เอกสารประกอบการประเมิน

ด้านที่ ๙ การรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๙.๓.๓ แผนงานการสร้างความตระหนักรู้ด้านการรักษาความปลอดภัยไซเบอร์

(Cybersecurity Awareness)

โรงพยาบาลสองแคว ประจำปีงบประมาณ ๒๕๖๙

วัตถุประสงค์ของเอกสาร

เอกสารฉบับนี้จัดทำขึ้นเพื่อใช้เป็นหลักฐานประกอบการประเมินข้อ ๙.๓.๓ แสดงให้เห็นว่าโรงพยาบาลมีการวางแผนและดำเนินกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรอย่างต่อเนื่อง ครอบคลุมประเด็นการใช้งานรหัสผ่าน การป้องกันฟิชชิง การคุ้มครองข้อมูลผู้ป่วย การใช้สื่อสังคมออนไลน์ การสำรองข้อมูล และการรับมือภัยคุกคามไซเบอร์

ชื่อเอกสาร	แผนงานการสร้างความตระหนักรู้ด้านการรักษาความปลอดภัยไซเบอร์
หน่วยงาน	งานเทคโนโลยีสารสนเทศ โรงพยาบาลสองแคว
ปีงบประมาณ	๒๕๖๙
สถานะเอกสาร	ใช้เป็นเอกสารแนบประกอบการประเมินข้อ ๙.๓.๓

๑. คำอธิบายประกอบเกณฑ์ข้อ ๙.๓.๓

โรงพยาบาลสองแควมีการจัดทำแผนงานการสร้างความตระหนักรู้ด้านการรักษาความปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร เพื่อให้บุคลากรทุกระดับมีความรู้ ความเข้าใจ และตระหนักถึงบทบาทหน้าที่ของตนเองในการป้องกันภัยคุกคามไซเบอร์และการคุ้มครองข้อมูลสำคัญของโรงพยาบาล โดยเฉพาะข้อมูลผู้ป่วยและข้อมูลส่วนบุคคล

แผนงานกำหนดกิจกรรมรายเดือนตลอดปีงบประมาณ ๒๕๖๙ พร้อมรายละเอียดการดำเนินงาน ผู้รับผิดชอบหลัก และกฎหมายหรือแนวทางที่เกี่ยวข้อง เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล แนวทาง NCSA และแนวทางการควบคุมพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์

การดำเนินงานประกอบด้วยการประกาศนโยบาย การอบรมพนักงานใหม่ การทดสอบความรู้ การเผยแพร่สื่อประชาสัมพันธ์ การซ้อมสถานการณ์ข้อมูลรั่วไหล การอบรมการปกป้องข้อมูลผู้ป่วย การแจ้งเตือนภัยคุกคาม การรณรงค์ Cyber Hygiene การอบรมผู้บริหาร การทดสอบ Phishing Simulation การทดสอบกู้คืนข้อมูลจาก Backup และการสรุปผลพร้อมรายงานผู้บริหาร

ดังนั้น โรงพยาบาลมีแผนงานและกิจกรรมสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์ที่ชัดเจน มีการกำหนดระยะเวลา กิจกรรม รายละเอียด ผู้รับผิดชอบ และแนวทางติดตามผล สอดคล้องตามเกณฑ์ข้อ ๙.๓.๓

๒. เอกสารอ้างอิงและหลักฐานประกอบ

- แผนงานการสร้างความตระหนักรู้ด้านการรักษาความปลอดภัยไซเบอร์ (Cybersecurity Awareness) ประจำปีงบประมาณ ๒๕๖๙
- สื่อประชาสัมพันธ์/Infographic ด้านความปลอดภัยไซเบอร์ เช่น การตั้งรหัสผ่านที่ปลอดภัย การป้องกัน Phishing การใช้ Wi-Fi อย่างปลอดภัย และการระวังพฤติกรรมเสี่ยง
- หลักฐานการสื่อสารหรือเผยแพร่ผ่านช่องทางภายใน เช่น LINE Group, บอร์ดประชาสัมพันธ์, หนังสือเวียน หรือช่องทางสื่อสารของโรงพยาบาล
- หลักฐานผลการดำเนินงาน เช่น รายชื่อผู้เข้าร่วมกิจกรรม แบบทดสอบ ภาพกิจกรรม รายงานสรุปผล หรือรายงานเสนอผู้บริหาร

๓. ตัวชี้วัดการติดตามผล

ลำดับ	ตัวชี้วัด	ค่าเป้าหมาย/หลักฐาน
๑	มีแผนงาน Cybersecurity Awareness ประจำปี	มีเอกสารแผนงานที่ได้รับทราบ/อนุมัติ
๒	บุคลากรได้รับการสื่อสารหรือเข้าร่วมกิจกรรมด้าน Cybersecurity	ไม่น้อยกว่าร้อยละ ๘๐ ของกลุ่มเป้าหมาย หรือมีหลักฐานการเผยแพร่
๓	มีการประเมินความรู้หรือทบทวนความเข้าใจ	มีแบบทดสอบ/แบบประเมิน/สรุปผลการรับรู้
๔	มีการรายงานผลการดำเนินงานต่อผู้บริหาร	อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีกิจกรรมสำคัญ

แผนงานการสร้างความตระหนักรู้ด้านการรักษาความปลอดภัยไซเบอร์

(Cybersecurity Awareness) โรงพยาบาลสองแคว ประจำปีงบประมาณ ๒๕๖๙

ระยะเวลาดำเนินการ	กิจกรรม	รายละเอียด	ผู้รับผิดชอบหลัก	กฎหมาย/แนวทางที่เกี่ยวข้อง
เมษายน ๒๕๖๙	ผู้บริหารประกาศนโยบายด้าน Cybersecurity & PDPA Policy	ประกาศนโยบายความมั่นคงปลอดภัยไซเบอร์และ PDPA ผ่านเอกสาร หนังสือเวียน หรือ LINE Group ของโรงพยาบาล เพื่อให้บุคลากรรับทราบและถือปฏิบัติร่วมกัน	ผู้อำนวยการ/งาน IT	พ.ร.บ.ไซเบอร์ ม.๔๔ / PDPA ม.๓๗
เมษายน ๒๕๖๙	Cyber Awareness Assessment	จัดทำแบบทดสอบออนไลน์หรือแบบประเมินความรู้ด้าน Cybersecurity เพื่อประเมินระดับความเข้าใจของบุคลากร	งาน IT	Governance
เมษายน ๒๕๖๙	Phishing & Social Engineering Awareness	เผยแพร่ Infographic หรือสื่อความรู้เกี่ยวกับ Phishing, Social Engineering และข้อควรระวังจากอีเมล ลิงก์ หรือข้อความหลอกลวง	งาน IT	NCSA Guideline
พฤษภาคม ๒๕๖๙	Data Breach Tabletop Exercise	ซ้อมแผนกรณีข้อมูลรั่วไหล การแจ้งเหตุภายในองค์กร และแนวทางการแจ้งเหตุภายใน ๗๒ ชั่วโมงตามกฎหมายที่เกี่ยวข้อง	งาน IT/ผู้เกี่ยวข้อง	PDPA ม.๓๗(๔)
พฤษภาคม ๒๕๖๙	Cyber Threat Update	แจ้งเตือนภัยคุกคามไซเบอร์ที่พบในปัจจุบัน เช่น Ransomware, Malware, Fake Link และแนวทางป้องกันเบื้องต้น	งาน IT	Cyber Threat Intelligence
พฤษภาคม ๒๕๖๙	Cyber Hygiene Campaign	รณรงค์การอัปเดตระบบและโปรแกรม Antivirus การล็อกหน้าจอ การไม่ใช้ Flash Drive ไม่ทราบแหล่งที่มา และการใช้งานเครื่องคอมพิวเตอร์อย่างปลอดภัย	งาน IT/ทุกหน่วยงาน	Basic Control
สิงหาคม ๒๕๖๙	Backup & Ransomware Drill	ทดสอบการกู้คืนข้อมูลจาก Backup จริง หรือซ้อมแนวทางการรับมือ Ransomware เพื่อประเมินความพร้อมของระบบและทีมงาน	งาน IT/ผู้เกี่ยวข้อง	Cyber Resilience
กันยายน ๒๕๖๙	Annual Cyber Review & KPI	สรุปผลการดำเนินกิจกรรม Cybersecurity Awareness ตัวชี้วัด ปัญหาอุปสรรค และข้อเสนอแนะ รายงานต่อผู้บริหารเพื่อใช้ปรับปรุงแผนปีถัดไป	งาน IT	Audit Ready

๔. หัวข้อสื่อประชาสัมพันธ์ที่ใช้สร้างความตระหนักรู้

๖.


รพ.สองแคว
บุคลากรใหม่ รอบรู้ภัยไซเบอร์
ปกป้องข้อมูลผู้ป่วยและองค์กรอย่างปลอดภัย
1 4 ภัยไซเบอร์ที่พบบ่อย
Phishing
อีเมลหรือข้อความปลอม
หลอกให้กดลิงก์หรือกรอกข้อมูล
Social Engineering
การหลอกถามข้อมูลสำคัญ
หรือแอบอ้างเป็นเจ้าหน้าที่
Malware / Ransomware
ไฟล์หรือโปรแกรมอันตราย
ทำให้ข้อมูลเสียหายหรือถูกล็อก
Public Wi-Fi Risk
การใช้ Wi-Fi สาธารณะ
เสี่ยงต่อการถูกดักข้อมูล
2 4 อย่า ลดความเสี่ยงข้อมูลรั่วไหล
http://
อย่าคลิก
ลิงก์หรือไฟล์แนบจาก
แหล่งที่ไม่น่าเชื่อถือ
*****
อย่าแชร์
รหัสผ่านหรือข้อมูลสำคัญ
กับผู้อื่น
อย่าเสียบ
Flash Drive / USB
ที่ไม่ทราบแหล่งที่มา
อย่ารอ
ให้อัปเดตระบบและโปรแกรม
เมื่อมีแจ้งเตือน
3 Checklist ความปลอดภัย
MFA
เปิดใช้การยืนยัน
ตัวตน 2 ชั้น
Strong Password
ใช้รหัสผ่านคาดเดายาก
มีตัวพิมพ์ใหญ่-เล็ก
ตัวเลข และสัญลักษณ์
Lock Screen
ล็อกหน้าจอทุกครั้ง
เมื่อไม่อยู่หน้าเครื่อง
Keep Updated
อัปเดตซอฟต์แวร์
และระบบป้องกันไวรัส
สม่ำเสมอ
VPN
Work Securely
ใช้เครือข่ายที่ปลอดภัย
และ VPN เมื่อจำเป็น
IT
ความปลอดภัยขององค์กร
เริ่มต้นที่คุณ
หยุด คิด ตรวจสอบ ก่อนคลิกทุกครั้ง
ฝ่ายเทคโนโลยีสารสนเทศ โรงพยาบาลสองแคว

รพ.สองแคว
หยุดภัยไซเบอร์
เริ่มต้นที่ตัวคุณ

5 พฤติกรรมเสี่ยงที่ต้องระวัง

1 ตั้งรหัสผ่านที่เดาง่าย

- หลีกเลี่ยงรหัสผ่านง่าย ๆ เช่น วันเกิด ชื่อ หรือ 123456
- ตั้งรหัสผ่านให้ซับซ้อน และเปิดใช้ 2FA หรือ MFA

2 คลิกลิงก์จาก SMS หรืออีเมลแปลกหน้า

- ตรวจสอบผู้ส่งก่อนทุกครั้ง
- อย่ากดลิงก์หรือกรอกข้อมูล หากไม่แน่ใจ

3 ใช้ Wi-Fi สาธารณะทำธุรกรรมสำคัญ

- หลีกเลี่ยงการเข้าสู่ระบบหรือทำธุรกรรมผ่าน Wi-Fi สาธารณะ
- หากจำเป็น ควรใช้เครือข่ายที่ปลอดภัยหรือ VPN

4 โพสต์ข้อมูลส่วนตัวลงโซเชียลมากเกินไป

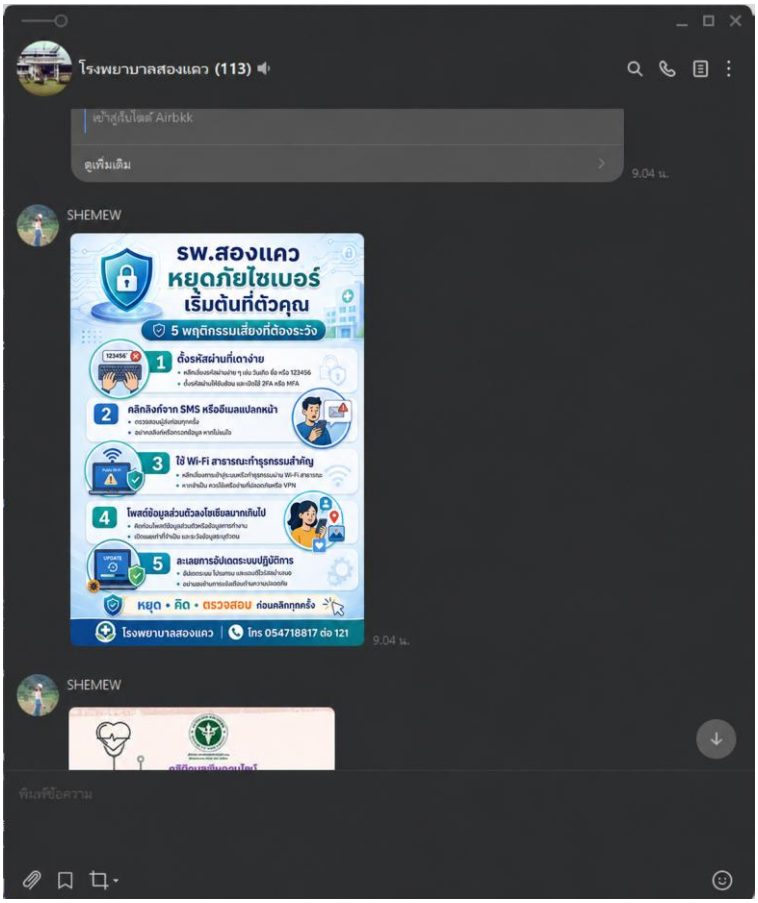
- คิดก่อนโพสต์ข้อมูลส่วนตัวหรือข้อมูลการทำงาน
- เปิดเผยเท่าที่จำเป็น และระวังข้อมูลระบุตัวตน

5 ละเลยการอัปเดตระบบปฏิบัติการ

- อัปเดตระบบ โปรแกรม และแอนติไวรัสสม่ำเสมอ
- อย่ามองข้ามการแจ้งเตือนด้านความปลอดภัย

หยุด • คิด • ตรวจสอบ ก่อนคลิกทุกครั้ง

โรงพยาบาลสองแคว | โทร 054718817 ต่อ 121



ลงชื่อผู้จัดทำ/ผู้รับผิดชอบ

ผู้จัดทำ	ลงชื่อ ..... (นางสาวตรีรัตน์ ทนันชัย) ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ วันที่ ๑ มิถุนายน ๒๕๖๙
ผู้อนุมัติ/รับทราบ	ลงชื่อ ..... (นายกุลพล ตั้งรัตนาพิบูล) ตำแหน่ง ผู้อำนวยการโรงพยาบาลสองแคว วันที่ ๑ มิถุนายน ๒๕๖๙