

## รายละเอียดคุณลักษณะเฉพาะพัสดุ

ครุภัณฑ์คอมพิวเตอร์ รายการ ระบบบริหารจัดการด้านความปลอดภัยทางไซเบอร์ จำนวน ระบบ 1

### มีรายละเอียดดังนี้

ระบบบริหารจัดการด้านความปลอดภัยทางไซเบอร์ มหาวิทยาลัยขอนแก่น จำนวน 1 ระบบ  
ประกอบด้วย

- 1.1 ระบบเครื่องแม่ข่ายประมวลผลประสิทธิภาพสูงแบบที่ 1 สำหรับ  
ระบบรวบรวมข้อมูล เพื่อการวิเคราะห์ความปลอดภัยของระบบเครือข่าย จำนวน 2 ชุด
- 1.2 ระบบเครื่องแม่ข่ายประมวลผลประสิทธิภาพสูงแบบที่ 2 สำหรับ Docker จำนวน 4 ชุด
- 1.3 ระบบเครื่องแม่ข่ายประมวลผลประสิทธิภาพสูงแบบที่ 3 สำหรับ Syslog จำนวน 1 ชุด
- 1.4 ระบบจัดเก็บข้อมูลภายนอกขนาดใหญ่ แบบที่ 1 จำนวน 1 ชุด
- 1.5 ระบบจัดเก็บข้อมูลภายนอกขนาดใหญ่ แบบที่ 2 จำนวน 1 ชุด

รายละเอียดคุณลักษณะเฉพาะพัสดุ มีข้อกำหนดคุณสมบัติทางเทคนิคขั้นต่ำดังต่อไปนี้

1.1 ระบบเครื่องแม่ข่ายประมวลผลประสิทธิภาพสูง แบบที่ 1 สำหรับ ระบบจัดเก็บและรวบรวม

ข้อมูลเพื่อการวิเคราะห์ความปลอดภัยของระบบเครือข่าย จำนวน 2 ชุด โดยมีคุณ

ลักษณะเฉพาะขั้นต่ำ เทียบเท่าหรือดีกว่าอย่างน้อยดังนี้

- 1.1.1 มีหน่วยประมวลผลกลาง (CPU) จำนวนแกนประมวลผล (Core) ไม่น้อยกว่า 64 แกนหลัก และมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.4 GHz จำนวน 1 หน่วย
- 1.1.2 หน่วยความจำหลัก (RAM) ชนิด ECC DDR5 หรือดีกว่า ความจุรวมไม่น้อยกว่า 512 GB
- 1.1.3 มี Solid State Disk (SSD) แบบ NVME ขนาดความจุไม่น้อยกว่า 3 TB (ก่อนทำการ Format) จำนวนไม่น้อยกว่า 2 หน่วย และ ขนาดความจุไม่น้อยกว่า 6 TB จำนวนไม่น้อยกว่า 5 หน่วย
- 1.1.4 มีช่องเชื่อมต่อระบบเครือข่ายภายนอกแบบ QSFP28 ที่ความเร็ว 100 GE จำนวนไม่น้อยกว่า 2 พอร์ต พร้อม Transceiver
- 1.1.5 มีอุปกรณ์จ่ายไฟฟ้า (Power Supply) ขนาดไม่น้อยกว่า 1,300 W จำนวนไม่น้อยกว่า 2 หน่วย
- 1.1.6 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิตพร้อมทั้งมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี
- 1.1.7 ผู้เสนอราคาต้องเสนอซอฟต์แวร์ตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์สำหรับเครื่องคอมพิวเตอร์ จำนวน 1 สิทธิการใช้งาน จำนวนไม่น้อยกว่า 2 ปี โดยมีคุณสมบัติขั้นต่ำดังต่อไปนี้

- 1.1.7.1 ซอฟต์แวร์ Endpoint Protection สามารถติดตั้งได้บนระบบปฏิบัติการต่อไปนี้ได้อย่างน้อย
  - 1.1.7.1.1 Microsoft Windows 8/8.1/10/11
  - 1.1.7.1.2 Microsoft Windows Server 2012/2016/2019
  - 1.1.7.1.3 MacOS 10/11/12
  - 1.1.7.1.4 Ubuntu 12/13/14/16/18/20
- 1.1.7.2 สามารถจัดกลุ่มความแตกต่างของ Endpoint ได้
- 1.1.7.3 มีหน้าจอสำหรับแสดงภาพรวมการตรวจภัยคุกคามหรือเหตุการณ์ทางด้านไซเบอร์ที่เกิดขึ้น (Dashboard)
- 1.1.7.4 สามารถแสดงข้อมูล Hostname, IP Address, OS Version และสถานะ Online/Offline เครื่อง Endpoint ได้
- 1.1.7.5 สามารถ Uninstall และ Restart/Reboot Endpoint Agent ได้
- 1.1.7.6 สามารถในการค้นหาไฟล์ต้องสงสัยที่อาจจะมียูในเครื่องคอมพิวเตอร์ (Infected File Tracking หรือ Threat Hunting)
- 1.1.7.7 สามารถจัดการภัยคุกคามตาม Event และภัยคุกคามต่อ Endpoint โดยการ Fix หรือ Cleanup และ Isolate ได้
- 1.1.7.8 สามารถในการควบคุมเครื่องคอมพิวเตอร์จากระยะไกล (Remote Support Control)
- 1.1.7.9 มีคุณลักษณะในการตรวจสอบไวรัสคอมพิวเตอร์ ดังนี้
  - 1.1.7.9.1 มีรูปแบบ Traditional Anti-Virus หรือ Signature-based หรือ Gene Analysis, AI-based, Behavioral และ Cloud based engine หรือ Cloud Threat Intelligent ได้
  - 1.1.7.9.2 สามารถตั้งเวลาในการตรวจสอบ (Scheduled Scan) การตรวจสอบทันที (Real Time Scan) การสั่งให้ตรวจสอบแบบ Manual Scan หรือ On Demand Scan เป็นต้น
  - 1.1.7.9.3 มีความสามารถในการสแกนช่องโหว่ (Vulnerability Scan), การอุดช่องโหว่ (Endpoint Patching) และการอุดช่องโหว่แบบเสมือน (Hot Patching)
  - 1.1.7.9.4 สามารถตรวจสอบไฟล์ประเภท Document, Script และ Compressed ได้
  - 1.1.7.9.5 มีคุณลักษณะในการตรวจจับ Web shell และ fileless attack ได้

- 1.1.7.9.6 สามารถป้องกันผู้ใช้งานสั่งปลดการทำงานและการถอดการติดตั้ง Endpoint เช่น การป้องกันโดยการกำหนดรหัสผ่าน Password ก่อนการออกจากโปรแกรมหรือการถอนการติดตั้ง
- 1.1.7.9.7 ผลิตภัณฑ์รองรับการควบคุมการใช้งาน Application ในเครื่องที่ติดตั้ง Agent ได้
- 1.1.7.9.8 มีคุณลักษณะในการตรวจจับและป้องกัน Ransomware ได้
- 1.1.7.9.9 มีความสามารถในการป้องกันและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์สำหรับเครื่องคอมพิวเตอร์ผู้ใช้งาน (Endpoint Protection and Response หรือ Endpoint Detection and Response)
- 1.1.7.9.10 สามารถค้นหา Audit Log หรือ Security log โดยสามารถกำหนด Time range, Endpoint name หรือ IP Address ได้
- 1.1.7.9.11 สามารถออกรายงานภัยคุกคามทางไซเบอร์ (Security Report หรือ Event Report) ในรูปแบบของ PDF ได้เป็นอย่างดี
- 1.1.7.9.12 สามารถทำงานร่วมกับอุปกรณ์สำหรับการตรวจจับและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ (Detection and Response) ที่มหาวิทยาลัยใช้อยู่ได้ ดังนี้
  - 1.1.7.9.12.1 สามารถส่งข้อมูล Security Log
  - 1.1.7.9.12.2 สามารถรองรับการทำงานแบบอัตโนมัติ (auto response) เช่น Isolate และ fix ได้
- 1.1.7.9.13 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิตพร้อมกับมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี
- 1.1.8 ผู้เสนอราคาต้องเสนอซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูล (Backup and Replication) โดยต้องมีคุณลักษณะขั้นต่ำ เทียบเท่าหรือดีกว่าอย่างน้อยดังนี้
  - 1.1.8.1 สามารถบริหารจัดการจากส่วนกลางได้ (Centralized console) ผ่านหน้า UI
  - 1.1.8.2 สามารถสำรองและกู้คืนข้อมูลบนระบบ VMware vSphere และ Microsoft Hyper-V โดยไม่จำเป็นต้องติดตั้ง Agent บนเครื่องคอมพิวเตอร์เสมือน
  - 1.1.8.3 สามารถกู้คืนข้อมูลในระดับไฟล์บน Guest OS ที่ใช้ระบบปฏิบัติการประเภท Microsoft Windows, Linux, Solaris, BSD และ Mac ได้
  - 1.1.8.4 สามารถสำรองและกู้คืนข้อมูลในระดับแอปพลิเคชันบนเครื่องคอมพิวเตอร์เสมือนได้ โดยไม่จำเป็นต้องติดตั้ง Agent ซึ่งต้องรองรับแอปพลิเคชัน อย่าง

- น้อยดังต่อไปนี้ Microsoft Active Directory, Microsoft SQL Server, Oracle, Microsoft Exchange, Microsoft SharePoint และ PostgreSQL
- 1.1.8.5 สามารถสำรองข้อมูล Transaction Log ของ Microsoft SQL Server, Archived Log ของ Oracle Database และ WAL ของ PostgreSQL ได้โดยไม่ต้องติดตั้ง Agent เพิ่มเติม
  - 1.1.8.6 สามารถสำรองและกู้คืนข้อมูลระบบฐานข้อมูลสำหรับ SAP HANA, Oracle RMAN และ Microsoft SQL Server ที่ทำงานอยู่บนเครื่องคอมพิวเตอร์แม่ข่ายเสมือนหรือบนเครื่องคอมพิวเตอร์แม่ข่ายกายภาพ (Physical server) ได้
  - 1.1.8.7 สามารถสำรองและกู้คืนข้อมูลประเภทไฟล์แชร์ได้ทั้ง CIFS และ NFS โดยต้องสามารถเลือก Path ที่ต้องการสำรองได้
  - 1.1.8.8 สามารถบีบอัด (Compression) ข้อมูลหรือลดความซ้ำซ้อน (Deduplication) ข้อมูลที่ทำการสำรองได้ด้วยซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอ
  - 1.1.8.9 มีเทคโนโลยี WAN Acceleration ที่ช่วยเพิ่มประสิทธิภาพการถ่ายโอนข้อมูล และลดปริมาณข้อมูลที่ส่งผ่าน WAN ในการทำ Backup Copy Job และ Replication Job
  - 1.1.8.10 สามารถกู้คืนเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Microsoft Windows และ Linux ที่อยู่ในรูปแบบ Virtual หรือ Physical ไปยัง Amazon EC2 ,Microsoft Azure และ Google Compute Engine ด้วยซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอได้
  - 1.1.8.11 สามารถสร้างกลุ่มของอุปกรณ์จัดเก็บข้อมูล ซึ่งเป็นที่เก็บไฟล์ข้อมูลสำรอง โดยประกอบด้วยอุปกรณ์จัดเก็บข้อมูลอย่างน้อยหนึ่งชุดหรือมากกว่า โดยการขยายสามารถใช้อุปกรณ์จัดเก็บข้อมูลต่างประเภทได้ และสามารถคัดลอกหรือย้ายชุดไฟล์ข้อมูลสำรองไปยัง Object storage ได้ เช่น Amazon S3, Microsoft Azure Blob Storage, Google Cloud Object Storage, IBM Cloud Object Storage และ Wasabi Google Cloud Object Storage
  - 1.1.8.12 สามารถสำรองข้อมูลไปยังอุปกรณ์จัดเก็บข้อมูลประเภท Object Storage ได้โดยตรง
  - 1.1.8.13 สามารถกู้คืนเครื่องคอมพิวเตอร์เสมือนเพื่อนำมาใช้งานได้แบบทันทีทันใด (Instant Recovery) โดยการเปิดเครื่องคอมพิวเตอร์เสมือนจากอุปกรณ์

จัดเก็บข้อมูลที่ทำหน้าที่เป็น Backup repository หรือ Backup storage ขึ้นมาใช้งานได้ และสามารถกู้คืนพร้อมกันหลายเครื่องได้

- 1.1.8.14 สามารถกู้คืนระบบฐานข้อมูลบน Microsoft SQL Server และ Oracle เพื่อนำมาใช้งานได้แบบทันทีทันใดจากอุปกรณ์จัดเก็บข้อมูลที่ทำหน้าที่เป็น Backup repository หรือ Backup storage โดยต้องสามารถทำการอ่านและเขียนข้อมูลได้
- 1.1.8.15 มีความสามารถที่เรียกว่า Immutability หรือ Immutable คือ การป้องกันไม่ให้ไฟล์ข้อมูลสำรองที่อยู่ในอุปกรณ์จัดเก็บข้อมูลที่ใช้ทำงานร่วมกับซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูล (Backup Repository หรือ Backup Storage) ถูกแก้ไขหรือลบได้ โดยสามารถกำหนดระยะเวลาในการทำ Immutability หรือ Immutable ได้ เพื่อป้องกันความเสียหายของข้อมูลจาก Ransomware หรือ malware ได้ โดยความสามารถดังกล่าวต้องสามารถทำงานร่วมกับ Linux Server, HPE StoreOnce, Amazon S3 Storage และ Microsoft Azure Storage
- 1.1.8.16 สามารถทำงานร่วมกับซอฟต์แวร์แอนตี้ไวรัส เพื่อทำการสแกนข้อมูล ก่อนทำการกู้คืนไปใช้งานบนระบบ Production ในกรณีที่พบเจอ Malware หรือสิ่งแปลกปลอมอื่นๆ โดยสามารถเลือกได้ว่า สามารถดำเนินการกู้คืนได้แต่ไม่อนุญาตให้ใช้งานพอร์ตเชื่อมต่อเครือข่าย หรือให้ยกเลิกการกู้คืน
- 1.1.8.17 สามารถตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์เสมือนบน VMware vSphere และ Microsoft Hyper-V ที่ได้สำรองข้อมูลไว้ (Recovery verification) โดยการจำลองการเปิดใช้งานบนสภาพแวดล้อมเสมือน โดยสามารถกำหนดตารางเวลาในการทดสอบได้แบบอัตโนมัติ นอกจากนี้ยังต้องมีความสามารถในการตรวจสอบความถูกต้องของข้อมูลว่ามีความเสียหายหรือไม่ และสามารถทำงานร่วมกับซอฟต์แวร์แอนตี้ไวรัสเพื่อสแกนหาว่ามี Malware หรือ Ransomware หรือไม่ และรวมถึงต้องสามารถออกรายงานเพื่อแสดงผลลัพธ์ของการทำงานได้
- 1.1.8.18 สามารถรองรับการเข้าใช้งานซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอได้ ด้วยวิธีที่เรียกว่า Multi-Factor Authentication
- 1.1.8.19 มีเครื่องมือที่ช่วยตรวจสอบว่าซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอนั้นได้ทำการตั้งค่าเป็นไปตามแนวทางปฏิบัติที่ดีที่สุด (Best practices) ด้านความปลอดภัยโดยอ้างอิงจากค่าพารามิเตอร์ต่างๆที่แนะนำบนซอฟต์แวร์หรือไม่

- 1.1.8.20 สามารถทำสำเนาข้อมูล (Replication) เครื่องคอมพิวเตอร์เสมือนบน VMware vSphere และ Microsoft Hyper-V ไปยังศูนย์คอมพิวเตอร์สำรอง (Disaster recovery site) และสามารถทำ Failover และ Failback เครื่องคอมพิวเตอร์เสมือนได้
- 1.1.8.21 มีลิขสิทธิ์ถูกต้องตามกฎหมายแบบ Open license ประเภท Subscription ครอบคลุมตามจำนวน Workload ที่ต้องการสำรองข้อมูล (VMs หรือ Physical หรือ VM บน Cloud instance) ไม่น้อยกว่า 1 Workloads เป็นเวลาไม่น้อยกว่า 2 ปี
- 1.1.8.22 เป็นผลิตภัณฑ์ซอฟต์แวร์ที่อยู่ในกลุ่ม Leaders ของ Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions ปีล่าสุด
- 1.1.8.23 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิต พร้อมกับมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี

## 1.2 ระบบเครื่องแม่ข่ายประมวลผลประสิทธิภาพสูง แบบที่ 2 สำหรับ Docker จำนวน 4 ชุด โดยต้องมีคุณลักษณะเฉพาะขั้นต่ำ เทียบเท่าหรือดีกว่าอย่างน้อยดังนี้

- 1.2.1 มีหน่วยประมวลผลกลาง (CPU) จำนวนแกนประมวลผล (Core) ไม่น้อยกว่า 32 แกนหลัก และมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 3.2 GHz จำนวน 1 หน่วย
- 1.2.2 หน่วยความจำหลัก (RAM) ชนิด ECC DDR5 หรือดีกว่า ความจุรวมไม่น้อยกว่า 256 GB
- 1.2.3 มี Solid State Disk (SSD) แบบ NVME ขนาดความจุไม่น้อยกว่า 3 TB (ก่อนทำการ Format) จำนวนไม่น้อยกว่า 4 หน่วย
- 1.2.4 มีช่องเชื่อมต่อระบบเครือข่ายภายนอกแบบ QSFP28 ที่ความเร็ว 100 GE จำนวนไม่น้อยกว่า 2 พอร์ต พร้อม Transceiver
- 1.2.5 มีอุปกรณ์จ่ายไฟฟ้า (Power Supply) ขนาดไม่น้อยกว่า 1,300 W จำนวนไม่น้อยกว่า 2 หน่วย
- 1.2.6 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิตพร้อมกับมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี
- 1.2.7 ผู้เสนอราคาต้องเสนอซอฟต์แวร์ตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์สำหรับเครื่องคอมพิวเตอร์ จำนวน 1 สิทธิการใช้งาน จำนวนไม่น้อยกว่า 2 ปี โดยมีคุณสมบัติขั้นต่ำดังต่อไปนี้

- 1.2.7.1 ซอฟต์แวร์ Endpoint Protection สามารถติดตั้งได้บนระบบปฏิบัติการต่อไปนี้ได้อย่างน้อย
  - 1.2.7.1.1 Microsoft Windows 8/8.1/10/11
  - 1.2.7.1.2 Microsoft Windows Server 2012/2016/2019
  - 1.2.7.1.3 MacOS 10/11/12
  - 1.2.7.1.4 Ubuntu 12/13/14/16/18/20
- 1.2.7.2 สามารถจัดกลุ่มความแตกต่างของ Endpoint ได้
- 1.2.7.3 มีหน้าจอสำหรับแสดงภาพรวมการตรวจภัยคุกคามหรือเหตุการณ์ทางด้านไซเบอร์ที่เกิดขึ้น (Dashboard)
- 1.2.7.4 สามารถแสดงข้อมูล Hostname, IP Address, OS Version และสถานะ Online/Offline เครื่อง Endpoint ได้
- 1.2.7.5 สามารถ Uninstall และ Restart/Reboot Endpoint Agent ได้
- 1.2.7.6 สามารถในการค้นหาไฟล์ต้องสงสัยที่อาจจะมียูอยู่ในเครื่องคอมพิวเตอร์ (Infected File Tracking หรือ Threat Hunting)
- 1.2.7.7 สามารถจัดการภัยคุกคามตาม Event และภัยคุกคามต่อ Endpoint โดยการ Fix หรือ Cleanup และ Isolate ได้
- 1.2.7.8 สามารถในการควบคุมเครื่องคอมพิวเตอร์จากระยะไกล (Remote Support Control)
- 1.2.7.9 มีคุณลักษณะในการตรวจสอบไวรัสคอมพิวเตอร์ ดังนี้
  - 1.2.7.9.1 มีรูปแบบ Traditional Anti-Virus หรือ Signature-based หรือ Gene Analysis, AI-based, Behavioral และ Cloud based engine หรือ Cloud Threat Intelligent ได้
  - 1.2.7.9.2 สามารถตั้งเวลาในการตรวจสอบ (Scheduled Scan) การตรวจสอบทันที (Real Time Scan) การสั่งให้ตรวจสอบแบบ Manual Scan หรือ On Demand Scan เป็นต้น
  - 1.2.7.9.3 มีความสามารถในการสแกนช่องโหว่ (Vulnerability Scan), การอุดช่องโหว่ (Endpoint Patching) และการอุดช่องโหว่แบบเสมือน (Hot Patching)
  - 1.2.7.9.4 สามารถตรวจสอบไฟล์ประเภท Document, Script และ Compressed ได้
  - 1.2.7.9.5 มีคุณลักษณะในการตรวจจับ Web shell และ fileless attack ได้

- 1.2.7.9.6 สามารถป้องกันผู้ใช้งานสั่งปลดการทำงานและการถอดการติดตั้ง Endpoint เช่น การป้องกันโดยการกำหนดรหัสผ่าน Password ก่อนการออกจากโปรแกรมหรือการถอนการติดตั้ง
- 1.2.7.9.7 ผลิตภัณฑ์รองรับการควบคุมการใช้งาน Application ในเครื่องที่ติดตั้ง Agent ได้
- 1.2.7.9.8 มีคุณลักษณะในการตรวจจับและป้องกัน Ransomware ได้
- 1.2.7.9.9 มีความสามารถในการป้องกันและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์สำหรับเครื่องคอมพิวเตอร์ผู้ใช้งาน (Endpoint Protection and Response หรือ Endpoint Detection and Response)
- 1.2.7.9.10 สามารถค้นหา Audit Log หรือ Security log โดยสามารถกำหนด Time range, Endpoint name หรือ IP Address ได้
- 1.2.7.9.11 สามารถออกรายงานภัยคุกคามทางไซเบอร์ (Security Report หรือ Event Report) ในรูปแบบของ PDF ได้เป็นอย่างน้อย
- 1.2.7.9.12 สามารถทำงานร่วมกับอุปกรณ์สำหรับการตรวจจับและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ (Detection and Response) ที่มหาวิทยาลัยใช้อยู่ได้ ดังนี้
  - 1.2.7.9.12.1 สามารถส่งข้อมูล Security Log
  - 1.2.7.9.12.2 สามารถรองรับการทำงานแบบอัตโนมัติ (auto response) เช่น Isolate และ fix ได้
- 1.2.7.9.13 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิตพร้อมกับมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี
- 1.2.8 ผู้เสนอราคาต้องเสนอซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูล (Backup and Replication) โดยต้องมีคุณลักษณะเฉพาะขั้นต่ำ เทียบเท่าหรือดีกว่าอย่างน้อยดังนี้
  - 1.2.8.1 สามารถบริหารจัดการจากส่วนกลางได้ (Centralized console) ผ่านหน้า UI
  - 1.2.8.2 สามารถสำรองและกู้คืนข้อมูลบนระบบ VMware vSphere และ Microsoft Hyper-V โดยไม่จำเป็นต้องติดตั้ง Agent บนเครื่องคอมพิวเตอร์เสมือน
  - 1.2.8.3 สามารถกู้คืนข้อมูลในระดับไฟล์บน Guest OS ที่ใช้ระบบปฏิบัติการประเภท Microsoft Windows, Linux, Solaris, BSD และ Mac ได้
  - 1.2.8.4 สามารถสำรองและกู้คืนข้อมูลในระดับแอปพลิเคชันบนเครื่องคอมพิวเตอร์เสมือนได้ โดยไม่จำเป็นต้องติดตั้ง Agent ซึ่งต้องรองรับแอปพลิเคชัน อย่าง



- น้อยดังต่อไปนี้ Microsoft Active Directory, Microsoft SQL Server, Oracle, Microsoft Exchange, Microsoft SharePoint และ PostgreSQL
- 1.2.8.5 สามารถสำรองข้อมูล Transaction Log ของ Microsoft SQL Server, Archived Log ของ Oracle Database และ WAL ของ PostgreSQL ได้โดยไม่ต้องติดตั้ง Agent เพิ่มเติม
  - 1.2.8.6 สามารถสำรองและกู้คืนข้อมูลระบบฐานข้อมูลสำหรับ SAP HANA, Oracle RMAN และ Microsoft SQL Server ที่ทำงานอยู่บนเครื่องคอมพิวเตอร์แม่ข่ายเสมือนหรือบนเครื่องคอมพิวเตอร์แม่ข่ายกายภาพ (Physical server) ได้
  - 1.2.8.7 สามารถสำรองและกู้คืนข้อมูลประเภทไฟล์แชร์ได้ทั้ง CIFS และ NFS โดยต้องสามารถเลือก Path ที่ต้องการสำรองได้
  - 1.2.8.8 สามารถบีบอัด (Compression) ข้อมูลหรือลดความซ้ำซ้อน (Deduplication) ข้อมูลที่ทำการสำรองได้ด้วยซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอ
  - 1.2.8.9 มีเทคโนโลยี WAN Acceleration ที่ช่วยเพิ่มประสิทธิภาพการถ่ายโอนข้อมูล และลดปริมาณข้อมูลที่ส่งผ่าน WAN ในการทำ Backup Copy Job และ Replication Job
  - 1.2.8.10 สามารถกู้คืนเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Microsoft Windows และ Linux ที่อยู่ในรูปแบบ Virtual หรือ Physical ไปยัง Amazon EC2 ,Microsoft Azure และ Google Compute Engine ด้วยซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอได้
  - 1.2.8.11 สามารถสร้างกลุ่มของอุปกรณ์จัดเก็บข้อมูล ซึ่งเป็นที่เก็บไฟล์ข้อมูลสำรอง โดยประกอบด้วยอุปกรณ์จัดเก็บข้อมูลอย่างน้อยหนึ่งชุดหรือมากกว่า โดยการขยายสามารถใช้อุปกรณ์จัดเก็บข้อมูลต่างประเภทได้ และสามารถคัดลอกหรือย้ายชุดไฟล์ข้อมูลสำรองไปยัง Object storage ได้ เช่น Amazon S3, Microsoft Azure Blob Storage, Google Cloud Object Storage, IBM Cloud Object Storage และ Wasabi Google Cloud Object Storage
  - 1.2.8.12 สามารถสำรองข้อมูลไปยังอุปกรณ์จัดเก็บข้อมูลประเภท Object Storage ได้โดยตรง
  - 1.2.8.13 สามารถกู้คืนเครื่องคอมพิวเตอร์เสมือนเพื่อนำมาใช้งานได้แบบทันทีทันใด (Instant Recovery) โดยการเปิดเครื่องคอมพิวเตอร์เสมือนจากอุปกรณ์

จัดเก็บข้อมูลที่ทำหน้าที่เป็น Backup repository หรือ Backup storage ขึ้นมาใช้งานได้ และสามารถกู้คืนพร้อมกันหลายเครื่องได้

- 1.2.8.14 สามารถกู้คืนระบบฐานข้อมูลบน Microsoft SQL Server และ Oracle เพื่อนำมาใช้งานได้แบบทันทีทันใดจากอุปกรณ์จัดเก็บข้อมูลที่ทำหน้าที่เป็น Backup repository หรือ Backup storage โดยต้องสามารถทำการอ่านและเขียนข้อมูลได้
- 1.2.8.15 มีความสามารถที่เรียกว่า Immutability หรือ Immutable คือ การป้องกันไม่ให้ไฟล์ข้อมูลสำรองที่อยู่ในอุปกรณ์จัดเก็บข้อมูลที่ใช้ทำงานร่วมกับซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูล (Backup Repository หรือ Backup Storage) ถูกแก้ไขหรือลบได้ โดยสามารถกำหนดระยะเวลาในการทำ Immutability หรือ Immutable ได้ เพื่อป้องกันความเสียหายของข้อมูลจากรansomware หรือ malware ได้ โดยความสามารถดังกล่าวต้องสามารถทำงานร่วมกับ Linux Server, HPE StoreOnce, Amazon S3 Storage และ Microsoft Azure Storage
- 1.2.8.16 สามารถทำงานร่วมกับซอฟต์แวร์แอนตี้ไวรัส เพื่อทำการสแกนข้อมูล ก่อนทำการกู้คืนไปใช้งานบนระบบ Production ในกรณีที่พบเจอ Malware หรือสิ่งแปลกปลอมอื่นๆ โดยสามารถเลือกได้ว่า สามารถดำเนินการกู้คืนได้แต่ไม่อนุญาตให้ใช้งานพอร์ตเชื่อมต่อเครือข่าย หรือให้ยกเลิกการกู้คืน
- 1.2.8.17 สามารถตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์เสมือนบน VMware vSphere และ Microsoft Hyper-V ที่ได้สำรองข้อมูลไว้ (Recovery verification) โดยการจำลองการเปิดใช้งานบนสภาพแวดล้อมเสมือน โดยสามารถกำหนดตารางเวลาในการทดสอบได้แบบอัตโนมัติ นอกจากนี้ยังต้องมีความสามารถในการตรวจสอบความถูกต้องของข้อมูลว่ามีความเสียหายหรือไม่ และสามารถทำงานร่วมกับซอฟต์แวร์แอนตี้ไวรัสเพื่อสแกนหาว่ามี Malware หรือ Ransomware หรือไม่ และรวมถึงต้องสามารถออกรายงานเพื่อแสดงผลลัพธ์ของการทำงานได้
- 1.2.8.18 สามารถรองรับการเข้าใช้งานซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอได้ ด้วยวิธีที่เรียกว่า Multi-Factor Authentication
- 1.2.8.19 มีเครื่องมือที่ช่วยตรวจสอบว่าซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอนั้นได้ทำการตั้งค่าเป็นไปตามแนวทางปฏิบัติที่ดีที่สุด (Best practices) ด้านความปลอดภัยโดยอ้างอิงจากค่าพารามิเตอร์ต่างๆที่แนะนำบนซอฟต์แวร์หรือไม่

- 1.2.8.20 สามารถทำสำเนาข้อมูล (Replication) เครื่องคอมพิวเตอร์เสมือนบน VMware vSphere และ Microsoft Hyper-V ไปยังศูนย์คอมพิวเตอร์สำรอง (Disaster recovery site) และสามารถทำ Failover และ Failback เครื่องคอมพิวเตอร์เสมือนได้
- 1.2.8.21 มีลิขสิทธิ์ถูกต้องตามกฎหมายแบบ Open license ประเภท Subscription ครอบคลุมตามจำนวน Workload ที่ต้องการสำรองข้อมูล (VMs หรือ Physical หรือ VM บน Cloud instance) 1 Workloads เป็นเวลาไม่น้อยกว่า 2 ปี
- 1.2.8.22 เป็นผลิตภัณฑ์ซอฟต์แวร์ที่อยู่ในกลุ่ม Leaders ของ Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions ปีล่าสุด
- 1.2.8.23 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิต พร้อมกับมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี

**1.3 ระบบเครื่องแม่ข่ายประมวลผลประสิทธิภาพสูง แบบที่ 3 สำหรับ Syslog จำนวน 1 ชุด โดยต้องมีคุณลักษณะเฉพาะขั้นต่ำ เทียบเท่าหรือดีกว่าอย่างน้อยดังนี้**

- 1.3.1 มีหน่วยประมวลผลกลาง (CPU) จำนวนแกนประมวลผล (Core) ไม่น้อยกว่า 16 แกนหลัก และมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 3.0 GHz จำนวน 1 หน่วย
- 1.3.2 หน่วยความจำหลัก (RAM) ชนิด ECC DDR5 หรือดีกว่า ความจุรวมไม่น้อยกว่า 128 GB
- 1.3.3 มี Solid State Disk (SSD) แบบ NVME ขนาดความจุไม่น้อยกว่า 3 TB (ก่อนทำการ Format) จำนวนไม่น้อยกว่า 2 หน่วย
- 1.3.4 มี Hard disk ขนาด 3.5 นิ้ว ความจุไม่น้อยกว่า 20TB จำนวนไม่น้อยกว่า 12 หน่วย
- 1.3.5 มีช่องเชื่อมต่อระบบเครือข่ายภายนอกแบบ QSFP28 ที่ความเร็ว 100 GE จำนวนไม่น้อยกว่า 2 พอร์ต พร้อม Transceiver
- 1.3.6 มีอุปกรณ์จ่ายไฟฟ้า (Power Supply) ขนาดไม่น้อยกว่า 1,300 W จำนวนไม่น้อยกว่า 2 หน่วย
- 1.3.7 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิตพร้อมกับมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี

- 1.3.8 ผู้เสนอราคาต้องเสนอซอฟต์แวร์ตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์สำหรับเครื่องคอมพิวเตอร์ จำนวน 1 สิทธิการใช้งาน จำนวนไม่น้อยกว่า 2 ปี โดยมีคุณสมบัติขั้นต่ำดังต่อไปนี้
  - 1.3.8.1 ซอฟต์แวร์ Endpoint Protection สามารถติดตั้งได้บนระบบปฏิบัติการต่อไปนี้ได้เป็นอย่างน้อย
    - 1.3.8.1.1 Microsoft Windows 8/8.1/10/11
    - 1.3.8.1.2 Microsoft Windows Server 2012/2016/2019
    - 1.3.8.1.3 MacOS 10/11/12
    - 1.3.8.1.4 Ubuntu 12/13/14/16/18/20
  - 1.3.8.2 สามารถจัดกลุ่มความแตกต่างของ Endpoint ได้
  - 1.3.8.3 มีหน้าจอสำหรับแสดงภาพรวมการตรวจจับภัยคุกคามหรือเหตุการณ์ทางด้านไซเบอร์ที่เกิดขึ้น (Dashboard)
  - 1.3.8.4 สามารถแสดงข้อมูล Hostname, IP Address, OS Version และสถานะ Online/Offline เครื่อง Endpoint ได้
  - 1.3.8.5 สามารถ Uninstall และ Restart/Reboot Endpoint Agent ได้
  - 1.3.8.6 สามารถในการค้นหาไฟล์ต้องสงสัยที่อาจจะมีอยู่ในเครื่องคอมพิวเตอร์ (Infected File Tracking หรือ Threat Hunting)
  - 1.3.8.7 สามารถจัดการภัยคุกคามตาม Event และภัยคุกคามต่อ Endpoint โดยการ Fix หรือ Cleanup และ Isolate ได้
  - 1.3.8.8 สามารถในการควบคุมเครื่องคอมพิวเตอร์จากระยะไกล (Remote Support Control)
  - 1.3.8.9 มีคุณลักษณะในการตรวจสอบไวรัสคอมพิวเตอร์ ดังนี้
    - 1.3.8.9.1 มีรูปแบบ Traditional Anti-Virus หรือ Signature-based หรือ Gene Analysis, AI-based, Behavioral และ Cloud based engine หรือ Cloud Threat Intelligent ได้
    - 1.3.8.9.2 สามารถตั้งเวลาในการตรวจสอบ (Scheduled Scan) การตรวจสอบทันที (Real Time Scan) การสั่งให้ตรวจสอบแบบ Manual Scan หรือ On Demand Scan เป็นต้น
    - 1.3.8.9.3 มีความสามารถในการสแกนช่องโหว่ (Vulnerability Scan), การอุดช่องโหว่ (Endpoint Patching) และการอุดช่องโหว่แบบเสมือน (Hot Patching)
    - 1.3.8.9.4 สามารถตรวจสอบไฟล์ประเภท Document, Script และ Compressed ได้

- 1.3.8.9.5 มีคุณลักษณะในการตรวจจับ Web shell และ fileless attack ได้
- 1.3.8.9.6 สามารถป้องกันผู้ใช้งานสั่งปลดการทำงานและการถอดการติดตั้ง Endpoint เช่น การป้องกันโดยการกำหนดรหัสผ่าน Password ก่อนการออกจากโปรแกรมหรือการถอนการติดตั้ง
- 1.3.8.9.7 ผลิตรหัสรับรองรับการควบคุมการใช้งาน Application ในเครื่องที่ติดตั้ง Agent ได้
- 1.3.8.9.8 มีคุณลักษณะในการตรวจจับและป้องกัน Ransomware ได้
- 1.3.8.9.9 มีความสามารถในการป้องกันและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์สำหรับเครื่องคอมพิวเตอร์ผู้ใช้งาน (Endpoint Protection and Response หรือ Endpoint Detection and Response)
- 1.3.8.9.10 สามารถค้นหา Audit Log หรือ Security log โดยสามารถกำหนด Time range, Endpoint name หรือ IP Address ได้
- 1.3.8.9.11 สามารถออกรายงานภัยคุกคามทางไซเบอร์ (Security Report หรือ Event Report) ในรูปแบบของ PDF ได้เป็นอย่างน้อย
- 1.3.8.9.12 สามารถทำงานร่วมกับอุปกรณ์สำหรับการตรวจจับและตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ (Detection and Response) ที่มหาวิทยาลัยใช้อยู่ ดังนี้
  - 1.3.8.9.12.1 สามารถส่งข้อมูล Security Log
  - 1.3.8.9.12.2 สามารถรองรับการทำงานแบบอัตโนมัติ (auto response) เช่น Isolate และ fix ได้
- 1.3.8.9.13 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิตพร้อมกับมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี
- 1.3.9 ผู้เสนอราคาต้องเสนอซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูล (Backup and Replication) โดยต้องมีคุณลักษณะเฉพาะขั้นต่ำ เทียบเท่าหรือดีกว่าอย่างน้อยดังนี้
  - 1.3.9.1 สามารถบริหารจัดการจากส่วนกลางได้ (Centralized console) ผ่านหน้า UI
  - 1.3.9.2 สามารถสำรองและกู้คืนข้อมูลบนระบบ VMware vSphere และ Microsoft Hyper-V โดยไม่จำเป็นต้องติดตั้ง Agent บนเครื่องคอมพิวเตอร์เสมือน
  - 1.3.9.3 สามารถกู้คืนข้อมูลในระดับไฟล์บน Guest OS ที่ใช้ระบบปฏิบัติการประเภท Microsoft Windows, Linux, Solaris, BSD และ Mac ได้

- 1.3.9.4 สามารถสำรองและกู้คืนข้อมูลในระดับแอปพลิเคชันบนเครื่องคอมพิวเตอร์เสมือนได้ โดยไม่จำเป็นต้องติดตั้ง Agent ซึ่งต้องรองรับแอปพลิเคชัน อย่างน้อยดังต่อไปนี้ Microsoft Active Directory, Microsoft SQL Server, Oracle, Microsoft Exchange, Microsoft SharePoint และ PostgreSQL
- 1.3.9.5 สามารถสำรองข้อมูล Transaction Log ของ Microsoft SQL Server, Archived Log ของ Oracle Database และ WAL ของ PostgreSQL ได้ โดยไม่ต้องติดตั้ง Agent เพิ่มเติม
- 1.3.9.6 สามารถสำรองและกู้คืนข้อมูลระบบฐานข้อมูลสำหรับ SAP HANA, Oracle RMAN และ Microsoft SQL Server ที่ทำงานอยู่บนเครื่องคอมพิวเตอร์แม่ข่ายเสมือนหรือบนเครื่องคอมพิวเตอร์แม่ข่ายกายภาพ (Physical server) ได้
- 1.3.9.7 สามารถสำรองและกู้คืนข้อมูลประเภทไฟล์แชร์ได้ทั้ง CIFS และ NFS โดยต้องสามารถเลือก Path ที่ต้องการสำรองได้
- 1.3.9.8 สามารถบีบอัด (Compression) ข้อมูลหรือลดความซ้ำซ้อน (Deduplication) ข้อมูลที่ทำการสำรองได้ด้วยซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอ
- 1.3.9.9 มีเทคโนโลยี WAN Acceleration ที่ช่วยเพิ่มประสิทธิภาพการถ่ายโอนข้อมูล และลดปริมาณข้อมูลที่ส่งผ่าน WAN ในการทำ Backup Copy Job และ Replication Job
- 1.3.9.10 สามารถกู้คืนเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Microsoft Windows และ Linux ที่อยู่ในรูปแบบ Virtual หรือ Physical ไปยัง Amazon EC2 ,Microsoft Azure และ Google Compute Engine ด้วยซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอได้
- 1.3.9.11 สามารถสร้างกลุ่มของอุปกรณ์จัดเก็บข้อมูล ซึ่งเป็นที่เก็บไฟล์ข้อมูลสำรอง โดยประกอบด้วยอุปกรณ์จัดเก็บข้อมูลอย่างน้อยหนึ่งชุดหรือมากกว่า โดยการขยายสามารถใช้อุปกรณ์จัดเก็บข้อมูลต่างประเภทได้ และสามารถคัดลอกหรือย้ายชุดไฟล์ข้อมูลสำรองไปยัง Object storage ได้ เช่น Amazon S3, Microsoft Azure Blob Storage, Google Cloud Object Storage, IBM Cloud Object Storage และ Wasabi Google Cloud Object Storage
- 1.3.9.12 สามารถสำรองข้อมูลไปยังอุปกรณ์จัดเก็บข้อมูลประเภท Object Storage ได้โดยตรง

- 1.3.9.13 สามารถกู้คืนเครื่องคอมพิวเตอร์เสมือนเพื่อนำมาใช้งานได้แบบทันทีทันใด (Instant Recovery) โดยการเปิดเครื่องคอมพิวเตอร์เสมือนจากอุปกรณ์จัดเก็บข้อมูลที่ทำหน้าที่เป็น Backup repository หรือ Backup storage ขึ้นมาใช้งานได้ และสามารถกู้คืนพร้อมกันหลายเครื่องได้
- 1.3.9.14 สามารถกู้คืนระบบฐานข้อมูลบน Microsoft SQL Server และ Oracle เพื่อนำมาใช้งานได้แบบทันทีทันใดจากอุปกรณ์จัดเก็บข้อมูลที่ทำหน้าที่เป็น Backup repository หรือ Backup storage โดยต้องสามารถทำการอ่านและเขียนข้อมูลได้
- 1.3.9.15 มีความสามารถที่เรียกว่า Immutability หรือ Immutable คือ การป้องกันไม่ให้ไฟล์ข้อมูลสำรองที่อยู่ในอุปกรณ์จัดเก็บข้อมูลที่ใช้ทำงานร่วมกับซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูล (Backup Repository หรือ Backup Storage) ถูกแก้ไขหรือลบได้ โดยสามารถกำหนดระยะเวลาในการทำ Immutability หรือ Immutable ได้ เพื่อป้องกันความเสียหายของข้อมูลจาก Ransomware หรือ malware ได้ โดยความสามารถดังกล่าวต้องสามารถทำงานร่วมกับ Linux Server, HPE StoreOnce, Amazon S3 Storage และ Microsoft Azure Storage
- 1.3.9.16 สามารถทำงานร่วมกับซอฟต์แวร์แอนตี้ไวรัส เพื่อทำการสแกนข้อมูล ก่อนทำการกู้คืนไปใช้งานบนระบบ Production ในกรณีที่พบเจอ Malware หรือสิ่งแปลกปลอมอื่นๆ โดยสามารถเลือกได้ว่า สามารถดำเนินการกู้คืนได้แต่ไม่อนุญาตให้ใช้งานพอร์ตเชื่อมต่อเครือข่าย หรือให้ยกเลิกการกู้คืน
- 1.3.9.17 สามารถตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์เสมือนบน VMware vSphere และ Microsoft Hyper-V ที่ได้สำรองข้อมูลไว้ (Recovery verification) โดยการจำลองการเปิดใช้งานบนสภาพแวดล้อมเสมือน โดยสามารถกำหนดตารางเวลาในการทดสอบได้แบบอัตโนมัติ นอกจากนี้ยังมีความสามารถในการตรวจสอบความถูกต้องของข้อมูลว่ามีความเสียหายหรือไม่ และสามารถทำงานร่วมกับซอฟต์แวร์แอนตี้ไวรัสเพื่อสแกนหาว่ามี Malware หรือ Ransomware หรือไม่ และรวมถึงต้องสามารถออกรายงานเพื่อแสดงผลลัพธ์ของการทำงานได้
- 1.3.9.18 สามารถรองรับการเข้าใช้งานซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอได้ ด้วยวิธีที่เรียกว่า Multi-Factor Authentication
- 1.3.9.19 มีเครื่องมือที่ช่วยตรวจสอบว่าซอฟต์แวร์ระบบสำรองและกู้คืนข้อมูลที่น่าเสนอนั้นได้ทำการตั้งค่าเป็นไปตามแนวทางปฏิบัติที่ดีที่สุด (Best

practices) ด้านความปลอดภัยโดยอ้างอิงจากค่าพารามิเตอร์ต่างๆที่แนะนำบนซอฟต์แวร์หรือไม่

- 1.3.9.20 สามารถทำสำเนาข้อมูล (Replication) เครื่องคอมพิวเตอร์เสมือนบน VMware vSphere และ Microsoft Hyper-V ไปยังศูนย์คอมพิวเตอร์สำรอง (Disaster recovery site) และสามารถทำ Failover และ Failback เครื่องคอมพิวเตอร์เสมือนได้
- 1.3.9.21 มีลิขสิทธิ์ถูกต้องตามกฎหมายแบบ Open license ประเภท Subscription ครอบคลุมตามจำนวน Workload ที่ต้องการสำรองข้อมูล (VMs หรือ Physical หรือ VM บน Cloud instance) 1 Workloads เป็นเวลาไม่น้อยกว่า 2 ปี
- 1.3.9.22 เป็นผลิตภัณฑ์ซอฟต์แวร์ที่อยู่ในกลุ่ม Leaders ของ Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions ปีล่าสุด
- 1.3.9.23 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิคจากบริษัทผู้ผลิต พร้อมกับมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี

#### 1.4 ระบบจัดเก็บข้อมูลขนาดใหญ่ แบบที่ 1 จำนวน 1 ชุด โดยต้องมีคุณลักษณะเฉพาะขั้นต่ำเทียบเท่าหรือดีกว่าอย่างน้อยดังนี้

- 1.4.1 เป็นอุปกรณ์ที่ทำหน้าที่จัดเก็บข้อมูลบนระบบเครือข่าย (Network-Attached Storage, NAS)
- 1.4.2 มีหน่วยประมวลผลเทียบเท่าได้ไม่ต่ำกว่า Xeon E-2378 มีแกนประมวลผลไม่น้อยกว่า 8 Core และ มีความเร็วสัญญาณนาฬิกาสูงสุดไม่น้อยกว่า 4.8 GHz
- 1.4.3 มีหน่วยความจำหลัก) RAM แบบ (UDIMM DDR4 ชนิด ECC หรือดีกว่า ขนาดไม่น้อยกว่า 64 และ GB รองรับการเพิ่มสูงสุดได้ไม่น้อยกว่า 128 GB
- 1.4.4 มี ไม่น้อยกว่า Flash Memory 5 GB
- 1.4.5 สามารถติดตั้ง Disk แบบ SATA ขนาด 3.5 นิ้ว ได้ไม่น้อยกว่า 24 ลูก และมี Expansion ที่สามารถติดตั้ง HDD รวมได้ไม่น้อยกว่า 48 ลูก พร้อมติดตั้ง HDD แบบ Enterprise Class ขนาดความจุไม่น้อยกว่า 20 TB ต่อ ลูก 1 จำนวน 72 ลูก
- 1.4.6 สามารถติดตั้ง Disk ขนาด 2.5 นิ้ว ได้ไม่น้อยกว่า 6 ลูก พร้อมติดตั้ง SSD ขนาดความจุไม่น้อยกว่า 4 TB ต่อ ลูก 1 จำนวน 6 ลูก
- 1.4.7 มี Disk Bay ที่สามารถเปลี่ยน Disk ได้แบบ Hot-swappable
- 1.4.8 มีช่องเชื่อมต่อ .USB 3.2 Gen 2 หรือดีกว่า จำนวนไม่น้อยกว่า 4 ช่อง



- 1.4.9 มีช่องเชื่อมต่อ PCIe จำนวนไม่น้อยกว่า 3 ช่อง
- 1.4.10 มีแหล่งจ่ายพลังงานที่ทำงานแบบ Redundant และ Hot-Swapping พร้อมโมดูลจ่ายพลังงานตามจำนวนที่ติดตั้งได้
- 1.4.11 มีช่องเชื่อมต่อระบบเครือข่ายแบบ 2.5 GbE จำนวน 2 ช่อง 10 GbE จำนวน 2 ช่อง และ 25 GbE จำนวน 4 ช่อง โดยสามารถทำ failover และ Port Trunking ได้
- 1.4.12 สามารถทำงานร่วมกับ Microsoft Active Directory (AD) (เพื่อทำ Domain Controller) ได้ และสามารถทำงานร่วมกับ LDAP ได้
- 1.4.13 สามารถทำงานร่วมกับโปรโตคอล CIFS/SMB, AFP, NFS, FTP, SFTP, TFTP, HTTPS, Telnet, SSH, iSCSI, SNMP และ SMTP ได้เป็นอย่างดี
- 1.4.14 สามารถทำงานร่วมกับเครื่องลูกข่ายที่ใช้ระบบปฏิบัติการ Microsoft Windows 2008 R2, 2012, 2012 R2, 2016 and 2019 หรือ Version ล่าสุด, Apple MAC OS X และ Linux & UNIX ได้เป็นอย่างดี
- 1.4.15 มีลักษณะการจัดการ File System สำหรับ Internal drive แบบ ZFS และ External drive แบบ EXT3 , EXT4 , NTFS , FAT32, HFS+ และ exFAT
- 1.4.16 สามารถบริหารจัดการหน่วยจัดเก็บข้อมูลแบบ Single Disk, JBOD, และ RAID 0/1/5/6/10/50/60 ได้เป็นอย่างดี
- 1.4.17 สามารถทำ Shared Folder Data Compression หรือ Shared Folder Data Deduplication หรือเทียบเท่าได้
- 1.4.18 สามารถทำ Real-time or scheduled replication over Snap Sync หรือเทียบเท่าได้
- 1.4.19 สามารถทำ Compression and Deduplication over Snap Sync หรือเทียบเท่าได้
- 1.4.20 สามารถบริหารจัดการด้านพลังงาน เช่น Wake on LAN และ Automatic power on after power recovery ได้เป็นอย่างดี
- 1.4.21 มี Module Transceiver ที่รองรับความเร็ว 25 GB จำนวน 4 หน่วย
- 1.4.22 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิค และการรับประกัน การสำรองอะไหล่ ไม่น้อยกว่า 2 ปี จากบริษัทผู้ผลิต ที่มีสำนักงานสาขาในประเทศไทย พร้อมต้องมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี
- 1.5 ระบบจัดเก็บข้อมูลขนาดใหญ่ แบบที่ 2 จำนวน 1 ชุด โดยต้องมีคุณสมบัติเฉพาะขั้นต่ำเทียบเท่าหรือดีกว่าอย่างน้อยดังนี้**
  - 1.5.1 มีหน่วยประมวลผลกลาง (CPU) ชนิด Intel Xeon ขนาดไม่น้อยกว่า 8 Core และมีความเร็วสัญญาณนาฬิกาพื้นฐานรวมไม่น้อยกว่า (CPU Frequency) 2.1 GHz. จำนวนอย่างน้อย 1 หน่วย

- 1.5.2 มี Hardware Encryption Engine
- 1.5.3 มีหน่วยความจำหลัก (System Memory) ไม่น้อยกว่า 32 GB ชนิด DDR4 หรือดีกว่า รองรับการขยายสูงสุดไม่น้อยกว่า GB 64
- 1.5.4 มีช่องใส่หน่วยจัดเก็บข้อมูล (Hard Disk) ไม่น้อยกว่า 12 Bays รองรับหน่วยจัดเก็บข้อมูล (Hard Disk) ชนิด SATA หรือ NL-SAS ขนาด 2.5” หรือ 3.5” แบบ Hot Swappable และรองรับหน่วยต่อขยาย (Expansion Units) ได้ไม่ต่ำกว่า 2 หน่วย หรือรองรับจำนวนหน่วยจัดเก็บข้อมูลไม่ต่ำกว่า 36 ลูก
- 1.5.5 มีหน่วยจัดเก็บข้อมูล (Hard Disk) Enterprise Grade ชนิด SATA หรือ NL-SAS หรือดีกว่า ขนาด 3.5” มีความจุไม่น้อยกว่า 16 TB จำนวน 10 หน่วย โดยมีคุณลักษณะขั้นต่ำ ดังนี้
  - 1.5.5.1 มี Interface Access Speed (Gb/s) ไม่ต่ำกว่า 6 Gbps
  - 1.5.5.2 มี Spindle Speed (RPM) ไม่ต่ำกว่า 7,200 RPM
  - 1.5.5.3 มี Buffer Size ไม่ต่ำกว่า 512 MiB
  - 1.5.5.4 อยู่ใน Product Compatible List ของสินค้าที่นำเสนอ เพื่อการเข้ากันของ Firmware และ ประสิทธิภาพการใช้งาน
- 1.5.6 มี USB 3.2 Gen 1 หรือดีกว่าไม่ต่ำกว่า 2 พอร์ต
- 1.5.7 มี Network Interface Port ความเร็ว 1 Gb ชนิด RJ-45 จำนวนไม่น้อยกว่า 4 Ports
- 1.5.8 มี Network Interface Port ความเร็ว 10 Gb ชนิด RJ-45 จำนวนไม่น้อยกว่า 2 Ports
- 1.5.9 มี Network Interface Port ความเร็ว 25 Gb ชนิด SFP28 จำนวนไม่น้อยกว่า 4 Ports
- 1.5.10 รองรับการทำ RAID 0, 1, 5, 6, 10, JBOD ได้เป็นอย่างดี
- 1.5.11 รองรับการทำ SSD Read / Write Cache และ SSD TRIM และทำ RAID Group ได้
- 1.5.12 สามารถทำงานในระบบ iSCSI หรือ IP SAN ได้
- 1.5.13 ตัวอุปกรณ์มีหน่วยจ่ายพลังงาน (Power Supply) จำนวน 2 หน่วย ทำงานแบบ Redundant
- 1.5.14 ตัวอุปกรณ์ถูกออกแบบให้สามารถติดตั้งในตู้ RACK ขนาด 19 นิ้ว มาตรฐานได้ โดยมีอุปกรณ์ติดตั้งใน Rack (ขาาราง) มาให้พร้อม
- 1.5.15 มีระบบปฏิบัติการ (OS) ติดตั้งมาให้พร้อมตัวเครื่องและมีลิขสิทธิ์ถูกต้องตามกฎหมาย
- 1.5.16 รองรับการใช้งานร่วมกับ Active Directory (AD) หรือ LDAP ได้เป็นอย่างดี
- 1.5.17 ตัวอุปกรณ์รองรับระบบ File System ชนิด Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT ได้เป็นอย่างดี
- 1.5.18 ตัวอุปกรณ์รองรับ Networking Protocols ชนิด SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN ได้เป็นอย่างดี

- 1.5.19 รองรับ Client ที่ใช้งานผ่านระบบ อย่างน้อย ดังนี้ Window 7 onwards, macOS 10.12 onwards
- 1.5.20 รองรับการทำ Virtualization อย่างน้อย ดังนี้ VMware vSphere 6.5, Microsoft Hyper-V, Citrix Ready, OpenStack
- 1.5.21 ผู้เสนอราคาต้องมีเอกสารรับรองการสนับสนุนทางเทคนิค และการรับประกัน การสำรองอะไหล่ ไม่น้อยกว่า 2 ปี จากบริษัทผู้ผลิต ที่มีสำนักงานสาขาในประเทศไทย พร้อมกับมีเอกสารรับรองการสนับสนุนทางเทคนิคให้กับมหาวิทยาลัยขอนแก่น โดยมีระยะเวลาไม่น้อยกว่า 2 ปี

## 2 การติดตั้ง และการบำรุงรักษา

2.1 ส่งมอบงาน ในงวดเดียว

2.2 รับประกันระบบที่เสนอ ไม่น้อยกว่า 1 ปี นับถัดจากวันส่งมอบ

3 ระยะเวลาส่งมอบครุภัณฑ์... 90... วัน

4 วงเงินในการจัดหา จำนวน 11,000,000 บาท (สิบเอ็ดล้านบาทถ้วน)