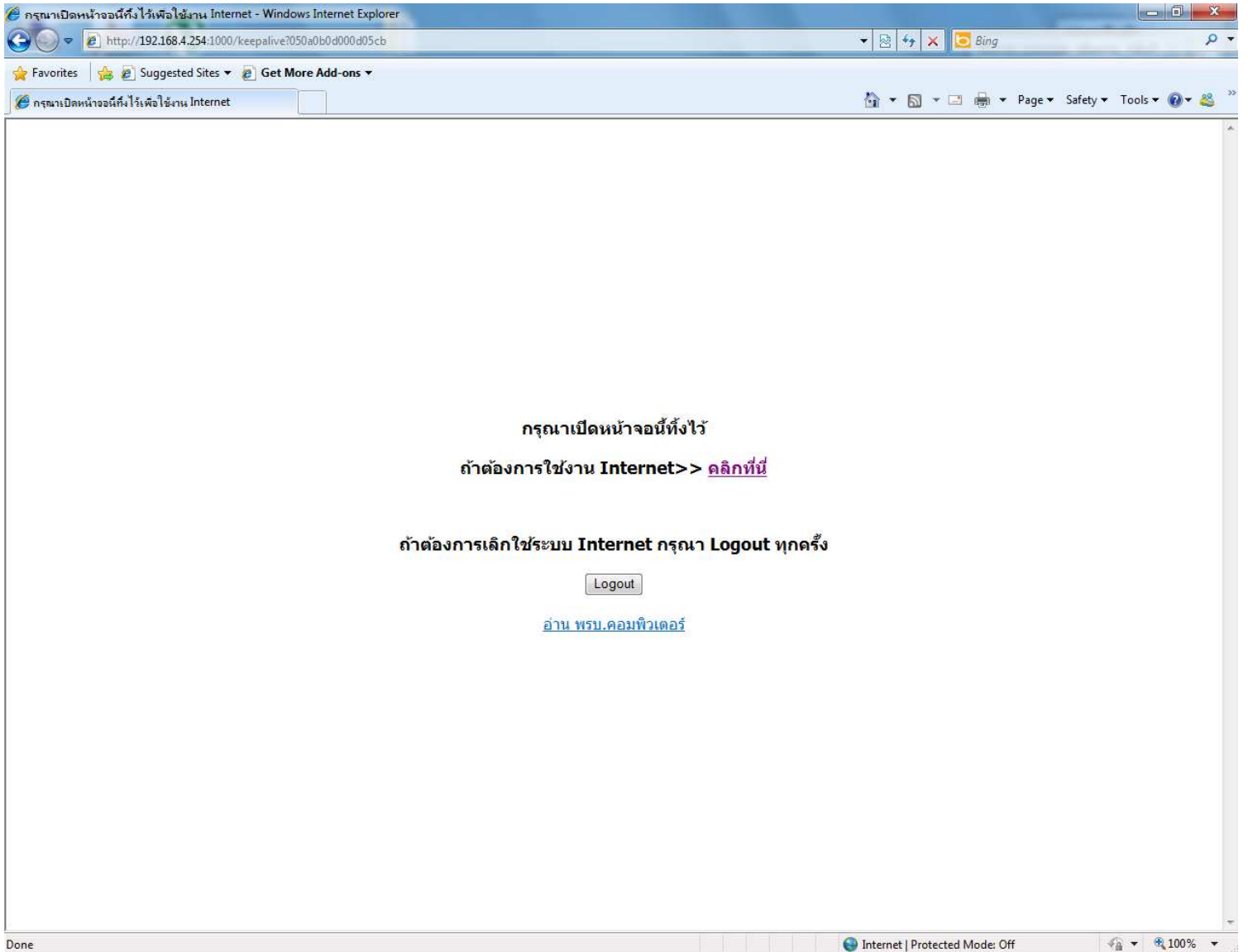
Account Details

Username:

Password:

Login

- หลังจาก Login แล้วจะได้หน้าต่าง Logout ขึ้นมาให้เปิดค้างไว้ ห้ามปิด!!! และเมื่อเลิกใช้บริการเครื่องข่าย ต้อง Logout ทุกครั้ง !!!



ข้อกำหนดทางการปฏิบัติงานสำหรับควบคุมการเข้าถึงสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข (Access rights)

1. การควบคุมการเข้าถึงระบบ (Access control)

ผู้บริหารสำนักงานปลัดกระทรวงสาธารณสุข ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางการปฏิบัติงาน และด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินทางด้านสารสนเทศ

2. การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)

2.1 การลงทะเบียนผู้ปฏิบัติงาน (User registration)

สำนักงานปลัดกระทรวงสาธารณสุข ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ สำหรับการลงทะเบียนผู้ปฏิบัติงานใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)

ผู้ดูแลระบบงานของสำนักงานปลัดกระทรวงสาธารณสุข ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

ผู้ดูแลระบบงานของสำนักงานปลัดกระทรวงสาธารณสุขต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย ซึ่งสำนักงานกระทรวงสาธารณสุขได้ดำเนินการตามนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีฯ ภายใต้แนวทางความมั่นคงปลอดภัยของกระทรวงเทคโนโลยีสารสนเทศนั้น การเข้าสู่ระบบอินเทอร์เน็ตของกระทรวงฯจึงได้กำหนดให้ user ทำการพิสูจน์ตัวตนโดย Login และระบุ Password ก่อนเข้าระบบ

ทั้งนี้หาก User ไม่ได้ตั้งระบบยกเลิกการจำ password ของ Internet explorer ไว้ อาจทำให้การเข้าใช้ระบบครั้งต่อไปมีปัญหาได้

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจึงได้จัดทำคู่มือยกเลิกการจำ password ของ Internet explorer มาพร้อมนี้เพื่อให้ใช้เป็นแนวทางปฏิบัติโดยทั่วกัน

2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

สำนักงานปลัดกระทรวงสาธารณสุขต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้

3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

3.1 การใช้งานรหัสผ่าน (Password use)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุขต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน

3.2 การป้องกันอุปกรณ์ที่ไม่มีผู้ปฏิบัติงานดูแล (Unattended user equipment)

บุคลากรใน สำนักงานปลัดกระทรวงสาธารณสุข ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีผู้ปฏิบัติงานดูแล

3.3 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)

สำนักงานปลัดกระทรวงสาธารณสุขต้องจัดทำนโยบายเพื่อควบคุมไม่ให้เกิดการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะ หรือพบเห็นได้ง่าย เป็นต้น

4. การควบคุมการเข้าถึงเครือข่าย (Network access control)

4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้

4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่ จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

4.4 การแบ่งแยกเครือข่าย (Segregation in networks)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ

4.5 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไป ตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอปพลิเคชันที่ใช้งานทางการปฏิบัติงานได้ระบุไว้

4.6 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียน ของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง

5.การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ

5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (User of system utilities)

ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว

5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่ง ตามที่กำหนดไว้

5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

6. การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and information access control)

6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

ผู้ดูแลระบบของ สำนักงานปลัดกระทรวงสาธารณสุข ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอปพลิเคชันตามนโยบาย ควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)

สำนักงานปลัดกระทรวงสาธารณสุข ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหาก ออกมาสำหรับระบบนี้โดยเฉพาะ

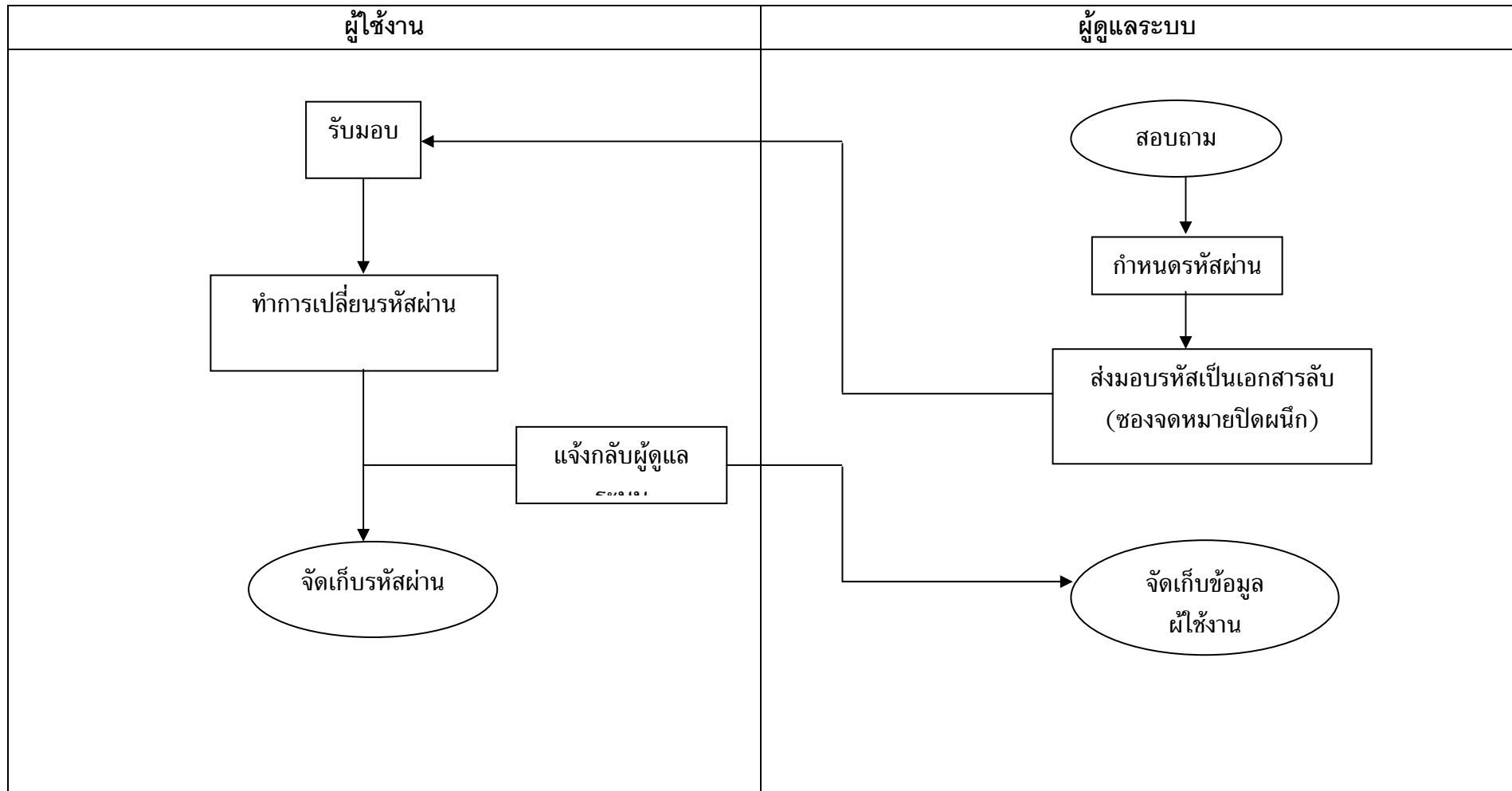
7. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)

สำนักงานปลัดกระทรวงสาธารณสุข ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้

7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

สำนักงานปลัดกระทรวงสาธารณสุข ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน



แผนผังการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

การกำหนดสิทธิ (Access Right) ในการอ่าน เขียน หรือใช้งานข้อมูลในระบบสารสนเทศสำหรับผู้ใช้งาน (User) กลุ่มต่าง ๆ ได้แก่ ประชาชน ส่วนราชการที่เกี่ยวข้อง และผู้บริหารของส่วนราชการ

ลำดับ ที่	กลุ่มผู้ใช้งาน	สิทธิในการเข้าใช้งาน					สถานภาพปัจจุบัน	แนวทางการ ดำเนินการ	หมายเหตุ
		อ่าน	เขียน (เพิ่มข้อมูล)	แก้ไข	ลบ	เงื่อนไข			
1	ผู้บริหารของส่วน ราชการ	✓	✓	✗	✗	สามารถเพิ่ม แก้ไขหรือลบ ข้อมูลได้ในกรณีที่บางระบบ ได้อนุญาตให้กระทำได้	- เป็นไปตามเงื่อนไข ที่กำหนด	- ทบทวนการกำหนด สิทธิในการเข้าใช้งาน ระบบสารสนเทศอย่าง เป็นระบบและ เหมาะสมกับ สถานการณ์ปัจจุบัน	
2	บุคลากรสำนักงาน ปลัดกระทรวง สาธารณสุข	✓	✓	✓	✓	สามารถเพิ่ม แก้ไข หรือลบ ข้อมูลได้ในกรณีที่บางระบบ อนุญาตให้กระทำได้ หรือ สำนักงานปลัดกระทรวง สาธารณสุขได้กำหนดสิทธิใน การเข้าใช้งานระบบให้ สามารถกระทำได้ ซึ่งจะ พิจารณาเป็นราย ๆ ไป	- เป็นไปตามเงื่อนไข ที่กำหนด		

ลำดับ ที่	กลุ่มผู้ใช้งาน	สิทธิในการเข้าใช้งาน					สถานภาพปัจจุบัน	แนวทางการ ดำเนินการ	หมายเหตุ
		อ่าน	เขียน (เพิ่มข้อมูล)	แก้ไข	ลบ	เงื่อนไข			
3	ส่วนราชการที่เกี่ยวข้อง	✓	×	×	×	สามารถเพิ่ม แก้ไขหรือลบ ข้อมูลได้ในกรณีที่บางระบบ ได้อนุญาตให้กระทำได้ หรือมี การทำข้อตกลงหรือยินยอม ระหว่างหน่วยงาน			
4	ประชาชนทั่วไป	✓	×	×	×	สามารถเพิ่ม แก้ไข หรือลบ ข้อมูลได้ในกรณีที่บางระบบ อนุญาตให้กระทำได้			