การใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัย

หน่วยการเรียนรู้ที่3

ความปลอดภัยของระบบสารสนเทศ

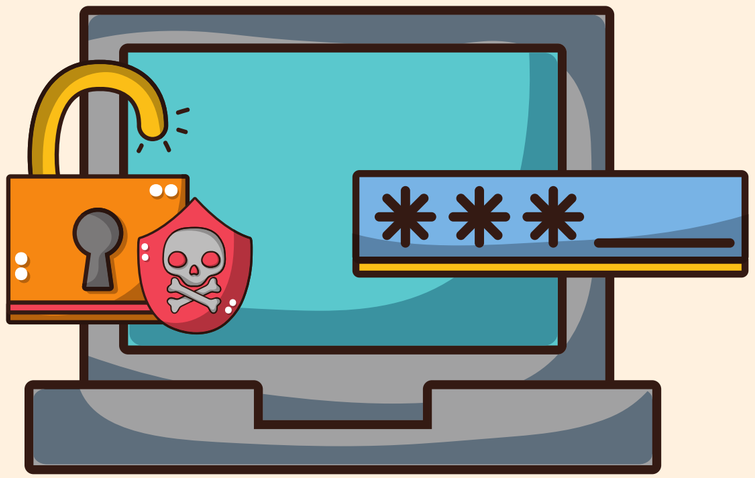
นโยบาย ขั้นตอนการปฏิบัติ และมาตรการทางเทคนิคที่นำมาใช้ป้องกันการใช้งานจากบุคคลภายนอก มาทำการขโมย หรือการทำความเสียหายต่อเทคโนโลยีสารสนเทศ

ภัยคุกคามต่อเทคโนโลยีสารสนเทศ แบ่งออกเป็น4ประเภท ดังนี้

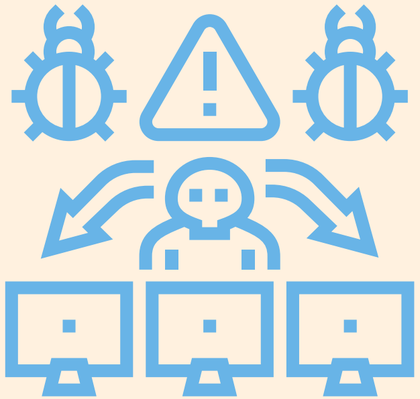
ภัยคุกคามต่อฮาร์ดแวร์

เป็นภัยคุกคามที่ทำให้อุปกรณ์คอมพิวเตอร์ฮาร์ดแวร์เกิดการเสียหาย เช่น คอมพิวเตอร์เกิดความผิดพลาดชำรุด เสียหายและไม่สามารถใช้งานได้

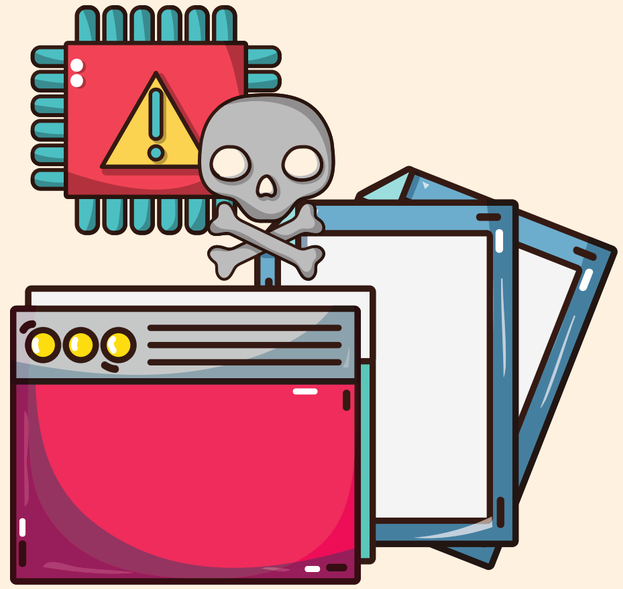
ภัยคุกคามต่อซอฟต์แวร์



เป็นภัยคุกคามที่ทำให้ซอฟต์แวร์ใช้งานไม่ได้หรือซอฟต์แวร์ทำงานผิดพลาด



ภัยคุกคามต่อระบบเครือข่ายและการสื่อสาร



เป็นภัยคุกคามที่ทำมีผลทำให้ระบบของเครือข่ายและการสื่อสารขัดข้อง ไม่สามารถใช้งานในระบบเครือข่ายและการสื่อสารได้

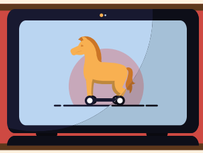
ภัยคุกคามต่อข้อมูล

เป็นภัยคุกคามที่ทำให้ข้อมูลที่เป็นส่วนตัวหรือ
เป็นความลับถูกเปิดเผยโดยไม่ได้รับอนุญาต
การเปลี่ยนแปลง การลบ การแก้ไข

รูปแบบภัยคุกคามต่อระบบรักษาความปลอดภัยทางคอมพิวเตอร์

ภัยคุกคามแก่ระบบ	เป็นภัยคุกคามจากผู้มีเจตนาร้ายเข้ามาทำการปรับเปลี่ยนแก้ไข หรือลบไฟล์ข้อมูลสำคัญภายในระบบคอมพิวเตอร์
ภัยคุกคาม ความเป็นส่วนตัว	เป็นภัยคุกคามที่แครกเกอร์(cracker) เข้ามาทำการเจาะข้อมูล ส่วนบุคคล หรือติดตามร่องรอยพฤติกรรมของผู้ใช้งาน
ภัยคุกคาม ต่อผู้ใช้และระบบ	เป็นภัยคุกคามที่ส่งผลเสียให้แก่ผู้ใช้งานและเครื่องคอมพิวเตอร์ เป็นอย่างมาก เช่น การล็อคเครื่องคอมพิวเตอร์
ภัยคุกคาม ที่ไม่มีเป้าหมาย	เป็นภัยคุกคามที่ไม่มีเป้าหมายแน่นอน เพียงแค่ต้องการสร้างจุด สนใจ โดยไม่ก่อให้เกิดความเสียหายขึ้น
ภัยคุกคาม ที่สร้างความรำคาญ	เป็นภัยคุกคามที่ไม่ก่อให้เกิดความเสียหายเช่น เปลี่ยนการตั้งค่าการ ทำงานของเครื่องคอมพิวเตอร์ให้ต่างไปจากที่เคยกำหนดไว้

รูปแบบภัยคุกคามต่อระบบรักษาความปลอดภัยทางคอมพิวเตอร์

มัลแวร์ (malware)	โปรแกรมที่ถูกสร้างขึ้นมาเพื่อขโมยข้อมูล	
ไวรัสคอมพิวเตอร์ (computer virus)	โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเพื่อทำลายข้อมูล	
ม้าโทรจัน (trojan horse)	โปรแกรมคอมพิวเตอร์ที่ถูกบรรจุเข้าไปเพื่อเก็บข้อมูลหรือทำลายข้อมูล	
หนอนคอมพิวเตอร์ (computer worm)	โปรแกรมที่แพร่กระจายผ่านอินเตอร์เน็ตเพื่อสร้างความเสียหาย หรือขโมยข้อมูล	
สปายแวร์ (spyware)	โปรแกรมที่ฝังตัวอยู่ในคอมพิวเตอร์ทำให้ทราบข้อมูลประวัติการใช้ของผู้ใช้งาน	

การป้องกันการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย

หมั่นตรวจสอบและอัปเดตระบบปฏิบัติการให้เป็นเวอร์ชั่นปัจจุบันและควรใช้ระบบปฏิบัติการและซอฟแวร์ที่ถูกลิขสิทธิ์

สังเกตขณะเปิดเครื่องว่ามีโปรแกรมไม่พึงประสงค์ทำงานขึ้นมาพร้อมกับการเปิดเครื่องหรือไม่

ติดตั้งโปรแกรมป้องกันไวรัสและมีการอัปเดตโปรแกรมป้องกันไวรัสและฐานข้อมูลไวรัสสม่ำเสมอ

ต้องlogin เข้าใช้งานทุกครั้ง และเมื่อไม่ได้อยู่หน้าจอคอมพิวเตอร์ควรล็อคหน้าจอให้อยู่ในสถานะที่ต้องใส่คำว่าlogin ใช้งาน

การป้องกันการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย

ติดตั้งไฟร์วอลล์ เพื่อป้องกันคนที่ไม่ได้รับอนุญาตไม่ให้เข้ามาใช้งานเครื่องคอมพิวเตอร์ซึ่งช่วยป้องกันการบุกรุกของแฮกเกอร์

ไม่ควรเข้าเว็บไซต์เสี่ยงภัย เช่น เว็บไซต์ลามกอนาจาร เว็บไซต์การพนัน เว็บไซต์แบบแนบไฟล์ .exe เว็บไซต์ที่มี pop-up หลายเพจ

ควรแบ็คอัปข้อมูลไว้ในอุปกรณ์หน่วยความจำอื่นนอกเหนือจากฮาร์ดดิสก์ เช่น flash drive,DVD เป็นต้น

ไม่เปิดเผยข้อมูลส่วนตัวผ่านสื่อสังคมออนไลน์ เช่น เลขที่บัตรประชาชน ประวัติการทำงาน เบอร์โทรศัพท์ หมายเลขบัตรเครดิต

ประโยชน์และโทษ

ประโยชน์ได้แก่

1.ใช้ในการติดต่อสื่อสารได้อย่างรวดเร็ว

2.ทำให้เกิดเทคโนโลยีใหม่ๆ

3.ใช้ในการสืบค้นข้อมูลจากแหล่งเรียนรู้ทางอินเตอร์เน็ตได้รวดเร็ว

4.ได้รับความรู้และความบันเทิง

โทษได้แก่

1.การมีส่วนร่วมในสังคมน้อยลง เพราะติดเทคโนโลยีมากขึ้น
2.มีโอกาสถูกขโมยข้อมูลการเข้าใช้โปรแกรมต่างๆ
3.ปัญหาการหลอกลวงที่ส่งมาทางอุปกรณ์เทคโนโลยี
4.ปัญหาด้านสุขภาพที่เกิดจากการใช้งานนานเกินไป

แฮกเกอร์
(Hacker)

แครกเกอร์
(Cracker)

แฮกเกอร์ (HACKER)

เป็นผู้เชี่ยวชาญที่มีความรู้ในการถอดรหัสหรือเจาะรหัสได้
มีวัตถุประสงค์ เพื่อทดสอบความสามารถของตนเอง
เป็นกลุ่มคนที่มีความรู้ด้านคอมพิวเตอร์
แสวงหาความรู้ใหม่ๆ อยากรู้ อยากลอง

แครกเกอร์ (CRACKER)

เป็นผู้เชี่ยวชาญที่มีความรู้ในการถอดรหัส
หรือเจาะรหัสได้ มีวัตถุประสงค์เพื่อบุกรุกระบบ
เพื่อขโมยข้อมูลหรือทำลายข้อมูลของคนอื่น
โดยผิดกฎหมาย

จริยธรรมในการใช้เทคโนโลยีสารสนเทศ

หลักศีลธรรมจรรยาที่กำหนดขึ้นเพื่อใช้เป็นแนวปฏิบัติ หรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศ จริยธรรมเกี่ยวกับการใช้เทคโนโลยีสารสนเทศแบ่งออกเป็น4ประเด็นดังนี้

1

ความเป็นส่วนตัว

สิทธิที่เจ้าของสามารถ
ที่จะควบคุม
ข้อมูลของตนเองใน
การเปิดเผยให้กับผู้อื่น

2

ความถูกต้อง

ข้อมูลควรได้รับ
การตรวจสอบ
ความถูกต้อง
รวมถึงการปรับปรุง
ข้อมูลให้ทันสมัยอยู่เสมอ

3

ความเป็นเจ้าของ

เป็นกรรมสิทธิ์ใน
การถือครองทรัพย์สิน
ซึ่งอาจเป็นทรัพย์สินทั่วไป
ที่จับต้องได้

4

การเข้าถึงข้อมูล

การกำหนดสิทธิ
ของผู้ใช้งาน
เพื่อเป็นการป้องกัน
การเข้าถึงข้อมูลลับ

จริยธรรมในการใช้เทคโนโลยีสารสนเทศ

ไม่ใช้คอมพิวเตอร์เพื่อก่ออาชญากรรม

ไม่ใช้คอมพิวเตอร์ในการโจรกรรมข้อมูลข่าวสาร

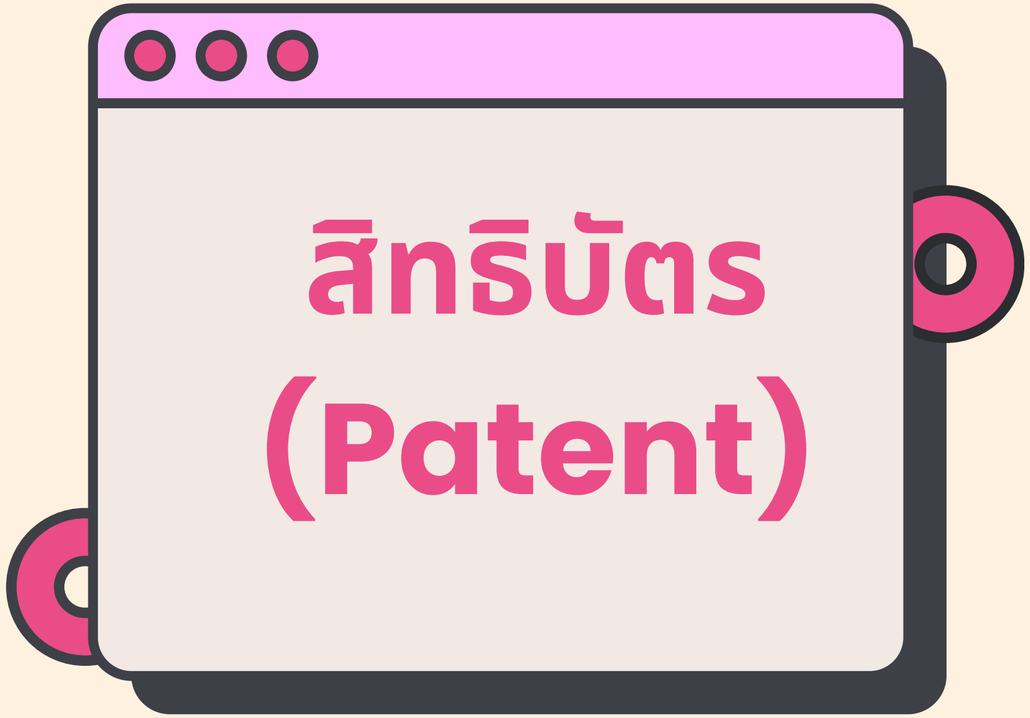
ไม่ใช้คอมพิวเตอร์รบกวนผู้อื่น

ไม่ใช้คอมพิวเตอร์สร้างหลักฐานเท็จ

ไม่ทำการสอดแนม แก้ไขเอกสารของผู้อื่น

ไม่ใช้คอมพิวเตอร์คัดลอกโปรแกรมที่มีลิขสิทธิ์


ลิขสิทธิ์
(Copyright)


สิทธิบัตร
(Patent)

ลิขสิทธิ์ (Copyright)

"สิทธิที่กฎหมายรับรองให้ผู้สร้างสรรค์กระทำการใดๆ
เกี่ยวกับงานที่ตนได้ทำขึ้น"
ซึ่งหลังจากมีการเผยแพร่แล้ว
ลิขสิทธิ์จะตกเป็นของผู้สร้างโดยอัตโนมัติ

ลิขสิทธิ์ (Copyright

การได้มาซึ่งสิทธิ์
1.สิทธิ์ในลิขสิทธิ์เกิดขึ้นทันที นับตั้งแต่สร้างสรรค์ผลงาน โดยไม่ต้องจดทะเบียน
2. มีอายุคุ้มครองต่อไปอีกถึง 50 ปี นับตั้งแต่ผู้สร้างสรรค์คนสุดท้ายเสียชีวิต
3. ให้ความคุ้มครองโดยอัตโนมัติแก่ทายาท

สิทธิบัตร (Patent)

“ หนังสือที่รัฐออกให้เพื่อคุ้มครอง
การประดิษฐ์หรือการออกแบบผลิตภัณฑ์
ต้องยื่นขอจดสิทธิบัตรไปยังกรม ทรัพย์สินทางปัญญา

ข้อกำหนด ข้อตกลงในการใช้แหล่งข้อมูล

แสดงที่มา (Attribution:By)
ต้องแสดงที่มาของชิ้นงานตามรูปแบบที่ผู้สร้างกำหนด

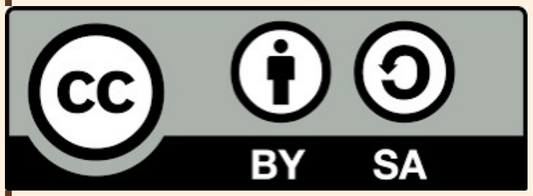
ไม่ใช้เพื่อการค้า (Noncommercial:NC
ไม่ให้นำข้อมูลนี้ไปใช้เพื่อวัตถุประสงค์ทางการค้า

ไม่ดัดแปลง (No Derivative works:ND)
ไม่แก้ไขดัดแปลงหรือสร้างงานจากงานนี้

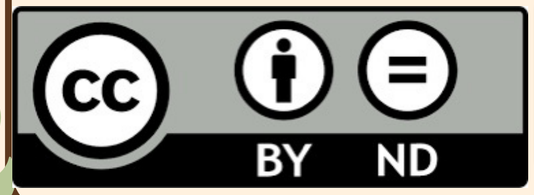
อนุญาตแบบเดียวกัน (Share Alike:SA)
ถ้าดัดแปลงชิ้นงานนี้ ต้องใช้สัญญาอนุญาต
แบบเดียวกันกับสัญญา ที่ใช้กับงานนี้เท่านั้น

ข้อกำหนด ข้อตกลงในการใช้แหล่งข้อมูล

CC-BY
ให้เผยแพร่ ดัดแปลง โดนต้องระบุที่มา

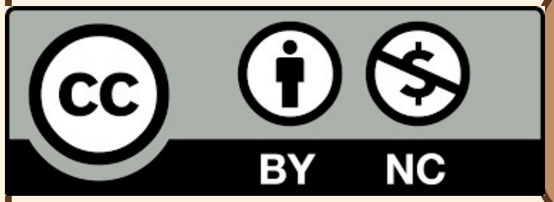


CC-BY-SA
ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มา และต้องเผยแพร่งานดัดแปลง โดยใช้สัญญาอนุญาตเดียวกัน



CC-BY-ND
ให้เผยแพร่ โดยต้องระบุที่มา แต่ห้ามดัดแปลง

ข้อกำหนด ข้อตกลงในการใช้แหล่งข้อมูล



CC-BY-NC
ให้เผยแพร่ ดัดแปลง โดยระบุที่มา
ถ้าห้ามใช้เพื่อการค้า

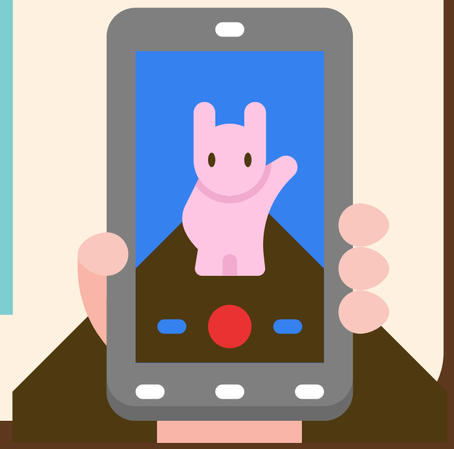
CC-BY-NC-SA
ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มาแต่ห้ามใช้เพื่อการค้า
และต้องเผยแพร่งานดัดแปลงโดยใช้สัญญาอนุญาตเดียวกัน

CC-BY-NC-ND
ให้เผยแพร่ โดยต้องระบุที่มา แต่ห้ามดัดแปลง
และห้ามใช้เพื่อการค้า

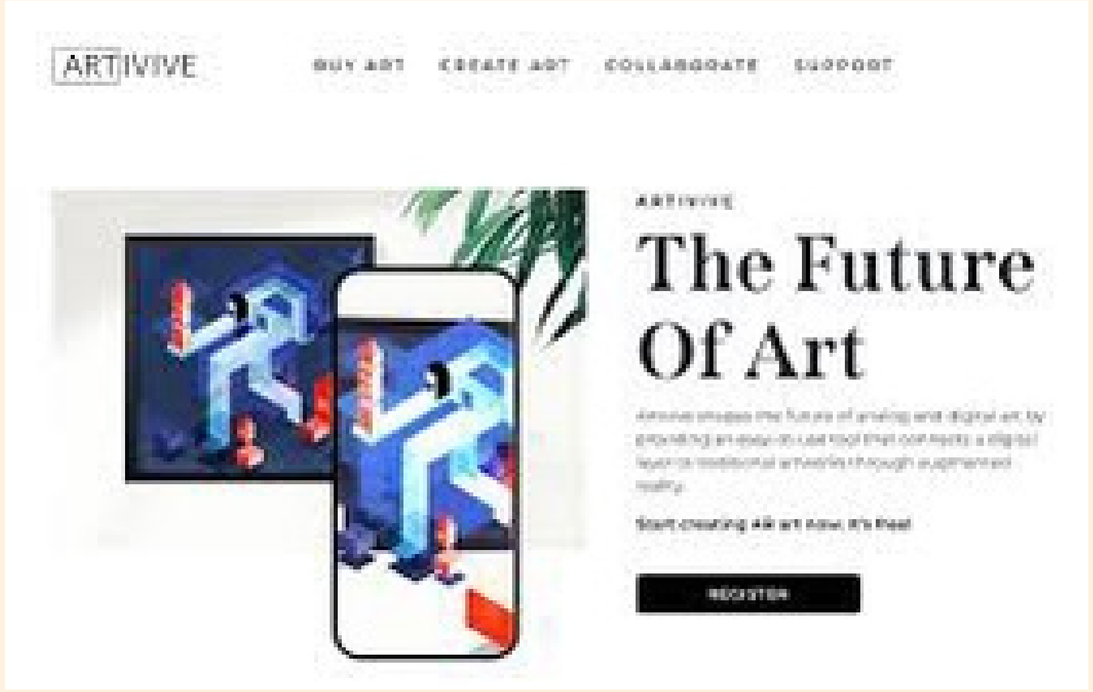
งานเก็บคะแนนชิ้นที่3

ให้นักเรียนสร้างชิ้นงานAugmented reality (AR)
โดยใช้เว็บไซต์Ativive โดยมีรายละเอียดดังนี้
ให้นักเรียนเลือกหัวข้อที่สนใจมา1หัวข้อดังนี้
1.รูปแบบภัยคุกคามด้านข้อมูลในคอมพิวเตอร์
2.การป้องกันการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย
3.วิธีป้องกันการถูกโจรกรรมข้อมูล
4.ประโยขน์และโทษจากการใช้เทคโนโลยีสารสนเทศ
5.การปฏิบัติตนเมื่อพบเนื้อหาที่ไม่เหมาะสม
จากนั้นสร้างโปสเตอร์จากหัวข้อที่ตัวเองเลือกโดยใช้
โปรแกรมCanva

ตัวอย่างชิ้นงาน

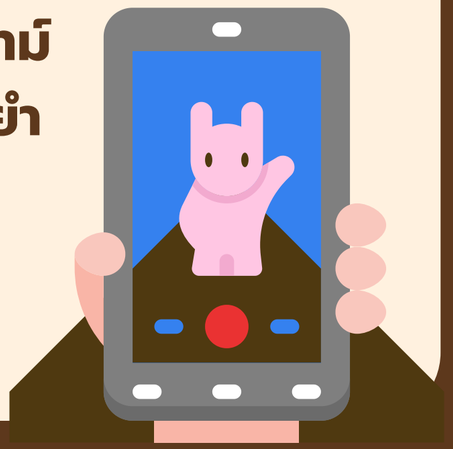


หน้าตาเว็บไซต์ที่จะใช้สร้างชิ้นงานAR



ทำความรู้จักกับAR

AR คืออะไร ความเป็นจริงเสริมเป็นสภาพแวดล้อมที่สร้างขึ้นเพื่อเลียนแบบสภาพแวดล้อมจริงๆ โดยอาศัยองค์ประกอบของการแสดงผลด้วยภาพแบบดิจิทัล รวมไปถึงเสียงและสิ่งกระตุ้นอื่นๆ ผ่านเทคโนโลยีฮอโลกราฟี AR ประกอบด้วยคุณสมบัติสามประการ ได้แก่ การผสมผสานระหว่างโลกดิจิทัลและโลกแห่งความเป็นจริง การโต้ตอบที่เกิดขึ้นแบบเรียลไทม์ และการระบุวัตถุเสมือนจริงและวัตถุจริงแบบ 3 มิติที่แม่นยำ



END