การตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ
และการประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด
และนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติ ปี 2569

****

วัตถุประสงค์

- บุคลากร รับทราบ เข้าใจ และยอมรับ ระเบียบด้านความมั่นคงปลอดภัยสารสนเทศ
- บุคลากร ปฏิบัติตามอย่างเคร่งครัด
- มีการ ประเมินผลและปรับปรุงกระบวนการบังคับใช้ อย่างต่อเนื่อง

เกณฑ์การประเมิน

- บุคลากร ทำแบบทดสอบผ่าน 10 ใน 15 ข้อ
- บุคลากรผ่านการประเมิน มากกว่าร้อยละ 80 ของจำนวนบุคลากรทั้งหมด

โรงพยาบาลสันกำแพงมีการให้บุคคลากรได้ทำแบบประเมินในการให้ความรู้ความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศ โดยใช้ Google form ในการตอบแบบประเมินมีผลการประเมิน ดังนี้

แบบทดสอบ ความรู้ด้านความมั่นคงปลอดภัยระบบสารสนเทศสำหรับบุคลากร จำนวน 15 ข้อ
1. รหัสผ่านที่ปลอดภัยควรมีลักษณะอย่างไร A. ใช้วันเกิด B. ใช้ 123456 C. มีตัวอักษร ตัวเลข และสัญลักษณ์ D. ใช้ชื่อเล่น • **เฉลย:** C
2. ห้ามเปิดเผยรหัสผ่านกับบุคคลใด A. เพื่อนร่วมงาน B. หัวหน้า C. เจ้าหน้าที่ IT D. ไม่มีใครเลย • **เฉลย:** D

3. หากพบอีเมลต้องสงสัยควรทำอย่างไร

A. เปิดอ่านทันที

B. คลิกลิงก์

C. ลบหรือแจ้ง IT

D. ส่งต่อให้เพื่อน

- **เฉลย:** C

4. การล็อกหน้าจอคอมพิวเตอร์ควรทำเมื่อใด

A. เลิกงาน

B. ทุกครั้งที่ลุกจากโต๊ะ

C. เมื่อมีคนมา

D. ไม่จำเป็น

- **เฉลย:** B

5. การใช้งาน USB ส่วนตัวกับคอมพิวเตอร์องค์กร

A. ใช้ได้เสมอ

B. ใช้ได้ถ้าเป็นของตัวเอง

C. ใช้ได้เมื่อได้รับอนุญาต

D. ใช้ได้เฉพาะวันหยุด

- **เฉลย:** C

6. ข้อมูลผู้ป่วยหรือข้อมูลสำคัญควรส่งผ่านช่องทางใด

A. LINE ส่วนตัว

B. Facebook

C. ระบบที่องค์กรกำหนด

D. อีเมลส่วนตัว

- **เฉลย:** C

7. ควรเปลี่ยนรหัสผ่านบ่อยแค่ไหน

A. ไม่ต้องเปลี่ยน

B. ทุกวัน

C. ตามระเบียบองค์กร เช่น ทุก 90 วัน

D. ปีละครั้ง

- **เฉลย:** C

8. การติดตั้งโปรแกรมในคอมพิวเตอร์องค์กร

A. ติดตั้งได้เอง

B. ขออนุญาต IT ก่อน

C. โหลดจากอินเทอร์เน็ตได้

D. ให้เพื่อนติดตั้ง

- **เฉลย:** B

9. หากทำอุปกรณ์คอมพิวเตอร์สูญหายควรทำอย่างไร

A. ไม่ต้องแจ้ง

B. แจ้งหัวหน้า/IT ทันที

C. ซื้อใหม่เอง

D. รอให้มีคนถาม

- **เฉลย:** B

10. การใช้ Wi-Fi สาธารณะในการทำงานควร

A. ใช้ได้เสมอ

B. ใช้ส่งข้อมูลสำคัญได้

C. หลีกเลี่ยงหรือใช้ VPN

D. ใช้เฉพาะกลางคืน

- **เฉลย:** C

11. หน้าที่ของบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศคืออะไร

A. เป็นหน้าที่ IT เท่านั้น

B. เป็นหน้าที่ทุกคน

C. เป็นหน้าที่ผู้บริหาร

D. ไม่เกี่ยวข้อง

- **เฉลย:** B

12. การเปิดไฟล์แนบจากอีเมลที่ไม่รู้จัก

A. เปิดทันที

B. เปิดดูได้

C. ไม่ควรเปิด

D. ส่งต่อให้เพื่อนเปิด

- **เฉลย:** C

13. หากพบเหตุการณ์ข้อมูลรั่วไหลควรทำอย่างไร

A. ปิดคอม

B. แจ้งหน่วยงานที่รับผิดชอบทันที

C. ไม่ต้องทำอะไร

D. ลบข้อมูล

- **เฉลย:** B

14. การใช้คอมพิวเตอร์องค์กรเพื่อดาวน์โหลดหนังหรือเกม

A. ทำได้

B. ทำได้ถ้าเร็ว

C. ไม่ควรทำ

D. ทำเฉพาะวันหยุด

- **เฉลย:** C

15. การออกจากระบบ (Log out) ควรทำเมื่อใด

A. ไม่ต้องทำ

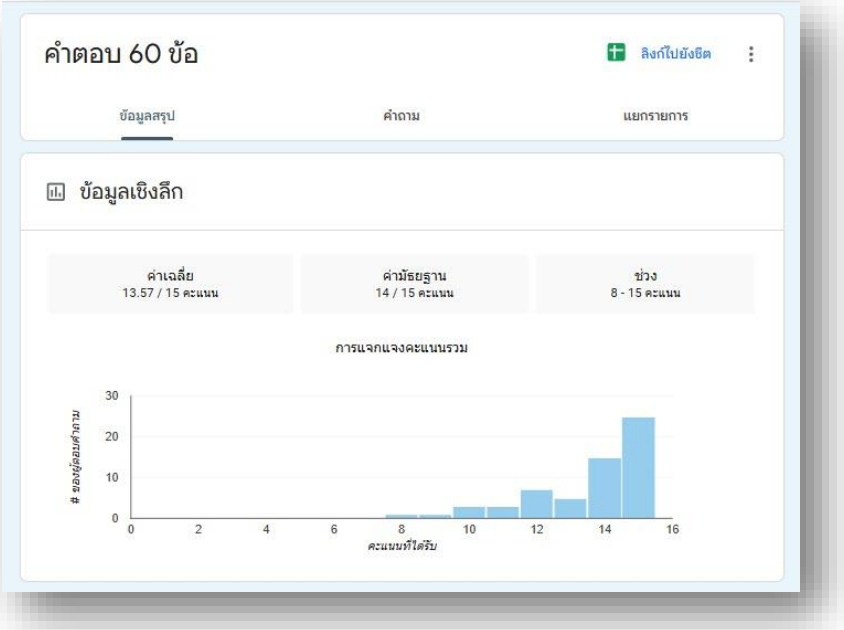
B. เมื่อเลิกใช้งานทุกครั้ง

C. สัปดาห์ละครั้ง

D. เดือนละครั้ง

- **เฉลย:** B

ผลการให้ความรู้ความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศ ดังนี้



จากจำนวนเจ้าหน้าที่ 60 คน

- ได้คะแนน สูงสุด 15 คะแนน 25 คน
- ได้คะแนน 14 คะแนน 15 คน
- ได้คะแนน 13 คะแนน 5 คน
- ได้คะแนน 12 คะแนน 7 คน
- ได้คะแนน 11 คะแนน 3 คน
- ได้คะแนน 10 คะแนน 3 คน
- ได้คะแนน 9 คะแนน 1 คน
- ได้คะแนน 8 คะแนน 1 คน

บุคลากรผ่านการประเมิน คิดเป็น 96.67 %