	สาขาวิชา : เทคโนโลยีสารสนเทศ **ชื่อวิชา : ระบบรักษาความปลอดภัยคอมพิวเตอร์เบื้องต้น** **รหัสวิชา : 20901-2006** **งาน : หน่วยที่ 1 เรื่อง ความรู้ทั่วไปเกี่ยวกับระบบรักษาความปลอดภัยคอมพิวเตอร์**	**ใบสั่งงาน** **แผ่นที่ : 1**	**หน้าที่**

<u>คำสั่ง</u> ให้เลือกคำตอบที่ถูกต้องที่สุดเพียงข้อเดียว

1. คำว่า "Firewall" ในบริบทของความปลอดภัยคอมพิวเตอร์หมายถึงอะไร
   - ก. โปรแกรมสำหรับสแกนไวรัส
   - ข. ฮาร์ดแวร์คอมพิวเตอร์
   - ค. อุปกรณ์เชื่อมต่ออินเทอร์เน็ต
   - ง. ระบบป้องกันการเข้าถึงผิดกฎ
2. การเข้าสู่ระบบด้วยการสร้างรหัสผ่านที่มีความซับซ้อนมีประโยชน์อย่างไร
   - ก. ลดความจำเป็นในการเปลี่ยนรหัสผ่าน
   - ข. ระบบจะทำงานได้เร็วขึ้น
   - ค. เพิ่มความปลอดภัยของบัญชีผู้ใช้
   - ง. ลดการบล็อกบัญชีผู้ใช้
3. การป้องกันการโจมตีแบบ "Phishing" คืออะไร
   - ก. การป้องกันการถูกโจมตีจากไวรัส
   - ข. การป้องกันการละเมิดลิขสิทธิ์
   - ค. การป้องกันการโจมตีทางไซเบอร์แบบลวดลาย
   - ง. การป้องกันการโจมตีด้วยการหลอกลวงข้อมูลส่วนตัว
4. อะไรคือ "Malware" ในระบบความปลอดภัยคอมพิวเตอร์
   - ก. ฮาร์ดแวร์ที่ใช้ในการเชื่อมต่อกับอินเทอร์เน็ต
   - ข. โปรแกรมที่ถูกออกแบบมาเพื่อทำความเสียหายหรือโจมตีคอมพิวเตอร์
   - ค. ระบบป้องกันไวรัส
   - ง. บริการโฮสติ้งเว็บ
5. ในทางเทคนิค "Encryption" คืออะไร
   - ก. กระบวนการที่ใช้เพื่อป้องกันการเชื่อมต่อกับอินเทอร์เน็ต
   - ข. การสร้างรหัสผ่านที่ปลอดภัย
   - ค. การเปลี่ยนข้อมูลให้เป็นรหัสลับเพื่อป้องกันการอ่านข้อมูลโดยไม่ได้รับอนุญาต
   - ง. การลบข้อมูลที่ไม่ได้ใช้
6. การอัปเดตซอฟต์แวร์เป็นขั้นตอนสำคัญในความปลอดภัยของคอมพิวเตอร์เพราะอะไร
   - ก. มันช่วยป้องกันการโจมตีแบบ Phishing
   - ข. มันทำให้คอมพิวเตอร์ทำงานได้เร็วขึ้น
   - ค. มันป้องกันการใช้งานไม่ถูกต้องของคอมพิวเตอร์
   - ง. มันแก้ไขบกพร่องความปลอดภัยที่มีในซอฟต์แวร์

	สาขาวิชา : เทคโนโลยีสารสนเทศ **ชื่อวิชา : ระบบรักษาความปลอดภัยคอมพิวเตอร์เบื้องต้น** **รหัสวิชา : 20901-2006** **งาน : หน่วยที่ 1 เรื่อง ความรู้ทั่วไปเกี่ยวกับระบบรักษาความปลอดภัยคอมพิวเตอร์**	**ใบสั่งงาน** **แผ่นที่ : 1**	**หน้าที่**

7. การสำรองข้อมูล (Backup) เป็นมาตรการใดที่สำคัญในการรักษาความปลอดภัยของข้อมูล

ก. การเปิดฟังก์ชันการกระทำ ข. การเปิดฟังก์ชันการอัปเดต

ค. การคัดลอกข้อมูลเป็นระยะ regular intervals ง. การปิดระบบอินเทอร์เน็ต

8. อะไรคือ "Two-factor authentication (2FA)" ในระบบความปลอดภัยของคอมพิวเตอร์

ก. กระบวนการการส่งข้อมูลผ่านทางอินเทอร์เน็ต ข. การตรวจสอบความถูกต้องของข้อมูล

ค. กระบวนการตรวจสอบสิทธิ์การเข้าถึง ง. การใช้สองขั้นตอนเพื่อตรวจสอบตัวตนของผู้ใช้

9. "Social engineering" เป็นเทคนิคใดที่มนุษย์โจมตีคอมพิวเตอร์โดยการหลอกลวงผู้ใช้

ก. การใช้โปรแกรมแฮ็กเกอร์ ข. การแฮ็กเข้าระบบ

ค. การใช้การสื่อสารและจิตวิญญาณเพื่อหลอกลวง ง. การใช้ความรู้ทางเทคนิค

10. การสร้างรหัสผ่านที่แข็งแรงควรปฏิบัติอย่างไร

ก. ใช้รหัสผ่านที่มีความยาวไม่น้อยกว่า 4 ตัวอักษร ข. ใช้รหัสผ่านที่ง่ายจำ

ค. ใช้รหัสผ่านเดียวกันสำหรับทุกบัญชี ง. ใช้รหัสผ่านที่มีตัวอักษรใหญ่และตัวเลข

<u>ลำดับขั้นตอนการปฏิบัติงาน</u>

1. เตรียมอุปกรณ์ในการปฏิบัติงานเช่น ปากกา ดินสอ ยางลบ
2. เตรียมคอมพิวเตอร์ที่ใช้ในการค้นหาข้อมูลเพิ่มเติม
3. ทำความเข้าใจรายละเอียดของโจทย์ในแต่ละข้อและทำการตอบคำถามให้ถูกต้องที่สุด

ข้อควรระวัง

1. แต่ละข้อไม่ควรตอบมากกว่า1 คำตอบ
2. ไม่ทำการขีดเขียน วาดรูป หรือใดๆที่ไม่มีส่วนเกี่ยวข้องกับคำตอบ

เครื่องมือและอุปกรณ์

1. เครื่องเขียน (ปากกา ดินสอ ยางลบ)
2. เครื่องคอมพิวเตอร์

เวลาในการปฏิบัติงาน

30 นาที

	สาขาวิชา : เทคโนโลยีสารสนเทศ **ชื่อวิชา : ระบบรักษาความปลอดภัยคอมพิวเตอร์เบื้องต้น** **รหัสวิชา : 20901-2006** **งาน : หน่วยที่ 2 เรื่อง การเข้ารหัสและถอดรหัสคอมพิวเตอร์**	**ใบสั่งงาน** **แผ่นที่ : 1**	**หน้าที่**

<u>คำสั่ง</u> ให้เลือกคำตอบที่ถูกต้องที่สุดเพียงข้อเดียว

1.การเข้ารหัสข้อมูลคือกระบวนการใด?

ก. การบีบอัดข้อมูล ข. การแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้

ค. การรวมข้อมูล ง. การควบคุมข้อมูล

2. รหัสผ่านเป็นตัวอย่างของข้อมูลที่ถูกเข้ารหัสอย่างไร

ก. ข้อมูลแบบเปิด ข. ข้อมูลแบบแก้ไข

ค. ข้อมูลแบบรหัส ง. ข้อมูลแบบแสดง

3. อะไรคือการเข้ารหัสแบบสมมาตร (Symmetric Encryption)

ก. การใช้คีย์สาธารณะและคีย์เดียว

ข. การใช้คีย์เฉพาะในการเข้ารหัสและถอดรหัส

ค. การใช้คีย์เดียวในการเข้ารหัสและถอดรหัส

ง. การใช้คีย์สาธารณะในการเข้ารหัสและคีย์เสม็ดส่วนตัวในการถอดรหัส

4. การถอดรหัสข้อมูลคือกระบวนการใด

ก. การแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้ ข. การเชื่อมต่อกับเครือข่าย

ค. การเปิดดูข้อมูลที่ถูกเข้ารหัส ง. การสร้างข้อมูลสุ่ม

5. การเข้ารหัสแบบ AES ใช้คีย์ขนาดเท่าไหร่

ก. 64 บิต ข. 128 บิต

ค. 256 บิต ง. 512 บิต

6. อะไรคือคีย์ที่ใช้ในการถอดรหัสแบบสมมาตร

ก. คีย์เดียวกันที่ใช้ในการเข้ารหัส ข. คีย์สาธารณะและคีย์ส่วนตัว

ค. คีย์ที่ไม่จำเป็นในการถอดรหัส ง. คีย์ที่สร้างขึ้นโดยระบบ

7.การเข้ารหัสแบบ RSA เป็นตัวอย่างของการเข้ารหัสแบบใด

ก. การเข้ารหัสแบบสมมาตร ข. การเข้ารหัสแบบการสลับ

ค. การเข้ารหัสแบบการเข้ารหัสคีย์สาธารณะ ง. การเข้ารหัสแบบการเข้ารหัสคีย์เดียว

	สาขาวิชา : เทคโนโลยีสารสนเทศ **ชื่อวิชา : ระบบรักษาความปลอดภัยคอมพิวเตอร์เบื้องต้น** **รหัสวิชา : 20901-2006** **งาน : หน่วยที่ 2 เรื่อง การเข้ารหัสและถอดรหัสคอมพิวเตอร์**	**ใบสั่งงาน** **แผ่นที่ : 1**	**หน้าที่**

8. การใช้การเข้ารหัสแบบ MD5 สำหรับการเก็บรหัสผ่านถือว่าปลอดภัยหรือไม่

ก. ปลอดภัย เพราะมีความยากต่อการถอดรหัส

ข. ไม่ปลอดภัย เพราะมีช่องโหว่ในการเข้ารหัส

ค. ปลอดภัย เพราะมีความยากต่อการบรรลุถึงคีย์

ง. ไม่ปลอดภัย เพราะมีความยากต่อการเชื่อมต่อเครือข่าย

9. ในการเข้ารหัสแบบการเข้ารหัสคีย์สาธารณะ (Public Key Encryption) มีคีย์อะไรสองอย่าง

ก. คีย์สาธารณะและคีย์เดียว ข. คีย์สาธารณะและคีย์ส่วนตัว

ค. คีย์เครือข่ายและคีย์ส่วนตัว ง. คีย์เข้ารหัสและคีย์ถอดรหัส

10. การใช้การเข้ารหัสแบบ SSL/TLS ในการเรียกข้อมูลจากเว็บไซต์ช่วยเพิ่มความปลอดภัยในข้อมูลในทางใด

ก. ความลับ ข. ความถูกต้อง

ค. ความเร็ว ง. ความสมบูรณ์

<u>ลำดับขั้นตอนการปฏิบัติงาน</u>

1. เตรียมอุปกรณ์ในการปฏิบัติงานเช่น ปากกา ดินสอ ยางลบ
2. เตรียมคอมพิวเตอร์ที่ใช้ในการค้นหาข้อมูลเพิ่มเติม
3. ทำความเข้าใจรายละเอียดของโจทย์ในแต่ละข้อและทำการตอบคำถามให้ถูกต้องที่สุด

ข้อควรระวัง

1. แต่ละข้อไม่ควรตอบมากกว่า1 คำตอบ
2. ไม่ทำการขีดเขียน วาดรูป หรือใดๆที่ไม่มีส่วนเกี่ยวข้องกับคำตอบ

เครื่องมือและอุปกรณ์

1. เครื่องเขียน (ปากกา ดินสอ ยางลบ)
2. เครื่องคอมพิวเตอร์

เวลาในการปฏิบัติงาน

30 นาที

	สาขาวิชา : เทคโนโลยีสารสนเทศ **ชื่อวิชา : ระบบรักษาความปลอดภัยคอมพิวเตอร์เบื้องต้น** **รหัสวิชา : 20901-2006** **งาน : ลักษณะของอาชญากรรม คอมพิวเตอร์**	**ใบสั่งงาน** **แผ่นที่ : 1**	**หน้าที่**

<u>คำสั่ง</u> จงแบ่งกลุ่มสรุปข้อความดังต่อไปนี้และนำเสนอหน้าชั้นเรียน

อาชญากรรมทางคอมพิวเตอร์คือการกระทำผิดกฎหมายและการละเมิดความปลอดภัยทางคอมพิวเตอร์โดยใช้เทคโนโลยีคอมพิวเตอร์ ลักษณะของอาชญากรรมทางคอมพิวเตอร์มีหลายรูปแบบและระดับความรุนแรง ซึ่งรวมถึง:

1. **การแฮกคอมพิวเตอร์ (Hacking)**: การเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายโดยไม่ได้รับอนุญาต แฮกเกอร์อาจเข้าถึงข้อมูลหรือระบบเพื่อเจตนาต่าง ๆ เช่น การโจมตีเพื่อขโมยข้อมูลส่วนบุคคลหรือข้อมูลทางธุรกิจ
2. **การโจมตีด้วยไวรัสและมัลแวร์ (Virus and Malware Attacks)**: การสร้างและแพร่กระจายไวรัสและโปรแกรมมัลแวร์เพื่อทำความเสียหายแก่ระบบคอมพิวเตอร์ โปรแกรมมัลแวร์อาจทำให้คอมพิวเตอร์ทำงานผิดปกติหรือถูกควบคุมโดยมัลแวร์
3. **การประนี้ผู้ใช้ (Phishing)**: การโจมตีโดยการส่งอีเมลล์หรือข้อความปลอมเพื่อหลอกผู้ใช้ให้เปิดลิงก์หรือให้ข้อมูลส่วนตัว เพื่อทำให้ผู้โจมตีสามารถเข้าถึงข้อมูลของผู้ใช้หรือระบบคอมพิวเตอร์
4. **การบิดเบือนข้อมูล (Data Tampering)**: การเปลี่ยนแปลงข้อมูลที่ถูกส่งหรือรับผ่านเครือข่าย เพื่อทำให้ข้อมูลไม่ถูกต้องหรือเสียหาย เช่น การแก้ไขข้อมูลการเงินในการทำธุรกรรมออนไลน์
5. **การโจมตีการบิดเบือนรหัสผ่าน (Password Cracking)**: การพยายามเดาหรือแฮกรหัสผ่านเพื่อเข้าถึงระบบหรือบัญชีของผู้ใช้โดยไม่ได้รับอนุญาต
6. **การปฏิเสธบริการ (Denial of Service, DoS)**: การโจมตีโดยทำให้ระบบหรือเครือข่ายไม่สามารถให้บริการได้ โดยการร้องขอบริการมากมายหรือโจมตีด้วยแหล่งข้อมูลที่มาก
7. **การปฏิเสธบริการแบบกระจาย (Distributed Denial of Service, DDoS)**: การโจมตีโดยใช้เครือข่ายของคอมพิวเตอร์ที่ติดเชื้อมากมายเพื่อทำให้ระบบหรือเครือข่ายไม่สามารถให้บริการได้
8. **การละเมิดความเป็นส่วนตัว (Privacy Violation)**: การเข้าถึงหรือเผยข้อมูลส่วนตัวของผู้ใช้โดยไม่ได้รับอนุญาต เช่น การแฮกบัญชีออนไลน์หรือการดักรับข้อมูลส่วนตัวผ่านเครือข่าย
9. **การเปิดโปรแกรมโปร่งใส (Backdoor Exploits)**: การใช้ช่องโหว่ในโปรแกรมหรือระบบเพื่อสร้างวิธีเข้าถึงระบบโดยไม่ได้รับอนุญาต
10. **การละเมิดลิขสิทธิ์ (Copyright Infringement)**: การละเมิดลิขสิทธิ์โดยการดาวน์โหลดหรือแจกจ่ายสิ่งพิมพ์หรือสื่อต่าง ๆ ที่มีลิขสิทธิ์โดยไม่ได้รับอนุญาต

ลักษณะของอาชญากรรมทางคอมพิวเตอร์อาจมีลักษณะการกระทำและเป้าหมายที่แตกต่างกันตามวัตถุประสงค์ของผู้โจมตี และมีผลกระทบต่อคอมพิวเตอร์และระบบข้อมูลในลักษณะที่แตกต่างกันด้วย

	สาขาวิชา : เทคโนโลยีสารสนเทศ **ชื่อวิชา : ระบบรักษาความปลอดภัยคอมพิวเตอร์เบื้องต้น** **รหัสวิชา : 20901-2006** **งาน : ลักษณะของอาชญากรรม คอมพิวเตอร์**	**ใบสั่งงาน** **แผ่นที่ : 1**	**หน้าที่**

ลำดับขั้นตอนการปฏิบัติงาน

1. เตรียมอุปกรณ์ในการปฏิบัติงานเช่น ปากกา ดินสอ ยางลบ
2. เตรียมคอมพิวเตอร์ที่ใช้ในการค้นหาข้อมูลเพิ่มเติม
3. ทำความเข้าใจรายละเอียดของโจทย์ในแต่ละข้อและทำการตอบคำถามให้ถูกต้องที่สุด

ข้อควรระวัง

1. อ่านโจทย์ให้ละเอียดแล้วตอบคำถามให้ชัดเจน ทำสไลด์เพื่อนำเสนอหน้าชั้นเรียน
2. ไม่ทำการขีดเขียน วาดรูป หรือใดๆที่ไม่มีส่วนเกี่ยวข้องกับคำตอบ

เครื่องมือและอุปกรณ์

1. เครื่องเขียน (ปากกา ดินสอ ยางลบ)
2. เครื่องคอมพิวเตอร์

เวลาในการปฏิบัติงาน

60 นาที

	สาขาวิชา : เทคโนโลยีสารสนเทศ **ชื่อวิชา : ระบบรักษาความปลอดภัยคอมพิวเตอร์เบื้องต้น** **รหัสวิชา : 20901-2006** **งาน : ประเภทของไวรัส**	**ใบสั่งงาน** **แผ่นที่ : 1**	**หน้าที่**

<u>คำสั่ง</u> จงอธิบายความหมายในหัวข้อดังต่อไปนี้ให้ถูกต้อง

1. ไวรัสโดยสาร (File Infector Virus):
2. ไวรัสตราบตาย (Non-Resident Virus):
3. ไวรัสรายวัน (Macro Virus):
4. ไวรัสอินเฟคเตอร์ (Boot Sector Virus):
5. ไวรัสตรวจสอบหลอด (Multipartite Virus):
6. ไวรัสร้ายแรง (Polymorphic Virus):
7. ไวรัสร้ายแรงแบบมีความตั้งใจ (Polymorphic Virus with Intent):
8. ไวรัสแอปเรนจ์ (Appender Virus):
9. ไวรัสเครือข่าย (Network Virus):
10. ไวรัสชาวบ้าน (Resident Virus):
11. ไวรัสโกสต์ (Ghost Virus):

<u>ลำดับขั้นตอนการปฏิบัติงาน</u>

1. เตรียมอุปกรณ์ในการปฏิบัติงานเช่น ปากกา ดินสอ ยางลบ
2. เตรียมคอมพิวเตอร์ที่ใช้ในการค้นหาข้อมูลเพิ่มเติม
3. ทำความเข้าใจรายละเอียดของโจทย์ในแต่ละข้อและทำการตอบคำถามให้ถูกต้องที่สุด

ข้อควรระวัง

1. อ่านโจทย์ให้ละเอียดแล้วตอบคำถามให้ชัดเจน
2. ไม่ทำการขีดเขียน วาดรูป หรือใดๆที่ไม่มีส่วนเกี่ยวข้องกับคำตอบ

เครื่องมือและอุปกรณ์

1. เครื่องเขียน (ปากกา ดินสอ ยางลบ)
2. เครื่องคอมพิวเตอร์

เวลาในการปฏิบัติงาน

60 นาที

	สาขาวิชา : เทคโนโลยีสารสนเทศ **ชื่อวิชา : ระบบรักษาความปลอดภัยคอมพิวเตอร์เบื้องต้น** **รหัสวิชา : 20901-2006** **งาน : วิธีป้องกันไวรัส คอมพิวเตอร์**	**ใบสั่งงาน** **แผ่นที่ : 1**	**หน้าที่**

<u>คำสั่ง</u> จงอธิบายความหมายในหัวข้อดังต่อไปนี้ให้ถูกต้อง

1. ไวรัสคอมพิวเตอร์คืออะไรและทำไมมันเป็นอันตรายต่อระบบคอมพิวเตอร์?
2. กล่าวถึงวิธีการติดตามและตรวจสอบไวรัสบนคอมพิวเตอร์ของคุณ
3. อธิบายหลักการของการสร้าง "วงแหวนความปลอดภัย" (Security Ring) เพื่อป้องกันไวรัส
4. อธิบายหลักการของการอัปเดต (Update) และทำไมการอัปเดตเป็นสิ่งสำคัญในการป้องกันไวรัส
5. จากการที่คุณทราบเกี่ยวกับการสร้างรหัสผ่านที่ปลอดภัย อธิบายวิธีการสร้างรหัสผ่านที่แข็งแรงและเลือกตัวเลือกการใช้รหัสผ่านที่ถูกต้อง
6. วิธีการหลีกเลี่ยงการติดเชื้อไวรัสผ่านอีเมลล์คือ
7. การสแกนไวรัสอย่างสม่ำเสมอในคอมพิวเตอร์สามารถทำได้โดยใช้
8. วิธีการป้องกันการติดเชื้อไวรัสจากเว็บไซต์ที่ไม่น่าเชื่อถือคือ
9. หากคุณรับข้อความอัปเดตรหัสผ่านจากธนาคารผ่านอีเมลล์ ควรทำอย่างไร
10. การป้องกันไวรัสคอมพิวเตอร์คืออะไรและทำไมมันสำคัญ

<u>ลำดับขั้นตอนการปฏิบัติงาน</u>

1. เตรียมอุปกรณ์ในการปฏิบัติงานเช่น ปากกา ดินสอ ยางลบ
2. เตรียมคอมพิวเตอร์ที่ใช้ในการค้นหาข้อมูลเพิ่มเติม
3. ทำความเข้าใจรายละเอียดของโจทย์ในแต่ละข้อและทำการตอบคำถามให้ถูกต้องที่สุด

ข้อควรระวัง

1. อ่านโจทย์ให้ละเอียดแล้วตอบคำถามให้ชัดเจน
2. ไม่ทำการขีดเขียน วาดรูป หรือใดๆที่ไม่มีส่วนเกี่ยวข้องกับคำตอบ

เครื่องมือและอุปกรณ์

1. เครื่องเขียน (ปากกา ดินสอ ยางลบ)
2. เครื่องคอมพิวเตอร์

เวลาในการปฏิบัติงาน

60 นาที

	สาขาวิชา : เทคโนโลยีสารสนเทศ **ชื่อวิชา : ระบบรักษาความปลอดภัยคอมพิวเตอร์เบื้องต้น** **รหัสวิชา : 20901-2006** **งาน : การรักษาความปลอดภัย บนเครือข่ายอินเตอร์เน็ต**	**ใบสั่งงาน** **แผ่นที่ : 1**	**หน้าที่**

<u>คำสั่ง</u> จงอธิบายความหมายในหัวข้อดังต่อไปนี้ให้ถูกต้อง

1. อธิบายความหมายของความปลอดภัยบนเครือข่ายอินเตอร์เน็ต และทำไมความปลอดภัยเป็นสิ่งสำคัญในระบบอินเตอร์เน็ต
2. ระบุและอธิบายประเภทหลัก ๆ ของการโจมตีบนเครือข่ายอินเตอร์เน็ต (เช่น การแฮกเกอร์, การดักรับข้อมูล)
3. อธิบายหลักการของการใช้ประจำระบบปฏิบัติการและโปรแกรมป้องกันไวรัสเพื่อประสิทธิภาพในการรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต
4. อธิบายหลักการของการใช้เครือข่ายส่วนตัว (Virtual Private Network, VPN) เพื่อเพิ่มความปลอดภัยในการส่งข้อมูลผ่านเครือข่ายอินเตอร์เน็ต
5. ระบุและอธิบายวิธีการป้องกันการโจมตีการบิดเบือนข้อมูล (Data Tampering) ในการสื่อสารผ่านเครือข่าย

<u>ลำดับขั้นตอนการปฏิบัติงาน</u>

1. เตรียมอุปกรณ์ในการปฏิบัติงานเช่น ปากกา ดินสอ ยางลบ
2. เตรียมคอมพิวเตอร์ที่ใช้ในการค้นหาข้อมูลเพิ่มเติม
3. ทำความเข้าใจรายละเอียดของโจทย์ในแต่ละข้อและทำการตอบคำถามให้ถูกต้องที่สุด

ข้อควรระวัง

1. อ่านโจทย์ให้ละเอียดแล้วตอบคำถามให้ชัดเจน
2. ไม่ทำการขีดเขียน วาดรูป หรือใดๆที่ไม่มีส่วนเกี่ยวข้องกับคำตอบ

เครื่องมือและอุปกรณ์

1. เครื่องเขียน (ปากกา ดินสอ ยางลบ)
2. เครื่องคอมพิวเตอร์

เวลาในการปฏิบัติงาน

60 นาที