แบบประเมินผลตนเองก่อนเรียน หน่วยที่ 1

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง **“ความรู้พื้นฐานเกี่ยวกับความมั่นคงปลอดภัยในระบบคอมพิวเตอร์”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใดคือวัตถุประสงค์ของการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์

    ก. เพื่อรักษาความลับ
    ข. เพื่อรักษาความครบถ้วนสมบูรณ์
    ค. เพื่อรักษาสภาพพร้อมใช้งาน
    ง. ข้อ ก. ข. และ ค. ถูก
    จ. ไม่มีคำตอบถูก

2. ช่องโหว่ของระบบคอมพิวเตอร์เกิดขึ้นได้ที่ส่วนใด

    ก. ฮาร์ดแวร์คอมพิวเตอร์
    ข. ซอฟต์แวร์คอมพิวเตอร์
    ค. ข้อมูล
    ง. บุคคล
    จ. ถูกทุกข้อ

3. การกำหนดนโยบายความมั่นคงปลอดภัยของระบบคอมพิวเตอร์อยู่ในขั้นตอนใดของกระบวนการจัดทำระบบบริหารจัดการความมั่นคงตามขั้นตอน PDCA

    ก. Problem
    ข. Plan
    ค. Do
    ง. Check
    จ. Act

4. ข้อใดจัดเป็นมาตรการจัดการความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ทางด้านโครงสร้างความมั่นคงปลอดภัยภายในองค์กร

    ก. การจัดทำเอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร
    ข. การควบคุมการเข้า-ออกในสถานที่บริเวณที่สำคัญ
    ค. การกำหนดหน้าที่ความรับผิดชอบของบุคลากรในการดูแลและป้องกันทรัพย์สินสารสนเทศ
    ง. การตรวจสอบและปรับปรุงนโยบายความมั่นคงปลอดภัยให้มีความทันสมัยอยู่เสมอ
    จ. การจัดให้มีบริเวณเฉพาะสำหรับบุคคลภายนอกในการเข้าถึงหรือส่งมอบผลิตภัณฑ์

5. การกำหนดมาตรการป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินออกไปใช้งานภายนอกองค์กร จัดเป็นมาตรการจัดการความมั่นคงปลอดภัยทางด้านใด
    ก. นโยบายความมั่นคงปลอดภัย
    ข. โครงสร้างความมั่นคงปลอดภัย
    ค. ความมั่นคงปลอดภัยทางกายภาพ
    ง. ความมั่นคงปลอดภัยเกี่ยวกับทรัพยากรบุคคล
    จ. การบริหารจัดการความต่อเนื่องในการดำเนินงาน
6. ข้อใดจัดเป็นการบริหารจัดการความมั่นคงปลอดภัยในทรัพย์สินขององค์กร
    ก. การจัดทำบัญชีทรัพย์สิน
    ข. การระบุผู้เป็นเจ้าของทรัพย์สิน
    ค. การจัดหมวดหมู่ทรัพย์สิน
    ง. การจัดทำป้ายชื่อเพื่อบ่งชี้ระดับชั้นความลับของทรัพย์สิน
    จ. ถูกทุกข้อ
7. การติดตั้งเครื่องสำรองไฟ (UPS) จัดเป็นมาตรการจัดการความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ทางด้านใด
    ก. การจัดหมวดหมู่ทรัพย์สิน
    ข. การบำรุงรักษาอุปกรณ์
    ค. การสำรองข้อมูล
    ง. อุปกรณ์สนับสนุนความมั่นคงปลอดภัยทางกายภาพ
    จ. อุปกรณ์สนับสนุนความมั่นคงปลอดภัยของบริเวณ
8. ข้อใดจัดเป็นมาตรการจัดการความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ที่เกี่ยวกับทรัพยากรบุคคล
    ก. การตรวจสอบคุณสมบัติของผู้สมัคร
    ข. การกำหนดเงื่อนไขในการจ้างงาน
    ค. การกำหนดบทลงโทษทางวินัยกรณีที่มีผู้ละเมิดความมั่นคงปลอดภัย
    ง. การระบุข้อตกลงที่จะไม่เปิดเผยความลับขององค์กรในสัญญาจ้าง
    จ. ถูกทุกข้อ
9. ข้อใดจัดเป็นมาตรการจัดการความมั่นคงปลอดภัยเพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์
    ก. การตรวจสอบสิทธิ์ในการเข้าถึง
    ข. กำหนดให้ผู้ใช้ต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว
    ค. กำหนดให้ผู้ใช้ต้องล็อกเอ้าท์ออกจากระบบทันทีเมื่อเสร็จสิ้นการใช้งาน
    ง. กำหนดให้พนักงานเก็บข้อมูลสำคัญไว้ในสถานที่ที่ปลอดภัย
    จ. ถูกทุกข้อ

10. ข้อใดจัดเป็นมาตรการจัดการความมั่นคงปลอดภัยด้านการจัดหา พัฒนาและบำรุงรักษาระบบสารสนเทศ

ก. การควบคุมการเข้า-ออกในสถานที่บริเวณที่สำคัญ

ข. การกำหนดหน้าที่ความรับผิดชอบของบุคลากรในการดูแลและป้องกันทรัพย์สินสารสนเทศ

ค. การจัดให้มีบริเวณเฉพาะสำหรับบุคคลภายนอกในการเข้าถึงหรือส่งมอบผลิตภัณฑ์

ง. การตรวจสอบข้อมูลนำเข้า ข้อมูลระหว่างการประมวลผล และข้อมูลส่งออก

จ. การตั้งสัญญาณนาฬิกาของระบบให้ตรงตามมาตรฐานเวลาสากล

แบบประเมินผลตนเองหลังเรียน หน่วยที่ 1

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง **“ความรู้พื้นฐานเกี่ยวกับความมั่นคงปลอดภัยในระบบคอมพิวเตอร์”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใดหมายถึง CIA เพื่อการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์

ก. เพื่อรักษาความลับ

ข. เพื่อรักษาความครบถ้วนสมบูรณ์

ค. เพื่อรักษาสภาพพร้อมใช้งาน

ง. ข้อ ก. ข. และ ค. ถูก

จ. ไม่มีคำตอบถูก

2. ไวรัสคอมพิวเตอร์เกิดขึ้นกับช่องโหว่ใดของระบบคอมพิวเตอร์

ก. ฮาร์ดแวร์คอมพิวเตอร์

ข. ซอฟต์แวร์คอมพิวเตอร์

ค. ข้อมูล

ง. บุคคล

จ. ข้อ ข. และ ค. ถูก

3. ในการทบทวนผลการประเมินความเสี่ยงต้องพิจารณาการเปลี่ยนแปลงของสิ่งใดร่วมด้วย

ก. โครงสร้างองค์กร

ข. วัตถุประสงค์และกระบวนการดำเนินงานขององค์กร

ค. เทคโนโลยีที่เกี่ยวข้อง

ง. เหตุการณ์ภายนอก

จ. ถูกทุกข้อ

4. การจัดทำข้อตกลงในเรื่องของการรักษาความลับ จัดเป็นมาตรการจัดการความมั่นคงปลอดภัยทางด้านใด
   - ก. นโยบายความมั่นคงปลอดภัย
   - ข. โครงสร้างความมั่นคงปลอดภัย
   - ค. ความมั่นคงปลอดภัยทางกายภาพ
   - ง. ความมั่นคงปลอดภัยทางด้านสิ่งแวดล้อม
   - จ. การบริหารจัดการความต่อเนื่องในการดำเนินงาน
5. ข้อใดจัดเป็นมาตรการจัดการความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ทางกายภาพ
   - ก. การจัดทำบัญชีทรัพย์สินสารสนเทศ
   - ข. การควบคุมการเข้า-ออกในสถานที่บริเวณที่สำคัญ
   - ค. การจัดทำเอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร
   - ง. การกำหนดหน้าที่ความรับผิดชอบของบุคลากรในการดูแลและป้องกันทรัพย์สินสารสนเทศ
   - จ. การตรวจสอบและปรับปรุงนโยบายความมั่นคงปลอดภัยให้มีความทันสมัยอยู่เสมอ
6. ข้อใดจัดเป็นมาตรการจัดการความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ในประเด็นของการจัดหมวดหมู่ทรัพย์สิน
   - ก. การระบุผู้เป็นเจ้าของทรัพย์สิน
   - ข. การกำหนดความรับผิดชอบของบุคลากรที่ทำหน้าที่ดูแลและป้องกันทรัพย์สิน
   - ค. การจัดทำข้อตกลงการรักษาความลับ
   - ง. การกำหนดระดับการป้องกันที่แตกต่างกันสำหรับทรัพย์สินที่มีชั้นความลับต่างกัน
   - จ. การจัดทำประตูทางเข้า-ออกที่มีการควบคุมหรือติดตั้งสัญญาณเตือนภัย
7. ข้อใดจัดเป็นมาตรการจัดการความมั่นคงปลอดภัยของอุปกรณ์คอมพิวเตอร์
   - ก. ไม่อนุญาตให้ใช้แผ่นดิสก์ในการบูตเครื่อง
   - ข. ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในบริเวณที่ติดตั้งอุปกรณ์คอมพิวเตอร์
   - ค. จัดวางหน้าจอคอมพิวเตอร์โดยหลีกเลี่ยงการมองเห็นข้อมูลที่สำคัญ
   - ง. บำรุงรักษาอุปกรณ์อย่างสม่ำเสมอตามรอบระยะเวลาที่ผู้ผลิตกำหนดไว้
   - จ. ถูกทุกข้อ
8. ข้อใดจัดเป็นมาตรการจัดการความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ที่เกี่ยวกับทรัพยากรบุคคล โดยระบุไว้ในช่วงระหว่างการจ้างงาน
   - ก. การตรวจสอบคุณสมบัติของผู้สมัคร
   - ข. การกำหนดเงื่อนไขในการจ้างงาน
   - ค. การกำหนดบทลงโทษทางวินัยกรณีที่มีผู้ละเมิดความมั่นคงปลอดภัย

ง. การกำหนดให้ต้องคืนทรัพย์สินขององค์กร

จ. การถอดถอนสิทธิ์

9. ข้อใดจัดเป็นมาตรการจัดการความมั่นคงปลอดภัยเพื่อควบคุมการเข้าถึงระบบปฏิบัติการ

ก. การระบุและพิสูจน์ตัวตนของผู้ใช้งาน

ข. กำหนดให้ผู้ใช้ต้องเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้

ค. อนุญาตการใช้งานโปรแกรมยูทิลิตีกับผู้ใช้ที่มีหน้าที่โดยตรงเท่านั้น

ง. กำหนดให้ระบบจำกัดช่วงระยะเวลาการเชื่อมต่อเพื่อเข้าใช้งาน

จ. ถูกทุกข้อ

10. การระบุและจัดลำดับของกระบวนการดำเนินงานที่สำคัญขององค์กร จัดเป็นมาตรการจัดการความมั่นคงปลอดภัยทางด้านใด

ก. โครงสร้างความมั่นคงปลอดภัย

ข. ความมั่นคงปลอดภัยทางกายภาพ

ค. ความมั่นคงปลอดภัยเกี่ยวกับทรัพยากรบุคคล

ง. การบริหารจัดการความต่อเนื่องในการดำเนินงาน

จ. การปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย

เฉลยแบบประเมินผลตนเองหน่วยที่ 1

ก่อนเรียน	**หลังเรียน**
1. ง.	1. ง.
2. จ.	2. จ.
3. ข.	3. จ.
4. ค.	4. ข.
5. ค.	5. ข.
6. จ.	6. ง.
7. ง.	7. จ.
8. จ.	8. ค.
9. จ.	9. จ.
10. ง.	10. ง.

แบบประเมินผลตนเองก่อนเรียนหน่วยที่ 2

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง **“ภัยคุกคามต่อความมั่นคงปลอดภัยในระบบคอมพิวเตอร์”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. เหตุการณ์น้ำท่วมห้องปฏิบัติการคอมพิวเตอร์ในโรงงานอุตสาหกรรม จัดเป็นภัยคุกคามต่อสิ่งใด
   - ก. ฮาร์ดแวร์
   - ข. ซอฟต์แวร์
   - ค. ข้อมูล
   - ง. สายสัญญาณระบบเครือข่าย
   - จ. ถูกทุกข้อ

2. การที่บุคคลบุกรุกระบบคอมพิวเตอร์เพื่อเปลี่ยนสถานะทางการเงินแล้วไปกู้เงินซื้อรถเบนซ์ จัดเป็นภัยคุกคามต่อระบบคอมพิวเตอร์ประเภทใด
   - ก. การเสแสร้ง
   - ข. การอนุมาน
   - ค. การปฏิเสธ
   - ง. การปลอมแปลง
   - จ. การขัดขวางระบบ

3. การกระทำที่ทำให้การควบคุมระบบตกอยู่ในมือผู้ที่ไม่มีสิทธิ์ เรียกว่า
   - ก. การฉ้อฉล
   - ข. การหลอกลวง
   - ค. การแย่งชิงระบบ
   - ง. การขัดขวางการทำงานของระบบ
   - จ. การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

4. การบุกรุกโจมตีระบบคอมพิวเตอร์ในประเทศไทยมีแนวโน้มเป็นอย่างไร เพราะเหตุใด
   - ก. เพิ่มขึ้น เพราะดาวน์โหลดเครื่องมือจากอินเทอร์เน็ตได้ง่าย
   - ข. เพิ่มขึ้น เนื่องจากระบบความปลอดภัยมีจุดอ่อนให้โจมตีมากขึ้น
   - ค. ลดลง เนื่องจากมีระบบความปลอดภัยสูงไม่สามารถบุกรุกได้
   - ง. ลดลง เนื่องจากรัฐมีความเข้มงวดมากขึ้น
   - จ. ลดลง เนื่องจากประชาชนมีคุณธรรม

5. ซอฟต์แวร์สำหรับตรวจจับและหยุดยั้งการทำงานของไวรัสและมัลแวร์อื่นๆ และอาจทำการแก้ไขให้กลับคืนสภาพเดิมได้ด้วย เรียกว่า
   - ก. ไฟร์วอลล์
   - ข. การเข้ารหัสลับข้อมูล
   - ค. ซอฟต์แวร์ป้องกันไวรัส
   - ง. เครือข่ายส่วนตัวเสมือน
   - จ. ระบบตรวจสอบการบุกรุก

6. ข้อใดมีความเสี่ยงว่าจะเป็นบุคคลอันตรายต่อระบบคอมพิวเตอร์
   - ก. พนักงานรักษาความปลอดภัย
   - ข. พนักงานทำความสะอาด
   - ค. พนักงานซ่อมบำรุง
   - ง. พนักงานต้อนรับ
   - จ. ถูกทุกข้อ

7. ข้อใดคือวิธีที่ดีที่สุดในการต่อต้านไวรัสที่คุกคามระบบคอมพิวเตอร์

ก. ซื้อเครื่องใหม่

ข. ลงโปรแกรมใหม่

ค. ลบไฟล์ที่ติดไวรัส

ง. เปลี่ยนฮาร์ดดิสก์

จ. ตรวจจับไฟล์ที่ติดไวรัส

8. ข้อใดคือความหมายของแฮกเกอร์หมวกขาว

ก. กลุ่มผู้สำรวจระบบมือใหม่

ข. กลุ่มผู้สำรวจระบบเพื่อแก้ไขจุดอ่อน

ค. กลุ่มผู้สำรวจระบบเพื่อบุกรุกทำลาย

ง. กลุ่มผู้สำรวจระบบโดยมิได้รับอนุญาต

จ. กลุ่มผู้สำรวจระบบโดยใช้สคริปต์สำเร็จรูป

9. ช่องทางลับสำหรับเข้าใช้งานระบบที่ผู้พัฒนาระบบอาจสร้างช่องไว้สำหรับการเข้าบำรุงรักษาโดยที่ไม่ต้องผ่านระบบรักษาความมั่นคงปกติ เรียกว่า

ก. แบกดอร์

ข. ลอจิกบอมบ์

ค. ม้าโทรจัน

ง. โมบายโค้ด

จ. มัลแวร์ลูกผสม

10. ข้อใดคือความแตกต่างระหว่างหนอนอินเทอร์เน็ตกับไวรัส

ก. หนอนอินเทอร์เน็ตแก้ไขได้ง่ายกว่าไวรัส

ข. หนอนอินเทอร์เน็ตป้องกันได้ แต่ไวรัสป้องกันไม่ได้

ค. หนอนอินเทอร์เน็ตแพร่กระจายได้ช้า แต่ไวรัสแพร่กระจายได้เร็ว

ง. หนอนอินเทอร์เน็ตโจมตีแบบสุ่ม แต่ไวรัสโจมตีที่เมนเฟรมเป็นจุดแรก

จ. หนอนอินเทอร์เน็ตแพร่ได้ด้วยตัวเอง แต่ไวรัสต้องมีการเรียกใช้ซอฟต์แวร์ที่มันฝังตัวอยู่

แบบประเมินผลตนเองหลังเรียนหน่วยที่ 2

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง **“ภัยคุกคามต่อความมั่นคงปลอดภัยในระบบคอมพิวเตอร์”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. เมื่อดาราดังนำคอมพิวเตอร์ไปซ่อม ช่างได้ลักลอบคัดลอกภาพลับไว้ไถเงิน จัดเป็นภัยคุกคามต่อสิ่งใด

ก. ฮาร์ดแวร์
ข. ซอฟต์แวร์
ค. ข้อมูล
ง. สายสัญญาณ
จ. ระบบเครือข่าย

2. การที่บุคคลบุกรุกระบบคอมพิวเตอร์เพื่อเปลี่ยนผลการเรียนให้เพิ่มขึ้น จัดเป็นภัยคุกคามต่อระบบคอมพิวเตอร์ประเภทใด

ก. การเสแสร้ง
ข. การอนุมาน
ค. การปฏิเสธ
ง. การปลอมแปลง
จ. การขัดขวางระบบ

3. การที่บุคคลภายในองค์กรจงใจเปิดเผยข้อมูลให้รั่วไหลสู่บุคคลภายนอกเรียกว่า

ก. การฉ้อฉล
ข. การหลอกลวง
ค. การแย่งชิงระบบ
ง. การขัดขวางการทำงานของระบบ
จ. การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

4. การบุกรุกโจมตีระบบคอมพิวเตอร์ในอนาคตมีแนวโน้มเป็นอย่างไร เพราะเหตุใด

ก. เพิ่มขึ้น เพราะดาวน์โหลดเครื่องมือจากอินเทอร์เน็ตได้ง่าย
ข. เพิ่มขึ้น เนื่องจากระบบความปลอดภัยมีจุดอ่อนให้โจมตีมากขึ้น
ค. ลดลง เนื่องจากมีระบบความปลอดภัยสูงไม่สามารถบุกรุกได้
ง. ลดลง เนื่องจากรัฐมีความเข้มงวดมากขึ้น
จ. ลดลง เนื่องจากประชาชนมีคุณธรรม

5. ระบบสำหรับตรวจสอบว่าการสื่อสารที่เกิดขึ้นเป็นไปตามเงื่อนไขที่กำหนดหรือไม่ หากไม่ใช่จะกรองการสื่อสารนั้นออกไป เรียกว่า

ก. ไฟร์วอลล์
ข. การเข้ารหัสลับข้อมูล
ค. ซอฟต์แวร์ป้องกันไวรัส
ง. เครือข่ายส่วนตัวเสมือน
จ. ระบบตรวจสอบการบุกรุก

6. ข้อใดมีความเสี่ยงว่าจะเป็นบุคคลอันตรายต่อระบบคอมพิวเตอร์

ก. พนักงานรักษาความปลอดภัย
ข. พนักงานทำความสะอาด
ค. พนักงานซ่อมบำรุง
ง. พนักงานต้อนรับ
จ. ถูกทุกข้อ

7. ข้อใดคือวิธีที่ดีที่สุดในการต่อต้านไวรัสที่คุกคามระบบคอมพิวเตอร์

ก. ซื้อเครื่องใหม่
ข. ลงโปรแกรมใหม่
ค. ลบไฟล์ที่ติดไวรัส
ง. เปลี่ยนฮาร์ดดิสก์
จ. ตรวจจับไฟล์ที่ติดไวรัส

8. ข้อใดคือความหมายของแฮกเกอร์หมวกดำ

ก. กลุ่มผู้สำรวจระบบมือใหม่
ข. กลุ่มผู้สำรวจระบบเพื่อแก้ไข
ค. กลุ่มผู้สำรวจระบบเพื่อบุกรุกทำลาย
ง. กลุ่มผู้สำรวจระบบโดยได้รับอนุญาต
จ. กลุ่มผู้สำรวจระบบโดยใช้สคริปต์สำเร็จรูป

9. โค้ดร้ายที่แฝงอยู่ในโปรแกรมปกติ ซึ่งโค้ดอันตรายนี้จะทำงานก็ต่อเมื่อมีตัวกระตุ้นบางอย่าง คล้ายกับการระเบิดเมื่อถึงเวลาที่กำหนด เรียกว่า

ก. แบกดอร์
ข. ลอจิกบอมบ์
ค. ม้าโทรจัน
ง. โมบายโค้ด
จ. มัลแวร์ลูกผสม

10. ข้อใดคือมัลแวร์

ก. ลอจิกบอมบ์
ข. แบกดอร์
ค. ไวรัส
ง. หนอน
จ. ถูกทุกข้อ

เฉลยแบบประเมินตนเองหน่วยที่ 2

ก่อนเรียน	หลังเรียน
1. จ	1. ค
2. ง	2. ง
3. ค	3. จ
4. ก	4. ก
5. ค	5. ก
6. จ	6. จ
7. จ	7. จ
8. ข	8. ค
9. ก	9. ข
10. จ	10.จ

แบบประเมินผลตนเองก่อนเรียนหน่วยที่ 3

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง **“การบริหารความมั่นคงปลอดภัยและความเสี่ยงในระบบคอมพิวเตอร์”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใดคือความหมายของการรักษาความลับ
   - ก. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการเปลี่ยนแปลงต่อผู้ได้รับอนุญาตเท่านั้น
   - ข. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการเปลี่ยนแปลงต่อผู้เป็นเจ้าของเท่านั้น
   - ค. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากสภาพใช้งานได้ต่อผู้ได้รับอนุญาตเท่านั้น
   - ง. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการแสดงต่อผู้ได้รับอนุญาตเท่านั้น
   - จ. ความสามารถในการเข้าถึงต่อผู้ได้รับอนุญาตเท่านั้น
2. ข้อใดคือความหมายของการรักษาความครบถ้วนถูกต้อง
   - ก. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากสภาพใช้งานได้ต่อผู้ได้รับอนุญาตเท่านั้น
   - ข. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากสภาพใช้งานได้ต่อผู้เป็นเจ้าของเท่านั้น
   - ค. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการเปลี่ยนแปลงต่อผู้ได้รับอนุญาตเท่านั้น
   - ง. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการแสดงต่อผู้ได้รับอนุญาตเท่านั้น
   - จ. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการแสดงต่อผู้เป็นเจ้าของเท่านั้น
3. ข้อใดคือความหมายของการรักษาสภาพพร้อมใช้งาน
   - ก. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากสภาพใช้งานได้ต่อผู้เป็นเจ้าของเท่านั้น
   - ข. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากสภาพใช้งานได้ต่อผู้ได้รับอนุญาตเท่านั้น
   - ค. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการเปลี่ยนแปลงต่อผู้ได้รับอนุญาตเท่านั้น
   - ง. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการแสดงต่อผู้ได้รับอนุญาตเท่านั้น
   - จ. การป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการแสดงต่อผู้เป็นเจ้าของเท่านั้น
4. ข้อใดคือความหมายของการอนุญาต (Authorization)
   - ก. ความสามารถในสภาพใช้งานได้ต่อผู้ได้รับอนุญาตเท่านั้น

ข. ความสามารถในการแสดงต่อผู้เป็นเจ้าของเท่านั้น

ค. ความสามารถในการแสดงต่อผู้ได้รับอนุญาตเท่านั้น

ง. ความสามารถในการเข้าถึงต่อผู้ได้รับอนุญาตเท่านั้น

5. ความสามารถในการเปลี่ยนแปลงข้อมูลต่อผู้ได้รับอนุญาตเท่านั้น ข้อใดคือความหมายของภาวะปฏิเสธไม่ได้

ก. ภาวะที่ระบบถูกติดตั้งระบบความมั่นคงปลอดภัยที่ทำการบันทึกการกระทำใดเกิดโดยผู้ใช้ใดๆ

ข. ภาวะที่ระบบถูกติดตั้งระบบความมั่นคงปลอดภัยที่แสดงการกระทำใดๆ ของผู้ใช้ที่ผ่านการพิสูจน์ตัวตนแล้ว

ค. ภาวะที่ระบบถูกติดตั้งระบบความมั่นคงปลอดภัยที่ระบุสิทธิ์การกระทำของผู้ใช้ใดๆ

ง. ภาวะที่ระบบถูกติดตั้งระบบความมั่นคงปลอดภัยที่สามารถระบุหรือติดตามได้ว่าการกระทำใดเกิดขึ้นโดยผู้ใช้ใด

จ. ภาวะที่ระบบถูกติดตั้งระบบความมั่นคงปลอดภัยที่ไม่สามารถแสดงการกระทำใดๆ ของผู้ใช้ใดๆ

6. ข้อใดคือความหมายของโอกาสเสี่ยงภัย

ก. ความอ่อนไหวของความเสียหายของสินทรัพย์ที่เกิดจากภัยคุกความไม่ว่าเจตนาหรือไม่

ข. ความน่าจะเป็นที่ช่องโหว่จะถูกเอาเปรียบโดยผู้บุกรุกโดยเจตนา

ค. ความน่าจะเป็นที่ช่องโหว่จะถูกเอาเปรียบโดยภัยคุกคามโดยเจตนา

ง. ความน่าจะเป็นที่ช่องโหว่จะถูกเอาเปรียบโดยผู้บุกรุกโดยไม่เจตนา

จ. ความน่าจะเป็นที่ช่องโหว่จะถูกเอาเปรียบโดยภัยคุกคามโดยไม่เจตนา

7. ข้อใดคือความหมายของความเสี่ยง

ก. ภาวะที่ภัยคุกคามอาจจะเกิดขึ้นต่อช่องโหว่ที่ก่อให้เกิดความเสียหายต่อสินทรัพย์

ข. ภัยคุกคามอาจจะเกิดขึ้นต่อช่องโหว่ที่ก่อให้เกิดความเสียหายต่อสินทรัพย์

ค. ช่องโหว่ที่ก่อให้เกิดความเสียหายต่อสินทรัพย์

ง. ความน่าจะเป็นที่ภัยคุกคามที่จะเกิดขึ้นต่อช่องโหว่ที่ก่อให้เกิดความเสียหายต่อสินทรัพย์

จ. ความน่าจะเป็นที่จะเกิดช่องโหว่ที่ก่อให้เกิดความเสียหายต่อสินทรัพย์

8. ข้อใดคือความหมายของสิ่งป้องกัน

ก. สิ่งของ อุปกรณ์ วิธีการ หรือเทคนิคใดที่สามารถลดช่องโหว่

ข. สิ่งของ อุปกรณ์ วิธีการ หรือเทคนิคใดที่สามารถป้องกันหรือต่อกรกับภัยคุกคามของระบบได้

ค. สิ่งของ อุปกรณ์ วิธีการ หรือเทคนิคใดที่ใช้ในการปรับปรุงการทำงานของระบบตามนโยบายความมั่นคงปลอดภัย

ง. สิ่งของ อุปกรณ์ วิธีการ หรือเทคนิคใดที่ใช้ในการปรับเปลี่ยนโครงสร้างระบบตามนโยบายความมั่นคงปลอดภัย

จ. ถูกทุกข้อ

9. ข้อใดกล่าวถูกต้องเกี่ยวกับการวิเคราะห์ความเสี่ยงเชิงปริมาณ

ก. เป็นการวิเคราะห์ที่สามารถประเมินค่าทุกอย่างได้

ข. เป็นการวิเคราะห์ที่รวมมูลค่าทางความคิดและความรู้สึกด้วย
ค. เป็นการวิเคราะห์ที่ประมาณความเสียหายออกมาได้ทุกรูปแบบ
ง. เป็นการวิเคราะห์ที่แสดงออกมาในรูปแบบของตัวเลขทางการเงิน
จ. ถูกทุกข้อ

10. ข้อใดถูกต้องเกี่ยวกับการวิเคราะห์ความเสี่ยงเชิงคุณภาพ
ก. เป็นการวิเคราะห์ที่แสดงออกมาในรูปแบบของตัวเลขทางการเงิน
ข. เป็นการวิเคราะห์ที่ใช้การประเมินมูลค่าของสินทรัพย์เป็นหลัก
ค. เป็นการวิเคราะห์ที่รวมมูลค่าทางความคิดและความรู้สึกด้วย
ง. เป็นการวิเคราะห์ที่ประมาณความเสียหายออกมาในรูปของการเงินเพียงอย่างเดียว
จ. ถูกทุกข้อ

แบบประเมินผลตนเองหลังเรียนหน่วยที่ 3

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง **“การบริหารความมั่นคงปลอดภัยและความเสี่ยงในระบบคอมพิวเตอร์”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

ใช้ตัวเลือกต่อไปนี้ ตอบคำถามข้อ 1 - 5
ก. การรักษาความลับ (Confidentiality)
ข. การรักษาความครบถ้วนถูกต้อง (Integrity)
ค. การรักษาสภาพพร้อมใช้งาน (Availability)
ง. การอนุญาต (Authorization)
จ. ภาวะปฏิเสธไม่ได้ (non-repudiation)

1. ข้อใดหมายถึงการป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการแสดงต่อผู้ได้รับอนุญาตเท่านั้น
2. ข้อใดมีความหมายถึงการป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากการเปลี่ยนแปลงต่อผู้ได้รับอนุญาตเท่านั้น
3. ข้อใดมีความหมายถึงการป้องกันทรัพยากรใดๆ ขององค์กรให้จำกัดอยู่เฉพาะจากสภาพใช้งานได้ต่อผู้ได้รับอนุญาตเท่านั้น
4. ข้อใดมีความหมายถึงความสามารถในการเข้าถึงต่อผู้ได้รับอนุญาตเท่านั้น
5. ข้อใดหมายถึงภาวะที่ระบบถูกติดตั้งระบบความมั่นคงปลอดภัยที่แสดงการกระทำใดๆ ของผู้ใช้ที่ผ่านการพิสูจน์ตัวตนแล้ว

ใช้ตัวเลือกต่อไปนี้ ตอบคำถามข้อ 6 - 8

ก. โอกาสเสี่ยงภัย
ข. ความเสี่ยง
ค. สิ่งป้องกัน
ง. สินทรัพย์
จ. ช่องโหว่

6. ข้อใดหมายถึงความอ่อนไหวของความเสียหายของสินทรัพย์ที่เกิดจากภัยคุกคามไม่ว่าเจตนาหรือไม่

7. ข้อใดหมายถึงความน่าจะเป็นที่ภัยคุกคามที่จะเกิดขึ้นต่อช่องโหว่ที่ก่อให้เกิดความเสียหายต่อสินทรัพย์

8. ข้อใดหมายถึงสิ่งของ อุปกรณ์ วิธีการ หรือเทคนิคใดที่สามารถลดช่องโหว่ ป้องกันหรือต่อกรกับภัยคุกคามของระบบได้

9. ข้อใดกล่าว**ไม่ถูกต้อง**เกี่ยวกับการวิเคราะห์ความเสี่ยงเชิงปริมาณ
ก. เป็นการวิเคราะห์ที่ถูกแสดงออกมาในรูปแบบของตัวเลขทางการเงิน
ข. เป็นการวิเคราะห์ที่ใช้การประเมินมูลค่าของสินทรัพย์เป็นหลัก
ค. เป็นการวิเคราะห์ที่รวมมูลค่าทางความคิดและความรู้สึกด้วย
ง. เป็นการวิเคราะห์ที่ประมาณความเสียหายออกมาในรูปของการเงินเพียงอย่างเดียว
จ. ทุกข้อกล่าวไม่ถูกต้อง

10. ข้อใดกล่าว**ไม่ถูกต้อง**เกี่ยวกับการวิเคราะห์ความเสี่ยงเชิงคุณภาพ
ก. เป็นการวิเคราะห์ที่สามารถประเมินค่าทุกอย่างได้
ข. เป็นการวิเคราะห์ที่รวมมูลค่าทางความคิดและความรู้สึกด้วย
ค. เป็นการวิเคราะห์ที่ประมาณความเสียหายออกมาได้ในหลายรูปแบบ
ง. เป็นการวิเคราะห์ที่ถูกแสดงออกมาในรูปแบบของตัวเลขทางการเงิน
จ. ทุกข้อกล่าวไม่ถูกต้อง

เฉลยแบบประเมินผลตนเองหน่วยที่ 3

ก่อนเรียน	**หลังเรียน**
1. ง.	1. ก.
2. ค.	2. ข.
3. ข.	3. ค.
4. ง.	4. ง.
5. ข.	5. จ.
6. ก.	6. ก.
7. ง.	7. ข.

8. ข.
9. ง.
10. ค.

8. ค.
9. ค.
10. ง.

แบบประเมินผลตนเองก่อนเรียน หน่วยที่ 4

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง **"วิทยาการรหัสลับ"**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. วิทยาการรหัสลับ (cryptography) เป็นศาสตร์ของการศึกษาเรื่องใด
   ก. การเข้ารหัสข้อมูลเพื่อปกปิดหรือซ่อนความหมายของข้อมูล
   ข. การถอดรหัสข้อมูลที่ถูกเข้ารหัส
   ค. การทำลายความน่าเชื่อถือของอัลกอริธึมการเข้ารหัส
   ง. การวิเคราะห์ข้อมูลที่ถูกเข้ารหัส
   จ. การพัฒนาวิธีการถอดรหัสให้มีความแม่นยำ
2. การพัฒนาอัลกอริธึมการเข้ารหัสลับโดยปกปิดไม่ให้ผู้อื่นรู้มีความเหมาะสมหรือไม่
   ก. เหมาะสม เนื่องจากจะไม่มีผู้อื่นล่วงรู้อัลกอริธึมนี้ได้
   ข. เหมาะสม เนื่องจากอัลกอริธึมที่พัฒนาขึ้นจะไม่มีข้อบกพร่อง
   ค. เหมาะสม เนื่องจากกุญแจที่สร้างจากอัลกอริธึมที่พัฒนาขึ้นจะมีความมั่นคงปลอดภัย
   ง. ไม่เหมาะสม เนื่องจากอัลกอริธึมที่พัฒนาขึ้นอาจมีข้อบกพร่องอย่างร้ายแรง และมีความเป็นไปได้ที่ผู้วิเคราะห์รหัสลับจะค้นพบข้อบกพร่องนั้น
   จ. ข้อ ก. ข. และ ค. ถูก
3. การพัฒนาอัลกอริธึมการเข้ารหัสลับแบบเปิดเผยอัลกอริธึมมีข้อดีอย่างไร
   ก. มีกลุ่มนักวิเคราะห์รหัสทำงานเชิงวิชาการในการค้นหาและแจ้งข้อบกพร่องของอัลกอริธึม
   ข. อัลกอริธึมที่ถูกนำมาประยุกต์ใช้ผ่านการวิเคราะห์ความมั่นคงปลอดภัยมาเป็นอย่างดี
   ค. จุดอ่อนและข้อบกพร่องของอัลกอริธึมการเข้ารหัสแบบเปิดเผยมักจะได้รับการแก้ไข
   ง. ข้อ ก. ข. และ ค. ถูก
   จ. ข้อ ก. ข. และ ค. ผิด
4. ข้อใดคือลักษณะเด่นของอัลกอริธึมการเข้ารหัสแบบกุญแจสมมาตร
   ก. ขนาดของกุญแจมีขนาด 56 บิต
   ข. ขนาดของกุญแจมีขนาด 128 บิต
   ค. กุญแจสำหรับเข้าและถอดรหัสเป็นกุญแจคนละดอก
   ง. กุญแจสำหรับเข้าและถอดรหัสเป็นกุญแจคนละดอกโดยเป็นกุญแจที่ถูกสร้างมาคู่กัน
   จ. ไม่มีข้อจำกัดเกี่ยวกับการจัดการกุญแจเมื่อมีผู้ใช้งานในระบบจำนวนมาก
5. อัลกอริธึมการเข้ารหัสในข้อใดเป็นอัลกอริธึมการเข้ารหัสแบบแทนที่ยุคแรกๆ
   ก. RC4
   ข. RSA

ค. Caesar Cipher
ง. DES
จ. Triple DES

6. ไซเฟอร์เท็กซ์ (cipher text) คืออะไร
   ก. ข้อความในไซเบอร์สเปซ
   ข. ข้อความที่ผ่านการเข้ารหัสโดยอัลกริธึมการเข้ารหัส
   ค. การวิเคราะห์การเข้ารหัส
   ง. อัลกอริธึมการเข้ารหัสแบบหนึ่ง
   จ. ข้อความปกติ
7. MD5 คืออะไร
   ก. Musical Director 5
   ข. Mutable Digest 5
   ค. แฮชชิ่งอัลกอริธึมรูปแบบหนึ่ง
   ง. อัลกอริธึมการเข้ารหัสลับแบบไม่ต้องใช้กุญแจรหัส
   จ. ไม่มีคำตอบถูก
8. ข้อมูลหรือข้อความที่มีเป็นชุดเดียวกัน หากได้รับการเปลี่ยนแปลงแก้ไขแล้วควรให้ผลของแฮชด้วยอัลกอริธึมเดียวกัน หมายถึงข้อใด
   ก. ผลแฮชที่ได้ควรมีค่าต่างกันเล็กน้อย
   ข. ผลแฮชที่ได้ควรมีค่าไม่แตกต่างกัน
   ค. ค่าแฮชที่ได้ควรมีค่าต่างกันอย่างมาก
   ง. มีความเป็นไปได้สูงที่ผลแฮชจะมีค่าเดียวกัน
   จ. ไม่มีคำตอบถูก
9. ขั้นตอนวิธีการเข้ารหัสแบบดีอีเอส (DES) เป็นอัลกอริธึมการเข้ารหัสแบบใด
   ก. แบบกุญแจสมมาตร
   ข. แบบกุญแจอสมมาตร
   ค. แบบทีละตัว (Stream Cipher)
   ง. แบบที่พัฒนาโดยดิฟฟี่-เฮลแมน
   จ. ไม่มีคำตอบถูก
10. อัลกอริธึมการเข้ารหัสลับแบบเออีเอส (AES) เป็นอัลกอริธึมการเข้ารหัสแบบบล็อกที่ถูกพัฒนาเพื่อ
   ก. ใช้แทนอัลกอริธึมการเข้ารหัสแบบซีซาร์
   ข. ใช้แทนอัลกอริธึมการเข้ารหัสแบบกุญแจอสมมาตร

ค. ใช้แทนอัลกอริธึมการแลกเปลี่ยนกุญแจ

ง. ใช้แทนอัลกอริธึมการเข้ารหัสแบบดีอีเอส

จ. ใช้แทนอัลกอริธึมการเข้ารหัสแบบอาร์ซีโฟร์

แบบประเมินผลตนเองหลังเรียน หน่วยที่ 4

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง **“วิทยาการรหัสลับ”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. อัลกอริธึมการเข้ารหัสแบบซีซาร์มีความอ่อนไหวเมื่อเปรียบเทียบกับอัลกอริธึมการเข้ารหัสลับในปัจจุบันเนื่องจาก
   ก. ถูกใช้มาเป็นเวลานาน
   ข. ให้ไซเฟอร์เท็กซ์ที่มีความซ้ำกันสูง ผู้วิเคราะห์อาจสามารถวิเคราะห์ข้อความปกติได้โดยง่าย
   ค. เป็นอัลกอริธึมแบบทีละตัว
   ง. ปลอดภัยจากการแทรกข้อความ
   จ. การพิสูจน์สิทธิ์สามารถกระทำได้ง่าย
2. แฮชชิ่งอัลกอริธึมที่ดีควรให้ผลของการแฮชที่มีลักษณะใด
   ก. มีโอกาสซ้ำกันน้อยมากหรือไม่มีโอกาสซ้ำกันเลย
   ข. เป็นการทำงานทางเดียวไม่สามารถย้อนกลับได้
   ค. เป็นการทำงานสองทางสามารถย้อนกลับได้
   ง. ข้อ ก. และ ข. ถูก
   จ. ข้อ ก. และ ค. ถูก
3. ขนาดกุญแจของอัลกอริธึมการเข้ารหัสแบบดีอีเอส (DES) มีขนาดเท่าใด
   ก. 32 บิต
   ข. 56 บิต
   ค. 64 บิต
   ง. 128 บิต
   จ. 256 บิต
4. การสลับที่และการแทนที่ในอัลกอริธึมการเข้ารหัสทำให้การวิเคราะห์อัลกอริธึมการเข้ารหัสทำได้ยาก เนื่องจากการสลับที่และแทนที่ทำให้เกิดข้อใด
   ก. ความสับสนของข้อมูลไซเฟอร์เท็กซ์
   ข. ความกระจายของข้อมูลไซเฟอร์เท็กซ์
   ค. ความซับซ้อนของข้อมูลไซเฟอร์เท็กซ์

ง. ความสับสนและการกระจายของข้อมูลไซเฟอร์เท็กซ์

จ. ไม่มีคำตอบถูก

5. หากท่านจำเป็นต้องเลือกอัลกอริธึมสำหรับการเข้ารหัสลับ ท่านจะเลือกอัลกอริธึมใดในการใช้งานระหว่าง ดีอีเอส (DES) และเออีเอส (AES) เพราะเหตุใด

   ก. DES เนื่องจากปลอดภัยต่อการวิเคราะห์รหัส

   ข. DES เนื่องจากกุญแจมีขนาดเล็กทำงานได้รวดเร็ว

   ค. AES เนื่องจากทำงานเป็นบล็อกที่มีขนาดใหญ่กว่าและทำงานได้เร็วกว่า

   ง. AES เนื่องจากมีความมั่นคงปลอดภัยสูงกว่าและขนาดของกุญแจมากกว่า

   จ. DES เนื่องจากมีข้อบกพร่องจากเทคนิคการวิเคราะห์กุญแจรหัสแต่เพียงอย่างเดียว

6. หากบุคคลจำนวน n คนต้องการสื่อสารกันอย่างมั่นคงปลอดภัยโดยการเข้ารหัสข้อความที่สื่อสารถึงกันด้วยอัลกอริธึมการเข้ารหัสแบบสมมาตร ต้องใช้กุญแจรหัสจำนวนเท่าใด

   ก. $\frac{(n-1)}{2}$

   ข. $\frac{n*(n-1)}{2}$

   ค. $\frac{(n)}{2}$

   ง. $\frac{n*(n-1)}{2n}$

   จ. $\frac{n^2*(n-1)}{2}$

7. อัลกอริธึมการเข้ารหัสแบบทีละตัว (stream cipher) มีความเร็วมากกว่าอัลกอริธึมการเข้ารหัสแบบเป็นกลุ่ม (block cipher) เพราะเหตุใด

   ก. ไม่สนใจการตรวจสอบข้อผิดพลาดของการทำงาน

   ข. การเปลี่ยนข้อความปกติเป็นไซเฟอร์เท็กซ์จะทำเป็นกลุ่มที่มีขนาดใหญ่ทำให้ทำงานได้เร็วกว่า

   ค. การเปลี่ยนข้อความปกติเป็นไซเฟอร์เท็กซ์จัดทำเรียงตามลำดับก่อนหลังไม่จำเป็นต้องรอให้ครบขนาด

   ง. การเปลี่ยนแปลงไซเฟอร์เท็กซ์ไม่สามารถตรวจสอบได้

   จ. ไซเฟอร์เท็กซ์ที่ได้มีขนาดเล็ก

8. ข้อใดเป็นหัวใจหลักของการใช้งานอัลกอริธึมการเข้ารหัส

   ก. ใช้อัลกอริธึมการเข้ารหัสที่มีข้อบกพร่องน้อยที่สุด

   ข. ไม่ใช้อัลกอริธึมการเข้ารหัสที่พัฒนาด้วยตนเอง

   ค. ใช้อัลกอริธึมการเข้ารหัสที่กุญแจรหัสมีขนาดใหญ่

ง. ใช้กุญแจรหัสที่ยากต่อการคาดเดาและไม่ปรากฏในพจนานุกรม

จ. ถูกทุกข้อ

9. การแลกเปลี่ยนกุญแจแบบดิฟฟี่-เฮลแมน ใช้หลักการใด

ก. การกระจาย

ข. สร้างกุญแจแล้วส่งให้กับผู้รับที่ต้องการผ่านช่องทางการสื่อสาร

ค. ไม่ต้องมีการรับส่งกุญแจผ่านช่องทางการสื่อสาร

ง. รับส่งกุญแจผ่านช่องทางการสื่อสารโดยการเข้ารหัสกุญแจ

จ. ไม่มีคำตอบถูก

10. เพราะเหตุใดการใช้งานการแลกเปลี่ยนกุญแจแบบดิฟฟี่-เฮลแมนจึงมีความมั่นคงปลอดภัยสูง

ก. การคำนวณกุญแจที่ใช้ในการเข้ารหัสเป็นไปไม่ได้ หากเลือกใช้จำนวนเฉพาะที่มีขนาดเหมาะสม

ข. กุญแจสามารถดักรับและคำนวณย้อนกลับได้แม้ว่าจะเลือกจำนวนเฉพาะที่มีค่าสูงมากก็ตาม

ค. การแยกตัวประกอบเพื่อหาค่าของกุญแจทำได้ง่าย ทำให้มีความรวดเร็วในการทำงาน

ง. การแลกเปลี่ยนกุญแจแบบนี้ถูกนำไปประยุกต์ใช้ในการเข้ารหัสลับแบบพับบลิกคีย์

จ. ถูกทุกข้อ

เฉลยแบบประเมินผลตนเองหน่วยที่ 4

ก่อนเรียน	**หลังเรียน**
11. ก.	11. ข.
12. ง.	12. ง.
13. ง.	13. ข.
14. ง.	14. ง.
15. ค.	15. ง.
16. ข.	16. ข.
17. ค.	17. ค.
18. ค.	18. จ.
19. ก.	19. ค.
20. ง.	20. ก.

แบบประเมินผลตนเองก่อนเรียนหน่วยที่ 5

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง **“ลายมือชื่อดิจิทัล”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

1. ข้อใดเป็นความหมายที่ถูกต้องที่สุดของลายมือชื่อดิจิทัลในแง่มุมของนักกฎหมาย
   ก. ตัวเลขใดๆ ที่ต้องเกิดจากการคำนวณและถูกเพิ่มเข้าไปในข้อมูล
   ข. ตัวอักษรใดๆ ที่เกิดจากการเลือกและถูกเพิ่มเข้าไปในชุดข้อมูล
   ค. ชุดข้อมูลใดๆ ที่ต้องเกิดจากการคำนวณและถูกเพิ่มเข้าไปในชุดข้อมูล
   ง. สัญลักษณ์ใดๆ ที่ต้องเกิดจากการเลือกและถูกเพิ่มเข้าไปในชุดข้อมูล
   จ. สัญลักษณ์ใดๆ ที่เกิดจากการเลือกและถูกเพิ่มเข้าไปในชุดข้อมูล
2. ข้อใดเป็นความหมายของลายมือชื่อดิจิทัลในแง่มุมของนักรักษาความปลอดภัยบนระบบคอมพิวเตอร์
   ก. ตัวเลขใดๆ ที่เกิดจากการคำนวณและถูกเพิ่มเข้าไปในข้อมูล
   ข. ตัวอักษรใดๆ ที่เกิดจากการเลือกและถูกเพิ่มเข้าไปในชุดข้อมูล
   ค. สัญลักษณ์ใดๆ ที่เกิดจากการเลือกและถูกเพิ่มเข้าไปในชุดข้อมูล
   ง. ชุดข้อมูลใดๆ ที่เกิดจากการคำนวณและถูกเพิ่มเข้าไปในชุดข้อมูล
   จ. ถูกทุกข้อ
3. ข้อใดคือวัตถุประสงค์ของการใช้ลายมือชื่อดิจิทัล
   ก. ใช้เป็นหลักฐาน ใช้ในการอนุมัติ และใช้เพื่อความสมบูรณ์ของเอกสาร
   ข. ใช้เป็นหลักฐาน ใช้ในการอนุมัติ และใช้ในการสร้างระเบียบแบบแผน
   ค. ใช้เป็นหลักฐาน ใช้เพื่อความครบถ้วนของเอกสาร และใช้ในการสร้างระเบียบแบบแผน
   ง. ใช้เพื่อความครบถ้วนของเอกสาร ใช้ในการอนุมัติ และใช้ในการสร้างระเบียบแบบแผน
   จ. ใช้เป็นหลักฐาน ใช้เพื่อความสมบูรณ์ของเอกสาร และใช้เพื่อความสมเหตุสมผล
4. ข้อใด**ไม่ใช่**พื้นฐานในการสร้างลายมือชื่อดิจิทัล
   ก. เจ้าของลายมือชื่อดิจิทัลจำเป็นต้องเป็นผู้มีความรู้เรื่องการสร้างลายมือชื่อดิจิทัล
   ข. ผู้ที่กระทำการลงลายมือชื่อดิจิทัลจำเป็นต้องเป็นผู้ที่ได้รับการรับรองแล้วว่าเชื่อถือได้
   ค. เอกสารที่นำมาลงลายมือชื่อนี้ต้องไม่สามารถถูกปลอมแปลงได้
   ง. ลายมือชื่อสามารถระบุถึงตัวตนของเจ้าของข้อความต้นฉบับได้
   จ. ทุกข้อคือพื้นฐานในการสร้างลายมือชื่อดิจิทัล
5. ข้อใด**ไม่ใช่**หลักการทำงานพื้นฐานของลายมือชื่อดิจิทัล
   ก. การสร้างกุญแจ
   ข. การสร้างลายมือชื่อ
   ค. การตรวจสอบใบรับรองของผู้สร้างลายมือชื่อ
   ง. การตรวจสอบลายมือชื่อ
   จ. ทุกข้อเป็นหลักการทำงานพื้นฐานของลายมือชื่อดิจิทัล

6. ข้อใดคือคุณสมบัติของลายมือชื่อดิจิทัล
   ก. การรักษาความลับ การรักษาความครบถ้วนถูกต้อง และ การรักษาสภาพพร้อมใช้งาน
   ข. การรักษาความลับ การรักษาความครบถ้วนถูกต้อง และ การปฏิเสธไม่ได้
   ค. การพิสูจน์ตัวตน การรักษาความครบถ้วนถูกต้อง และ การรักษาสภาพพร้อมใช้งาน
   ง. การรักษาความลับ การพิสูจน์ตัวตน และ การปฏิเสธไม่ได้
   จ. การพิสูจน์ตัวตน การรักษาความครบถ้วนถูกต้อง และ การปฏิเสธไม่ได้
7. ข้อใดกล่าว**ไม่ถูกต้อง**เกี่ยวกับการย่อยข้อความ
   ก. ใช้ในการเพิ่มความเร็วในการสร้างลายมือชื่อดิจิทัล
   ข. ใช้ในการลดขนาดข้อมูลต้นฉบับก่อนนำไปทำการสร้างลายมือชื่อ
   ค. ใช้ในการเพิ่มประสิทธภาพในการรักษาความสมบูรณ์ของข้อมูล
   ง. ใช้ในการลดขนาดของลายมือชื่อดิจิทัล
   จ. สร้างความเหมาะสมให้กับข้อความต้นฉบับและการเข้ารหัส
8. ข้อใดต่อไปนี้**ไม่ใช่**ขนาดของลายมือชื่อดิจิทัลที่ได้จากการสร้างลายมือชื่อแบบ DMDC
   ก. 192 บิต
   ข. 128 บิต
   ค. 64 บิต
   ง. 32 บิต
   จ. 8 บิต
9. ข้อใดคือลายมือชื่อดิจิทัลที่ได้จากการสร้างลายมือชื่อแบบ MD5
   ก. “9691 EB0C”
   ข. “7B1B 1C00 A1D3 4E7C”
   ค. “3BD7 3D8C 145D E697 8C94 4855 5042 3D7D”
   ง. “4887 8397 9801 D679 394B D834 28C2 8E41 2B8D EE05”
   จ. “4887 8397 9801 D679 394B D834 28C2 8E41 2B8D EE05 7B1B 1C00”
10. ข้อใดต่อไปนี้คือขนาดของลายมือชื่อดิจิทัลที่ได้จากการสร้างลายมือชื่อแบบ SHA-1
    ก. 160 บิต
    ข. 128 บิต
    ค. 64 บิต
    ง. 32 บิต
    จ. 16 บิต

แบบประเมินผลตนเองหลังเรียนหน่วยที่ 5

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง **“ลายมือชื่อดิจิทัล”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

1. ข้อใดเป็นความหมายที่ถูกต้องที่สุดของลายมือชื่อดิจิทัลในแง่มุมของนักกฎหมาย
   ก. ตัวเลขใดๆ ที่เกิดจากการคำนวณและถูกเพิ่มเข้าไปในข้อมูล
   ข. ตัวอักษรใดๆ ที่เกิดจากการเลือกและถูกเพิ่มเข้าไปในชุดข้อมูล
   ค. ชุดข้อมูลใดๆ ที่เกิดจากการคำนวณและถูกเพิ่มเข้าไปในชุดข้อมูล
   ง. สัญลักษณ์ใดๆ ที่เกิดจากการเลือกและถูกเพิ่มเข้าไปในชุดข้อมูล
   จ. สัญลักษณ์ใดๆที่เกิดจากการเลือกและถูกเพิ่มเข้าไปในชุดข้อมูล
2. ข้อใดเป็นความหมายของลายมือชื่อดิจิทัลในแง่มุมของนักรักษาความปลอดภัยบนระบบคอมพิวเตอร์
   ก. ตัวเลขใดๆ ที่เกิดจากการคำนวณและถูกเพิ่มเข้าไปในข้อมูล
   ข. ตัวอักษรใดๆ ที่เกิดจากการเลือกและถูกเพิ่มเข้าไปในชุดข้อมูล
   ค. สัญลักษณ์ใดๆ ที่เกิดจากการเลือกและถูกเพิ่มเข้าไปในชุดข้อมูล
   ง. ชุดข้อมูลใดๆ ที่เกิดจากการคำนวณและถูกเพิ่มเข้าไปในชุดข้อมูล
   จ. ถูกทุกข้อ
3. ข้อใด**ไม่ใช่**วัตถุประสงค์ของการใช้ลายมือชื่อดิจิทัล
   ก. ใช้เป็นหลักฐาน
   ข. ใช้ในการอนุมัติ
   ค. ใช้เพื่อความสมบูรณ์ของเอกสาร
   ง. ใช้ในการสร้างระเบียบแบบแผน
   จ. ใช้ในการสร้างประสิทธิภาพและความสมเหตุสมผล
4. ข้อใดต่อไปนี้เป็นพื้นฐานในการสร้างลายมือชื่อดิจิทัล
   - a) ผู้ที่กระทำการลงลายมือชื่อแบบดิจิทัลจำเป็นต้องเป็นผู้ที่ได้รับการรับรองแล้วว่าเชื่อถือได้
   - b) เอกสารที่นำมาลงลายมือชื่อนี้ต้องไม่สามารถถูกปลอมแปลงได้
   - c) ลายมือชื่อดิจิทัลต้องสามารถถอดรหัสออกมาได้ข้อความต้นฉบับ
   - d) ลายมือชื่อสามารถระบุถึงตัวตนของเจ้าของข้อความต้นฉบับได้

   ก. a b และ c
   ข. a b และ d
   ค. a c และ d
   ง. b c และ d
   จ. a b c และ d

5. ข้อใดคือหลักการทำงานพื้นฐานของลายมือชื่อดิจิทัล
   ก. การสร้างกุญแจ การสร้างลายมือชื่อ
   ข. การสร้างกุญแจ การสร้างลายมือชื่อ การตรวจสอบใบรับรองของผู้สร้างลายมือชื่อ
   ค. การสร้างกุญแจ การสร้างลายมือชื่อ การตรวจสอบลายมือชื่อ
   ง. การสร้างกุญแจ การสร้างลายมือชื่อ การตรวจสอบใบรับรองของผู้สร้างลายมือชื่อ การตรวจสอบลายมือชื่อ
   จ. การสร้างกุญแจ การสร้างลายมือชื่อ การตรวจสอบลายมือชื่อ การพิสูจน์ตัวตนของเจ้าของข้อความ
6. ข้อใด**ไม่ใช่**คุณสมบัติของลายมือชื่อดิจิทัล
   ก. การพิสูจน์ตัวตน
   ข. การปฏิเสธไม่ได้
   ค. การรักษาความครบถ้วนถูกต้อง
   ง. การรักษาความลับ
   จ. ทุกข้อคือคุณสมบัติของลายมือชื่อดิจิทัล
7. ข้อใดคือประโยชน์ของการย่อยข้อความต้นฉบับก่อนนำไปสร้างลายมือชื่อ
   ก. ช่วยเพิ่มประสิทธิภาพในการส่งข้อมูล
   ข. ช่วยในการลดขนาดของลายมือชื่อดิจิทัล
   ค. ช่วยให้ง่ายในการถอดรหัสลายมือชื่อดิจิทัลมาเป็นข้อความต้นฉบับ
   ง. ช่วยให้ง่ายในการตรวจสอบผู้ทำการสร้างลายมือชื่อดิจิทัล
   จ. ใช้ในการเพิ่มประสิทธิภาพในการรักษาความสมบูรณ์ของข้อมูล
8. ข้อใดถูกต้องเกี่ยวกับการสร้างลายมือชื่อดิจิทัลแบบ DMDC
   ก. สามารถเลือกได้ว่ามีขนาดเป็น 16 32 64 หรือ 128 บิต
   ข. มีขนาดเพียงแค่ 128 บิตเท่านั้น
   ค. มีขนาดเพียงแค่ 160 บิตเท่านั้น
   ง. มีขนาดคงที่ไม่ขึ้นอยู่กับขนาดของข้อมูล
   จ. มีขนาดไม่คงที่ขึ้นอยู่กับขนาดของข้อมูล
9. ข้อใดถูกต้องเกี่ยวกับการสร้างลายมือชื่อดิจิทัลแบบ MD-5
   ก. สามารถเลือกได้ว่ามีขนาดเป็น 8 32 64 หรือ 128 บิต
   ข. มีขนาดเพียงแค่ 128 บิตเท่านั้น
   ค. มีขนาดเพียงแค่ 160 บิตเท่านั้น
   ง. มีขนาดเพียงแค่ 192 บิตเท่านั้น
   จ. มีขนาดไม่คงที่ขึ้นอยู่กับขนาดของข้อมูล
10. ข้อใดคือลายมือชื่อดิจิทัลที่ได้จากการสร้างลายมือชื่อแบบ SHA-1

ก. “28C2 8E41 2B8D EE05 3BD7 3D8C 145D E697 8C94 4855 5042 3D7D”

ข. “4887 8397 9801 D679 394B D834 28C2 8E41 2B8D EE05”

ค. “3BD7 3D8C 145D E697 8C94 4855 5042 3D7D”

ง. “7B1B 1C00 A1D3 4E7C”

จ. “9691 EB0C”

เฉลยแบบประเมินผลตนเองหน่วยที่ 5

ก่อนเรียน	**หลังเรียน**
21. จ.	21. จ.
22. ง.	22. ง.
23. ข.	23. ค.
24. ก.	24. ข.
25. ค.	25. ค.
26. จ.	26. ง.
27. ง.	27. จ.
28. ก.	28. ก.
29. ค.	29. ข.
30. ก.	30. ข.

แบบประเมินผลตนเองก่อนเรียนหน่วยที่ 8

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง “**ความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์**”

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ระบบเครือข่ายอินเทอร์เน็ตจัดเป็นระบบเครือข่ายประเภทใด
   ก. ระบบเครือข่ายคอมพิวเตอร์ส่วนบุคคล
   ข. ระบบเครือข่ายคอมพิวเตอร์กึ่งส่วนบุคคล
   ค. ระบบเครือข่ายคอมพิวเตอร์ที่ไว้ใจได้
   ง. ระบบเครือข่ายคอมพิวเตอร์สาธารณะ
   จ. ถูกทุกข้อ
2. แนวป้องกันระบบเครือข่ายคอมพิวเตอร์ภายนอกประกอบด้วยอะไรบ้าง
   ก. ระบบเครือข่ายคอมพิวเตอร์แบบเขตปลอดทหาร
   ข. เราท์เตอร์ภายนอก ไฟร์วอลล์
   ค. เครื่องพร็อกซีเซิร์ฟเวอร์ เครื่องเว็บเซิร์ฟเวอร์
   ง. เราท์เตอร์ภายใน ไฟร์วอลล์
   จ. เครื่องไคลเอนท์ เครื่องเซิร์ฟเวอร์ประมวลผล
3. เทคโนโลยีที่ช่วยให้ระบบเครือข่ายคอมพิวเตอร์ในองค์กรสามารถส่งข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ที่ไม่น่าเชื่อถือหรือระบบเครือข่ายคอมพิวเตอร์ที่ใช้งานร่วมกันได้อย่างปลอดภัย เรียกว่า เทคโนโลยีใด
   ก. การสร้างอุโมงค์เครือข่าย
   ข. ระบบเครือข่ายแบบเขตปลอดทหาร
   ค. การเข้าถึงระบบเครือข่ายระยะไกล
   ง. ระบบเครือข่ายคอมพิวเตอร์ท้องถิ่นเสมือน
   จ. การแปลหมายเลขแอดเดรสเครือข่าย
4. เพราะเหตุใด *การไม่บันทึกการทำงาน* จึงจัดเป็นช่องโหว่ที่สำคัญที่สุด เมื่อเกิดการตัดขาดการเชื่อมต่ออุโมงค์เครือข่าย
   ก. เครื่องลูกข่ายสร้างเส้นทางการเชื่อมต่อระหว่างระบบเครือข่ายภายในและระบบเครือข่ายอินเทอร์เน็ตอีกเส้นทางไปพร้อมๆ กับเส้นทางเดิม
   ข. ผู้บุกรุกอาศัยการรับรองตัวจริงขโมยข้อมูลสำคัญ และสร้างจุดเชื่อมต่อเพื่อเจาะระบบเครือข่ายตำแหน่งใหม่ก่อนที่การรับรองตัวตนจะหมดอายุหรือปิดตัวลง
   ค. ข้อมูลสำคัญถูกย้ายไปเก็บที่ฮาร์ดดิสก์ฝั่งของเครื่องผู้ใช้ปลายทาง
   ง. ระบบรักษาความมั่นคงปลอดภัยของศูนย์กลางไม่ได้ครอบคลุมเครื่องคอมพิวเตอร์ของผู้ใช้ปลายทาง
   จ. ไม่มีรายงานใดๆ แจ้งแก่เครื่องเซิร์ฟเวอร์ต้นทางว่าเครื่องคอมพิวเตอร์ของผู้ใช้งานปลายทางถูกโจมตี
5. ข้อใดไม่จัดเป็นภัยคุกคามภายนอกระบบเครือข่ายคอมพิวเตอร์ทางกายภาพ
   ก. การตัดขาดการเชื่อมต่อ การปฏิเสธการให้บริการ
   ข. พายุสุริยะ บุคคลภายนอก
   ค. น้ำท่วม แผ่นดินไหว
   ง. ไฟไหม้ ฟ้าผ่า
   จ. การลักลอบขโมยอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์

6. ข้อใดเป็นการรักษาความมั่นคงปลอดภัยโดยใช้เทคนิคการบีบอัดไฟล์เอกสาร เพื่อทำให้ไฟล์เอกสารมีขนาดเล็กลงและยากต่อการถอดรหัสได้เอง
   - ก. เอสเอสแอล
   - ข. การเข้ารหัสลับเอกสาร
   - ค. พีจีพี
   - ง. ลายเซ็นดิจิทัล
   - จ. ซีเคียวร์เอชทีทีพี

7. ข้อใดเป็นแนวปฏิบัติที่ดีที่สุดในการรักษาความมั่นคงปลอดภัยแก่เครื่องเวิร์คสเตชัน
   - ก. บันทึกงานลงฮาร์ดดิสก์สำรองทุกครั้งที่ประมวลผลเสร็จ
   - ข. ตั้งกฎไฟร์วอลล์เพื่อบล็อคแพ็กเกตข้อมูลที่ถูกส่งมาจากผู้บุกรุก
   - ค. การตั้งรหัสผ่านที่มีความซับซ้อน
   - ง. การกำหนดสิทธิ์การเข้าถึงข้อมูลระดับต่างๆ แก่ผู้ใช้งาน
   - จ. ล็อกออฟ หรือล็อคหน้าจอคอมพิวเตอร์ หากหยุดการใช้งานหรือออกจากที่ปฏิบัติงานชั่วคราว

8. กระบวนการพิสูจน์ตัวตนโดยโพรโทคอลเคอร์เบอโรส์แบบพื้นฐานที่ไม่ซับซ้อน มีลักษณะสำคัญอย่างไร
   - ก. มีผู้ใช้งานได้หลายยูเซอร์ ไม่จำกัดงานบริการ แต่ต้องผ่านเครื่องเซิร์ฟเวอร์เพียง 1 เครื่องเท่านั้น
   - ข. มีผู้ใช้งานได้ 1 ยูเซอร์ ต้องการใช้บริการ 1 งาน ผ่านเครื่องเซิร์ฟเวอร์ได้ไม่จำกัด
   - ค. มีผู้ใช้งานเพียง 1 ยูเซอร์ ต้องการใช้บริการ 1 งาน ผ่านเครื่องเซิร์ฟเวอร์ 1 เครื่อง
   - ง. มีผู้ใช้งานได้หลายยูเซอร์ ต้องการใช้บริการ 1 งาน ผ่านเครื่องเซิร์ฟเวอร์ 1 เครื่อง
   - จ. ไม่จำกัดจำนวนผู้ใช้งาน จำนวนงานบริการและจำนวนเครื่องเซิร์ฟเวอร์

9. โพรโทคอลใดถูกใช้งานเป็นโพรโทคอลพิสูจน์ตัวตนทั่วๆ ไป เช่น การพิสูจน์ตัวตนโดยใช้สมาร์ทการ์ด เคอร์เบอโรส์ กุญแจสาธารณะ และรหัสผ่าน
   - ก. โพรโทคอลอีเอพี
   - ข. โพรโทคอลอีเอพีโอเวอร์แลน
   - ค. โพรโทคอลเรเดียส
   - ง. โพรโทคอลทีเอซีเอซีเอสพลัส
   - จ. ไม่มีคำตอบถูก

10. ข้อใดไม่ใช่โพรโทคอลการรักษาความมั่นคงปลอดภัยเลเยอร์ที่ 2
   - ก. L2F
   - ข. L2TP
   - ค. PPTP
   - ง. IPSec
   - จ. ดาต้าลิงค์โพรโทคอล

แบบประเมินผลตนเองหลังเรียนหน่วยที่ 8

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง “**ความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์**”

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใดกล่าวผิดเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์สาธารณะ

ก. เช่น ระบบเครือข่ายอินเทอร์เน็ต

ข. เป็นระบบเครือข่ายที่เชื่อถือไม่ได้

ค. เป็นระบบเครือข่ายที่ไม่เป็นที่รู้จัก

ง. ข้อมูลที่ไหลเวียนบนระบบเครือข่ายเป็นข้อมูลที่ไม่สำคัญมากนัก

จ. ทุกข้อกล่าวถูกต้อง

2. แนวป้องกันระบบเครือข่ายคอมพิวเตอร์ภายในประกอบด้วยอะไรบ้าง

ก. เราท์เตอร์ภายนอก ไฟร์วอลล์

ข. เราท์เตอร์ภายใน ระบบเครือข่ายแบบเขตปลอดทหาร

ค. เครื่องเมลล์เซิร์ฟเวอร์ เครื่องพร็อกซีเซิร์ฟเวอร์

ง. ข้อ ก. และ ค. ถูก

จ. ข้อ ข. และ ค. ถูก

3. หากระบบรักษาความปลอดภยของเครื่องโฮสต์ใน DMZ ถูกบุกรุก จะส่งผลกระทบต่อระบบเครือข่ายคอมพิวเตอร์อย่างไร

ก. เซิร์ฟเวอร์ฐานข้อมูลสำคัญขององค์กรไม่เกิดความเสียหายแต่อย่างใด

ข. ระบบเครือข่ายคอมพิวเตอร์ภายในเกิดความเสียหายทั้งหมด

ค. เว็บเซิร์ฟเวอร์ เซิร์ฟเวอร์ฐานข้อมูลเกิดความเสียหาย

ง. เมลล์เซิร์ฟเวอร์ พร็อกซีเซิร์ฟเวอร์ สามารถทำงานได้โดยปกติ

จ. ไฟร์วอลล์หรือเราท์เตอร์ภายในยอมให้ผู้บุกรุกเข้ามาแต่โดยดี

4. ข้อใดเป็นลักษณะของช่องโหว่การสื่อสารประเภท *การแยกอุโมงค์เครือข่าย*

ก. ระบบรักษาความมั่นคงปลอดภัยของศูนย์กลางไม่ได้ครอบคลุมเครื่องคอมพิวเตอร์ของผู้ใช้ปลายทาง

ข. ผู้บุกรุกอาศัยการรับรองตัวตนเพื่อขโมยข้อมูลสำคัญ และสร้างจุดเชื่อมต่อเพื่อเจาะระบบเครือข่ายตำแหน่งใหม่ก่อนที่การรับรองตัวตนจะหมดอายุหรือปิดตัวลง

ค. เครื่องลูกข่ายสร้างเส้นทางการเชื่อมต่อระหว่างระบบเครือข่ายภายในและระบบเครือข่ายอินเทอร์เน็ตอีกเส้นทางไปพร้อมๆ กับเส้นทางเดิม

ง. ข้อมูลสำคัญถูกย้ายไปเก็บที่ฮาร์ดดิสก์ฝั่งของเครื่องผู้ใช้ปลายทาง

จ. ไม่มีรายงานใดๆ แจ้งแก่เครื่องเซิร์ฟเวอร์ต้นทางว่าเครื่องคอมพิวเตอร์ของผู้ใช้งานปลายทางถูกโจมตี

5. ข้อใดแตกต่างจากพวก

ก. การปลอมแปลงหมายเลขไอพี

ข. การตัดขาดการเชื่อมต่อ

ค. การปลอมแปลงเส้นทางจราจรโดยดัดแปลงข้อความ ICMP

ง. การปฏิเสธการให้บริการ

จ. การทำให้ระบบเครือข่ายล่ม

6. การรักษาความมั่นคงปลอดภัยเบื้องต้นแบบ *การเข้ารหัสลับการเชื่อมต่อ* มีลักษณะเป็นอย่างไร

ก. ผู้ส่งเข้ารหัสเอกสาร ส่วนผู้รับเป็นผู้ถอดรหัสเอกสาร ผู้ใช้งานทุกคนที่มีอีเมลแอดเดรสสามารถใช้งานการเข้ารหัสลับเอกสารได้

ข. เข้ารหัสลับข้อมูลก่อนส่งไประบบเครือข่ายคอมพิวเตอร์ แล้วผู้รับปลายทางใช้ซอฟต์แวร์เอสเอสแอลแปลงข้อความกลับเป็นเอกสารที่สามารถอ่านได้

ค. การป้องกันไม่ให้ผู้อื่นสามารถอ่านเนื้อความข้อมูลที่ส่งไปได้โดยการผสมผสานเนื้อความของไฟล์ใหม่ให้ซับซ้อน ผู้ใช้งานอื่นไม่สามารถเข้าใจได้

ง. การเข้ารหัสลับการส่งข้อมูลระหว่างระบบเครือข่ายคอมพิวเตอร์ฝั่งต้นทางและปลายทางที่มีการรับส่งข้อมูลระหว่างกันบ่อยๆ ทั้ง 2 ฝั่งตกลงใช้กุญแจเข้ารหัสที่มีความซับซ้อนเป็นพิเศษร่วมกัน

จ. ผู้ส่งทำการเข้ารหัสลับเอกสารโดยใช้กุญแจส่วนบุคคล ส่วนผู้รับปลายทางทำการถอดรหัสลับเอกสารโดยใช้กุญแจสาธารณะ

7. การทบทวนการจัดเส้นทางใหม่ของโมเด็ม และตรวจสอบการบริการต่างๆ ของระบบเครือข่ายคอมพิวเตอร์จากภายนอกผ่านโมเด็มเป็นประจำ เป็นการรักษาความมั่นคงปลอดภัยให้แก่โมเด็มประเภทใด

ก. การป้องกันการรั่วไหลของข้อมูล

ข. การตรวจสอบการร้องขอเพื่อเข้าถึงระบบเครือข่าย

ค. การเรียกกลับโมเด็ม

ง. การใช้อิเล็กทรอนิกส์การ์ด

จ. การใช้ระบบล็อกอิเล็กทรอนิกส์

8. กระบวนการพิสูจน์ตัวจริงโดยโพรโทคอลเคอร์เบอโรส์แบบใช้ตั๋วผ่านทาง มีลักษณะสำคัญอย่างไร

ก. มีผู้ใช้งานเพียง 1 ยูเซอร์ ต้องการใช้บริการ 1 งานผ่านเครื่องเซิร์ฟเวอร์ 1 เครื่อง

ข. มีผู้ใช้งานได้ 1 ยูเซอร์ ต้องการใช้บริการ 1 งานผ่านเครื่องเซิร์ฟเวอร์ได้ไม่จำกัด

ค. มีผู้ใช้งานได้หลายยูเซอร์ ต้องการใช้บริการ 1 งานผ่านเครื่องเซิร์ฟเวอร์ 1 เครื่อง

ง. มีผู้ใช้งานได้ 1 ยูเซอร์ ไม่จำกัดจำนวนงานบริการและจำนวนเครื่องเซิร์ฟเวอร์

จ. ไม่จำกัดจำนวนผู้ใช้งาน งานบริการ และเครื่องเซิร์ฟเวอร์

9. โพรโทคอลใดเป็นโพรโทคอลพิสูจน์ตัวตนสำหรับการเข้าถึงระยะไกลมายังระบบเครือข่ายแลนกลาง

ก. โพรโทคอลอีเอพี

ข. โพรโทคอลอีเอพีโอเวอร์แลน

ค. โพรโทคอลเรเดียส

ง. โพรโทคอลทีเอซีเอซีเอสพลัส

จ. ไม่มีคำตอบถูก

10. ข้อใดเป็นโพรโทคอลการรักษาความมั่นคงปลอดภัยเลเยอร์ที่ 3

ก. ดาต้าลิงค์โพรโทคอล

ข. IPSec

ค. L2F

ง. L2TP

จ. PPTP

เฉลยแบบประเมินผลตนเองหน่วยที่ 8

ก่อนเรียน	หลังเรียน
1. ง.	1. จ.
2. ข.	2. จ.
3. ก.	3. ก.
4. จ.	4. ค.
5. ก.	5. ค.
6. ค.	6. ง.
7. จ.	7.ก.
8. ค.	8. ง.
9. ก.	9. ข.
10.ง.	10. ข.

แบบประเมินผลตนเองก่อนเรียน หน่วยที่ 9

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง "**เทคโนโลยีการรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์**"

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใดระบุความหมายของไฟร์วอลล์ได้ถูกต้องที่สุด
   ก. ระบบคอมพิวเตอร์ที่มีหน้าที่จัดการการจราจรบนระบบเครือข่าย
   ข. ซอฟต์แวร์ที่ทำหน้าที่กรองแพ็กเกตข้อมูลที่เข้ามาในระบบเครือข่าย
   ค. ฮาร์ดแวร์ที่ทำหน้าที่กรองแพ็กเกตข้อมูลที่ส่งออกไปยังระบบเครือข่ายภายนอก
   ง. กำแพงกั้นภัยคุกคามต่างๆ ที่มาจากภายนอก
   จ. ศูนย์กลางการจัดการความมั่นคงปลอดภัยในระบบเครือข่ายคอมพิวเตอร์ที่ประกอบด้วยกลุ่มฮาร์ดแวร์และซอฟต์แวร์
2. แพ็กเกตข้อมูลประเภทใดบ้างที่จะถูกตรวจสอบโดยไฟร์วอลล์ที่ระดับชั้นเน็ตเวิร์คหรือแพ็กเกตฟิลเตอร์ริงไฟร์วอลล์
   ก. แพ็กเกตข้อมูลที่อยู่ไอพีต้นทางและปลายทาง
   ข. แพ็กเกตข้อมูลอินเทอร์เน็ตโพรโทคอล
   ค. แพ็กเกตข้อมูลที่อยู่ไอพีของผู้ส่งและผู้รับ เซสชันโพรโทคอลต่างๆ หมายเลขพอร์ตแอพพลิเคชันต้นทางและปลายทาง
   ง. แพ็กเกตข้อมูลโพรโทคอลการรักษาความมั่นคงปลอดภัยในระบบเครือข่ายคอมพิวเตอร์
   จ. แพ็กเกตข้อมูลการเชื่อมต่อและการถ่ายโอนระหว่างต้นทางไปยังปลายทาง
3. Back Door คืออะไร มีบทบาทอย่างไรในการรักษาความมั่นคงปลอดภัยในระบบเครือข่ายคอมพิวเตอร์
   ก. เป็นเส้นทางที่ผู้บุกรุกใช้เข้ามาโจมตีระบบโดยอยู่ด้านหลังไฟร์วอลล์
   ข. เป็นช่องทางที่ผู้บุกรุกทำการฝังไว้ก่อนหน้าเพื่อเข้ามาเจาะระบบเครือข่ายคอมพิวเตอร์ โดยที่ไฟร์วอลล์ไม่สามารถตรวจเจอได้
   ค. ช่องทางเข้าออกในระบบเครือข่ายคอมพิวเตอร์โดยติดตั้งอยู่ด้านหลังเราท์เตอร์
   ง. เป็นอุปกรณ์ที่ใช้ในการตรวจสอบการเข้าถึงเครื่องคอมพิวเตอร์โฮสต์จากผู้ใช้ภายนอก
   จ. เป็นการใช้เครื่องคอมพิวเตอร์แม่ข่ายเพียงเครื่องเดียวแยกการเชื่อมต่อระหว่างระบบเครือข่ายอินทราเน็ตและระบบเครือข่ายอินเทอร์เน็ต
4. ไฟร์วอลล์ที่อาศัยระบบเครือข่ายรอบนอกทำหน้าที่เป็นไฟร์วอลล์แยกระบบเครือข่ายอินทราเน็ตออกจากระบบเครือข่ายอินเทอร์เน็ต คือไฟร์วอลล์ประเภทใด
   ก. สกรีนซับเน็ตไฟร์วอลล์
   ข. ดูอัลโฮมโฮสต์ไฟร์วอลล์
   ค. สกรีนโฮสต์ไฟร์วอลล์
   ง. ซอฟต์แวร์ไฟร์วอลล์
   จ. ไฟร์วอลล์บนระบบปฏิบัติการ
5. Rule sets คืออะไร มีหน้าที่การทำงานอย่างไร
   ก. การบล็อคการจราจรเครือข่ายขาเข้าไม่ให้ผู้บุกรุกเข้ามาเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์
   ข. บอร์ดควบคุมโครงสร้างการทำงานของไฟร์วอลล์
   ค. ผลิตภัณฑ์ไฟร์วอลล์ประเภทหนึ่งที่สามารถสร้างข้อกำหนดกฎการอนุญาตการเข้าถึงข้อมูลได้เอง
   ง. กลุ่มหมายเลขไอพีที่ถูกสกัดกั้นไม่ให้เข้ามาในระบบเครือข่าย

จ. ชุดของข้อกำหนดไฟร์วอลล์ เพื่อใช้ในการตรวจสอบหรือกรองแพ็กเกตข้อมูล

---

6. ข้อใดระบุหน้าที่ของ NIDS ได้ถูกต้องที่สุด
    - ก. ระบบตรวจจับการบุกรุกระบบเครือข่ายคอมพิวเตอร์
    - ข. ระบบตรวจจับการบุกรุกระบบเครือข่ายคอมพิวเตอร์ผ่านเครือข่าย
    - ค. ระบบตรวจจับการบุกรุกระบบเครือข่ายคอมพิวเตอร์ผ่านโฮสต์
    - ง. ระบบหยั่งผลการตรวจสอบการรักษาความมั่นคงปลอดภัย
    - จ. ระบบตรวจจับความผิดปกติในระบบเครือข่ายคอมพิวเตอร์
7. ข้อใดเป็นผลที่เกิดจากการรีเซ็ตทีซีพี
    - ก. ทำให้ตัวตรวจจับสามารถบันทึกการจราจรเครือข่ายที่ส่งไปมาระหว่างผู้บุกรุกระบบและเครื่องที่ถูกโจมตีได้
    - ข. เกิดการตั้งกฎไฟร์วอลล์เพื่อบล็อคแพ็กเกตข้อมูลที่ถูกส่งมาจากผู้บุกรุก
    - ค. เกิดการสร้างไอพีลวงเพื่อเข้ามาโจมตีระบบ
    - ง. เกิดการยกเลิกเซสชันทีซีพีบนเครื่องที่ถูกบุกรุก
    - จ. เกิดการมอนิเตอร์บันทึกการเข้าออกระบบ
8. การตรวจจับที่ทำงานร่วมกับเราท์เตอร์และไฟร์วอลล์เพื่อบล็อคการจราจรที่บุกรุกเข้ามาในเครือข่าย หรือตัดการเชื่อมต่อกับหมายเลขไอพีของผู้บุกรุก เป็นการตรวจจับประเภทใด
    - ก. การตรวจจับแบบแอคทิฟ
    - ข. การตรวจจับแบบแพสซิฟ
    - ค. ฮันนีพอต
    - ง. การตรวจจับความผิดปกติ
    - จ. การจับคู่รูปแบบ
9. การที่ระบบทรัสต์สามารถปิดช่องทางการโจมตีระบบเครือข่ายได้ เนื่องจากมีการทำงานร่วมกับอุปกรณ์ใด
    - ก. ไฟร์วอลล์
    - ข. เราท์เตอร์
    - ค. รายการควบคุมการเข้าถึง
    - ง. สวิตซ์
    - จ. ถูกทุกข้อ
10. นักเจาะระบบสามารถใช้การประมวลผลแบบกลุ่มเมฆช่องทางใดบ้างในการเข้าโจมตีระบบเครือข่าย
    - ก. การส่งอีเมลล์ การสนทนาออนไลน์
    - ข. การพิสูจน์ตัวจริงและการอนุญาต
    - ค. การหาแหล่งข้อมูล การให้บริการข้อมูล การรันแอพพลิเคชันต่างๆ
    - ง. การรักษาความเป็นส่วนตัวของผู้ใช้งาน
    - จ. การแบ่งปันไฟล์ การอัพโหลดไฟล์

แบบประเมินผลตนเองหลังเรียน หน่วยที่ 9

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง “**เทคโนโลยีการรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์**”

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใดเรียงลำดับการติดตั้งไฟร์วอลล์ในระบบเครือข่ายคอมพิวเตอร์จาก**ภายในไปภายนอก**ได้ถูกต้อง
    - ก. เครื่องคอมพิวเตอร์โฮสต์ เครือข่ายอินทราเน็ต ไฟร์วอลล์ เราท์เตอร์ เครือข่ายอินเทอร์เน็ต
    - ข. เครือข่ายอินเทอร์เน็ต เราท์เตอร์ ไฟร์วอลล์ เครือข่ายอินทราเน็ต เครื่องคอมพิวเตอร์โฮสต์
    - ค. เครือข่ายอินเทอร์เน็ต เราท์เตอร์ เครือข่ายอินทราเน็ต เครื่องคอมพิวเตอร์โฮสต์ ไฟร์วอลล์
    - ง. เครือข่ายอินเทอร์เน็ต เครือข่ายอินทราเน็ต เครื่องคอมพิวเตอร์โฮสต์ เราท์เตอร์ ไฟร์วอลล์
    - จ. เราท์เตอร์ ไฟร์วอลล์ เครือข่ายอินเทอร์เน็ต เครือข่ายอินทราเน็ต เครื่องคอมพิวเตอร์โฮสต์
2. ข้อใดเป็นข้อดีของการใช้ไฟร์วอลล์แบบสเตตฟูลแพ็กเกตฟิลเตอร์ริงไฟร์วอลล์
    - ก. เป็นไฟร์วอลล์ที่ตรวจสอบเนื้อหาแพ็กเกตข้อมูลทั้งหมด
    - ข. ใช้เวลากรองข้อมูลนานกว่าไฟร์วอลล์แบบแพ็กเกตฟิลเตอร์ริงไฟร์วอลล์
    - ค. มีการบันทึกสถานะแพ็กเกตข้อมูลที่เข้ามาก่อนหน้านี้
    - ง. ข้อ ก. และ ข้อ ค. ถูก
    - จ. ข้อ ข. และ ข้อ ค. ถูก
3. ข้อใดเป็นลักษณะสำคัญของดูอัลโฮมโฮสต์ไฟร์วอลล์
    - ก. เป็นไฟร์วอลล์ที่ใช้เครื่องแม่ข่ายเพียงเครื่องเดียวแบ่งแยกระบบเครือข่ายภายในออกจากเครือข่ายภายนอก
    - ข. เครื่องคอมพิวเตอร์แม่ข่ายสามารถเชื่อมต่อเข้ากับระบบเครือข่ายได้สองระบบ โดยอาศัยการ์ดเน็ตเวิร์ค
    - ค. เป็นไฟร์วอลล์ที่ระดับชั้นแอพพลิเคชันหรือที่ระดับชั้นเซอร์กิต
    - ง. เป็นไฟร์วอลล์ที่มีความมั่นคงปลอดภัยสูง โดยมีพร็อกซีซอฟต์แวร์ทำหน้าที่ควบคุมการไหลของแพ็กเกตข้อมูล
    - จ. ถูกทุกข้อ
4. ข้อใดเป็นคุณสมบัติที่สำคัญที่สุดสำหรับชุดของข้อกำหนดไฟร์วอลล์**สำหรับจุดเข้าถึงหลายจุด**
    - ก. สามารถรักษาการทำงานให้สอดคล้องกับไฟร์วอลล์อื่นๆ และทราบสถานะการทำงานได้
    - ข. จำกัดการเข้าถึงข้อมูลและระบบเครือข่าย
    - ค. มีการให้รายละเอียดชุดของข้อกำหนดไฟร์วอลล์ต่างๆ มากที่สุดเท่าที่จะทำได้ เพื่อใช้ปรับเปลี่ยนชุดของข้อกำหนดไฟร์วอลล์ต่างๆ เพิ่มเติมที่เกิดขึ้นภายหลัง
    - ง. มีการใช้เครื่องมือหรือซอฟต์แวร์กลางทำหน้าที่จัดการชุดของข้อกำหนดไฟร์วอลล์ต่างๆ ที่แตกต่างกัน
    - จ. สามารถปรับเปลี่ยนชุดของข้อกำหนดไฟร์วอลล์ได้โดยอัตโนมัติ
5. ข้อใดกล่าว**ไม่**ถูกต้องเกี่ยวกับระบบตรวจจับการบุกรุกระบบเครือข่ายคอมพิวเตอร์ผ่านโฮสต์
    - ก. เป็นการรักษาความมั่นคงปลอดภัยให้แก่เครื่องแม่ข่ายระบบเครือข่ายที่บรรจุข้อมูลสำคัญเท่านั้น
    - ข. ซอฟต์แวร์ของ HIDS สามารถป้องกันเครื่องโฮสต์ทุกเครื่องที่ติดตั้งบนระบบเครือข่าย
    - ค. มีการมอนิเตอร์แฟ้มบันทึกการเข้าออกระบบ

ง. มีการดำเนินการตรวจจับแพ็กเกตข้อมูลที่ผ่านเข้าออกโฮสต์เฉพาะกรณีต้องสงสัยเท่านั้น

จ. มีการติดตั้งซอฟต์แวร์ตัวแทนเพื่อตรวจจับการบุกรุกทั้งจากภายในและภายนอก

6. ผู้ดูแลระบบจะได้รับการแจ้งเตือนเมื่อมีผู้บุกรุกเข้ามาในระบบเครือข่ายเมื่อไฟล์ผลรวมตรวจสอบเป็นอย่างไร

ฉ. ไฟร์ผลรวมตรวจสอบมีค่าไม่เปลี่ยนแปลง

ช. ไฟร์ผลรวมตรวจสอบถูกบันทึกไว้

ซ. ไฟล์ผลรวมตรวจสอบเกิดการเปลี่ยนค่าจากเดิม

ฌ. ไฟล์ผลรวมตรวจสอบถูกลบทิ้ง

ญ. ไฟล์ผลรวมตรวจสอบมีค่าเป็นศูนย์

7. กระบวนการสแกนหาการทำงานที่ผิดปกติบนระบบเครือข่ายคอมพิวเตอร์ โดยอ้างอิงจากบันทึกการทำงานในสภาวะปกติ เป็นการตรวจจับการบุกรุกประเภทใด

ก. การตรวจจับแบบแพสซิฟ

ข. การตรวจจับแบบแอคทิฟ

ค. การจับคู่รูปแบบ

ง. การตรวจสอบการใช้งานผิดประเภท

จ. การตรวจจับความผิดปกติ

8. ระบบหรือทรัพยากรที่ใช้ในการหยั่งผลการตรวสอบหรือเป็นตัวกลางทดสอบความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ เรียกว่าอะไร

ก. การแจ้งเตือนภัย

ข. ฮันนีพอต

ค. ไฟร์วอลล์

ง. โซนอลาร์ม

จ. แบคดอร์

9. ระบบทรัสต์แบบอุโมงค์หรือเกตเวย์ มีลักษณะการทำงานอย่างไร

ก. มีการสร้างอุโมงค์เครือข่ายโดยเข้ารหัสการเข้าถึงระหว่างระบบเครือข่ายคอมพิวเตอร์ภายใน

ข. มีการประมวลผลแบบกระจาย

ค. มีการวางฮาร์ดแวร์แบบเชื่อมต่อเป็นแนวต่อกัน

ง. มีการใช้ระบบควบคุมและรวบรวมข้อมูลที่ใช้ในการตรวจสอบสาธารณะ

จ. ถูกทุกข้อ

10. ลักษณะที่ผู้ใช้งานเข้าไปใช้งานการประมวลผลแบบกลุ่มเมฆผ่านไซต์ระบบประมวลผลเทียมที่ถูกปลอมแปลงขึ้นมา เรียกว่าอะไร

ก. การโจมตีระบบคอมพิวเตอร์เสมือน

ข. การลงทะเบียนเพื่อเข้าใช้ระบบ การแก้ไขรหัสผ่าน

ค. การโจมตีจากระบบเครือข่ายส่วนขยาย

ง. การปลอมตัวเป็นผู้ให้บริการระบบประมวลผลแบบกลุ่มเมฆ

จ. การพิสูจน์ตัวจริงและการอนุญาต

เฉลยแบบประเมินผลตนเอง หน่วยที่ 9

ก่อนเรียน	**หลังเรียน**
1. จ.	1. ก.
2. ค.	2. ง.
3. ข.	3. จ.
4. ก.	4. ค.
5. จ.	5. ข.
6. ข.	6. ค.
7. ง.	7. จ.
8. ก.	8. ข.
9. จ.	9. ก.
10. ค.	10. ง.

แบบประเมินผลตนเองก่อนเรียน หน่วยที่ 11

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง **“ความมั่นคงปลอดภัยของระบบงานประยุกต์บนเว็บ”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. การพิสูจน์สิทธิ์ในระบบงานประยุกต์บนเว็บมีความแตกต่างจากการพิสูจน์สิทธิ์ในระบบงานประยุกต์ที่ทำงานบนสถาปัตยกรรมแบบไคลเอนต์/เซิร์ฟเวอร์ เนื่องจาก
   ก. ระบบงานประยุกต์บนเว็บทำงานบนโพรโทคอลเอชทีทีพี (HTTP) ซึ่งเป็นโพรโทคอลที่ไม่จดจำสถานะของการเชื่อมต่อ
   ข. การพิสูจน์สิทธิ์ในระบบงานประยุกต์บนเว็บสามารถทำได้ง่าย เนื่องจากโพรโทคอลเอชทีทีพี (HTTP) เป็นโพรโทคอลที่สามารถจดจำสถานะของการเชื่อมต่อได้
   ค. การพิสูจน์สิทธิ์ในระบบงานประยุกต์บนเว็บสามารถทำได้ง่ายกว่า
   ง. การพิสูจน์สิทธิ์ในระบบงานประยุกต์บนเว็บทำได้รวดเร็วกว่า
   จ. การพิสูจน์สิทธิ์ในระบบงานประยุกต์บนเว็บไม่สามารถทำได้อย่างมั่นคงปลอดภัย
2. โพรโทคอลเอชทีทีพี (HTTP) และเอชทีทีพีเอส (HTTPS) มีความแตกต่างกันอย่างไรในด้านของการรักษาความมั่นคงปลอดภัยข้อมูล
   ก. HTTP มีความมั่นคงปลอดภัยสูงเนื่องจากข้อมูลถูกเข้ารหัสลับแบบอาร์เอสเอ
   ข. HTTP มีความมั่นคงปลอดภัยสูงเนื่องจากได้รับความนิยมทั่วไป
   ค. HTTP มีคุณสมบัติในการเก็บสถานะของการเชื่อมต่อ
   ง. HTTP มีคุณสมบัติในการเข้ารหัสระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์ทำให้มั่นใจได้ว่าข้อมูลที่รับส่งมีความมั่นคงปลอดภัย
   จ. HTTP ไม่มีคุณสมบัติในการเข้ารหัสระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์ ข้อมูลที่รับส่งอาจถูกดักรับและเปลี่ยนแปลงแก้ไขได้
3. ข้อใดเป็นข้อจำกัดของการใช้งานการร้องขอแบบ GET
   ก. พารามิเตอร์และค่าต่างๆ จะปรากฏในเว็บเบราว์เซอร์
   ข. ในเว็บเบราว์เซอร์บางผลิตภัณฑ์ไม่สนับสนุนการร้องขอแบบ GET ที่มีขนาดเกิน 256 ตัวอักษร
   ค. เมื่อจัดการสถานะด้วยการใช้คิวรีสตริงค์จะทำให้เปิดเผยข้อมูลที่ใช้ในการจัดการสถานะ
   ง. ข้อ ก. ข. และ ค. ถูก
   จ. ข้อ ก. ข. และ ค. ผิด
4. การพิสูจน์สิทธิ์แบบง่ายและการพิสูจน์สิทธิ์แบบไดเจสต์แตกต่างกันอย่างไร
   ก. การพิสูจน์สิทธิ์แบบง่ายใช้อัลกอริธึมการเข้ารหัสในการรักษาความลับ
   ข. การพิสูจน์สิทธิ์แบบง่ายใช้การแปลงข้อความด้วยอัลกอริธึมแบบ Base64
   ค. การพิสูจน์สิทธิ์แบบไดเจสต์ใช้อัลกอริธึมแบบ MD5

ง. การพิสูจน์สิทธิ์แบบง่ายมีความมั่นคงปลอดภัยสูงกว่าการพิสูจน์สิทธิ์แบบไดเจสต์

จ. ไม่แตกต่างกัน

5. ช่องโหว่และภัยคุกคามที่เกิดขึ้นกับระบบงานประยุกต์บนเว็บมักเกิดกับส่วนใด

ก. ช่องโหว่ภายในระบบงานประยุกต์

ข. ช่องโหว่ของระบบปฏิบัติการและโปรแกรมให้บริการเว็บ (เว็บเซิร์ฟเวอร์)

ค. การประมวลผลข้อมูลที่ได้รับโดยปราศจากการวิเคราะห์

ง. ข้อ ก. ข. และ ค. ถูก

จ. ข้อ ก. ข. และ ค. ผิด

6. ผู้บุกรุกจะทำการลบร่องรอยการบุกรุกโดยการลบข้อมูล log ของระบบงานประยุกต์บนเว็บเพื่ออะไร

ก. ทำลายความน่าเชื่อถือของระบบงาน

ข. ป้องกันการติดตามตรวจสอบ

ค. ป้องกันผู้บุกรุกอื่นไม่ให้เข้าบุกรุกซ้ำรอย

ง. ป้องกันระบบให้ตนเองสามารถเข้าใช้งานได้ตลอดไป

จ. ล่อลวงผู้ดูแลระบบให้เข้าใจผิด

7. SQL Injection คืออะไร

ก. หัวฉีดระบบ จัดทำเพื่อเพิ่มความเร็วให้กับระบบ

ข. ชุดคำสั่งสำหรับจัดการฐานข้อมูลเพื่อเพิ่มความเร็วในการทำงาน

ค. การป้อนชุดคำสั่งภาษาเอสคิวแอลโดยหวังผลให้สามารถจัดการฐานข้อมูลของระบบงานประยุกต์ได้

ง. การเรียกโปรแกรมประยุกต์บนเครื่องเป้าหมายเพื่อให้ทำงานผ่าน System Call

จ. การใช้งานชุดคำสั่งภาษาเอสคิวแอลในการบริหารจัดการระบบฐานข้อมูลของระบบงานประยุกต์บนเว็บ

8. การแจ้งข้อผิดพลาดของระบบงาน “มาก” และให้รายละเอียดมากจนเกินไปอาจส่งผลร้ายต่อระบบงานเพราะเหตุใด

ก. ผู้ใช้งานอาจตำหนิข้อบกพร่องของระบบงาน

ข. แฮกเกอร์นิยมเข้าเจาะระบบเนื่องจากมีข้อผิดพลาดมาก

ค. แฮกเกอร์อาจไม่สนใจเข้าเจาะระบบเนื่องจากมีข้อผิดพลาดมาก

ง. ผู้ใช้งานเข้าใจถึงสาเหตุของข้อบกพร่องของระบบทำให้แก้ปัญหาได้ง่าย

จ. แฮกเกอร์อาจเข้าใจถึงข้อบกพร่องและกระบวนการทำงานของระบบ

9. การโจมตีแบบบรูตฟอร์ซ (Brute force) คืออะไร

ก. การโจมตีระบบด้วยการทำให้ระบบปฏิเสธการให้บริการ

ข. การโจมตีระบบด้วยการส่งชุดคำสั่งเอสคิวแอลเข้าสู่ระบบ

ค. การโจมตีระบบด้วยการส่ง Sync packet จำนวนมากเข้าสู่ระบบ

ง. การโจมตีระบบด้วยการปลอมแปลงและล่อลวงจนกระทั่งได้ข้อมูลซึ่งทำให้เข้าสู่ระบบได้

จ. การโจมตีระบบด้วยการใช้ชื่อผู้เข้าใช้และรหัสผ่านส่งเข้าสู่ระบบจนสามารถเข้าสู่ระบบสำเร็จ

10. การใช้งานระบบงานประยุกต์บนเว็บโดยมิได้ดำเนินการเลิกใช้งาน (log out) อาจส่งผลอย่างไร
    ก. ไม่มีผลร้ายแต่อย่างใด
    ข. ระบบอาจยกเลิกบริการได้
    ค. อาจถูกผู้ไม่หวังดีขโมยเซสชันได้
    ง. อาจถูกโจมตีด้วยเทคนิคการบรูตฟอร์ซได้
    จ. อาจถูกโจมตีด้วยเทคนิควิศวกรรมทางสังคมได้

แบบประเมินผลตนเองหลังเรียน หน่วยที่ 11

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง **"ความมั่นคงปลอดภัยของระบบงานประยุกต์บนเว็บ"**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใด**ไม่**ถือเป็นช่องโหว่และภัยคุกคามหลักของระบบงานประยุกต์บนเว็บ
    ก. ช่องโหว่และภัยคุกคามจากภัยธรรมชาติ
    ข. ช่องโหว่และภัยคุกคามที่เกี่ยวกับการรับข้อมูลและแสดงผล
    ค. ช่องโหว่และภัยคุกคามที่เกี่ยวข้องกับการจัดการสถานะของการเชื่อมต่อ
    ง. ข้อ ก. และ ข.
    จ. ข้อ ก. และ ค.
2. ข้อใดเป็นลักษณะเฉพาะของโพรโทคอลเอชทีทีพี
    ก. เป็นโพรโทคอลที่ได้รับความนิยมสูง
    ข. เป็นโพรโทคอลที่จดจำสถานะของการเชื่อมต่อ
    ค. เป็นโพรโทคอลสำหรับการรับส่งข้อมูลจดหมายอิเล็กทรอนิกส์
    ง. เป็นโพรโทคอลที่ไม่จดจำสถานะของการเชื่อมต่อ
    จ. ข้อ ก. ข. และ ค. ถูก
3. เว็บเบราว์เซอร์แสดงผล HTTP ERROR 404 หมายถึงข้อใด
    ก. เว็บเบราว์เซอร์ไม่พบชื่อโดเมนที่ต้องการ
    ข. การจัดการสถานะของการเชื่อมต่อผิดพลาด
    ค. การร้องขอของเว็บเบราว์เซอร์ถูกเปลี่ยนไปยังเส้นทางอื่น
    ง. ข้อผิดพลาดอันเนื่องมาจากการเชื่อมต่อล้มเหลว
    จ. เว็บเซิร์ฟเวอร์ไม่พบทรัพยากรที่เบราว์เซอร์ต้องการ
4. เว็บเบราว์เซอร์แสดงผล HTTP ERROR 401 หมายถึงข้อใด
    ก. การจัดการสถานะของการเชื่อมต่อล้มเหลว

ข. ทรัพยากรที่ร้องขอมีการจำกัดสิทธิ์ จะต้องดำเนินพิสูจน์สิทธิ์การเข้าถึงเสียก่อน

ค. เว็บเบราว์เซอร์ไม่พบชื่อโดเมนที่ต้องการ

ง. การร้องขอของเว็บเบราว์เซอร์ถูกเปลี่ยนไปยังเส้นทางอื่น

จ. ข้อผิดพลาดอันเนื่องมาจากการเชื่อมต่อล้มเหลว

5. หากเว็บเบราว์เซอร์แสดงค่า login.php?username=korakoch&password=12345678 บนแอดเดรสบาร์ แสดงว่าเว็บเบราว์เซอร์ส่งการร้องขอชนิดใดไปยังเว็บเซิร์ฟเวอร์

ก. GET

ข. POST

ค. HEAD

ง. LOGIN

จ. TRACE

6. ในการใช้งานโพรโทคอลเอชทีทีพีเอส (HTTPS) ซึ่งดำเนินการเข้ารหัสข้อมูลที่รับระหว่างเบราว์เซอร์และเว็บเซิร์ฟเวอร์ หากเบราว์เซอร์ตรวจสอบพบความผิดปกติเนื่องจากข้อผิดพลาดเกี่ยวกับการเข้ารหัส ผู้ใช้จะทราบได้อย่างไร

ก. การแจ้งเตือนในขั้นตอนการเตรียมการรับ-ส่ง (ขั้นตอนที่ 1)

ข. การเตรียมการเกี่ยวกับการเข้ารหัสลับ (ขั้นตอนที่ 2)

ค. การแจ้งเตือน เช่น “ใบรับรองผิดพลาด” ซึ่งเป็นขั้นตอนที่ 3 ของการทำงาน

ง. การส่งข้อมูลไปยังระดับชั้นขนส่ง (transport layer)

จ. ไม่มีคำตอบถูก

7. ระบบงานประยุกต์บนเว็บปลอดภัยจากการโจมตีด้วยเทคนิควิศวกรรมทางสังคมหรือไม่ เพราะเหตุใด

ก. ปลอดภัย เนื่องจากเทคนิควิศวกรรมทางสังคมไม่มุ่งเน้นทำลายระบบงานประยุกต์บนเว็บ

ข. ปลอดภัย เนื่องจากเทคนิควิศวกรรมทางสังคมเป็นการโจมตีทางอ้อม

ค. ไม่ปลอดภัย เนื่องจากผู้ไม่หวังดีอาจดำเนินการปิดระบบงานประยุกต์บนเว็บได้

ง. ไม่ปลอดภัย เนื่องจากผู้ไม่หวังดีอาจเปลี่ยนแปลงแก้ไขข้อมูลที่จัดเก็บในระบบงานประยุกต์บนเว็บได้

จ. ไม่ปลอดภัย เนื่องจากหากมีผู้ไม่หวังดีสามารถเข้าใช้งานระบบได้เป็นการทำให้ความมั่นคงปลอดภัย ซึ่งประกอบด้วย การรักษาความลับ การรักษาบูรณภาพข้อมูล การรักษาความพร้อมใช้ เสียหายไปจากที่กำหนดในนโยบาย

8. การพัฒนาระบบงานประยุกต์บนเว็บควรให้มีการจัดทำระบบจัดเก็บข้อมูลสถานะ (log) ของระบบงานหรือไม่

ก. ไม่จำเป็น เนื่องจากการเข้าถึงระบบงานสามารถตรวจสอบได้จากเว็บเซิร์ฟเวอร์

ข. ไม่จำเป็น เนื่องจากเสียพื้นที่ไปโดยเปล่าประโยชน์

ค. ไม่จำเป็น เนื่องจากมีความยุ่งยากซับซ้อนกว่าตัวระบบงานประยุกต์เอง

ง. จำเป็น เนื่องจากต้องใช้ในการวิเคราะห์ความต้องการของระบบ

   จ. จำเป็น เนื่องจากหากมีข้อผิดพลาดกับระบบจะเป็นส่วนสำคัญในการกู้คืนและตรวจสอบการละเมิดความมั่นคงปลอดภัยได้อีกทางหนึ่ง

9. ข้อใดคือข้อดีของการจัดการสถานะของการเชื่อมต่อด้วย URL
   ก. เป็นการให้บริการแบบอัตโนมัติผ่านหน้าเว็บเพจ
   ข. ข้อมูลการจัดการสถานะของการเชื่อมต่อสามารถเข้าใจได้
   ค. สามารถใช้เทคนิคนี้ได้กับโปรแกรมเว็บเบราว์เซอร์ทุกโปรแกรมแม้ว่าโปรแกรมจะไม่ยอมให้มีการสร้างคุกกี้ก็ตาม
   ง. สามารถจัดการสถานะของการเชื่อมต่อได้อย่างรวดเร็ว
   จ. สถานะของการเชื่อมต่อสามารถถ่ายโอนข้ามโปรแกรมเว็บเบราว์เซอร์ได้

10. ข้อใดคือข้อดีของการจัดการสถานะของการเชื่อมต่อผ่านฟอร์มของเอชทีเอ็มแอล (HTML)
   ก. สามารถใช้กับเว็บเบราว์เซอร์ทุกโปรแกรมโดยไม่จำเป็นต้องมีคุกกี้และสามารถรองรับการจัดการข้อมูลจำนวนมาก
   ข. การปลอมแปลงสถานะของการเชื่อมต่อทำได้ง่ายกว่าการจัดการด้วย URL
   ค. ความมั่นคงปลอดภัยสูงกว่าการจัดการสถานะแบบคุกกี้
   ง. ความมั่นคงปลอดภัยสูงกว่าการจัดการสถานะแบบเซสชัน
   จ. ถูกทุกข้อ

เฉลยแบบประเมินผลตนเองหน่วยที่ 11

ก่อนเรียน	**หลังเรียน**
1. ก.	1. ก.
2. จ.	2. ง.
3. ง.	3. จ.
4. ค.	4. ข.
5. ง.	5. ก.
6. ข.	6. ค.
7. ค.	7. จ.
8. จ.	8. จ.
9. จ.	9. ค.
10. ค.	10. ก.

แบบประเมินผลตนเองก่อนเรียน หน่วยที่ 12

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง **“ความมั่นคงปลอดภัยของฐานข้อมูล”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใดหมายถึงฐานข้อมูล
   - ก. ข้อเท็จจริงที่เกี่ยวข้องกับบุคคล สถานที่ สิ่งของ สินค้า หรือเหตุการณ์ที่สนใจ ซึ่งอยู่ในรูปของตัวเลข ข้อความ ภาพ เสียง
   - ข. ระบบหรือกระบวนการจัดการกับข้อมูล
   - **ค. ที่สำหรับเก็บข้อมูลจำนวนมากที่มีความเกี่ยวข้องสัมพันธ์กัน**
   - ง. ซอฟต์แวร์ที่ทำหน้าที่ควบคุมดูแลการเข้าถึงข้อมูลในฐานข้อมูล
   - จ. ถูกทุกข้อ
2. ข้อใดคือคุณลักษณะของโครงสร้างฐานข้อมูลแบบสัมพันธ์
   - ก. มีส่วนประกอบที่สำคัญคือ เรคอร์ดและเซต
   - **ข. เป็นแบบตาราง ประกอบด้วย แถวและคอลัมน์**
   - ค. สามารถนำข้อมูลกลับมาใช้ซ้ำหรือสืบทอดคุณสมบัติได้
   - ง. ข้อมูลมีความสัมพันธ์กันแบบลำดับชั้นลดหลั่นกันจากบนลงล่าง
   - จ. ไม่มีคำตอบถูก
3. ข้อใดเป็นความต้องการด้านความมั่นคงปลอดภัยของฐานข้อมูล
   - ก. ต้องการความครบถ้วนสมบูรณ์ของข้อมูล
   - ข. ต้องการควบคุมการเข้าถึงข้อมูล
   - ค. ต้องการตรวจสอบการกระทำกับข้อมูล
   - ง. ต้องการรักษาสภาพพร้อมใช้งาน
   - **จ. ถูกทุกข้อ**
4. ข้อใดเป็นการเตรียมความพร้อมเพื่อรักษาสภาพพร้อมใช้งานฐานข้อมูล
   - ก. ระบบสำรองข้อมูล
   - ข. ระบบพิสูจน์ตัวตนของผู้ใช้
   - ค. ระบบควบคุมภาวะการใช้ข้อมูลพร้อมกัน
   - **ง. ข้อ ก. และ ค. ถูก**
   - จ. ข้อ ข. และ ค. ถูก
5. ข้อใด**ไม่ใช่**กฎควบคุมความถูกต้องของสถานะข้อมูล
   - ก. กฎควบคุมค่าในโดเมน
   - ข. กฎควบคุมค่าของแอตทริบิวต์ที่เป็นคีย์หลัก
   - ค. กฎควบคุมโครงสร้างแอตทริบิวต์

ง. กฎควบคุมความถูกต้องของการอ้างอิง

จ. กฎควบคุมความถูกต้องที่กำหนดไว้ในกระบวนการทำรายการ

6. การกำหนดให้ผู้ใช้ป้อนชื่อผู้ใช้และรหัสผ่านก่อนเข้าใช้งานฐานข้อมูล เป็นการควบคุมการเข้าถึงข้อมูลแบบใด

ก. การสร้างตารางเสมือน

ข. การพิสูจน์ตัวตนของผู้ใช้

ค. การเข้าถึงข้อมูลระดับรีเลชัน

ง. การเข้าถึงข้อมูลระดับแอตทริบิวต์

จ. การกำหนดสิทธิ์การเข้าถึงข้อมูล

7. ในการสำรองข้อมูลมีข้อควรพิจารณาอย่างไร

ก. เลือกรูปแบบการสำรองข้อมูลให้เหมาะสมกับลักษณะงานขององค์กร

ข. ทำการสำรองข้อมูลเป็นระยะอย่างสม่ำเสมอ

ค. เก็บข้อมูลสำรองไว้ในที่ที่ปลอดภัย

ง. ประกันภัยให้ครอบคลุมถึงความเสียหายของข้อมูล

จ. ถูกทุกข้อ

8. ข้อใดคือคุณสมบัติของรายการดำเนินการหรือทรานแซกชัน

ก. ความเป็นอันหนึ่งอันเดียว

ข. ความสอดคล้อง

ค. ความเป็นส่วนตัวแยกออกจากกัน

ง. ความทนทาน

จ. ถูกทุกข้อ

9. ปัญหาข้อมูลสูญหายในระหว่างการปรับปรุงข้อมูลเกิดขึ้นจากอะไร

ก. การประมวลผลสอดแทรกระหว่างกัน ทำให้ผลลัพธ์จากการปรับปรุงข้อมูลเกิดความผิดพลาดขึ้น

ข. การอนุญาตให้รายการหนึ่งสามารถอ่านผลลัพธ์จากรายการอื่นได้ ในขณะที่ข้อมูลนั้นยังอยู่ระหว่างการประมวลผลซึ่งยังไม่ได้ยอมรับว่าทำเสร็จสมบูรณ์แล้ว

ค. การนำเอาข้อมูลที่ปรับปรุงยังไม่แล้วเสร็จไปใช้

ง. การนำเอาข้อมูลที่ปรับปรุงแล้วไปใช้ แต่ต่อมาข้อมูลนั้นมีการโรลแบ็ค

จ. ไม่มีคำตอบถูก

10. “ล็อคตาย” คืออะไร

ก. ล็อคทั้งฐานข้อมูล

ข. ล็อคเฉพาะตารางที่กำหนด

ค. ทรานแซกชันตั้งแต่ 2 รายการขึ้นไป ต่างฝ่ายต่างล็อคข้อมูลไว้เพื่อรอที่จะใช้ข้อมูลอื่น ทำให้ไม่สามารถประมวลผลข้อมูลต่อไปได้

ง. อนุญาตให้อ่านข้อมูลได้ แต่ไม่อนุญาตให้ปรับปรุงข้อมูลนี้โดยเด็ดขาด

จ. ไม่อนุญาตให้รายการอื่นใช้ข้อมูล ข้อมูลจะถูกใช้งานได้เพียงผู้เดียวคือผู้ทำการล็อคเป็นคนแรกเท่านั้น

แบบประเมินผลตนเองหลังเรียน หน่วยที่ 12

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง **“ความมั่นคงปลอดภัยของฐานข้อมูล”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใดกล่าวถูกต้องเกี่ยวกับข้อมูล ฐานข้อมูล ระบบฐานข้อมูล และระบบจัดการฐานข้อมูล

ก. ข้อมูล คือข้อเท็จจริงที่เกี่ยวข้องกับบุคคล สถานที่ สิ่งของ สินค้า หรือเหตุการณ์ที่สนใจ ซึ่งอยู่ในรูปของตัวเลข ข้อความ ภาพ เสียง

ข. ฐานข้อมูล คือที่สำหรับเก็บข้อมูลจำนวนมากที่มีความเกี่ยวข้องสัมพันธ์กัน

ค. ระบบฐานข้อมูล คือระบบหรือกระบวนการจัดการกับข้อมูล ประกอบด้วย ฐานข้อมูล และระบบจัดการฐานข้อมูล

ง. ระบบจัดการฐานข้อมูล คือซอฟต์แวร์ที่ทำหน้าที่ควบคุมดูแลการเข้าถึงข้อมูลในฐานข้อมูล

จ. ถูกทุกข้อ

2. ข้อใดคือความสำคัญของระบบฐานข้อมูล

ก. ลดความซ้ำซ้อนของข้อมูล

ข. ข้อมูลมีความสอดคล้องกัน

ค. มีการควบคุมความถูกต้องของข้อมูล

ง. มีการควบคุมความมั่นคงปลอดภัยของข้อมูล

จ. ถูกทุกข้อ

3. ส่วนใดของโครงสร้างฐานข้อมูลแบบสัมพันธ์ที่เรียกว่า “แอตทริบิวต์”

ก. แถวซึ่งใช้เก็บรายการข้อมูล

ข. คอลัมน์ซึ่งใช้เก็บคุณสมบัติของข้อมูล

ค. ข้อมูลที่มีการควบคุมมาตรฐาน

ง. ข้อมูลที่มีการกำหนดกฎควบคุมความถูกต้อง

จ. ข้อมูลในตารางหนึ่งที่มีความสัมพันธ์กับข้อมูลในตารางอื่น

4. ระบบสำรองและฟื้นสภาพข้อมูลช่วยสนับสนุนความต้องการด้านใดของความมั่นคงปลอดภัยฐานข้อมูล

ก. ความครบถ้วนสมบูรณ์ของฐานข้อมูลทางกายภาพ

ข. ความครบถ้วนสมบูรณ์ของฐานข้อมูลทางตรรกะ

ค. การรักษาสภาพพร้อมใช้งาน

ง. ข้อ ก. และ ค. ถูก

จ. ข้อ ข. และ ค. ถูก

5. ข้อใดเป็นกฎควบคุมความถูกต้องในขั้นตอนของการปรับปรุงข้อมูล

ก. กฎควบคุมค่าในโดเมน

ข. กฎควบคุมโครงสร้างแอตทริบิวต์

ค. กฎควบคุมค่าของแอตทริบิวต์ที่เป็นคีย์หลัก

ง. กฎควบคุมความถูกต้องของการอ้างอิง

จ. กฎควบคุมความถูกต้องที่กำหนดไว้ในกระบวนการทำรายการ

6. การจำกัดให้ผู้ใช้แต่ละคนสามารถมองเห็นและใช้งานข้อมูลในตารางเดียวกันได้เฉพาะส่วนที่ตนเกี่ยวข้องเท่านั้น เป็นการควบคุมการเข้าถึงข้อมูลแบบใด

ก. การสร้างตารางเสมือน

ข. การพิสูจน์ตัวตนของผู้ใช้

ค. การเข้าถึงข้อมูลระดับรีเลชัน

ง. การเข้าถึงข้อมูลระดับแอตทริบิวต์

จ. การกำหนดสิทธิ์การเข้าถึงข้อมูล

7. ข้อใดคือขั้นตอนวิธีที่ใช้ในการฟื้นสภาพข้อมูล

ก. วิเคราะห์ ทำซ้ำ ยกเลิกการกระทำ

ข. ตรวจสอบ ยกเลิก ทำซ้ำ

ค. บันทึก ลบ ยกเลิก

ง. บันทึก หยุด ทำซ้ำ

จ. ไม่มีคำตอบถูก

8. Rollback คืออะไร

ก. การกำหนดให้ทรานแซกชันเริ่มต้นทำงาน

ข. การบอกถึงความสำเร็จในการทำงานของทรานแซกชัน

ค. การกำหนดให้ทรานแซกชันดำเนินการสำเร็จและสิ้นสุดการทำงาน

ง. การกำหนดให้ทรานแซกชันยกเลิกการทำงานแล้วย้อนกลับไปยังจุดตรวจสอบ

จ. การกำหนดให้บันทึกทรานแซกชันลงในจุดตรวจสอบ

9. จากข้อมูลการดำเนินงานของทรานแซกชันต่อไปนี้ ข้อใดคือผลลัพธ์ที่ถูกต้องของยอดเงินคงเหลือ

เวลา	ทรานแซกชันที่ 1	ทรานแซกชันที่ 2	ยอดเงินคงเหลือ (Bal)
T1		Begin	100
T2	Begin	Read	100
T3	Read	Bal = Bal - 30	100
T4	Bal = Bal + 20	Write	70
T5	Write	Commit	120
T6	Commit		120

ก. 70

ข. 80

ค. 90

ง. 100

จ. 120 ถูกต้องแล้ว

10. ข้อใดหมายถึงการควบคุมภาวะการใช้ข้อมูลพร้อมกันด้วยการพิจารณาแนวทางที่ดีที่สุด

ก. การแก้ปัญหาความขัดแย้งระหว่างข้อมูล

ข. การแก้ปัญหาข้อมูลไม่ได้รับการยืนยันความสมบูรณ์

ค. การแก้ปัญหาข้อมูลสูญหายระหว่างการปรับปรุงข้อมูล

ง. การประทับเวลากำกับไว้ให้กับแต่ละรายการ เพื่อใช้ในการจัดเรียงลำดับรายการก่อนและหลัง

จ. การปล่อยให้ทรานแซกชันสามารถประมวลผลได้โดยไม่ต้องมีการตรวจสอบความครบถ้วนถูกต้องล่วงหน้า แต่จะทำการตรวจสอบก่อนบันทึกลงฐานข้อมูลจริง

เฉลยแบบประเมินผลตนเองหน่วยที่ 12

ก่อนเรียน	หลังเรียน
1. ค.	1. จ.
2. ข.	2. จ.
3. จ.	3. ข.
4. ง.	4. ง.
5. จ.	5. จ.
6. ข.	6. ก.
7. จ.	7. ก.
8. จ.	8. ง.
9. ก.	9. ค.
10. ค.	10. จ.

แบบประเมินผลตนเองก่อนเรียน หน่วยที่ 13

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง “**กฎหมายและจริยธรรมเกี่ยวกับความมั่นคงปลอดภัยในระบบคอมพิวเตอร์**”

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใด**ไม่**ถูกต้องเกี่ยวกับกฎหมายธุรกรรมทางอิเล็กทรอนิกส์

   ก. เป็นกฎหมายที่รับรองการทำธุรกรรมทางแพ่งและพาณิชย์ที่กระทำด้วยวิธีการทางอิเล็กทรอนิกส์

   ข. เป็นกฎหมายที่กำหนดให้คู่กรณีสามารถนำเอกสารของข้อมูลอิเล็กทรอนิกส์มาใช้เป็นพยานหลักฐานในศาลได้

   ค. เป็นกฎหมายที่รับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์

   ง. เป็นกฎหมายที่รับรองสถานะของลายมือชื่ออิเล็กทรอนิกส์

   จ. เป็นกฎหมายที่กำหนดหลักเกณฑ์เกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์

2. ข้อใดถูกต้องเกี่ยวกับกฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

   ก. เป็นกฎหมายที่กำหนดหลักเกณฑ์เกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์

   ข. เป็นกฎหมายที่คุ้มครองการกระทำความผิดต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

   ค. เป็นกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบคอมพิวเตอร์

   ง. เป็นกฎหมายที่เป็นกฎหมายที่รับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์

   จ. เป็นกฎหมายที่รับรองสถานะของลายมือชื่ออิเล็กทรอนิกส์

3. ลายมือชื่ออิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 หมายถึงข้อใด

   ก. ลายนิ้วมือที่ได้จากการแสกน

   ข. ลายมือชื่อที่สร้างขึ้นด้วยระบบกุญแจคู่

   ค. ม่านตา

   ง. รหัสผ่าน

   จ. ถูกทุกข้อ

4. ข้อใดเป็นธุรกรรมที่ถูกยกเว้นตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ไม่ให้กระทำด้วยวิธีการทางอิเล็กทรอนิกส์

   ก. การยื่นแบบชำระภาษีออนไลน์

   ข. การชำระค่าบริการผ่านเครือข่าย

   ค. การโอนเงินผ่านธนาคาร

   ง. การซื้อสินค้าบนเว็บไซต์

   จ. การจดทะเบียนสมรส

5. ข้อใดเป็นความผิดฐานรบกวนระบบคอมพิวเตอร์ของผู้อื่น ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ก. การทำดีโอเอส (Denial of Service หรือ DoS)
ข. การเจาะระบบคอมพิวเตอร์ (Hacking)
ค. การเผยแพร่ภาพลามกบนเว็บไซต์
ง. การส่งสปายแวร์ (Spyware)
จ. การส่งแสปมเมล์ (Spam mail)

6. ข้อใดถูกต้องเกี่ยวกับจริยธรรม

ก. เป็นสิ่งที่ออกโดยรัฐ
ข. มีบทลงโทษที่ชัดเจนและแน่นอน
ค. บัญญัติไว้เป็นลายลักษณ์อักษร
ง. มุ่งควบคุมความประพฤติของบุคคล
จ. เป็นแบบแผนความประพฤติของคนในสังคม

7. จริยธรรมและคอมพิวเตอร์มีความสัมพันธ์กันในด้านใด

ก. ความเป็นส่วนตัว ความถูกต้องแม่ยำของข้อมูล การใช้ข้อมูล และจัดเก็บข้อมูล
ข. ความเป็นส่วนตัว ความถูกต้องแม่ยำของข้อมูล ความเป็นเจ้าของทรัพย์สินทางปัญญา และการจัดเก็บข้อมูล
ค. การใช้ข้อมูล การจัดเก็บข้อมูล ความถูกต้องแม่ยำของข้อมูล ความเป็นเจ้าของทรัพย์สินทางปัญญา และการเข้าถึงข้อมูล
ง. ความเป็นส่วนตัว ความถูกต้องแม่ยำของข้อมูล ความเป็นเจ้าของทรัพย์สินทางปัญญา และการเข้าถึงข้อมูล
จ. ไม่มีคำตอบถูก

8. แนวคิดทางจริยธรรมที่ว่า “การตัดสินใจกระทำการอย่างใดอย่างหนึ่งนั้นจะต้องเป็นผลดีที่สุดต่อทุกคน ในขณะเดียวกันก็ต้องเป็นผลเสียน้อยที่สุดต่อทุกคนด้วย” มาจากทฤษฎีใด

ก. ทฤษฎีอัตนิยม
ข. ทฤษฎีอรรถประโยชน์นิยม
ค. ทฤษฎีทัณฑวิทยา
ง. ทฤษฎีจริยธรรมเชิงหน้าที่
จ. ทฤษฎีจริยธรรมเชิงโครงสร้าง

9. แนวคิดทางจริยธรรมที่ว่า “การกระทำที่มีคุณค่าทางจริยธรรมอันเป็นสิ่งที่สมควรต้องกระทำนั้น คือการกระทำที่เป็นหน้าที่” มาจากทฤษฎีใด

ก. ทฤษฎีอัตนิยม
ข. ทฤษฎีอรรถประโยชน์นิยม
ค. ทฤษฎีทัณฑวิทยา
ง. ทฤษฎีจริยธรรมเชิงหน้าที่
จ. ทฤษฎีจริยธรรมเชิงโครงสร้าง

10. สถาบันความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security institute: CSI) เป็นหน่วยงานที่ทำหน้าที่ใด
    - ก. ดำเนินการและสนับสนุน การตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์และเครือข่าย
    - ข. สร้างความเชื่อมั่นและให้การรับรองบุคลากรด้านความมั่นคงปลอดภัยของสารสนเทศเป็นหลัก
    - **ค. ให้บริการฝึกอบรมและความรู้ทางด้านระบบคอมพิวเตอร์ เครือข่าย และความมั่นคงปลอดภัยของสารสนเทศแก่ผู้ประกอบการ**
    - ง. เป็นศูนย์รวมการแลกเปลี่ยนความรู้ของบรรดานักปฏิบัติการด้านความมั่นคงปลอดภัยของสารสนเทศ
    - จ. ถูกทุกข้อ

แบบประเมินผลตนเองหลังเรียน หน่วยที่ 13

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง ““**กฎหมายและจริยธรรมเกี่ยวกับความมั่นคงปลอดภัยในระบบคอมพิวเตอร์**””

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใด**ไม่**ถูกต้องเกี่ยวกับกฎหมายธุรกรรมทางอิเล็กทรอนิกส์
    - ก. เป็นกฎหมายที่รับรองการทำธุรกรรมทางแพ่งและพาณิชย์ที่กระทำด้วยวิธีการทางอิเล็กทรอนิกส์
    - ข. เป็นกฎหมายที่กำหนดให้คู่กรณีสามารถนำเอกสารของข้อมูลอิเล็กทรอนิกส์มาใช้เป็นพยานหลักฐานในศาลได้
    - **ค. เป็นกฎหมายที่กำหนดหลักเกณฑ์เกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์**
    - ง. เป็นกฎหมายที่รับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์
    - จ. เป็นกฎหมายที่รับรองสถานะของลายมือชื่ออิเล็กทรอนิกส์
2. ข้อใดถูกต้องเกี่ยวกับกฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
    - ก. เป็นกฎหมายที่กำหนดหลักเกณฑ์เกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์
    - ข. เป็นกฎหมายที่รับรองสถานะของลายมือชื่ออิเล็กทรอนิกส์
    - ค. เป็นกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในระบบคอมพิวเตอร์
    - ง. เป็นกฎหมายที่เป็นกฎหมายที่รับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์
    - **จ. เป็นกฎหมายที่คุ้มครองการกระทำความผิดต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์**
3. ข้อใด**ไม่ใช่**ลายมือชื่ออิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
    - ก. ลายนิ้วมือที่ได้จากการแสกน
    - ข. ลายมือชื่อที่สร้างขึ้นด้วยระบบกุญแจคู่
    - ค. ม่านตา
    - ง. รหัสผ่าน
    - **จ. ทุกข้อเป็นลายมือชื่ออิเล็กทรอนิกส์**

4. ข้อใดเป็นธุรกรรมที่ถูกยกเว้นตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ไม่ให้กระทำด้วยวิธีการทางอิเล็กทรอนิกส์
    ก. การยื่นแบบชำระภาษีออนไลน์
    ข. การจดทะเบียนสมรส
    ค. การชำระค่าบริการผ่านเครือข่าย
    ง. การโอนเงินผ่านธนาคาร
    จ. การซื้อสินค้าบนเว็บไซต์
5. ข้อใดเป็นความผิดฐานรบกวนระบบคอมพิวเตอร์ของผู้อื่น ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
    ก. การเจาะระบบคอมพิวเตอร์ (Hacking)
    ข. การเผยแพร่ภาพลามกบนเว็บไซต์
    ค. การส่งสปายแวร์ (Spyware)
    ง. การทำดีโอเอส (Denial of Service **หรือ** DoS)
    จ. การส่งแสปมเมล์ (Spam mail)
6. ข้อใดถูกต้องเกี่ยวกับจริยธรรม
    ก. เป็นสิ่งที่ออกโดยรัฐ
    ข. มีบทลงโทษที่ชัดเจนและแน่นอน
    ค. เป็นแบบแผนความประพฤติของคนในสังคม
    ง. บัญญัติไว้เป็นลายลักษณ์อักษร
    จ. มุ่งควบคุมความประพฤติของบุคคล
7. จริยธรรมและคอมพิวเตอร์มีความสัมพันธ์กันในด้านใด
    ก. การใช้ข้อมูล การจัดเก็บข้อมูล ความถูกต้องแม่ยำของข้อมูล ความเป็นเจ้าของทรัพย์สินทางปัญญา และการเข้าถึงข้อมูล
    ข. **ความเป็นส่วนตัว ความถูกต้องแม่ยำของข้อมูล ความเป็นเจ้าของทรัพย์สินทางปัญญา และการเข้าถึงข้อมูล**
    ค. ความเป็นส่วนตัว ความถูกต้องแม่ยำของข้อมูล การใช้ข้อมูล และจัดเก็บข้อมูล
    ง. ความเป็นส่วนตัว ความถูกต้องแม่ยำของข้อมูล ความเป็นเจ้าของทรัพย์สินทางปัญญา และการจัดเก็บข้อมูล
    จ. ไม่มีคำตอบถูก
8. แนวคิดทางจริยธรรมที่ว่า “การตัดสินใจกระทำการอย่างใดอย่างหนึ่งนั้นจะต้องเป็นผลดีที่สุดต่อทุกคน ในขณะเดียวกันก็ต้องเป็นผลเสียน้อยที่สุดต่อทุกคนด้วย” มาจากทฤษฎีใด
    ก. ทฤษฎีอรรถประโยชน์นิยม

ข. ทฤษฎีทัณฑวิทยา

ค. ทฤษฎีอัตนิยม

ง. ทฤษฎีจริยธรรมเชิงหน้าที่

จ. ทฤษฎีจริยธรรมเชิงโครงสร้าง

9. แนวคิดทางจริยธรรมที่ว่า “การกระทำที่มีคุณค่าทางจริยธรรมอันเป็นสิ่งที่สมควรต้องกระทำนั้น คือการกระทำที่เป็นหน้าที่” มาจากทฤษฎีใด

ก. ทฤษฎีอัตนิยม

ข. ทฤษฎีจริยธรรมเชิงหน้าที่

ค. ทฤษฎีจริยธรรมเชิงโครงสร้าง

ง. ทฤษฎีอรรถประโยชน์นิยม

จ. ทฤษฎีทัณฑวิทยา

10. สถาบันความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security institute: CSI) เป็นหน่วยงานที่ทำหน้าที่ใด

ก. ให้บริการฝึกอบรมและความรู้ทางด้านระบบคอมพิวเตอร์ เครือข่าย และความมั่นคงปลอดภัยของสารสนเทศแก่ผู้ประกอบการ

ข. ดำเนินการและสนับสนุน การตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์และเครือข่าย

ค. สร้างความเชื่อมั่นและให้การรับรองบุคลากรด้านความมั่นคงปลอดภัยของสารสนเทศเป็นหลัก

ง. เป็นศูนย์รวมการแลกเปลี่ยนความรู้และพัฒนาของบรรดานักปฏิบัติการด้านความมั่นคงปลอดภัยของสารสนเทศ

จ. ถูกทุกข้อ

เฉลยแบบประเมินผลตนเองหน่วยที่ 13

ก่อนเรียน	**หลังเรียน**
1. จ.	1. ค.
2. ข.	2. จ.
3. จ.	3. จ.
4. จ.	4. ข.
5. ก.	5. ง.
6. จ.	6. ค.
7. ง.	7. ข.
8. ก.	8. ค.
9. ง.	9. ข.
10. ค.	10. ก.

แบบประเมินผลตนเองก่อนเรียน หน่วยที่ 14

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง **“นโยบายการรักษาความมั่นคงปลอดภัยแบบยั่งยืน”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใดคือความหมายของมาตรฐาน ISO-27000
   - *ก.* มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยห่วงโซ่อุปทาน
   - **ข. มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล**
   - ค. มาตรฐานการบริหารคุณภาพ
   - ง.มาตรฐานการจัดการด้านความปลอดภัยสำหรับอุตสาหกรรมอาหาร
   - จ. มาตรฐานการจัดการพลังงาน
2. ข้อใดคือความหมายของ ISMS (Information Security Management System)
   - ก. ระบบที่ใช้ในการจัดการการวางแผนของระบบความมั่นคงปลอดภัย
   - ข. ระบบที่ใช้ในการจัดการการประยุกต์ของระบบความมั่นคงปลอดภัย
   - ค. ระบบที่ใช้ในการจัดการการประเมินของระบบความมั่นคงปลอดภัย
   - ง.ระบบที่ใช้ในการจัดการการเฝ้าระวังของระบบความมั่นคงปลอดภัย
   - **จ. ถูกทุกข้อ**
3. ข้อใดคือความหมายของมาตรฐาน ISO-28000
   - ***ก.* มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยห่วงโซ่อุปทาน**
   - ข. มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล
   - ค. มาตรฐานการบริหารคุณภาพ
   - ง.มาตรฐานการจัดการด้านความปลอดภัยสำหรับอุตสาหกรรมอาหาร
   - จ. มาตรฐานการจัดการพลังงาน
4. ข้อใดกล่าวถูกต้องเกี่ยวกับแบบจำลอง PDCA
   - ก. Predict-Do-Check-Act
   - **ข. Plan-Do-Check-Act**
   - ค. Plan-Do-Correct-Act
   - ง. Plan-Do-Check-Adjust
   - จ. Predict-Do-Correct-Adjust
5. ในการสอบใบรับรองความสามารถแบบ CISSP มีหัวข้อกี่หัวข้อ
   - ก. 8
   - ข. 9
   - **ค. 10**

ง. 11

จ. 12

6. ข้อใด**ไม่**ถูกต้องเกี่ยวกับใบรับรองความสามารถแบบ CISSP

ก. ต้องต่ออายุทุกๆ 5 ปี

ข. ต้องมีแต้ม CPE อย่างน้อย 85 ภายในเวลา 3 ปี

ค. ต้องมีผู้เซ็นรับรองในการต่ออายุ

ง. ต้องจ่ายเงินรายปี ปีละ 120 ดอลล่าห์สหรัฐ

จ. ทุกข้อไม่ถูกต้อง

7. มาตรฐานการรักษาความมั่นคงตามแบบกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารอ้างอิงมาตรฐานใดเป็นสำคัญ

ก. มาตรฐาน ISO-9001

ข. มาตรฐาน ISO-27000

ค. มาตรฐาน ISO-2800

ง.มาตรฐาน ISO-14000

จ. มาตรฐาน ISO-50001

8. ข้อใด**ไม่ใช่**ขั้นตอนในการปฏิบัติตามแนวทางมาตรฐานความมั่นคงปลอดภัยของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ก. กำหนดบทบาทและหน้าที่สำคัญ

ข. จัดทำเอกสารที่เกี่ยวข้อง

ค. จัดทำข้อกำหนดบัญชีชั้นความลับของเอกสาร

ง. จัดทำการพัฒนาและกำหนดนโยบายด้านความมั่นคงปลอดภัย

จ. การทำแผนพัฒนาระบบเครือข่ายให้ทันสมัย

9. ข้อใด**ไม่ใช่**การปฏิบัติตามแนวทางมาตรฐานความมั่นคงปลอดภัยของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ก. การพัฒนาและดำเนินงานสำหรับกระบวนการปฏิบัติงานตามมาตรฐานความมั่นคงปลอดภัย

ข. การตรวจสอบและการออกใบประเมินระบบ

ค. การดำเนินงานความมั่นคงปลอดภัยและการจัดการเหตุด้านความมั่นคงปลอดภัย

ง. การติดตามและประเมินผล

จ. การเปรียบเทียบข้อดีและข้อเสียประสิทธิภาพของเทคโนโลยีด้านการรักษาความปลอดภัยแต่ละประเภท

10. ข้อใดเรียงลำดับขั้นตอนในการบริหารความเสี่ยงตามแนวทางมาตรฐานความมั่นคงปลอดภัยของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ถูกต้อง

ก. บ่งชี้ปัจจัยความเสี่ยง กำหนดสภาวะแวดล้อม ระบุและจัดลำดับความเสี่ยง วิเคราะห์ความเสี่ยง พัฒนาแผนรับมือ

ข. บ่งชี้ปัจจัยความเสี่ยง กำหนดสภาวะแวดล้อม วิเคราะห์ความเสี่ยง ระบุและจัดลำดับความเสี่ยง พัฒนาแผนรับมือ

ค. กำหนดสภาวะแวดล้อม บ่งชี้ปัจจัยความเสี่ยง วิเคราะห์ความเสี่ยง ระบุและจัดลำดับความเสี่ยง พัฒนาแผนรับมือ

ง. กำหนดสภาวะแวดล้อม ระบุและจัดลำดับความเสี่ยง วิเคราะห์ความเสี่ยง พัฒนาแผนรับมือ

จ. กำหนดสภาวะแวดล้อม บ่งชี้ปัจจัยความเสี่ยง วิเคราะห์ความเสี่ยง พัฒนาแผนรับมือ

แบบประเมินผลตนเองหลังเรียน หน่วยที่ 14

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง **“นโยบายการรักษาความมั่นคงปลอดภัยแบบยั่งยืน”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. ข้อใดคือมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล

ก. มาตรฐาน ISO-9001
ข. มาตรฐาน ISO-27000
ค. มาตรฐาน ISO-2800
ง. มาตรฐาน ISO-14000
จ. มาตรฐาน ISO-50001

2. ข้อใด**ไม่ใช่**ความหมายของ ISMS (Information Security Management System)

ก. ระบบที่ใช้ในการจัดการการวางแผนของระบบความมั่นคงปลอดภัย
ข. ระบบที่ใช้ในการจัดการการประยุกต์ของระบบความมั่นคงปลอดภัย
ค. ระบบที่ใช้ในการจัดการการประเมินของระบบความมั่นคงปลอดภัย
ง. ระบบที่ใช้ในการจัดการการเฝ้าระวังของระบบความมั่นคงปลอดภัย
จ. ทุกข้อคือความหมายของ ISMS

3. ข้อใดคือมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยห่วงโซ่อุปทาน

ก. มาตรฐาน ISO-9001
ข. มาตรฐาน ISO-27000
ค. มาตรฐาน ISO-28000
ง. มาตรฐาน ISO-14000
จ. มาตรฐาน ISO-50001

4. ข้อใด**ไม่**ถูกต้องเกี่ยวกับหัวข้อของแบบจำลอง PDCA
    - ก. P-Plan คือ การวางแผน
    - **ข. P-Predict คือ การคาดการความเสี่ยงที่จะเกิด**
    - ค. D-Do คือ การลงมือทำ
    - ง. C-Check คือ การตรวจสอบ
    - จ. A-Act คือ การลงมือแก้ไข
5. ข้อใด**ไม่ใช่**หัวข้อในการสอบใบรับรองความสามารถแบบ CISSP
    - ก. ความมั่นคงปลอดภัยทางกายภาพ
    - ข. เทคโนโลยีรหัสลับ
    - **ค. ลายมือชื่อดิจิทัล**
    - ง. ความมั่นคงปลอดภัยเครือข่ายและโทรคมนาคม
    - จ. การวางแผนธุรกิจแบบต่อเนื่องและการกู้ภัยธรรมชาติ
6. ข้อใด**ไม่**ถูกต้องเกี่ยวกับใบรับรองความสามารถแบบ CISSP
    - ก. ต้องต่ออายุทุกๆ 3 ปี
    - ข. ต้องมีแต้ม CPE อย่างน้อย 120 ภายในเวลา 3 ปี
    - **ค. ต้องมีผู้เซ็นรับรองในการต่ออายุ**
    - ง. ต้องจ่ายเงินรายปี ปีละ 85 ดอลล่าห์สหรัฐ
    - จ. ทุกข้อถูกต้อง
7. มาตรฐานในข้อใด ถูกใช้อ้างอิงในการออกมาตรฐานการรักษาความมั่นคงตามแบบกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
    - ก. มาตรฐาน ISO-9001
    - **ข. มาตรฐาน ISO-27000**
    - ค. มาตรฐาน ISO-2800
    - ง. มาตรฐาน ISO-14000
    - จ. มาตรฐาน ISO-50001
8. ข้อใดระบุขั้นตอนในการปฏิบัติตามแนวทางมาตรฐานความมั่นคงปลอดภัยของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร**ไม่**ถูกต้อง
    1. กำหนดบทบาทและหน้าที่สำคัญ
    2. จัดทำเอกสารที่เกี่ยวข้อง
    3. จัดทำข้อกำหนดบัญชีชั้นความลับของเอกสาร
    4. จัดทำการพัฒนาและกำหนดนโยบายด้านความมั่นคงปลอดภัย
    5. การทำแผนพัฒนาระบบเครือข่ายให้ทันสมัย
    - ก. 1 2 และ 3
    - ข. 1 2 และ 4
    - ค. 1 3 และ 4
    - ง. 1 2 3 และ 4
    - **จ. 1 2 3 4 และ 5**

9. ข้อใด**ไม่ใช่**การปฏิบัติตามแนวทางมาตรฐานความมั่นคงปลอดภัยของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
    1. การทำพัฒนาและดำเนินงานสำหรับกระบวนการปฏิบัติงานตามมาตรฐานความมั่นคงปลอดภัย
    2. การตรวจสอบและการออกใบประเมินระบบ
    3. การดำเนินงานความมั่นคงปลอดภัยและการจัดการเหตุด้านความมั่นคงปลอดภัย
    4. การติดตามและประเมินผล
    5. การเปรียบเทียบข้อดีและข้อเสียประสิทธิภาพของเทคโนโลยีด้านการรักษาความปลอดภัยแต่ละประเภท

    ก. 1 2 และ 3
    ข. 1 2 และ 4
    ค. 1 3 และ 4
    ง. 1 2 3 และ 4
    จ. 1 2 3 4 และ 5
10. ข้อใด**ไม่ใช่**ขั้นตอนในการบริหารความเสี่ยงตามแนวทางมาตรฐานความมั่นคงปลอดภัยของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
    ก. บ่งชี้ปัจจัยความเสี่ยง
    ข. กำหนดสภาวะแวดล้อม
    ค. วิเคราะห์ความเสี่ยง
    ง. ระบุและจัดลำดับความเสี่ยง
    จ. การจำลองความเสี่ยงก่อนการเลือกวิธีการรับมือ

เฉลยแบบประเมินผลตนเองหน่วยที่ 14

ก่อนเรียน	**หลังเรียน**
1. ข.	1. ข.
2. จ.	2. จ.
3. ก.	3. ค.
4. ข.	4. ข.
5. ค.	5. ค.
6. จ.	6. ค.
7. ข.	7. ข.
8. จ.	8. จ.
9. จ.	9. จ.
10. ค.	10. จ.

แบบประเมินผลตนเองก่อนเรียน หน่วยที่ 15

วัตถุประสงค์ เพื่อประเมินความรู้เดิมของนักศึกษาเกี่ยวกับเรื่อง **“กรณีศึกษาการโจมตีระบบความมั่นคงปลอดภัย”**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. การใช้ชุดคำสั่ง SQL เพื่อโจรกรรมข้อมูลของลูกค้าเป็นกรณีศึกษาที่สามารถพบได้จากการโจมตีประเภทใด
    ก. การโจมตีแบบตลุย
    ข. การโจมตีโดยการเพิ่มอักขระพิเศษเพื่อดึงข้อมูลจากฐานข้อมูล
    ค. การโจมตีโดยการฝังโปรแกรมภาษาสคริปต์เพื่อทำงานอัตโนมัติผ่านเว็บไซต์
    ง. การโจมตีด้วยเว็บไซต์หลอกลวงผ่านทางจดหมายอิเล็กทรอนิกส์
    จ. การโจมตีเพื่อค้นหารหัสผ่านจากโปรแกรมประยุกต์
2. จากกรณีศึกษาในหน่วยการสอนที่ 15 การโจมตีเว็บไซต์โดยการเพิ่มชุดอักขระพิเศษเพื่อดึงข้อมูลจากฐานข้อมูล แบ่งออกได้เป็นกี่รูปแบบ
    ก. 1 รูปแบบ
    ข. 2 รูปแบบ
    ค. 3 รูปแบบ
    ง. 4 รูปแบบ
    จ. 5 รูปแบบ
3. จากกรณีศึกษาของการโจมตีแบบตลุย ชื่อบัญชีผู้ใช้ในข้อใดที่ถูกโจมตีบ่อย
    ก. account
    ข. admin
    ค. backup
    ง. opera
    จ. ถูกทุกข้อ
4. การโจมตีโดยใช้พจนานุกรมเป็นการโจมตีที่มีความคล้ายคลึงกับการโจมตีประเภทใด
    ก. การโจมตีโดยการเพิ่มอักขระพิเศษเพื่อดึงข้อมูลจากฐานข้อมูล
    ข. การโจมตีโดยการฝังโปรแกรมภาษาสคริปต์เพื่อทำงานอัตโนมัติผ่านเว็บไซต์
    ค. การโจมตีด้วยเว็บไซต์หลอกลวงผ่านทางจดหมายอิเล็กทรอนิกส์
    ง. การโจมตีแบบตลุย
    จ. การโจมตีเพื่อค้นหารหัสผ่านจากโปรแกรมประยุกต์
5. ข้อใด**ไม่ใช่**กรณีศึกษาของการโจมตีแบบคนกลาง
    ก. การลดระดับความสามารถในการเข้ารหัส
    ข. การย้อนรุ่นของระบบ

ค. การเปลี่ยนกุญแจเข้ารหัส

ง. การใช้พจนานุกรม

จ. การเปลี่ยนแปลงหรือแก้ไขข้อความ

6. ข้อใดคือวิธีป้องกันของกรณีศึกษาจากการโจมตีแบบคนกลางโดยการเปลี่ยนกุญแจเข้ารหัส

ก. พัฒนาระบบการสื่อสารของคอมพิวเตอร์ที่มีกระบวนการส่ง “Finished Message”

ข. ใช้ค่าคงที่จำเพาะซึ่งเป็นค่าลับที่ถูกผูกติดไว้กับข้อความ ซึ่งทั้งค่าจำเพาะและข้อความดังกล่าวจะถูกเข้ารหัส

ค. ใช้ลายมือชื่อดิจิทัล

ง. ใช้ข้อความแฮชเพื่อช่วยในการตรวจสอบข้อความ

จ. ไม่มีข้อใดถูก

7. จากกรณีศึกษาการโจมตีโพรโทคอล DHCP แบบปฏิเสธการบริการ คนร้ายมีจุดประสงค์การโจมตีคือ

ก. เพื่อให้ได้มาซึ่งข้อมูลของรหัสผ่านหรือกุญแจที่ใช้ในการเข้ารหัส

ข. เพื่อให้สามารถเข้าใจระบบการใช้กุญแจของผู้ใช้บริการ

ค. เพื่อทำให้ผู้ใช้บริการไม่สามารถใช้งานระบบเครือข่ายได้

ง. เพื่อทดสอบช่องโหว่ของระบบคอมพิวเตอร์

จ. ไม่มีข้อใดถูกต้อง

8. ข้อใด**ไม่ใช่**กรณีศึกษาของการวิเคราะห์การโจมตีด้วยการตรวจสอบลายเซ็นบนระบบเครือข่าย

ก. การโจมตีขณะที่มีการถ่ายโอนแฟ้ม

ข. การโจมตีแบบพีเอชเอฟ

ค. การโจมตีโดยการส่งข้อมูลแบบกระจาย

ง. การโจมตีแบบตลุย

จ. ถูกทุกข้อ

9. การโจมตีประเภทใดที่มีการเรียกใช้คำสั่ง “SITE Exec” ระยะไกล

ก. การโจมตีขณะที่มีการถ่ายโอนแฟ้ม

ข. การโจมตีแบบพีเอชเอฟ

ค. การโจมตีโดยการส่งข้อมูลแบบกระจาย

ง. การโจมตีแบบตลุย

จ. ถูกทุกข้อ

10. การโจมที่คนร้ายส่งชุดข้อมูลที่มีต้นทางและปลายเดียวกันเข้าสู่ระบบด้วยวิธีบอร์ดแคส เป็นการโจมตีแบบใด

ก. การโจมตีขณะที่มีการถ่ายโอนแฟ้ม

ข. การโจมตีแบบพีเอชเอฟ

ค. การโจมตีโดยการส่งข้อมูลแบบกระจาย

ง. การโจมตีแบบตลุย

จ. ถูกทุกข้อ

แบบประเมินผลตนเองหลังเรียน หน่วยที่ 15

วัตถุประสงค์ เพื่อประเมินความก้าวหน้าในการเรียนรู้ของนักศึกษาเกี่ยวกับเรื่อง **"กรณีศึกษาการโจมตีระบบความมั่นคงปลอดภัย"**

คำแนะนำ ขอให้นักศึกษาอ่านคำถามแล้วเขียนวงกลมล้อมรอบข้อคำตอบที่ถูกต้องที่สุด

---

1. การโจมตีโดยการเพิ่มอักขระพิเศษเพื่อดึงข้อมูลจากฐานข้อมูลเพื่อโจรกรรมข้อมูลของลูกค้าสามารถทำได้อย่างไร
   - ก. สร้างเว็บไซต์ปลอม
   - **ข. การใช้ชุดคำสั่ง SQL**
   - ค. ฝังโปรแกรมภาษาสคริปต์เพื่อทำงานอัตโนมัติผ่านเว็บไซต์
   - ง. หลอกลวงผ่านทางจดหมายอิเล็กทรอนิกส์โดยใช้เว็บไซต์
   - จ. หารหัสผ่านจากโปรแกรมประยุกต์
2. การโจมตีเว็บไซต์คือการเพิ่มชุดอักขระพิเศษเพื่อดึงข้อมูลจากฐานสามารถทำได้อย่างไร
   - ก. การใช้ชุดคำสั่ง SQL
   - ข. ตรวจจับอุปกรณ์ IPS
   - ค. ฝังโปรแกรมภาษาสคริปต์เพื่อทำงานอัตโนมัติผ่านเว็บไซต์
   - **ง. ข้อ ก. และ ข. ถูก**
   - จ. ถูกทุกข้อ
3. ชื่อบัญชีผู้ใช้ใดที่ถูกใช้บ่อยในการโจมตีแบบตลุย
   - ก. acc010101
   - ข. backupdata
   - **ค. user**
   - ง. test789
   - จ. webcreator
4. การโจมตีแบบตลุยสามารถกระทำได้ด้วยวิธีการใด
   - ก. การใช้ชุดคำสั่ง SQL
   - ข. ตรวจจับอุปกรณ์ IPS
   - ค. ฝังโปรแกรมภาษาสคริปต์เพื่อทำงานอัตโนมัติผ่านเว็บไซต์
   - **ง. การโจมตีโดยใช้พจนานุกรม**
   - จ. ถูกทุกข้อ

5. ข้อใดคือกรณีศึกษาของการโจมตีแบบคนกลาง
   - ก. การใช้ชุดคำสั่ง SQL
   - ข. ตรวจจับอุปกรณ์ IPS
   - ค. การเปลี่ยนแปลงหรือแก้ไขข้อความ
   - **ง. การลดระดับความสามารถในการเข้ารหัส**
   - จ. การใช้พจนานุกรม
6. ข้อใดเป็นกรณีศึกษาจากการโจมตีแบบคนกลางโดยการเปลี่ยนกุญแจเข้ารหัส
   - **ก. ใช้ลายมือชื่อดิจิทัล**
   - ข. ใช้ข้อความแฮชเพื่อช่วยในการตรวจสอบข้อความ
   - ค. พัฒนาระบบการสื่อสารของคอมพิวเตอร์ที่มีกระบวนการส่ง “Finished Message”
   - ง. ใช้ค่าคงที่จำเพาะซึ่งเป็นค่าลับที่ถูกผูกติดไว้กับข้อความ ซึ่งทั้งค่าจำเพาะและข้อความดังกล่าวจะถูกเข้ารหัส
   - จ. ไม่มีข้อใดถูก
7. ข้อใดถูกต้องจากกรณีศึกษาการโจมตีโพรโทคอล DHCP แบบปฏิเสธการบริการ
   - ก. ผู้ประสงค์ร้ายทำเพื่อให้ได้มาซึ่งข้อมูลของรหัสผ่านหรือกุญแจที่ใช้ในการเข้ารหัส
   - ข. ผู้ประสงค์ร้ายทำเพื่อให้สามารถเข้าใจระบบการใช้กุญแจของผู้ใช้บริการ
   - **ค. ผู้ประสงค์ร้ายทำเพื่อทำให้ผู้ใช้บริการไม่สามารถใช้งานระบบเครือข่ายได้**
   - ง. ผู้ประสงค์ร้ายทำเพื่อทดสอบช่องโหว่ของระบบคอมพิวเตอร์
   - จ. ไม่มีข้อใดถูกต้อง
8. ข้อใดคือกรณีศึกษาของการวิเคราะห์การโจมตีด้วยการตรวจสอบลายเซ็นบนระบบเครือข่าย
   - ก. การโจมตีด้วยเว็บไซต์หลอกลวงผ่านทางจดหมายอิเล็กทรอนิกส์
   - ข. การโจมตีเพื่อค้นหารหัสผ่านจากโปรแกรมประยุกต์
   - **ค. การโจมตีโดยการส่งข้อมูลแบบกระจาย**
   - ง. การโจมตีแบบตลุย
   - จ. ถูกทุกข้อ
9. ข้อใดคือการโจมตีขณะที่มีการถ่ายโอนแฟ้ม
   - **ก. การเรียกใช้คำสั่ง “SITE Exec” ระยะไกล**
   - ข. การใช้ชุดคำสั่ง SQL
   - ค. การตรวจจับอุปกรณ์ IPS
   - ง. การเปลี่ยนแปลงหรือแก้ไขข้อความ
   - จ. ถูกทุกข้อ

10. ข้อใดคือความหมายของการโจมตีโดยการส่งข้อมูลแบบกระจาย

ก. การโจมตีที่ใช้ชุดคำสั่ง SQL

ข. การโจมตีที่เปลี่ยนแปลงหรือแก้ไขข้อความ

ค. การโจมตีที่มีการเรียกใช้คำสั่ง “SITE Exec” ระยะไกล

ง. การโจมตีที่คนร้ายส่งชุดข้อมูลที่มีต้นทางและปลายเดียวกันเข้าสู่ระบบด้วยวิธีบอร์ดแคส

จ. ถูกทุกข้อ

เฉลยแบบประเมินผลตนเองหน่วยที่ 15

ก่อนเรียน	**หลังเรียน**
1. ข.	1. ข.
2. ข.	2. ง.
3. จ.	3. ค.
4. ง.	4. ง.
5. ง.	5. ง.
6. ค.	6. ก.
7. ค.	7. ค.
8. ง.	8. ค.
9. ก.	9. ก.
10. ค.	10. ง.