	นโยบายการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)	รหัสเอกสาร	KSC MOPH-Policy-04
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	1 ธ.ค. 2568 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นางสาวศิรดา สว่างสุข	นายชัพ ธิราขันธ์	นายภูจิตต์ ตรีบำเพ็ญ
ตำแหน่ง	นักสาธารณสุขปฏิบัติการ	นักจัดการงานทั่วไปชำนาญการ	ผู้อำนวยการโรงพยาบาลเกาะสีชัง
วันเดือนปี	24 พฤศจิกายน 2568	28 พฤศจิกายน 2568	28 พฤศจิกายน 2568

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	1 ธ.ค. 68	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

	นโยบายการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)	รหัสเอกสาร	KSC MOPH-Policy-04
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	1 ธ.ค. 2568 ใช้ภายในเท่านั้น

นโยบายการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards Policy)

อ้างอิง : นโยบาย (ข้อ 3.1), ประมวลและกรอบ [ข้อ 22.2.1, ข้อ 22.2.2, ข้อ 22.2.3, ข้อ 22.2.4]

1. วัตถุประสงค์ (Objective)

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยสำหรับการกำหนดค่าระบบสารสนเทศ เพื่อป้องกันความเสี่ยงและลดช่องโหว่ที่อาจเกิดขึ้นจากการกำหนดค่าระบบที่ไม่ปลอดภัย

2. ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงการกำหนดค่าระบบทั้งหมดในองค์กร รวมถึงเซิร์ฟเวอร์, คอมพิวเตอร์, อุปกรณ์เครือข่าย และแอปพลิเคชันที่ใช้งานภายในโรงพยาบาลเกาะสีชัง

3. หลักการรักษาความมั่นคงปลอดภัย (Security Principles)

โรงพยาบาลเกาะสีชังต้องปฏิบัติตามหลักการรักษาความมั่นคงปลอดภัยอย่างน้อยดังต่อไปนี้

1. **สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)**
   - ระบบฐานข้อมูลของโรงพยาบาลเกาะสีชังจะต้องถูกกำหนดให้พนักงานแต่ละคนเข้าถึงข้อมูลเฉพาะส่วนที่เกี่ยวข้องกับหน้าที่ของตนเท่านั้น เช่น เจ้าหน้าที่ฝ่ายการเงินจะสามารถเข้าถึงข้อมูลการเงิน แต่ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลของพนักงานได้
2. **การแบ่งแยกหน้าที่ (Separation of Duties)**
   - ในโรงพยาบาลเกาะสีชังจะต้องมีการแบ่งแยกหน้าที่กันอย่างชัดเจน
3. **การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน**
   - โรงพยาบาลเกาะสีชังกำหนดให้ผู้ใช้ทุกคนต้องตั้งรหัสผ่านที่ประกอบด้วยอักษรพิมพ์ใหญ่, อักษรพิมพ์เล็ก, ตัวเลข และอักขระพิเศษ และต้องมีความยาวอย่างน้อย 8 - 12 ตัวอักษร

4. **การลบบัญชีที่ไม่ได้ใช้**
    - บัญชีของพนักงานที่ลาออกจะถูกลบออกจากระบบภายใน 24 ชั่วโมง หลังจากที่พนักงานคนนั้นออกจากโรงพยาบาลเกาะสีชัง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต
5. **การลบบริการและแอปพลิเคชันที่ไม่จำเป็น**
    - เซิร์ฟเวอร์ของโรงพยาบาลเกาะสีชังจะถูกกำหนดค่าให้ลบคอมไพเลอร์ (Compiler) และแอปพลิเคชันที่ไม่จำเป็น เช่น แอปพลิเคชันที่ใช้สำหรับการทดสอบหรือสนับสนุนจากผู้ให้บริการภายนอก เพื่อป้องกันการโจมตีที่อาจเกิดขึ้นจากช่องโหว่ในแอปพลิเคชันเหล่านั้น
6. **การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน**
    - ในการตั้งค่าเครือข่ายของโรงพยาบาลเกาะสีชัง พอร์ตที่ไม่ได้ใช้งาน เช่น พอร์ต FTP จะถูกปิดเพื่อป้องกันการโจมตีที่อาจเกิดขึ้นจากการเข้าถึงผ่านพอร์ตเหล่านั้น
7. **การป้องกันมัลแวร์ (Malware Protection)**
    - คอมพิวเตอร์ทุกเครื่องในโรงพยาบาลเกาะสีชังจะต้องติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์เป็นประจำ รวมถึงมีการสแกนระบบแบบอัตโนมัติทุกสัปดาห์
8. **การปรับปรุงซอฟต์แวร์และแพตช์ความมั่นคงปลอดภัยของระบบ**
    - เซิร์ฟเวอร์ของโรงพยาบาลเกาะสีชังจะได้รับการอัปเดตซอฟต์แวร์และติดตั้งแพตช์ความมั่นคงปลอดภัยที่ปล่อยออกมาโดยผู้ผลิตซอฟต์แวร์ภายใน 48 ชั่วโมงหลังจากที่แพตช์เหล่านั้นถูกปล่อยออกมา เพื่อป้องกันการโจมตีจากช่องโหว่ที่เป็นที่รู้จัก

4. การตรวจสอบและการปฏิบัติตามนโยบาย (Audit and Compliance)

โรงพยาบาลเกาะสีชังต้องดำเนินการตรวจสอบการปฏิบัติตามนโยบายนี้อย่างสม่ำเสมอ โดยการตรวจสอบการตั้งค่าระบบและการใช้งานสิทธิ์ต่าง ๆ และรายงานผลการตรวจสอบต่อผู้บริหารที่เกี่ยวข้อง นโยบายนี้ต้องได้รับการทบทวนและปรับปรุงอย่างต่อเนื่องเพื่อให้สอดคล้องกับภัยคุกคามและเทคโนโลยีที่เปลี่ยนแปลงไป

5. การฝ่าฝืนนโยบาย (Policy Violations)

ผู้ใช้งานใดที่ฝ่าฝืนนโยบายนี้จะต้องได้รับการพิจารณาและอาจต้องรับโทษตามมาตรการที่กำหนดไว้ในกฎระเบียบของโรงพยาบาลเกาะสีชัง

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ