การสอบประกาศนียบัตร CompTIA A+ วัตถุประสงค์ของ Core 2

รหัสข้อสอบ: **CORE 2 (220-1102)**

CompTIA

เกี่ยวกับข้อสอบ

ผู้สมัครสอบสามารถใช้เอกสารฉบับนี้เพื่อช่วยเตรียมความพร้อมสำหรับข้อสอบ CompTIA A+ 220-1102 ได้ ท่านจะต้องผ่านการทดสอบสองชุดจึงจะได้รับประกาศนียบัตร CompTIA A+ ซึ่งได้แก่ Core 1 (220-1101) และ Core 2 (220-1102) ข้อสอบ Core 1 (220-1101) และ Core 2 (220-1102) สำหรับประกาศนียบัตร CompTIA A+ จะเป็นการยืนยันว่าผู้สมัครที่สอบผ่านมีความรู้และทักษะที่จำเป็นสำหรับการดำเนินการดังต่อไปนี้

- ติดตั้ง กำหนดค่า และบำรุงรักษาอุปกรณ์คอมพิวเตอร์ อุปกรณ์เคลื่อนที่ และซอฟต์แวร์ให้กับผู้ใช้ปลายทาง
- ซ่อมบำรุงชิ้นส่วนต่าง ๆ ตามความต้องการของลูกค้า
- เข้าใจพื้นฐานด้านระบบเครือข่ายและประยุกต์ใช้วิธีพื้นฐานในการรักษาความปลอดภัยทางไซเบอร์เพื่อลดภัยคุกคาม
- ทำการวินิจฉัยได้อย่างเหมาะสมและปลอดภัย แก้ไขและบันทึกปัญหาเกี่ยวกับฮาร์ดแวร์และซอฟต์แวร์ที่พบได้ทั่วไป
- ประยุกต์ใช้ทักษะในการแก้ปัญหาและให้บริการสนับสนุนลูกค้าโดยใช้ทักษะการสื่อสารที่เหมาะสม
- เข้าใจพื้นฐานของการเขียนสคริปต์ เทคโนโลยีระบบคลาวด์ ระบบเสมือน และการนำหลากหลาย OS ไปใช้ภายในสภาพแวดล้อมองค์กร

คุณสมบัติเหล่านี้เทียบเท่ากับประสบการณ์ภาคปฏิบัติเป็นระยะเวลา 12 เดือนในการประกอบอาชีพผู้ให้บริการสนับสนุนในศูนย์ช่วยเหลือ ช่างเทคนิคผู้ให้บริการสนับสนุนเดสก์ท็อป หรือช่างเทคนิคผู้ให้บริการภาคสนาม ตัวอย่างเนื้อหาเหล่านี้มีเป้าหมายเพื่ออธิบายวัตถุประสงค์ของการสอบเท่านั้น โดยไม่ถือว่าเป็นรายการหัวข้อเนื้อหาทั้งหมดของข้อสอบชุดนี้

การรับรองการสอบ

การสอบ CompTIA A+ Core 2 (220-1102) ผ่านการรับรองจากสถาบันมาตรฐานอเมริกัน (ANSI) ตามมาตรฐาน ISO 17024 ซึ่งผ่านการทบทวนและปรับปรุงวัตถุประสงค์ของข้อสอบอย่างสม่ำเสมอ

การจัดทำข้อสอบ

ข้อสอบ CompTIA เป็นผลจากการประชุมเชิงปฏิบัติการของผู้เชี่ยวชาญในหัวข้อเนื้อหาที่สำคัญ และผลสำรวจเกี่ยวกับทักษะและความรู้ที่จำเป็นสำหรับผู้ประกอบวิชาชีพด้าน IT ระดับเริ่มต้น

นโยบายการใช้เนื้อหาที่ได้รับอนุญาตของ CompTIA

CompTIA Certifications, LLC ไม่มีส่วนเกี่ยวข้องกับและไม่ได้อนุญาต สนับสนุน หรือยอมให้มีการใช้เนื้อหาใดที่จัดหาให้โดยเว็บไซต์การฝึกอบรมภายนอกที่ไม่ได้รับอนุญาต (หรือที่เรียกว่า “Brain Dump”) ผู้ที่ใช้เนื้อหาดังกล่าวเพื่อเตรียมความพร้อมสำหรับการสอบ CompTIA ใด ๆ จะถูกเพิกถอนประกาศนียบัตรของตนและถูกระงับไม่ให้ดำเนินการทดสอบในอนาคตตามข้อตกลงผู้สมัครสอบ CompTIA เนื่องจากต้องการสื่อสารเกี่ยวกับนโยบายการสอบของ CompTIA ว่าด้วยการใช้เนื้อหาการเรียนรู้ที่ไม่ได้รับอนุญาตอย่างชัดเจนยิ่งขึ้น CompTIA ขอให้ผู้สมัครสอบประกาศนียบัตรทุกท่านไปที่นโยบายการสอบประกาศนียบัตร CompTIA โปรดทบทวนนโยบายทั้งหมดของ CompTIA ก่อนที่จะเริ่มต้นกระบวนการเรียนรู้สำหรับการสอบ CompTIA ใด ๆ ผู้สมัครสอบจะต้องปฏิบัติตามข้อตกลงผู้สมัครสอบ CompTIA หากผู้สมัครสอบมีข้อสงสัยว่าเนื้อหาการเรียนรู้ถือว่าไม่ได้รับอนุญาตหรือไม่ (หรือที่เรียกว่า “Brain Dump”) ผู้สมัครสอบควรติดต่อ CompTIA ที่ examsecurity@comptia.org เพื่อตรวจสอบยืนยัน

โปรดทราบ

รายการตัวอย่างที่ระบุไว้ในรูปแบบหัวข้อย่อยไม่ใช่รายการที่ครบถ้วนสมบูรณ์ ตัวอย่างอื่น ๆ ของเทคโนโลยี กระบวนการ หรืองานที่เกี่ยวข้องกับวัตถุประสงค์แต่ละข้ออาจรวมอยู่ในข้อสอบด้วย แม้ว่าจะไม่ได้ระบุอยู่ในรายการหรือถูกกล่าวถึงในเอกสารวัตถุประสงค์ฉบับนี้ก็ตาม CompTIA มีการดำเนินการทบทวนเนื้อหาข้อสอบและปรับปรุงคำถามในข้อสอบอย่างสม่ำเสมอ เพื่อให้ข้อสอบของเรามีข้อมูลเป็นปัจจุบันและเพื่อรักษาความปลอดภัยในการเก็บรักษาคำถามให้เป็นความลับ ในกรณีที่จำเป็น เราจะจัดทำข้อสอบฉบับปรับปรุงโดยอ้างอิงจากจุดประสงค์ของข้อสอบเดิม โปรดทราบว่าสื่อเตรียมสอบทั้งหมดที่เกี่ยวข้องจะยังคงสามารถใช้ได้อยู่

รายละเอียดการทดสอบ

ข้อสอบที่กำหนด	A+ Core 2 (220-1102)
จำนวนคำถาม	สูงสุด 90 ข้อ
ประเภทคำถาม	ข้อสอบแบบเลือกตอบและอ้างอิงตามผลการดำเนินงาน
ระยะเวลาการทดสอบ	90 นาที
ประสบการณ์ที่แนะนำ	ประสบการณ์ภาคปฏิบัติเป็นระยะเวลา 12 เดือนในการประกอบอาชีพช่างเทคนิคผู้ให้บริการสนับสนุนในศูนย์ช่วยเหลือ ช่างเทคนิคผู้ให้บริการสนับสนุนเดสก์ท็อป หรือช่างเทคนิคผู้ให้บริการภาคสนาม
คะแนนสอบผ่าน	700 (ในระดับคะแนน 100-900)

วัตถุประสงค์การสอบ (ขอบเขต)

ตารางด้านล่างแสดงขอบเขตที่ข้อสอบชุดนี้วัดผลและสัดส่วนการให้คะแนน

ขอบเขต		อัตราส่วนร้อยของข้อสอบ
1.0	ระบบปฏิบัติการ Windows	31%
2.0	การรักษาความปลอดภัย	25%
3.0	การแก้ไขปัญหาซอฟต์แวร์	22%
4.0	ขั้นตอนการปฏิบัติงาน	22%
รวม		**100%**

หมายเหตุสำหรับ WINDOWS 11

Microsoft® Windows® เวอร์ชันที่ไม่ได้มีการยุติการสนับสนุน Mainstream Support (ตามที่ Microsoft กำหนด) จนถึงและรวมถึง Windows 11 เป็นขอบเขตเนื้อหาที่มุ่งหมายในประกาศนียบัตร ดังนั้น วัตถุประสงค์ที่ไม่ได้ระบุเวอร์ชันที่เฉพาะเจาะจงของ Microsoft Windows ในวัตถุประสงค์หลักสามารถรวมถึงเนื้อหาที่เกี่ยวข้องกับ Windows 10 และ Windows 11 ตามที่เกี่ยวข้องกับบทบาทหน้าที่การงาน

1.0 ระบบปฏิบัติการ

1.1 ระบุคุณสมบัติพื้นฐานของ Microsoft Windows รุ่นต่าง ๆ

- **Windows 10 รุ่นต่าง ๆ**
  - Home
  - Pro
  - Pro for Workstations
  - Enterprise
- **ความแตกต่างของคุณสมบัติ**
  - ระหว่างการเข้าถึงโดเมนและเวิร์กกรุ๊ป
  - ลักษณะเดสก์ท็อป/อินเทอร์เฟซผู้ใช้
  - ความพร้อมใช้งานของโปรโตคอลเดสก์ท็อปจากระยะไกล (Remote Desktop Protocol หรือ RDP)
  - ข้อจำกัดในการรองรับหน่วยความจำเข้าถึงโดยสุ่ม (Random-access Memory หรือ RAM)
  - BitLocker
  - gpedit.msc
- **เส้นทางการอัปเกรด**
  - การอัปเกรดในตัว

1.2 ใช้เครื่องมือบรรทัดคำสั่งของ Microsoft ที่เหมาะสมตามสถานการณ์สมมติ

- **การนำทาง**
  - cd
  - dir
  - md
  - rmdir
  - อินพุตการนำทาง:
    - C: หรือ D: หรือ x:
- **เครื่องมือบรรทัดคำสั่ง**
  - ipconfig
  - ping
  - hostname
  - netstat
  - nslookup
  - chkdsk
  - net user
  - net use
  - tracert
  - format
  - xcopy
  - copy
  - robocopy
  - gpupdate
  - gpresult
  - shutdown
  - sfc
  - [command name] /?
  - diskpart
  - pathping
  - winver

1.3 ใช้คุณสมบัติและเครื่องมือของระบบปฏิบัติการ (OS) ของ Microsoft Windows 10 ตามสถานการณ์สมมติ

- **ตัวจัดการงาน**
  - บริการ
  - การเริ่มต้น
  - ประสิทธิภาพ
  - กระบวนการ
  - ผู้ใช้
- **สแนปอินคอนโซลการจัดการ Microsoft (Microsoft Management Console หรือ MMC)**
  - ตัวแสดงเหตุการณ์ (eventvwr.msc)
  - การจัดการดิสก์ (diskmgmt.msc)
  - ตัวกำหนดเวลางาน (taskschd.msc)
  - ตัวจัดการอุปกรณ์ (devmgmt.msc)
  - ตัวจัดการใบรับรอง (certmgr.msc)
  - ผู้ใช้และกลุ่มภายใน (lusrmgr.msc)
  - ตัวตรวจสอบประสิทธิภาพ (perfmon.msc)
  - ตัวแก้ไขนโยบายกลุ่ม (gpedit.msc)
- **เครื่องมือเพิ่มเติม**
  - ข้อมูลระบบ (msinfo32.exe)
  - ตัวตรวจสอบทรัพยากร (resmon.exe)
  - การกำหนดค่าระบบ (msconfig.exe)
  - การล้างข้อมูลบนดิสก์ (cleanmgr.exe)
  - การจัดเรียงข้อมูลบนดิสก์ (dfrgui.exe)
  - ตัวช่วยแก้ไขรีจิสทรี (regedit.exe)

1.4 ใช้ยูทิลิตี้แผงควบคุมของ Microsoft Windows 10 ตามสถานการณ์สมมติ

- **ตัวเลือกอินเทอร์เน็ต**
- **อุปกรณ์และเครื่องพิมพ์**
- **โปรแกรมและคุณสมบัติ**
- **ศูนย์เครือข่ายและการแบ่งปัน**
- **ระบบ**
- **ไฟร์วอลล์ของ Windows Defender**
- **จดหมาย**
- **เสียง**
- **บัญชีผู้ใช้**
- **ตัวจัดการอุปกรณ์**
- **ตัวเลือกการจัดทำดัชนี**
- **เครื่องมือด้านการดูแลระบบ**
- **ตัวเลือก File Explorer**
  - ดูไฟล์ที่ซ่อน
  - ซ่อนนามสกุลไฟล์
  - ตัวเลือกทั่วไป
  - ตัวเลือกการแสดงผล
- **ตัวเลือกพลังงาน**
  - ไฮเบอร์เนต
  - แผนพลังงาน
  - สลีป/หยุดชั่วคราว
  - สแตนด์บาย
  - เลือกว่าการปิดฝาจะดำเนินการใด
  - เปิดใช้การเริ่มทำงานด่วน
  - การหยุดใช้งาน Universal Serial Bus (USB) ที่เลือกชั่วคราว
- **ความง่ายในการเข้าถึง**

1.5 ใช้การตั้งค่า Windows ที่เหมาะสมตามสถานการณ์สมมติ

- **เวลาและภาษา**
- **การอัปเดตและการรักษาความปลอดภัย**
- **การตั้งค่าส่วนบุคคล**
- **แอป**
- **ความเป็นส่วนตัว**
- **ระบบ**
- **อุปกรณ์**
- **เครือข่ายและอินเทอร์เน็ต**
- **การเล่นเกม**
- **บัญชี**

1.6 กำหนดค่าคุณสมบัติระบบเครือข่าย Microsoft Windows บนไคลเอนต์/เดสก์ท็อปตามสถานการณ์สมมติ

- **ระหว่างเวิร์กกรุ๊ปและโดเมน**
  - ทรัพยากรที่ใช้งานร่วมกัน
  - เครื่องพิมพ์
  - เซิร์ฟเวอร์ไฟล์
  - ไดรฟ์ที่แมป
- **การตั้งค่าไฟร์วอลล์ OS ภายใน**
  - ข้อจำกัดและข้อยกเว้นของแอปพลิเคชัน
  - การกำหนดค่า
- **การกำหนดค่าเครือข่ายฝั่งไคลเอนต์**
  - แบบแผนการกำหนดที่อยู่โปรโตคอลอินเทอร์เน็ต (IP)
  - การตั้งค่าระบบโดเมนเนม (DNS)
  - ซับเน็ตมาสก์
  - เกตเวย์
  - ระหว่างแบบแบบคงที่และแบบไดนามิก
- **สร้างการเชื่อมต่อเครือข่าย**
  - เครือข่ายส่วนตัวเสมือน (VPN)
  - แบบไร้สาย
  - แบบมีสาย
  - เครือข่ายบริเวณกว้างแบบไร้สาย (Wireless Wide Area Network หรือ WWAN)
- **การตั้งค่าพร็อกซี**
- **ระหว่างเครือข่ายสาธารณะและเครือข่ายส่วนตัว**
- **การระบุ File Explorer แบบเส้นทางเครือข่าย**
- **การเชื่อมต่อและข้อจำกัดตามปริมาณ**

1.7 ใช้แนวคิดเกี่ยวกับการติดตั้งและการกำหนดค่าตามสถานการณ์สมมติ

- **ข้อกำหนดเกี่ยวกับระบบสำหรับแอปพลิเคชัน**
  - ระหว่างข้อกำหนดของแอปพลิเคชันที่ขึ้นต่อกันแบบ 32 บิตและ 64 บิต
  - ระหว่างการ์ดจอเฉพาะและการ์ดจอที่ผสานรวม
  - ข้อกำหนดของ Video Random-access Memory (VRAM)
  - ข้อกำหนดของ RAM
  - ข้อกำหนดของหน่วยประมวลผลกลาง (CPU)
  - โทเค็นฮาร์ดแวร์ภายนอก
  - ข้อกำหนดด้านพื้นที่จัดเก็บ
- **ข้อกำหนดของ OS สำหรับแอปพลิเคชัน**
  - ความเข้ากันได้ของ OS กับแอปพลิเคชัน
  - ระหว่าง OS แบบ 32 บิตและ 64 บิต
- **วิธีการกระจาย**
  - ระหว่างสื่อทางกายภาพและสื่อที่ดาวน์โหลดได้
  - ISO ที่ติดตั้งได้
- **ข้อควรพิจารณาอื่น ๆ สำหรับแอปพลิเคชันใหม่**
  - ผลกระทบต่ออุปกรณ์
  - ผลกระทบต่อเครือข่าย
  - ผลกระทบต่อการปฏิบัติงาน
  - ผลกระทบต่อธุรกิจ

1.8 อธิบายประเภทต่าง ๆ ของ OS ทั่วไปและวัตถุประสงค์

- **OS สำหรับเวิร์กสเตชัน**
  - Windows
  - Linux
  - macOS
  - Chrome OS
- **OS สำหรับโทรศัพท์มือถือ/แท็บเล็ต**
  - iPadOS
  - iOS
  - Android
- **ประเภทระบบไฟล์ต่าง ๆ**
  - New Technology File System (NTFS)
  - File Allocation Table 32 (FAT32)
  - Third Extended Filesystem (ext3)
  - Fourth Extended Filesystem (ext4)
  - Apple File System (APFS)
  - Extensible File Allocation Table (exFAT)
- **ข้อจำกัดด้านวงจรอายุการใช้งานของผู้ให้บริการ**
  - ผลิตภัณฑ์ตกรุ่น (EOL)
  - ข้อจำกัดการอัปเดต
- **ข้อกังวลด้านความเข้ากันได้ระหว่าง OS ต่าง ๆ**

1.9 ดำเนินการติดตั้งและอัปเกรด OS ในสภาพแวดล้อม OS ที่หลากหลายตามสถานการณ์สมมติ

- **วิธีการบูต**
  - USB
  - สื่อออปติคัล
  - เครือข่าย
  - โซลิดสเตต/แฟลชไดรฟ์
  - การใช้อินเทอร์เน็ต
  - ไดรฟ์ภายนอก/ชนิดถอดเปลี่ยนได้โดยไม่ต้องรีสตาร์ทเครื่อง (Hot-swappable)
  - ฮาร์ดไดรฟ์ภายใน (พาร์ติชัน)
- **ประเภทการติดตั้ง**
  - การอัปเกรด
  - พาร์ติชันการกู้คืน
  - การติดตั้งใหม่ทั้งหมด
  - การใช้อิมเมจ
  - การติดตั้งเพื่อซ่อมแซม
  - การติดตั้งเครือข่ายจากระยะไกล
  - ข้อควรพิจารณาอื่น ๆ
    - ไดรเวอร์ของบุคคลที่สาม
- **การแบ่งพาร์ติชัน**
  - ตารางพาร์ติชัน GUID (Globally Unique Identifier Partition Table)
  - มาสเตอร์บูตเรกคอร์ด (MBR)
- **รูปแบบไดรฟ์**
- **ข้อควรพิจารณาด้านการอัปเกรด**
  - ไฟล์ที่สำรองข้อมูลและการกำหนดลักษณะของผู้ใช้
  - การสนับสนุน/ความเข้ากันได้ย้อนหลังของแอปพลิเคชันและไดรเวอร์
  - ความเข้ากันได้ของฮาร์ดแวร์
- **การอัปเดตคุณสมบัติ**
  - วงจรอายุการใช้งานของผลิตภัณฑ์

1.10 ระบุคุณสมบัติและเครื่องมือทั่วไปของ macOS/OS เดสก์ท็อป

- **การติดตั้งและการถอนการติดตั้งแอปพลิเคชัน**
  - ประเภทไฟล์
    - .dmg
    - .pkg
    - .app
  - App Store
  - กระบวนการถอนการติดตั้ง
- **ข้อจำกัดเกี่ยวกับ Apple ID และองค์กร**
- **แนวทางปฏิบัติที่ดีที่สุด**
  - การสำรองข้อมูล
  - โปรแกรมป้องกันไวรัส
  - การอัปเดต/แพตช์
- **การกำหนดลักษณะระบบ**
  - การแสดงผล
  - เครือข่าย
  - เครื่องพิมพ์
  - เครื่องสแกน
  - ความเป็นส่วนตัว
  - ความช่วยเหลือพิเศษ
  - Time Machine
- **คุณสมบัติ**
  - หลายเดสก์ท็อป
  - Mission Control
  - Keychain
  - Spotlight
  - iCloud
  - รูปแบบ Gestures
  - Finder
  - Remote Disc
  - Dock
- **ดิสก์ยูทิลิตี้**
- **FileVault**
- **เทอร์มินัล**
- **การบังคับให้ออก (Force Quit)**

1.11 ระบุคุณสมบัติและเครื่องมือทั่วไปของไคลเอนต์ Linux /OS เดสก์ท็อป

- **คำสั่งทั่วไป**
  - ls
  - pwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - su/sudo
  - apt-get
  - yum
  - ip
  - df
  - grep
  - ps
  - man
  - top
  - find
  - dig
  - cat
  - nano
- **แนวทางปฏิบัติที่ดีที่สุด**
  - การสำรองข้อมูล
  - โปรแกรมป้องกันไวรัส
  - การอัปเดต/แพตช์
- **เครื่องมือ**
  - Shell/Terminal
  - Samba

2.0 การรักษาความปลอดภัย

2.1 สรุปข้อมูลเกี่ยวกับมาตรการรักษาความความปลอดภัยต่าง ๆ และวัตถุประสงค์ของมาตรการเหล่านั้น

- **การรักษาความปลอดภัยทางกายภาพ**
  - ห้องโถงที่มีการควบคุมการเข้าถึง
  - เครื่องอ่านป้ายชื่อ
  - กล้องวิดีโอวงจรปิด
  - ระบบสัญญาณเตือน
  - เซ็นเซอร์จับการเคลื่อนไหว
  - การล็อกประตู
  - การล็อกอุปกรณ์
  - ยาม
  - เสากั้น
  - รั้ว
- **การรักษาความปลอดภัยทางกายภาพของพนักงาน**
  - อุปกรณ์ฮาร์ดแวร์รักษาความปลอดภัยที่มีการตรวจสอบยืนยันบุคคลในตัว (Key Fob)
  - สมาร์ทการ์ด
  - กุญแจ
  - ชีวมาตร
    - เครื่องสแกนม่านตา
    - เครื่องสแกนลายนิ้วมือ
    - เครื่องสแกนฝ่ามือ
  - แสงสว่าง
  - เครื่องตรวจจับแม่เหล็ก
- **การรักษาความปลอดภัยเชิงตรรกะ**
  - หลักการให้สิทธิ์ให้น้อยที่สุดเท่าที่เป็นไปได้
  - รายการควบคุมการเข้าถึง (ACL)
  - การยืนยันตัวตนแบบหลายปัจจัย (MFA)
  - อีเมล
  - Hard Token
  - Soft Token
  - บริการข้อความสั้น (SMS)
  - การโทรด้วยเสียง
  - แอปพลิเคชันยืนยันตัวตน
- **การจัดการอุปกรณ์เคลื่อนที่ (MDM)**
- **ไดเรกทอรีที่ใช้งาน (Active Directory)**
  - สคริปต์การเข้าสู่ระบบ
  - โดเมน
  - นโยบายกลุ่ม/การอัปเดต
  - หน่วยองค์กร
  - โฟลเดอร์หลัก
  - การนำทางโฟลเดอร์ใหม่
  - กลุ่มการรักษาความปลอดภัย

2.2 เปรียบเทียบข้อเหมือนและต่างของโปรโตคอลการรักษาความปลอดภัยไร้สายและวิธีการยืนยันตัวตน

- **โปรโตคอลและการเข้ารหัส**
  - WiFi Protected Access 2 (WPA2)
  - WPA3
  - Temporal Key Integrity Protocol (TKIP)
  - Advanced Encryption Standard (AES)
- **การยืนยันตัวตน**
  - Remote Authentication Dial-In User Service (RADIUS)
  - Terminal Access Controller Access-Control System (TACACS+)
  - Kerberos
  - Multifactor

2.3 ตรวจจับ ลบ และป้องกันมัลแวร์โดยใช้เครื่องมือและวิธีการที่เหมาะสมตามสถานการณ์สมมติ

- **มัลแวร์**
  - โทรจัน
  - รูทคิท
  - ไวรัส
  - สปายแวร์
  - แรนซัมแวร์
  - ตัวบันทึกการพิมพ์ (Keylogger)
  - ไวรัสบูตเซกเตอร์
  - ตัวขุดคริปโต (Cryptominer)
- **เครื่องมือและวิธีการ**
  - โหมดการกู้คืน
  - โปรแกรมป้องกันไวรัส
  - โปรแกรมป้องกันมัลแวร์
  - ไฟร์วอลล์ซอฟต์แวร์
  - การฝึกอบรมป้องกันการฟิชชิง
  - การให้ความรู้แก่ผู้ใช้เกี่ยวกับภัยคุกคามทั่วไป
  - การติดตั้ง OS ใหม่

2.4 อธิบายการโจมตี ภัยคุกคาม และช่องโหว่ทั่วไปเกี่ยวกับวิศวกรรมสังคม

- **วิศวกรรมสังคม**
  - ฟิชชิง
  - วิชชิง
  - การแอบดูข้อมูลโดยยืนข้างหลังมองข้ามไหล่ (Shoulder Surfing)
  - เวลลิง (Whaling)
  - การลักลอบเข้าบริเวณต้องจำกัดโดยไม่ได้รับอนุญาต (Tailgating)
  - การปลอมตัวเป็นผู้อื่น
  - การค้นข้อมูลจากถังขยะ
  - การปล่อยสัญญาณปลอม (Evil Twin)
- **ภัยคุกคาม**
  - การปฏิเสธการให้บริการแบบกระจายตัว (DDoS)
  - การปฏิเสธการให้บริการ (DoS)
  - ช่องโหว่ของซอฟต์แวร์ที่ผู้พัฒนาซอฟต์แวร์ยังไม่ค้นพบ (Zero-day Attack)
  - การปลอมตัว (Spoofing)
  - การโจมตีบนเส้นทาง
  - การโจมตีแบบ Brute-force
  - การโจมตีโดยใช้พจนานุกรม
  - ภัยคุกคามที่เกิดขึ้นภายในองค์กร
  - การฉีดภาษามาตรฐานในการเข้าถึงฐานข้อมูล (SQL)
  - การส่งสคริปต์ข้ามเว็บไซต์ (XSS)
- **ช่องโหว่**
  - ระบบที่ไม่เป็นไปตามข้อกำหนด
  - ระบบที่ไม่มีการแพตช์
  - ระบบที่ไม่มีการปกป้องคุ้มครอง (ไม่มีการป้องกันไวรัส/ไม่มีไฟร์วอลล์)
  - OS ที่ตกรุ่นแล้ว
  - การให้พนักงานนำอุปกรณ์ส่วนตัวมาทำงานเอง (BYOD)

2.5 จัดการและกำหนดค่าการตั้งค่าการรักษาความปลอดภัยพื้นฐานใน Microsoft Windows OS ตามสถานการณ์สมมติ

- **Defender Antivirus**
  - เปิดใช้งาน/ปิดใช้งาน
  - คำนิยามที่อัปเดต
- **ไฟร์วอลล์**
  - เปิดใช้งาน/ปิดใช้งาน
  - การรักษาความปลอดภัยของพอร์ต
  - การรักษาความปลอดภัยของแอปพลิเคชัน
- **ผู้ใช้และกลุ่ม**
  - ระหว่างบัญชีในเครื่องและบัญชี Microsoft
  - บัญชีมาตรฐาน
  - ผู้ดูแลระบบ
  - ผู้ใช้ที่เป็นผู้เยี่ยมชม (Guest User)
  - ผู้ใช้ระดับสูง (Power User)
- **ตัวเลือกการลงชื่อเข้าใช้ OS**
  - ชื่อผู้ใช้และรหัสผ่าน
  - หมายเลขประจำตัวบุคคล (PIN)
  - ลายนิ้วมือ
  - การจดจำใบหน้า
  - การลงชื่อเข้าใช้เพียงครั้งเดียว (SSO)
- **ระหว่างสิทธิ์ NTFS และสิทธิ์การใช้ร่วมกัน**
  - แอตทริบิวต์ไฟล์และโฟลเดอร์
  - การสืบทอด
- **ระหว่างการเรียกใช้ในฐานะผู้ดูแลระบบและในฐานะผู้ใช้มาตรฐาน**
  - การควบคุมบัญชีผู้ใช้ (User Account Control หรือ UAC)
- **BitLocker**
- **BitLocker To Go**
- **ระบบไฟล์เข้ารหัส (Encrypting File System หรือ EFS)**

2.6 กำหนดค่าเวิร์กสเตชันให้ตรงตามแนวทางปฏิบัติที่ดีที่สุดด้านการรักษาความปลอดภัยตามสถานการณ์สมมติ

- **การเข้ารหัสข้อมูลที่พักอยู่**
- **แนวทางปฏิบัติที่ดีที่สุดเกี่ยวกับรหัสผ่าน**
  - ข้อกำหนดด้านความซับซ้อนของรหัสผ่าน
    - ความยาว
    - ประเภทอักขระ
  - ข้อกำหนดด้านการหมดอายุ
  - รหัสผ่านระบบอินพุต/เอาต์พุตพื้นฐาน (BIOS)/ส่วนต่อประสานเฟิร์มแวร์ Unified ที่ขยายได้ (UEFI)
- **แนวทางปฏิบัติที่ดีที่สุดเกี่ยวกับผู้ใช้ปลายทาง**
  - ใช้การล็อกภาพพักหน้าจอ
  - ออกจากระบบเมื่อไม่มีการใช้งาน
  - รักษาความปลอดภัย/ปกป้องฮาร์ดแวร์ที่สำคัญ (เช่น แล็ปท็อป)
  - รักษาความปลอดภัยของข้อมูลที่ระบุตัวบุคคลได้ (PII) และรหัสผ่าน
- **การจัดการบัญชี**
  - จำกัดสิทธิ์ของผู้ใช้
  - จำกัดเวลาลงชื่อเข้าใช้
  - ปิดใช้งานบัญชีผู้เยี่ยมชม
  - ใช้การล็อกบัญชีหากพยายามเข้าสู่ระบบล้มเหลว
  - ใช้การล็อกเมื่อหมดเวลา/การล็อกหน้าจอ
- **เปลี่ยนชื่อผู้ใช้และรหัสผ่านเริ่มต้นของผู้ใช้ที่เป็นผู้ดูแลระบบ**
- **ปิดใช้งาน AutoRun**
- **ปิดใช้งาน AutoPlay**

2.7 อธิบายวิธีทั่วไปสำหรับการรักษาความปลอดภัยของอุปกรณ์เคลื่อนที่และอุปกรณ์การทำงานสำเร็จรูป

- **การล็อกหน้าจอ**
  - การจดจำใบหน้า
  - รหัส PIN
  - ลายนิ้วมือ
  - รูปแบบ
  - การปัดนิ้ว
- **การลบข้อมูลจากระยะไกล**
- **แอปพลิเคชันค้นหาตำแหน่ง**
- **การอัปเดต OS**
- **การเข้ารหัสอุปกรณ์**
- **แอปพลิเคชันการสำรองข้อมูลจากระยะไกล**
- **ข้อจำกัดหากพยายามเข้าสู่ระบบล้มเหลว**
- **ซอฟต์แวร์ป้องกันไวรัส/มัลแวร์**
- **ไฟร์วอลล์**
- **นโยบายและขั้นตอน**
  - ระหว่างการนำอุปกรณ์ของตนมาใช้ในการทำงาน (BYOD) และอุปกรณ์ที่เป็นขององค์กร
  - ข้อกำหนดด้านความปลอดภัยของโปรไฟล์
- **อินเทอร์เน็ตของสรรพสิ่ง (IoT)**

2.8 ใช้วิธีการทำลายและกำจัดข้อมูลทั่วไปตามสถานการณ์สมมติ

- **การทำลายทางกายภาพ**
  - การขุดเจาะ
  - การใช้เครื่องทำลายเอกสาร
  - การใช้สนามแม่เหล็ก (Degaussing)
  - การเผาทำลาย
- **แนวทางปฏิบัติเกี่ยวกับการรีไซเคิลหรือการปรับเปลี่ยนวัตถุประสงค์**
  - การลบ/การล้างข้อมูล
  - การฟอร์แมตระดับต่ำ (Low Level Formatting)
  - การฟอร์แมตมาตรฐาน (Standard Formatting)
- **แนวคิดเกี่ยวกับการจัดหาจากภายนอก**
  - ผู้ให้บริการที่เป็นบุคคลที่สาม
  - การรับรองการทำลาย/การรีไซเคิล

2.9 กำหนดค่าการตั้งค่าการรักษาความปลอดภัยที่เหมาะสมของเครือข่ายแบบมีสายและแบบไร้สายในสำนักงานขนาดเล็ก/โฮมออฟฟิศ (SOHO) ตามสถานการณ์สมมติ

- **การตั้งค่าเราเตอร์ที่บ้าน**
  - การเปลี่ยนรหัสผ่านเริ่มต้น
  - การกรอง IP
  - การอัปเดตเฟิร์มแวร์
  - การกรองเนื้อหา
  - การจัดวางทางกายภาพ/ตำแหน่งที่ปลอดภัย
  - การจองโปรโตคอลการกำหนดค่าโฮสต์แบบไดนามิก (DHCP)
  - IP ของเครือข่ายบริเวณกว้าง (WAN) แบบคงที่
  - Universal Plug and Play (UPnP)
  - ซับเน็ตที่ผ่านการคัดกรอง (Screened Subnet)
- **เฉพาะไร้สาย**
  - การเปลี่ยนชุดตัวระบุบริการ (SSID)
  - การปิดใช้งานการกระจายสัญญาณ SSID
  - การตั้งค่าการเข้ารหัส
  - การปิดการเข้าถึงของผู้เยี่ยมชม
  - การเปลี่ยนช่องสัญญาณ
- **การตั้งค่าไฟร์วอลล์**
  - การปิดใช้งานพอร์ตที่ไม่มีการใช้งาน
  - การโอน/การแมปพอร์ต

2.10 ติดตั้งและกำหนดค่าการตั้งค่าเบราว์เซอร์และการตั้งค่ารักษาความปลอดภัยที่เกี่ยวข้องตามสถานการณ์สมมติ

- **การดาวน์โหลด/การติดตั้งเบราว์เซอร์**
  - แหล่งที่เชื่อถือ
    - การแฮช
  - แหล่งที่ไม่น่าเชื่อถือ
- **ส่วนขยายและปลั๊กอิน**
  - แหล่งที่เชื่อถือ
  - แหล่งที่ไม่น่าเชื่อถือ
- **ตัวจัดการรหัสผ่าน**
- **การเชื่อมต่อ/เว็บไซต์ที่ปลอดภัย – ใบรับรองที่ถูกต้อง**
- **การตั้งค่า**
  - เครื่องมือปิดกั้นป๊อปอัพ (Pop-up Blocker)
  - การล้างข้อมูลการท่องเว็บ
  - การล้างแคช
  - โหมดการท่องเว็บส่วนตัว
  - การซิงค์ข้อมูลการลงชื่อเข้าใช้/ข้อมูลเบราว์เซอร์
  - ตัวบล็อกโฆษณา

3.0 การแก้ไขปัญหาซอฟต์แวร์

3.1 แก้ไขปัญหาทั่วไปสำหรับ OS ของ Windows ตามสถานการณ์สมมติ

- **ปัญหาที่พบบ่อย**
  - Blue Screen of Death (BSOD)
  - ประสิทธิภาพที่เชื่องช้า
  - บัญหาการบูต
  - การปิดเครื่องเองบ่อยครั้ง
  - บริการไม่เริ่มทำงาน
  - แอปพลิเคชันหยุดทำงาน
  - คำเตือนหน่วยความจำต่ำ
  - คำเตือนทรัพยากรตัวควบคุม USB
  - ความไม่เสถียรของระบบ
  - ไม่พบ OS
  - ดารโหลดโปรไฟล์ช้า
  - เวลาไม่ตรง
- **ขั้นตอนการแก้ไขปัญหาทั่วไป**
  - รีบูต
  - รีสตาร์ตบริการ
  - ถอนการติดตั้ง/ติดตั้งใหม่/อัปเดตแอปพลิเคชัน
  - เพิ่มทรัพยากร
  - ตรวจสอบข้อกำหนด
  - ตรวจสอบไฟล์ระบบ
  - ซ่อมแซม Windows
  - กู้คืน
  - ทำอิมเมจใหม่
  - ย้อนการอัปเดตกลับเป็นเวอร์ชันก่อนหน้า
  - สร้างโปรไฟล์ Windows ใหม่

3.2 แก้ไขปัญหาด้านการรักษาความปลอดภัยทั่วไปของคอมพิวเตอร์ส่วนบุคคล (พีซี) ตามสถานการณ์สมมติ

- **ปัญหาที่พบบ่อย**
  - การไม่สามารถเข้าถึงเครือข่าย
  - การแจ้งเตือนเดสก์ท็อป
  - การแจ้งเตือนเท็จเกี่ยวกับการปกป้องของการป้องกันไวรัส
  - ไฟล์ระบบหรือไฟล์ส่วนบุคคลที่มีการดัดแปลง
    - ไฟล์หาย/ไฟล์มีการเปลี่ยนชื่อ
  - การแจ้งเตือนที่ไม่พึงประสงค์ภายใน OS
  - การอัปเดต OS ไม่สำเร็จ
- **อาการที่เกี่ยวข้องกับเบราว์เซอร์**
  - ป๊อบอัพแบบสุ่ม/ป๊อบอัพที่แสดงถี่
  - การเตือนเกี่ยวกับใบรับรอง
  - การเปลี่ยนเส้นทาง

3.3 ใช้ขั้นตอนตามแนวทางปฏิบัติที่ดีที่สุดในการกำจัดมัลแวร์ตามสถานการณ์สมมติ

1. สำรวจและตรวจสอบอาการของมัลแวร์
2. กักกันระบบที่ได้รับผลกระทบ
3. ปิดใช้งาน System Restore ใน Windows
4. พยายามแก้ไขระบบที่ได้รับผลกระทบ
   ก. อัปเดตซอฟต์แวร์ป้องกันมัลแวร์
   ข. เทคนิคการสแกนและลบ (เช่น เซฟโหมด สภาพแวดล้อมก่อนการติดตั้ง)
5. กำหนดเวลาการสแกนและรันการอัปเดต
6. เปิดใช้งาน System Restore และสร้างจุดคืนค่าใน Windows
7. ให้ความรู้กับผู้ใช้ปลายทาง

3.4 แก้ไขปัญหาทั่วไปของ OS และแอปพลิเคชันบนมือถือตามสถานการณ์สมมติ

- **ปัญหาที่พบบ่อย**
  - การเรียกใช้แอปพลิเคชันไม่สำเร็จ
  - การเปิดแอปพลิเคชันไม่สำเร็จ/แอปพลิเคชันเกิดข้อขัดข้อง
  - การอัปเดตแอปพลิเคชันไม่สำเร็จ
  - การตอบสนองช้า
  - การอัปเดต OS ไม่สำเร็จ
  - ปัญหาอายุการใช้งานแบตเตอรี่
  - การรีบูตแบบสุ่ม
  - ปัญหาความสามารถในการเชื่อมต่อ
    - Bluetooth
    - WiFi
    - การสื่อสารระยะใกล้ (NFC)
    - AirDrop
  - หน้าจอไม่หมุนโดยอัตโนมัติ

3.5 แก้ไขปัญหาทั่วไปด้านการรักษาความปลอดภัยของ OS และแอปพลิเคชันบนมือถือตามสถานการณ์สมมติ

- **ข้อกังวลด้านการรักษาความปลอดภัย**
  - ทรัพยากรแพ็กเกจแอนดรอยด์ (APK)
  - โหมดนักพัฒนา
  - การเข้าถึงรูท/เจลเบรก
  - Bootleg/แอปพลิเคชันที่เป็นอันตราย
    - การปลอมแปลงแอปพลิเคชัน
- **ปัญหาที่พบบ่อย**
  - อัตราการรับส่งข้อมูลเครือข่ายสูง
  - เวลาตอบสนองช้า
  - การแจ้งเตือนขีดจำกัดการใช้งานข้อมูล
  - ความสามารถในการเชื่อมต่ออินเทอร์เน็ตที่จำกัด
  - ไม่มีการเชื่อมต่ออินเทอร์เน็ต
  - โฆษณาจำนวนมาก
  - การเตือนด้านการรักษาความปลอดภัยที่เป็นเท็จ
  - พฤติกรรมที่ไม่คาดคิดของแอปพลิเคชัน
  - ไฟล์/ข้อมูลส่วนบุคคลรั่วไหล

4.0 ขั้นตอนการปฏิบัติงาน

4.1 ปรับใช้แนวทางปฏิบัติที่ดีที่สุดที่เกี่ยวข้องกับการจัดการข้อมูลในระบบการจัดทำเอกสารและการสนับสนุนตามสถานการณ์สมมติ

- **ระบบทิกเก็ต**
  - ข้อมูลผู้ใช้
  - ข้อมูลอุปกรณ์
  - คำอธิบายเกี่ยวกับปัญหา
  - หมวดหมู่
  - ความรุนแรง
  - ระดับการยกระดับ
  - การสื่อสารอย่างเป็นลายลักษณ์อักษรที่ชัดเจนและกระชับ
    - คำอธิบายเกี่ยวกับปัญหา
    - บันทึกความคืบหน้า
    - การแก้ไขปัญหา
- **การจัดการสินทรัพย์**
  - รายการสินค้าคงคลัง
  - ระบบฐานข้อมูล
  - ป้ายและ ID ของสินทรัพย์
  - วงจรอายุของการจัดซื้อ
  - การรับประกันและการอนุญาต
  - ผู้ใช้ที่มอบหมาย
- **ประเภทของเอกสาร**
  - นโยบายการใช้งานที่ยอมรับได้ (AUP)
  - แผนภาพรูปแบบการเชื่อมต่อเครือข่าย (Network Topology Diagram)
  - ข้อกำหนดด้านการปฏิบัติตามกฎระเบียบ
    - หน้าจอเริ่มต้น (Splash Screen)
  - รายงานเกี่ยวกับเหตุการณ์
  - ขั้นตอนการปฏิบัติงานมาตรฐาน
    - ขั้นตอนการติดตั้งแพ็กเกจซอฟต์แวร์ที่กำหนดเอง
  - รายการตรวจสอบการตั้งค่าสำหรับผู้ใช้ใหม่
  - รายการตรวจสอบการเลิกใช้งานของผู้ใช้ปลายทาง
- **ฐานข้อมูลความรู้/บทความ**

4.2 อธิบายแนวทางปฏิบัติที่ดีที่สุดในการจัดการการเปลี่ยนแปลงพื้นฐาน

- **กระบวนการทางธุรกิจที่มีการบันทึกไว้**
  - แผนการย้อนกลับเป็นเวอร์ชันก่อนหน้า
  - การทดสอบแซนด์บ็อกซ์
  - พนักงานผู้รับผิดชอบ
- **การจัดการการเปลี่ยนแปลง**
  - แบบฟอร์มการร้องขอ
  - วัตถุประสงค์การเปลี่ยนแปลง
  - ขอบเขตการเปลี่ยนแปลง
  - วันที่และเวลาของการเปลี่ยนแปลง
  - ระบบที่ได้รับผลกระทบ/ผลกระทบ
  - การวิเคราะห์ความเสี่ยง
    - ระดับความเสี่ยง
  - การอนุมัติของคณะกรรมการการเปลี่ยนแปลง
  - การยอมรับของผู้ใช้ปลายทาง

4.3 ใช้วิธีการสำรองข้อมูลและกู้คืนเวิร์กสเตชันตามสถานการณ์สมมติ

- **การสำรองและกู้คืน**
  - แบบเต็มรูปแบบ
  - เฉพาะส่วนที่เพิ่มขึ้นมา (Incremental)
  - เฉพาะส่วนที่มีการเปลี่ยนแปลง (Differential)
  - แบบสังเคราะห์
- **การทดสอบการสำรองข้อมูล**
  - ความถี่
- **แผนการหมุนเวียนการสำรองข้อมูล**
  - ระหว่างในพื้นที่และนอกพื้นที่
  - Grandfather-father-son (GFS)
  - กฎการสำรองข้อมูลแบบ 3-2-1

4.4 ดำเนินการตามขั้นตอนด้านความปลอดภัยทั่วไปตามสถานการณ์สมมติ

- **สายรัดป้องกันไฟฟ้าสถิต (ESD)**
- **แผ่น ESD**
- **การต่อสายดินของอุปกรณ์**
- **การจัดการพลังงานไฟฟ้าอย่างเหมาะสม**
- **การจัดการและการเก็บชิ้นส่วนอย่างเหมาะสม**
- **ถุงป้องกันไฟฟ้าสถิต**
- **การปฏิบัติตามข้อบังคับของรัฐบาล**
- **ความปลอดภัยส่วนบุคคล**
  - การถอดปลั๊กก่อนซ่อมบำรุง PC
  - เทคนิคการยก
  - ความปลอดภัยทางไฟและไฟฟ้า
  - แว่นครอบตานิรภัย
  - หน้ากากกรองอากาศ

4.5 สรุปผลกระทบต่อสิ่งแวดล้อมและการควบคุมด้านสิ่งแวดล้อมในพื้นที่

- **เอกสารข้อมูลความปลอดภัย (MSDS)/ เอกสารสำหรับการจัดการและกำจัดทิ้ง**
  - การกำจัดแบตเตอรี่อย่างเหมาะสม
  - การกำจัดหมึกอย่างเหมาะสม
  - การกำจัดอุปกรณ์และสินทรัพย์อื่น ๆ อย่างเหมาะสม
- **การตระหนักเกี่ยวกับระดับอุณหภูมิและความชื้น รวมถึงการถ่ายเทอากาศที่เหมาะสม**
  - การจัดวางอุปกรณ์/ตำแหน่ง
  - การกำจัดฝุ่น
  - ลมอัด/สุญญากาศ
- **กระแสไฟกระชาก เหตุการณ์กระแสไฟฟ้าตัด และกระแสไฟฟ้าขัดข้อง**
  - แบตเตอรี่สำรอง
  - อุปกรณ์ป้องกันไฟกระชาก

4.6 อธิบายความสำคัญของเนื้อหา/กิจกรรมต้องห้าม รวมถึงแนวคิดเกี่ยวกับความเป็นส่วนตัว การอนุญาต และนโยบาย

- **การตอบสนองต่อเหตุการณ์**
  - เส้นทางการรับ-ส่งพยานหลักฐาน
  - แจ้งฝ่ายบริหารจัดการ/หน่วยงานบังคับใช้กฎหมายตามความจำเป็น
  - ลำเนาไดร์ฟ (ความสมบูรณ์ของข้อมูลและการเก็บรักษา)
  - เอกสารประกอบเหตุการณ์
- **การจัดการสิทธิ์ดิจิทัล (DRM)/ข้อตกลงการอนุญาตใช้งานสำหรับผู้ใช้ปลายทาง (EULA)**
  - ใบอนุญาตที่ถูกต้อง
  - ใบอนุญาตที่ไม่หมดอายุ
  - ระหว่างใบอนุญาตสำหรับการใช้งานส่วนบุคคลและใบอนุญาตสำหรับการใช้งานในองค์กร
  - ใบอนุญาตแบบโอเพนซอร์ส
- **ข้อมูลที่มีการควบคุม**
  - ธุรกรรมบัตรเครดิต
  - ข้อมูลส่วนบุคคลที่รัฐบาลออกให้
  - PII
  - ข้อมูลสาธารณสุข
  - ข้อกำหนดเกี่ยวกับการเก็บรักษาข้อมูล

4.7 ใช้เทคนิคการสื่อสารที่เหมาะสมและความเป็นมืออาชีพตามสถานการณ์สมมติ

- **รูปลักษณ์และเครื่องแต่งกายที่เป็นมืออาชีพ**
  - แต่งกายให้เหมาะสมกับสภาพแวดล้อมที่กำหนด
    - เครื่องแต่งกายที่เป็นทางการ
    - ชุดลำลองทางธุรกิจ
- **การใช้ภาษาที่เหมาะสมและหลีกเลี่ยงการใช้ศัพท์เฉพาะตัวย่อ สแลง เมื่อสามารถทำได้**
- **รักษาทัศนคติเชิงบวก/ความมั่นใจในโครงการ**
- **รับฟังอย่างกระตือรือร้น จดบันทึก และหลีกเลี่ยงการขัดจังหวะลูกค้า**
- **ระมัดระวังเรื่องวัฒนธรรม**
  - ใช้ชื่อตำแหน่งทางอาชีพที่เหมาะสม เมื่อเกี่ยวข้อง
- **ตรงต่อเวลา (หากล่าช้า ต้องแจ้งลูกค้าก่อนเสมอ)**
- **หลีกเลี่ยงสิ่งรบกวน**
  - สายโทรศัพท์ส่วนตัว
  - การส่งข้อความ/เว็บไซต์โซเชียลมีเดีย
  - การขัดจังหวะด้วยเรื่องส่วนตัว
- **รับมือกับลูกค้าหรือสถานการณ์ที่ยุ่งยาก**
  - ไม่โต้เถียงกับลูกค้าและ/หรือต่อต้าน
  - หลีกเลี่ยงการเมินเฉยต่อปัญหาของลูกค้า
  - หลีกเลี่ยงการตัดสินด้วยความเห็นส่วนตัว
  - ทำความเข้าใจคำพูดของลูกค้าให้กระจ่าง (ถามคำถามปลายเปิดเพื่อตีวงปัญหาให้แคบลงและพูดทวนปัญหาหรือคำถามเพื่อตรวจสอบว่าเข้าใจถูกต้อง)
  - ไม่เปิดเผยข้อมูลประสบการณ์ผ่านสื่อโซเชียลมีเดียต่าง ๆ
- **กำหนดความคาดหวัง/ระยะเวลา และสถานะการสื่อสารกับลูกค้า และดำเนินการให้สำเร็จตามที่กำหนด**
  - เสนอตัวเลือกในการซ่อมแซม/เปลี่ยนตามความจำเป็น
  - จัดทำเอกสารหลักฐานการให้บริการอย่างเหมาะสม
  - ติดตามผลกับลูกค้า/ผู้ใช้ภายหลังการให้บริการเพื่อตรวจสอบความพึงพอใจ
- **จัดการกับข้อมูลที่เป็นความลับและเป็นส่วนตัวของลูกค้าอย่างเหมาะสม**
  - ที่อยู่ในคอมพิวเตอร์ เดสก์ท็อป เครื่องพิมพ์ ฯลฯ

4.8 อธิบายพื้นฐานการเขียนสคริปต์

- **ประเภทไฟล์สคริปต์**
  - .bat
  - .ps1
  - .vbs
  - .sh
  - .js
  - .py
- **กรณีการใช้งานสำหรับการเขียนสคริปต์**
  - ระบบอัตโนมัติพื้นฐาน
  - การรีสตาร์ทเครื่อง
  - การแมปไดรฟ์เครือข่ายใหม่
  - การติดตั้งแอปพลิเคชัน
  - การสำรองข้อมูลอัตโนมัติ
  - การเก็บรวบรวมข้อมูล
  - การดำเนินการอัปเดต
- **ข้อควรพิจารณาอื่น ๆ เมื่อใช้สคริปต์**
  - การนำมัลแวร์เข้าสู่ระบบโดยไม่ได้ตั้งใจ
  - เปลี่ยนการตั้งค่าระบบโดยไม่ได้ตั้งใจ
  - เบราว์เซอร์หรือระบบหยุดทำงานเนื่องจากการใช้ทรัพยากรอย่างไม่ถูกต้อง

4.9 ใช้เทคโนโลยีการเข้าถึงจากระยะไกลตามสถานการณ์สมมติ

- **วิธี/เครื่องมือ**
  - RDP
  - VPN
  - คอมพิวเตอร์เครือข่ายเสมือน (VNC)
  - Secure Shell (SSH)
  - การติดตามและการจัดการจากระยะไกล (RMM)
  - Microsoft Remote Assistance (MSRA)
  - เครื่องมือของของบุคคลที่สาม
    - ซอฟต์แวร์การใช้หน้าจอร่วมกัน
    - ซอฟต์แวร์การประชุมทางวิดีโอ
    - ซอฟต์แวร์การโอนย้ายไฟล์
    - ซอฟต์แวร์การจัดการเดสก์ท็อป
- **ข้อควรพิจารณาด้านการรักษาความปลอดภัยของวิธีการเข้าถึงแต่ละวิธี**

รายการคำย่อของ CompTIA A+ Core 2 (220-1102)

รายการต่อไปนี้คืออักษรย่อที่ปรากฏในข้อสอบ CompTIA A+ Core 2 (220-1102) ผู้สมัครสอบควรทบทวนรายการทั้งหมดและศึกษาหาความรู้ในการปฏิบัติงานเกี่ยวกับอักษรย่อทั้งหมดที่ระบุไว้เพื่อเป็นการเตรียมความพร้อมสำหรับการสอบที่ครอบคลุม

คำย่อ	คำจำกัดความ
AAA	Authentication, Authorization, and Accounting
AC	Alternating Current
ACL	Access Control List (รายการควบคุมการเข้าถึง)
ADF	Automatic Document Feeder
AES	Advanced Encryption Standard (มาตรฐานการเข้ารหัสลับขั้นสูง)
AP	Access Point
APFS	Apple File System
APIPA	Automatic Private Internet Protocol Addressing
APK	Android Package
ARM	Advanced RISC [Reduced Instruction Set Computer] Machine
ARP	Address Resolution Protocol (โปรโตคอลการสื่อสารที่ใช้ในการค้นหาที่อยู่เลเยอร์ลิงก์)
ATA	Advanced Technology Attachment
ATM	Asynchronous Transfer Mode
ATX	Advanced Technology Extended
AUP	Acceptable Use Policy (นโยบายการใช้งานที่ยอมรับได้)
BIOS	Basic Input/Output System
BSOD	Blue Screen of Death
BYOD	Bring Your Own Device (นำอุปกรณ์ของคุณมาเอง)
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CD	Compact Disc
CDFS	Compact Disc File System
CDMA	Code-Division Multiple Access
CERT	Computer Emergency Response Team
CIFS	Common Internet File System
CMD	Command Prompt
CMOS	Complementary Metal-Oxide Semiconductor
CPU	Central Processing Unit (หน่วยประมวลผลกลางของคอมพิวเตอร์)
CRL	Certificate Revocation List
DC	Direct Current
DDoS	Distributed Denial of Service (การโจมตีโดยปฏิเสธการให้บริการ)
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol (โปรโตคอลที่ใช้ในการจัดการที่รวดเร็วอัตโนมัติและการจัดการส่วนกลาง)
DIMM	Dual Inline Memory Module
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System (ระบบที่มีไว้สำหรับบริหารจัดการข้อมูลของชื่อโดเมนเนม)
DoS	Denial of Service
DRAM	Dynamic Random-Access Memory
DRM	Digital Rights Management (การจัดการสิทธิดิจิทัล)
DSL	Digital Subscriber Line
DVI	Digital Visual Interface
DVI-D	Digital Visual Interface-Digital
ECC	Error Correcting Code
EFS	Encrypting File System
EMI	Electromagnetic Interference
EOL	End-of-Life
eSATA	External Serial Advanced Technology Attachment
ESD	Electrostatic Discharge
EULA	End-User License Agreement
exFAT	Extensible File Allocation Table
ext	Extended File System
FAT	File Allocation Table
FAT12	12-Bit File Allocation Table
FAT16	16-bit File Allocation Table
FAT32	32-bit File Allocation Table
FSB	Front-Side Bus
FTP	File Transfer Protocol (โปรโตคอลการโอนย้ายไฟล์)
GFS	Grandfather-Father-Son
GPS	Global Positioning System
GPT	GUID [Globally Unique Identifier] Partition Table
GPU	Graphics Processing Unit
GSM	Global System for Mobile Communications
GUI	Graphical User Interface

คำย่อ	คำจำกัดความ
GUID	Globally Unique Identifier
HAL	Hardware Abstraction Layer
HAV	Hardware-assisted Virtualization
HCL	Hardware Compatibility List
HDCP	High-bandwidth Digital Content Protection
HDD	Hard Disk Drive
HDMI	High-Definition Multimedia Interface
HSM	Hardware Security Module (โมดูลความปลอดภัยของฮาร์ดแวร์)
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol (โปรโตคอลการถ่ายโอนข้อความหลายมิติ)
HTTPS	Hypertext Transfer Protocol Secure (โปรโตคอลการถ่ายโอนข้อความหลายมิติอย่างปลอดภัย)
I/O	Input/Output (อินพุต/เอาต์พุต)
IaaS	Infrastructure as a Service (การให้บริการโครงสร้างพื้นฐาน)
ICR	Intelligent Character Recognition
IDE	Integrated Drive Electronics
IDS	Intrusion Detection System (ระบบตรวจจับการบุกรุก)
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Mail Access Protocol
IOPS	Input/Output Operations Per Second
IoT	Internet of Things (อินเทอร์เน็ตของสรรพสิ่ง)
IP	Internet Protocol (โปรโตคอลอินเทอร์เน็ต)
IPS	Intrusion Prevention System (ระบบตรวจสอบการบุกรุก)
IPS	In-plane Switching
IPSec	Internet Protocol Security (การรักษาความปลอดภัยของโปรโตคอลอินเทอร์เน็ต)
IR	Infrared
IrDA	Infrared Data Association
IRP	Incident Response Plan
ISO	International Organization for Standardization (องค์การระหว่างประเทศว่าด้วยการมาตรฐาน)
ISP	Internet Service Provider (ผู้ให้บริการอินเทอร์เน็ต)
ITX	Information Technology eXtended
KB	Knowledge Base
KVM	Keyboard-Video-Mouse
LAN	Local Area Network (เครือข่ายเฉพาะที่)
LC	Lucent Connector
LCD	Liquid Crystal Display (จอภาพผลึกเหลว)
LDAP	Lightweight Directory Access Protocol (โปรโตคอลที่ใช้ในการค้นหาและเข้าถึงข้อมูลหรืออ็อบเจกต์ต่าง ๆ ได้อย่างรวดเร็วด้วยระบบไดเรกทอรี)
LED	Light-emitting Diode (ไดโอดเปล่งแสง)
MAC	Media Access Control/Mandatory Access Control
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MDM	Mobile Device Management (ซอฟต์แวร์สำหรับบริหารจัดการ และควบคุมอุปกรณ์ภายในองค์กร)
MFA	Multifactor Authentication (การยืนยันตัวตนโดยใช้หลายปัจจัย)
MFD	Multifunction Device
MFP	Multifunction Printer
MMC	Microsoft Management Console
MOU	Memorandum of Understanding (บันทึกความเข้าใจ)
MSDS	Material Safety Data Sheet
MSRA	Microsoft Remote Assistance
MX	Mail Exchange (การแลกเปลี่ยนเมล)
NAC	Network Access Control (การควบคุมการเข้าถึงเครือข่าย)
NAT	Network Address Translation
NDA	Non-disclosure Agreement (ข้อตกลงไม่เปิดเผยข้อมูล)
NetBIOS	Networked Basic Input/Output System
NetBT	NetBIOS over TCP/IP [Transmission Control Protocol/Internet Protocol]
NFC	Near-field Communication
NFS	Network File System (ระบบไฟล์เครือข่าย)
NIC	Network Interface Card (การ์ดเชื่อมต่อเครือข่าย)
NTFS	New Technology File System
NVMe	Non-volatile Memory Express
OCR	Optical Character Recognition
OLED	Organic Light-emitting Diode (ไดโอดเปล่งแสงอินทรีย์)
ONT	Optical Network Terminal
OS	Operating System (ระบบปฏิบัติการ)
PaaS	Platform as a Service (การให้บริการแพลตฟอร์ม)
PAN	Personal Area Network (เครือข่ายส่วนบุคคล)
PC	Personal Computer (คอมพิวเตอร์ส่วนบุคคล)
PCIe	Peripheral Component Interconnect Express
PCL	Printer Command Language (ภาษาควบคุมเครื่องพิมพ์)
PE	Preinstallation Environment
PII	Personally Identifiable Information (ข้อมูลที่ระบุตัวบุคคลได้)
PIN	Personal Identification Number (หมายเลขประจำตัวบุคคล)
PKI	Public Key Infrastructure (เทคโนโลยีระบบรหัสแบบกุญแจสาธารณะ)
PoE	Power over Ethernet
POP3	Post Office Protocol 3
POST	Power-on Self-Test
PPP	Point-to-Point Protocol
PRL	Preferred Roaming List
PSU	Power Supply Unit
PXE	Preboot Execution Environment
RADIUS	Remote Authentication Dial-in User Service (เกณฑ์วิธีการเชื่อมต่อเพื่อพิสูจน์ตัวจริงระยะไกลในบริการของผู้ใช้)

คำย่อ	คำจำกัดความ
RAID	Redundant Array of Independent (หรือ Inexpensive) Disks
RAM	Random-access Memory (หน่วยความจำเข้าถึงโดยสุ่ม)
RDP	Remote Desktop Protocol (โปรโตคอลเดสก์ท็อประยะไกล)
RF	Radio Frequency (ความถี่วิทยุ)
RFI	Radio Frequency Interference
RFID	Radio Frequency Identification
RJ11	Registered Jack Function 11 (ปลั๊กเชื่อมต่อมาตรฐานฟังก์ชัน 11)
RJ45	Registered Jack Function 45 (ปลั๊กเชื่อมต่อมาตรฐานฟังก์ชัน 45)
RMM	Remote Monitoring and Management (การตรวจสอบและการจัดการจากระยะไกล)
RTO	Recovery Time Objective
SaaS	Software as a Service (การให้บริการซอฟต์แวร์)
SAN	Storage Area Network (เครือข่ายพื้นที่จัดเก็บ)
SAS	Serial Attached SCSI [Small Computer System Interface]
SATA	Serial Advanced Technology Attachment
SC	Subscriber Connector
SCADA	Supervisory Control and Data Acquisition (การควบคุมกำกับดูแลและเก็บข้อมูล)
SCP	Secure Copy Protection
SCSI	Small Computer System Interface
SDN	Software-defined Networking
SFTP	Secure File Transfer Protocol
SIM	Subscriber Identity Module
SIMM	Single Inline Memory Module
S.M.A.R.T.	Self-monitoring Analysis and Reporting Technology (เทคโนโลยีการตรวจสอบ การวิเคราะห์และการรายงานผลด้วยตนเอง)
SMB	Server Message Block (โปรโตคอลมาตรฐานเครือข่ายที่ใช้แชร์ไฟล์)
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SODIMM	Small Outline Dual Inline Memory Module
SOHO	Small Office/Home Office
SPF	Sender Policy Framework (วิธีการตรวจสอบอีเมลจากผู้ส่งจริง)
SQL	Structured Query Language (ภาษามาตรฐานในการเข้าถึงฐานข้อมูล)
SRAM	Static Random-access Memory
SSD	Solid-State Drive
SSH	Secure Shell (โปรโตคอลสำหรับเครือข่ายคอมพิวเตอร์ที่ออกแบบมาเพื่อให้เข้าถึงไปยังคอมพิวเตอร์เครื่องอื่น)
SSID	Service Set Identifier (ตัวระบุชุดบริการ)

คำย่อ	คำจำกัดความ
SSL	Secure Sockets Layer (ชั้นซ็อกเก็ตปลอดภัย)
SSO	Single Sign-on (ลงชื่อพิสูจน์ตัวตนเพียงครั้งเดียว)
ST	Straight Tip
STP	Shielded Twisted Pair
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol (โปรโตคอลการควบคุมการส่ง)
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol (โปรโตคอลการถ่ายโอนไฟล์เล็กน้อย)
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security (โปรโตคอลความปลอดภัยที่เข้ารหัสอีเมล)
TN	Twisted Nematic
TPM	Trusted Platform Module (โมดูลแพลตฟอร์มที่เชื่อถือได้)
UAC	User Account Control
UDP	User Datagram Protocol (โปรโตคอลดาตาแกรมของผู้ใช้)
UEFI	Unified Extensible Firmware Interface (ส่วนต่อประสานเฟิร์มแวร์ที่ขยายได้แบบรวมกัน)
UNC	Universal Naming Convention
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus (ระบบยูเอสบี)
UTM	Unified Threat Management (การจัดการภัยคุกคามเบ็ดเสร็จในเครื่องเดียว)
UTP	Unshielded Twisted Pair
VA	Vertical Alignment
VDI	Virtual Desktop Infrastructure (โครงสร้างพื้นฐานจำลองคอมพิวเตอร์เสมือน)
VGA	Video Graphics Array
VLAN	Virtual LAN [Local Area Network]
VM	Virtual Machine
VNC	Virtual Network Computer
VoIP	Voice over Internet Protocol (โปรโตคอลการสื่อสารทางเสียงผ่านอินเทอร์เน็ต)
VPN	Virtual Private Network (เครือข่ายส่วนตัวเสมือน)
VRAM	Video Random-access Memory
WAN	Wide Area Network (เครือข่ายบริเวณกว้าง)
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider (ผู้ให้บริการอินเทอร์เน็ตไร้สาย)
WLAN	Wireless LAN [Local Area Network]
WMN	Wireless Mesh Network
WPA	WiFi Protected Access
WWAN	Wireless Wide Area Network
XSS	Cross-site Scripting (การเขียนสคริปต์ข้ามไซต์)

รายการฮาร์ดแวร์และซอฟต์แวร์ที่มีการเสนอของ CompTIA A+ Core 2 (220-1102)

**CompTIA แนบตัวอย่างรายการฮาร์ดแวร์และซอฟต์แวร์มาในที่นี้เพื่อช่วยเหลือผู้สมัครสอบในการเตรียมตัวสอบ A+ Core 2 (220-1102) รายการนี้ยังอาจมีประโยชน์ต่อบริษัทฝึกอบรมที่ต้องการสร้างองค์ประกอบห้องปฏิบัติการสำหรับจัดการฝึกอบรม รายการย่อยในแต่ละหัวข้อเป็นเพียงตัวอย่างโดยคร่าวเท่านั้น

อุปกรณ์

- แท็บเล็ต/สมาร์ทโฟน Apple
- แท็บเล็ต/สมาร์ทโฟน Android
- แท็บเล็ต Windows
- Chromebook
- แล็ปท็อป Windows/แล็ปท็อป Mac/แล็ปท็อป Linux
- เดสก์ท็อป Windows/เดสก์ท็อป Mac/เดสก์ท็อป Linux
- Windows Server พร้อมไดเรกทอรีที่ใช้งานและการจัดการการพิมพ์
- จอแสดงผล
- เครื่องฉาย
- เราเตอร์/สวิตช์ SOHO
- อุปกรณ์กระจายสัญญาณ
- โทรศัพท์ Voice over Internet Protocol (VoIP)
- เครื่องพิมพ์
  - แบบเลเซอร์/พ่นหมึก
  - แบบไร้สาย
  - เครื่องพิมพ์ 3-D
  - แบบความร้อน
- อุปกรณ์ป้องกันไฟกระชาก
- ระบบกำลังไฟฟ้าต่อเนื่อง (UPS)
- อุปกรณ์อัจฉริยะ (อุปกรณ์อินเทอร์เน็ตของสรรพสิ่ง [IoT])
- เซิร์ฟเวอร์ที่มีไฮเปอร์ไวเซอร์
- Punchdown Block
- แผงกระจายสายสัญญาณ
- เว็บแคม
- ลำโพง
- ไมโครโฟน

อะไหล่/ฮาร์ดแวร์

- แผงวงจรหลัก
- RAM
- ฮาร์ดไดรฟ์
- แหล่งจ่ายไฟ
- การ์ดจอ
- การ์ดเสียง
- การ์ดเครือข่าย
- การ์ดเชื่อมต่อเครือข่าย (Network Interface Card หรือ NIC) แบบไร้สาย
- พัดลม/อุปกรณ์ระบายความร้อน/แผ่นระบายความร้อน
- CPU
- ขั้วต่อ/สายเคเบิลคละชนิด
  - USB
  - ระบบส่งสัญญาณมัลติมีเดียความละเอียดสูง (High-Definition Multimedia Interface หรือ HDMI)
  - DisplayPort
  - อินเทอร์เฟซภาพดิจิทัล (Digital Visual Interface หรือ DVI)
  - อาร์เรย์กราฟิกวิดีโอ (Video Graphics Array หรือ VGA)
- อะแดปเตอร์
  - อะแดปเตอร์ Bluetooth
- สายเคเบิลเครือข่าย
- สายเคเบิล/ขั้วต่อเครือข่ายที่ไม่มีขั้วปลาย
- อะแดปเตอร์ไฟฟ้ากระแสสลับ (AC)
- ออปติคัลไดรฟ์
- สกรู/แสตนด์ออฟ
- เคส
- ชุดบำรุงรักษา
- เมาส์/คีย์บอร์ด
- Keyboard-video-mouse (KVM)
- สายเคเบิลคอนโซล
- โซลิดสเตตไดรฟ์ (SSD)

เครื่องมือ

- ไขควง
- มัลติมิเตอร์
- คีมตัดสายไฟ
- เครื่องมือย้ำสาย
- คีมเข้าหัวสาย
- อุปกรณ์ทดสอบแหล่งจ่ายไฟ
- คีมปอกสายไฟ
- ชุดเครื่องมือช่างมาตรฐาน
- สายรัดป้องกันไฟฟ้าสถิต (ESD)
- สารนำความร้อน
- อุปกรณ์ทดสอบสายเคเบิล
- โทนเนอร์สายเคเบิล
- เครื่องวิเคราะห์ WiFi
- Serial Advanced Technology Attachment (SATA) เข้ากับขั้วต่อ USB

ซอฟต์แวร์

- OS
  - Linux
  - Chrome OS
  - Microsoft Windows
  - macOS
  - Android
  - iOS
- ดิสก์ Preinstallation Environment (PE)/Compact Disc (CD) แบบไลฟ์
- ซอฟต์แวร์ป้องกันไวรัส
- ซอฟต์แวร์ระบบเสมือน
- โปรแกรมป้องกันมัลแวร์
- ซอฟต์แวร์ไดรเวอร์