

การเปรียบเทียบประสิทธิภาพการทำงาน ความปลอดภัย และการจัดเก็บไฟล์ข้อมูล กรณีศึกษาการปรับใช้ Nextcloud ในองค์กร

Performance, Security, and File Storage Comparison, Case Study of Nextcloud Implementation in Organizations

วรพงศ์ แสงปิยะเพชร^{1*}, ปรียาภรณ์ สุขงาม² และ ศราวุฒิ สิทธารถ³

Vorapong Sangpiyaphet^{1*}, Preeyaphorn Sukngam² and Sarawut Sittharod³

ฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล^{1, 2, 3}

Siriraj Information Technology Department

Faculty of Medicine Siriraj Hospital, Mahidol University^{1, 2, 3}

e-mail: vorapong.san@mahidol.ac.th¹, preeyaporn.suk@mahidol.edu², sarawut.shi@mahidol.edu³

Received: August 28, 2024; Revised: March 6, 2024; Accepted: March 20, 2025

บทคัดย่อ

ปัจจุบันเทคโนโลยีการจัดเก็บข้อมูลบนคลาวด์ และแพลตฟอร์มการทำงานร่วมกันแบบโอเพนซอร์สได้รับความนิยมเพิ่มขึ้น เนื่องจากช่วยลดต้นทุน และเพิ่มความยืดหยุ่นในการดำเนินงานขององค์กร บทความนี้มุ่งศึกษาการนำ Nextcloud มาใช้เป็นแนวทางการแก้ปัญหาการจัดเก็บข้อมูล และแพลตฟอร์มการทำงานร่วมกันภายในองค์กร โดยเน้นการประเมินประสิทธิภาพด้านความปลอดภัย ความสามารถในการปรับขยาย และความสะดวกในการใช้งาน ผ่านการวิเคราะห์เชิงเปรียบเทียบกับแพลตฟอร์มอื่น เช่น ownCloud และ Seafile รวมถึงการศึกษาแนวทางการปรับใช้ Nextcloud ให้เหมาะสมกับองค์กรผ่านกรณีศึกษาที่แท้จริง ผลการศึกษาพบว่า Nextcloud มีความสามารถในการปรับแต่งสูง และสามารถผสมผสานรวมกับระบบภายในองค์กรได้ดี แต่มีข้อจำกัดในด้านการบริหารจัดการและการบำรุงรักษาเมื่อเทียบกับแพลตฟอร์มอื่นเชิงพาณิชย์ นอกจากนี้ บทความยังเสนอแนวทางการกำหนดค่าความปลอดภัย และแนวปฏิบัติที่ช่วยเพิ่มประสิทธิภาพการใช้งานให้เหมาะสมกับบริบทขององค์กร ผลลัพธ์จากการศึกษานี้จะเป็นแนวทางให้ผู้บริหาร และผู้ดูแลระบบสามารถตัดสินใจเลือกใช้แพลตฟอร์มการทำงานร่วมกัน และการจัดเก็บข้อมูลแบบโอเพนซอร์สได้อย่างเหมาะสมและมีประสิทธิภาพ

คำสำคัญ: Nextcloud การจัดเก็บข้อมูลบนคลาวด์ แพลตฟอร์มการทำงานร่วมกันแบบโอเพนซอร์ส ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

Abstract

In recent years, cloud storage technologies and open-source collaboration platforms have gained increasing popularity due to their cost-effectiveness and operational flexibility for organizations. This article examines the adoption of Nextcloud as a solution for organizational data storage and collaboration, focusing on evaluating its performance in terms of security, scalability, and usability. The study employs comparative analysis with other platforms, including ownCloud and Seafile, and explores best practices for implementing Nextcloud effectively through real-world case studies. The findings reveal that Nextcloud offers a high degree of customization and strong integration capabilities with internal organizational systems. However,

it presents certain limitations in management and maintenance compared to commercial alternatives. Additionally, the article proposes security configuration guidelines and operational practices to enhance system performance and ensure alignment with organizational contexts. The results provide practical insights for executives and system administrators in selecting and implementing open-source collaboration and cloud storage platforms that are both efficient and suitable for organizational needs.

Keyword: Nextcloud Cloud Storage, Open-Source Collaborative Platform, Information Technology Security

ความนำ

ในยุคดิจิทัลปัจจุบันเทคโนโลยีมีบทบาทสำคัญในทุกภาคส่วนของการดำเนินงาน และมีการพัฒนาอย่างต่อเนื่อง องค์กร และบุคคลทั่วไปสามารถใช้ประโยชน์จากเทคโนโลยีเพื่อปรับปรุงประสิทธิภาพของโครงสร้างพื้นฐาน และลดความเหลื่อมล้ำในการเข้าถึงข้อมูลข่าวสาร (แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 (พ.ศ. 2566–2570), 2565) การจัดการข้อมูลและการทำงานร่วมกันอย่างมีประสิทธิภาพ กลายเป็นปัจจัยสำคัญที่ส่งผลต่อความสำเร็จขององค์กร การจัดเก็บข้อมูลบนคลาวด์ และแพลตฟอร์มการทำงานร่วมกันแบบโอเพนซอร์สเป็นทางเลือกที่น่าสนใจและมีประสิทธิภาพสำหรับองค์กรต่าง ๆ

หนึ่งในแพลตฟอร์มที่ได้รับความนิยมในด้านนี้คือ Nextcloud ซึ่งเป็นระบบจัดเก็บข้อมูลบนคลาวด์ และแพลตฟอร์มการทำงานร่วมกันแบบโอเพนซอร์ส Nextcloud ถูกพัฒนาขึ้นเพื่อให้บริการการจัดเก็บ และจัดการข้อมูลที่มีความปลอดภัยและมีประสิทธิภาพ โดยช่วยให้องค์กรสามารถเก็บรักษาข้อมูล และทำงานร่วมกันได้อย่างราบรื่นผ่านอินเทอร์เน็ตที่ใช้ทำงานง่าย และมีฟังก์ชันการทำงานที่หลากหลาย ไม่ว่าจะเป็นการแชร์ไฟล์ การประสานงานระหว่างทีม หรือการเข้าถึงข้อมูลจากทุกที่ทุกเวลา

บทความนี้จะนำเสนอข้อดี และข้อเสียของแพลตฟอร์มการทำงานร่วมกันแบบโอเพนซอร์ส รวมทั้งนำเสนอกรณีตัวอย่างการพัฒนา และการนำเทคโนโลยีของ Nextcloud มาพัฒนาต่อยอดในบริบทขององค์กรที่ต้องการบริหารจัดการการจัดเก็บข้อมูลบนคลาวด์ส่วนตัวที่มีความปลอดภัย และพร้อมใช้งานอยู่ตลอดเวลา เพื่อให้เห็นภาพรวมถึงประโยชน์ และความเป็นไปได้ในการปรับใช้แพลตฟอร์มนี้ในบริบทที่หลากหลายมากยิ่งขึ้น ทั้งนี้เพื่อให้ผู้อ่านมีข้อมูลที่ครบถ้วน และสามารถตัดสินใจเลือกใช้เทคโนโลยีที่เหมาะสมกับความต้องการขององค์กรได้อย่างมั่นใจ

แพลตฟอร์มการทำงานร่วมกันแบบโอเพนซอร์ส (Open Source Collaboration Platforms)

แพลตฟอร์มการทำงานร่วมกันแบบโอเพนซอร์ส (Open Source Collaboration Platforms) คือซอฟต์แวร์ที่อนุญาตให้ทีมงานและองค์กรต่าง ๆ ทำงานร่วมกันได้อย่างมีประสิทธิภาพ โดยสามารถเข้าถึงโค้ด และปรับแต่งได้ตามความต้องการ Khosravi (2022) ได้อธิบายเกี่ยวกับแพลตฟอร์มการทำงานร่วมกันแบบโอเพนซอร์ส ยกตัวอย่าง เช่น Nextcloud, Carbonio Community Edition, ownCloud และ Seafile ซึ่งได้รับความนิยมเนื่องจากสามารถปรับแต่งตามความต้องการเฉพาะขององค์กรได้ง่าย มีความโปร่งใสในการพัฒนา การปรับปรุง และไม่มีค่าใช้จ่ายในการใช้ซอฟต์แวร์ ข้อดีอื่น ๆ ได้แก่ ความสามารถในการควบคุมข้อมูลได้อย่างเต็มที่ การมีชุมชนผู้ใช้ และนักพัฒนาที่ช่วยสนับสนุน อย่างไรก็ตาม ข้อเสียบางประการคือ การต้องการทรัพยากรในการบริหารจัดการและการรักษาความปลอดภัยของระบบเอง

การจัดเก็บข้อมูลบนคลาวด์

Kochovski (2024) ได้อธิบายเกี่ยวกับการจัดเก็บข้อมูลบนคลาวด์ทั้งในรูปแบบออนพรีมิส (On-Premises) และออนคลาวด์ (On-Cloud) ช่วยให้องค์กรเก็บรักษาข้อมูลจำนวนมากได้โดยไม่ต้องลงทุนในโครงสร้างพื้นฐานทางกายภาพ นอกจากนี้ยังมีข้อดีอื่น ๆ เช่น การเข้าถึงข้อมูลได้จากทุกที่ทุกเวลา ความยืดหยุ่นในการขยายขนาดการจัดเก็บ และการสำรองข้อมูลอัตโนมัติ อย่างไรก็ตาม ข้อเสียบางประการรวมถึงความกังวลเกี่ยวกับความปลอดภัยของข้อมูล ความเป็นส่วนตัว และความเสี่ยงในการพึ่งพาผู้ให้บริการคลาวด์

แนวคิดเกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Cyber Security)

แนวคิดเกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Cyber Security) เป็นปัจจัยสำคัญที่องค์กรต้องให้ความสำคัญอย่างยิ่งในยุคดิจิทัลปัจจุบัน การเพิ่มขึ้นของการใช้เทคโนโลยีดิจิทัลในองค์กรต่าง ๆ ได้นำมาซึ่งความเสี่ยงด้านความปลอดภัยที่หลากหลาย การตระหนักรู้และความเข้าใจเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรจึงมีความสำคัญอย่างยิ่ง การศึกษาของ Nifakos และคณะ (2021) พบว่าความรู้ทั่วไปเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ และความเข้าใจในนโยบายที่เกี่ยวข้องมีผลต่อความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรในองค์กร นอกจากนี้ การวิจัยโดย Buja และคณะ (2021) ได้พัฒนาโมเดลการตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้สูงอายุ ซึ่งชี้ให้เห็นถึงความสำคัญของการเสริมสร้างความรู้ และการฝึกอบรมด้านความปลอดภัยไซเบอร์ในกลุ่มบุคคลต่าง ๆ การเสริมสร้างความรู้ด้านความปลอดภัยไซเบอร์ในองค์กรสามารถทำได้ผ่านการฝึกอบรม และการสร้างนโยบายที่ชัดเจน ซึ่งจะช่วยลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น

การมีนโยบายความมั่นคงปลอดภัยสารสนเทศที่ชัดเจน และการฝึกอบรมที่เหมาะสมจะช่วยให้องค์กรสามารถป้องกัน และรับมือกับภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ ดังนั้น การลงทุนในด้านการฝึกอบรม และการสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์จึงเป็นสิ่งที่องค์กรไม่ควรมองข้าม

จากการศึกษา พบว่าการรักษาความลับ ความถูกต้องของข้อมูล และความพร้อมใช้งานระบบ ตรงกับหลักการ CIA Triad หรือในบางครั้งเรียกว่า AIC Triad เป็นหลักการด้านการรักษาความปลอดภัยข้อมูลสารสนเทศ Walkowski (2019) ได้ศึกษาหลัก CIA Triad ซึ่งเป็นแนวคิดพื้นฐานในด้าน ความปลอดภัยทางไซเบอร์ ที่ใช้เป็นกรอบแนวคิดในการปกป้องข้อมูล และระบบสารสนเทศ โดยประกอบด้วย 3 องค์ประกอบหลัก ได้แก่

1. Confidentiality (ความลับของข้อมูล)
 - 1.1 ปกป้องไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูล
 - 1.2 ใช้วิธีการเข้ารหัส (Encryption) การควบคุมสิทธิการเข้าถึง (Access Control) และการรับรองตัวตน (Authentication)
2. Integrity (ความสมบูรณ์ของข้อมูล)
 - 2.1 ทำให้แน่ใจว่าข้อมูลไม่ได้ถูกเปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต
 - 2.2 ใช้เทคนิคแฮชชิง (Hashing) ลายมือชื่อดิจิทัล (Digital Signature) และการควบคุมเวอร์ชันของข้อมูล
3. Availability (ความพร้อมใช้ของข้อมูล)
 - 3.1 ข้อมูล และระบบต้องสามารถเข้าถึงและใช้งานได้เมื่อจำเป็น

- 3.2 ใช้มาตรการป้องกันการโจมตีทางไซเบอร์ (Distributed Denial of Service: DDoS)
- 3.3 การกระจายปริมาณการใช้งาน หรือโหลดให้กับเซิร์ฟเวอร์หลาย ๆ เครื่อง (Load Balancing)
- 3.4 การสำรองข้อมูล (Backup & Redundancy)

ความจำเป็นของระบบจัดเก็บข้อมูลภายในองค์กรสำหรับข้อมูลที่เป็นความลับ

มนพ การกล้า และคณะ (2565) ได้ทำการศึกษา การก้าวเข้าสู่ยุคอินเทอร์เน็ตในทุกสิ่ง (Internet of Things) ซึ่งอุปกรณ์ต่าง ๆ มีโปรแกรมใช้งานร่วมกับคอมพิวเตอร์ ซึ่งในปัจจุบันองค์กรต่าง ๆ ต้องเผชิญกับความท้าทายด้านการจัดเก็บข้อมูล โดยเฉพาะข้อมูลที่มีความสำคัญและมีความลับสูง เช่น ข้อมูลทางการเงิน ข้อมูลลูกค้า ข้อมูลเชิงกลยุทธ์ หรือเอกสารภายในที่เกี่ยวข้องกับการดำเนินธุรกิจ ซึ่งข้อมูลเหล่านี้ต้องได้รับการจัดเก็บและบริหารจัดการภายในองค์กรเพื่อให้เป็นไปตามนโยบายด้านความปลอดภัย และการปฏิบัติตามข้อบังคับทางกฎหมาย เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ General Data Protection Regulation (GDPR) การจัดเก็บข้อมูลในระบบคลาวด์สาธารณะ เช่น Google Drive, Dropbox หรือ OneDrive อาจไม่ตอบโจทย์ในกรณีที่ต้องการการความเป็นส่วนตัวสูงสุด และต้องการควบคุมข้อมูลอย่างสมบูรณ์ เนื่องจากข้อมูลจะถูกจัดเก็บไว้บนเซิร์ฟเวอร์ของผู้ให้บริการที่อยู่นอกองค์กร ซึ่งอาจมีความเสี่ยงต่อการเข้าถึงจากบุคคลที่สามหรือปัญหาด้านความปลอดภัยที่องค์กรไม่สามารถควบคุมได้

คลาวด์สตอเรจแบบโอเพนซอร์สบนเซิร์ฟเวอร์ภายในองค์กรจึงกลายเป็นทางเลือกที่เหมาะสม เนื่องจากเป็นซอฟต์แวร์ คลาวด์ส่วนตัว (Private Cloud) ที่ช่วยให้องค์กรสามารถสร้างระบบจัดเก็บข้อมูลภายในองค์กรเอง โดยไม่ต้องพึ่งพาผู้ให้บริการภายนอก องค์กรสามารถกำหนดนโยบายการเข้าถึงข้อมูล กำหนดสิทธิ์ของผู้ใช้ และควบคุมมาตรการด้านความปลอดภัยได้อย่างเต็มรูปแบบ ทำให้คลาวด์สตอเรจแบบโอเพนเป็นโซลูชันที่ตอบโจทย์สำหรับองค์กรที่ต้องการ เก็บรักษาข้อมูลสำคัญภายในองค์กร และต้องการความปลอดภัยสูงสุด ด้วยเหตุนี้ การเลือกใช้ซอฟต์แวร์จัดเก็บข้อมูลจึงเป็นปัจจัยสำคัญในการบริหารจัดการเอกสารดิจิทัลภายในองค์กร ซึ่งจะถูกกล่าวถึงในหัวข้อถัดไปเกี่ยวกับซอฟต์แวร์ที่ใช้สำหรับการจัดเก็บ หรือสำรองเอกสารในระบบสารสนเทศ

ซอฟต์แวร์ที่ใช้สำหรับการจัดเก็บหรือสำรองเอกสารในระบบสารสนเทศ

ในยุคดิจิทัล เอกสารในรูปแบบดิจิทัลมีบทบาทสำคัญอย่างมากในองค์กร เนื่องจากเป็นแหล่งข้อมูลหลักที่ใช้ในการบริหารจัดการ การดำเนินงาน และการสื่อสารภายในองค์กร การจัดเก็บ และสำรองข้อมูลอย่างปลอดภัยจึงเป็นสิ่งจำเป็นเพื่อป้องกันการสูญหายของข้อมูล การรั่วไหลของข้อมูล และการเข้าถึงโดยไม่ได้รับอนุญาต ปัจจุบันมีซอฟต์แวร์หลายประเภทที่ใช้สำหรับจัดเก็บ หรือสำรองข้อมูล เช่น Google Drive, Dropbox, OneDrive และ pCloud ซึ่งเป็นระบบคลาวด์สาธารณะที่ได้รับความนิยม เนื่องจากใช้งานง่าย และมีค่าใช้จ่ายไม่สูง อย่างไรก็ตาม องค์กรที่มีข้อมูลที่ต้องการ ความปลอดภัยสูง หรือต้องการควบคุมข้อมูลทั้งหมดภายในองค์กร เช่น องค์กรทางด้านสาธารณสุข องค์กรทางการศึกษา หรือหน่วยงานราชการ ฯลฯ อาจพบว่าระบบคลาวด์สาธารณะมีข้อจำกัดหลายประการ เช่น

1. ความเสี่ยงด้านความปลอดภัย-ข้อมูลอาจถูกจัดเก็บบนเซิร์ฟเวอร์ของผู้ให้บริการที่อยู่นอกองค์กร ทำให้เกิดความเสี่ยงด้านการเข้าถึงข้อมูลจากบุคคลที่สาม
2. ข้อจำกัดด้านการกำหนดนโยบาย-องค์กรไม่สามารถควบคุมการเข้าถึงหรือกำหนดค่าความปลอดภัยของข้อมูลได้อย่างเต็มที่

3. ข้อกำหนดด้านกฎหมาย และการปฏิบัติตามกฎระเบียบ (Compliance) หลายองค์กร โดยเฉพาะภาคการเงิน หน่วยงานราชการ หรือองค์กรที่ต้องปฏิบัติตามกฎหมาย เช่น PDPA (Personal Data Protection Act) และ GDPR (General Data Protection Regulation) อาจต้องการโซลูชันที่สามารถเก็บข้อมูลภายในองค์กรได้

ดังนั้นการจัดเก็บและสำรองข้อมูลอย่างปลอดภัยจึงเป็นสิ่งที่จำเป็น ซึ่งซอฟต์แวร์ Nextcloud ได้มีการนำเสนอโซลูชันการจัดเก็บคลาวด์ส่วนตัว ที่ช่วยให้ผู้ใช้ควบคุม ข้อมูลของตนเองได้อย่างสมบูรณ์

ทางคณะผู้เขียนได้ดำเนินการศึกษา วิเคราะห์ และเปรียบเทียบ Nextcloud กับซอฟต์แวร์ประเภทเดียวกันในตลาด เพื่อช่วยให้ผู้อ่านตัดสินใจว่า Nextcloud เหมาะกับความต้องการของผู้อ่านหรือไม่ ซึ่งคุณสมบัติหลักของซอฟต์แวร์ การจัดเก็บข้อมูลส่วนตัวในรูปแบบคลาวด์นั้นจะประกอบด้วยคุณสมบัติหลักที่สำคัญซึ่งถือว่าเป็นหัวใจสำคัญของการใช้งานซอฟต์แวร์การจัดเก็บข้อมูลส่วนตัวในองค์กรต่าง ๆ ดังแสดงในตารางที่ 1

ตารางที่ 1

เปรียบเทียบคุณสมบัติของแต่ละซอฟต์แวร์ สำหรับการจัดเก็บข้อมูลส่วนตัว

คุณสมบัติ	Nextcloud	Dropbox	Google Drive	OneDrive
โฮสต์	ส่วนตัว หรือสาธารณะ	สาธารณะ	สาธารณะ	สาธารณะ
พื้นที่จัดเก็บ	ขึ้นอยู่กับขนาดกับเนื้อที่ การจัดการขององค์กร	2 GB	15GB	5GB
การรักษาความปลอดภัย	1. การเข้ารหัสจากต้นทางถึงปลายทาง (End-to-End Encryption) 2. การตรวจสอบสิทธิ์แบบสองชั้น (Two Factor Authenticate)			
การแชร์ไฟล์	1. ง่ายดาย 2. กำหนดสิทธิ์การเข้าถึงตามกิจกรรม			
การซิงค์ข้อมูล	รองรับ	รองรับ	รองรับ	รองรับ
การปรับแต่ง	รองรับ	ไม่รองรับ	ไม่รองรับ	ไม่รองรับ

โดยงานวิจัยของ จรรยา สาวีลี (2567) ได้ทำการเปรียบเทียบประสิทธิภาพการทำงานของคลาวด์สตอเรจแบบโอเพนซอร์ส 5 โปรแกรม ได้แก่ Nextcloud, ownCloud, Seafile, Pydio และ Tonido บนเซิร์ฟเวอร์แบบเวอร์ชวลไลเซชัน ผลการวิจัยพบว่า Nextcloud มีความโดดเด่นในด้าน เวลาตอบสนอง (Response Time) และ อัตราการส่งข้อมูล (Throughput) ซึ่งเป็นปัจจัยสำคัญสำหรับองค์กรที่ต้องการ ระบบที่รองรับการทำงานร่วมกันแบบเรียลไทม์ และมีประสิทธิภาพในการถ่ายโอนไฟล์ อย่างไรก็ตาม ด้านแบนด์วิดท์การดาวน์โหลดและอัปโหลด (Bandwidth) พบว่า Seafile และ Pydio มีผลลัพธ์ที่ดีกว่า Nextcloud เล็กน้อย เนื่องจากโครงสร้างพื้นฐานและการออกแบบของซอฟต์แวร์แต่ละตัวแตกต่างกัน ดังแสดงในตารางที่ 2

ตารางที่ 2

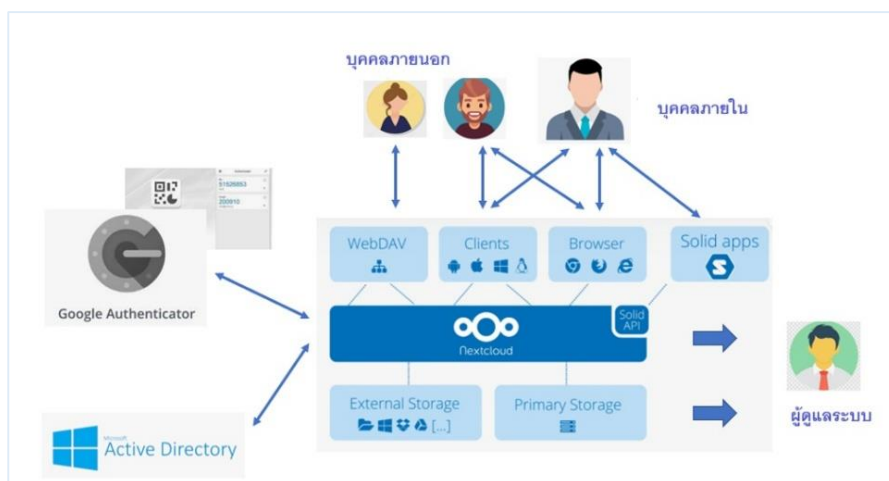
การจัดลำดับประสิทธิภาพของคลาวด์สตอเรจด้านต่าง ๆ

เปรียบเทียบ ประสิทธิภาพ ด้านต่าง ๆ	การจัดลำดับประสิทธิภาพ Cloud Storage				
	ดีมาก	ดี	ปานกลาง	น้อย	น้อยที่สุด
Bandwidth (Download)	Pydio	Tonido	Seafile	Nextcloud	ownCloud
Bandwidth (Upload)	Seafile	Pydio	Tonido	Nextcloud	ownCloud
ResponseTime	Nextcloud	Pydio	Owncloud	Seafile	Tonido
Throughput	Nextcloud	Owncloud	Pydio	Tonido	Seafile

จากการเปรียบเทียบทำให้เห็นว่า Nextcloud จึงเป็นตัวเลือกที่เหมาะสมสำหรับองค์กรที่ต้องการความเป็นส่วนตัวสูงสุด และต้องการควบคุมข้อมูลสำคัญทั้งหมดด้วยตนเอง ซึ่งในหัวข้อต่อไปนี้จะนำเสนอกรณีศึกษาขององค์กรที่นำ Nextcloud มาใช้เป็นโซลูชันหลักสำหรับการจัดเก็บเอกสารในระบบสารสนเทศ เพื่อให้เห็นถึงการนำไปใช้งานจริง และผลลัพธ์ที่ได้รับจากการปรับใช้ระบบนี้ (จรรยา สาวีถี, 2567)

กรณีศึกษา: การใช้งาน Nextcloud เพื่อการจัดเก็บเอกสารในระบบสารสนเทศ

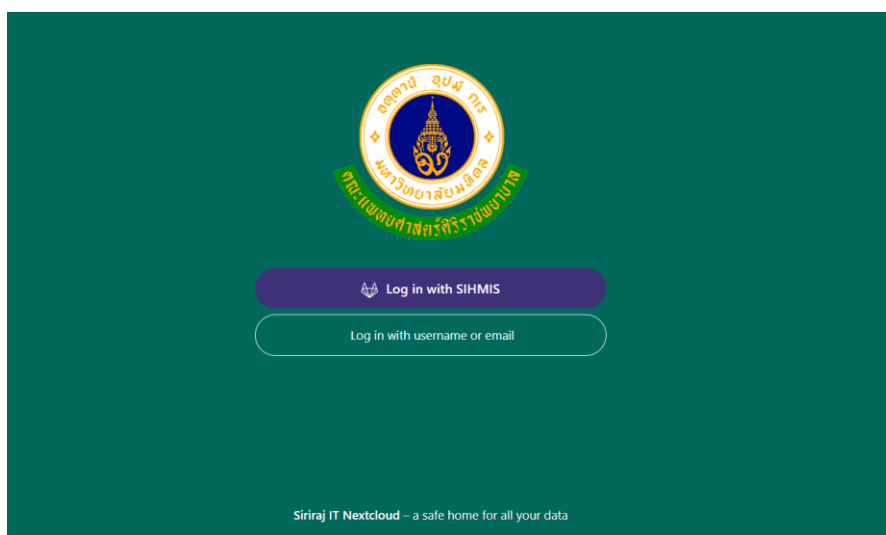
Nextcloud เป็นแพลตฟอร์มการจัดเก็บข้อมูลบนคลาวด์ และการทำงานร่วมกันที่ได้รับการยอมรับอย่างกว้างขวาง Nextcloud มุ่งเน้นการรักษาความปลอดภัย และความเป็นส่วนตัวของข้อมูลโดยมีการเข้ารหัสทั้งในระดับไฟล์ และการรับส่งข้อมูล นอกจากนี้ Nextcloud ยังมีฟีเจอร์การทำงานร่วมกันที่หลากหลาย เช่น การแชร์ไฟล์ การทำงานร่วมกันบนเอกสารแบบเรียลไทม์ และการซิงค์ข้อมูลระหว่างอุปกรณ์ต่าง ๆ



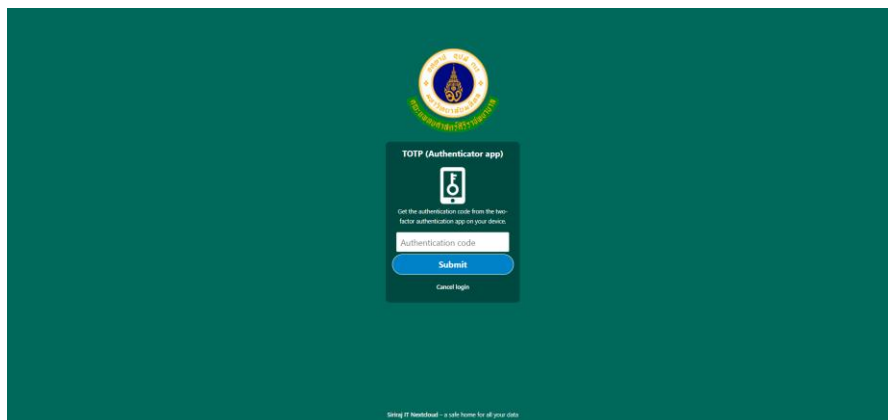
ภาพที่ 1 สถาปัตยกรรมการทำงานของระบบ Nextcloud จากกรณีศึกษา

จากภาพที่ 1 ทางคณะผู้เขียนจะอธิบายการทำงานเป็น 2 ส่วน โดยส่วนแรก จะเป็นการทำงานเชิงสถาปัตยกรรมการทำงานของระบบ (System Architecture) โดยเราจะเริ่มติดตั้งซอฟต์แวร์ Nextcloud บนระบบเครือข่ายของคณะแพทยศาสตร์ศิริราชพยาบาล และดำเนินการติดตั้งระบบฐานข้อมูล และกำหนดพื้นที่ในการเก็บข้อมูล และทำการตั้งค่าระบบการตรวจสอบตัวตน (Active Directory) ของคณะฯ และเชื่อมกับระบบ Google Authenticate สำหรับการทำการตรวจสอบสิทธิ์แบบสองชั้น (Two Factor Authenticate) ซึ่งจะดำเนินการโดยผู้ดูแลระบบ ส่วนที่สองจะอธิบายการใช้งาน ซึ่งจะประกอบด้วย 2 ส่วนด้วยกันคือ 1. ผู้ดูแลระบบทำหน้าที่ในการตั้งค่าสำหรับจัดการดูแลระบบ และบันทึกข้อมูลการใช้งาน 2. ผู้ใช้งานซึ่งจะมีทั้งบุคลากรภายในและภายนอกฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล สำหรับบุคลากรของฝ่ายฯ จะใช้ระบบตรวจสอบตัวตน (Active Directory) ด้วย Username และ Password เดียวกับระบบ eDocument ของคณะฯ แต่ถ้าเป็นบุคลากรภายนอกต้องใช้ Username, Password และจะต้องตรวจสอบอีกรอบบนระบบ Google Authenticate ซึ่งจะเป็นการตรวจสอบแบบการยืนยันแบบสองชั้นตอน (Two Factor Authenticate)

โดยการนำมาใช้นั้น ทางคณะผู้เขียนจะยกตัวอย่างการนำ Nextcloud มาใช้ในการบริหารจัดการเอกสารระหว่างกลุ่มคนใช้งานภายในองค์กรสองกลุ่ม จากภาพที่ 2 โดยจะแบ่งการเข้าใช้งานสู่ระบบ Nextcloud ออกเป็นสองกลุ่มใหญ่ดังนี้ หนึ่งคือกลุ่มของคนภายในองค์กรที่จะต้องใช้งานผ่านระบบตรวจสอบตัวตน (Active Directory) และกลุ่มที่สองนั้นคือกลุ่มผู้ใช้งานที่ไม่ได้เป็นบุคคลภายในองค์กรโดยตรง แต่เป็นกลุ่มคนจากภายนอกองค์กรที่จำเป็นจะต้องทำงานร่วมกันในการบริหารจัดการโครงการ จากภาพที่ 3 เมื่อเข้าสู่ระบบแล้วจะพบกับรหัสผ่านแบบใช้ครั้งเดียวตามเวลา (Time-based One Time Password, TOTP) โดยผู้ที่ต้องการใช้งานจะต้องทำการเข้าสู่ระบบผ่านการกรอกข้อมูลจาก Google Authenticate อีกครั้งหนึ่งก่อนที่จะเข้าสู่ระบบ Nextcloud เพื่อเป็นการป้องกันอีกชั้นหนึ่ง ซึ่งถูกเรียกว่าการยืนยันแบบสองชั้นตอน (Two Factor Authenticate)

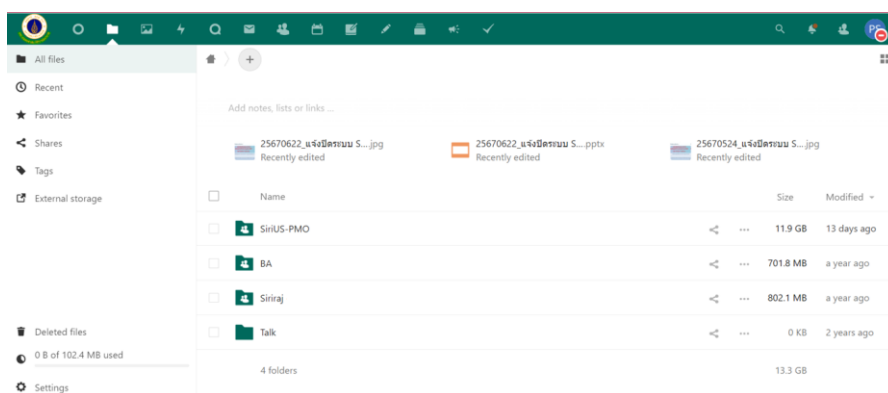


ภาพที่ 2 รูปหน้าจอล็อกอินของโปรแกรม Nextcloud



ภาพที่ 3 รูปหน้าจอการกรอก TOTP (Authentication App) ของโปรแกรม Nextcloud

จากภาพที่ 4 หลังจากการเข้าใช้งานแล้วนั้น จะพบกับหน้าจอการใช้งานที่เข้าใจได้ง่าย โดยคณะผู้เขียนจะขอลำถึงเมนูที่ชื่อว่า Files ซึ่งจะรวบรวมข้อมูลที่ถูกจัดเก็บข้อมูลใน Nextcloud เอาไว้ โดยโฟลเดอร์ที่พบเห็นจะเป็นการถูกบริหารจัดการจากผู้ดูแลระบบซึ่งแยกกลุ่มของผู้ใช้งานเอาไว้ โดยทางคณะผู้เขียนจะขอยกตัวอย่างในกรณีศึกษาหนึ่งหนึ่งคือการทำงานในกลุ่มของผู้ใช้งานภายในองค์กร ภายในโฟลเดอร์การทำงานนี้จะมีแต่บุคลากรขององค์กรเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านี้ได้ ซึ่งอาจจะเป็นข้อมูลที่เป็นความลับ และไม่ต้องการเปิดเผยกับบุคคลภายนอก สองคือกลุ่มโฟลเดอร์ของบุคคลภายนอก ซึ่งในกรณีนี้ศึกษานี้จะใช้เพื่อการทำงานร่วมกันของคนภายนอกองค์กรที่ต้องทำงานร่วมกันกับคนภายในองค์กร โดยบุคลากรโดยทั่วไปขององค์กรไม่อาจมองเห็น และเข้าถึงข้อมูลในส่วนนี้ นอกเสียจากผู้ดูแลระบบเท่านั้น และส่วนที่สามคือส่วนของการทำงานร่วมกันในการบริหารโครงการ ซึ่งในส่วนนี้จะเห็นพื้นที่ ๆ สามารถเข้าถึงโดยคนภายในองค์กร และคนภายนอกองค์กรที่จะต้องทำงานร่วมกัน ซึ่งเป็นพื้นที่ที่ใช้ในการแลกเปลี่ยนข้อมูลในการทำงานร่วมกันใน Nextcloud



ภาพที่ 4 รูปหน้าโฟลเดอร์การจัดเก็บเอกสารของโปรแกรม Nextcloud

ข้อดีของกรณีศึกษา: การใช้งาน Nextcloud เพื่อการจัดเก็บเอกสารในระบบสารสนเทศ

1. ความปลอดภัย: การเข้ารหัสข้อมูล และการกำหนดสิทธิ์การเข้าถึงที่ละเอียดอ่อน
2. ความยืดหยุ่น: สามารถปรับแต่ง และขยายพีเออร์ตามความต้องการ
3. การสนับสนุนชุมชน: มีชุมชนผู้ใช้ และนักพัฒนาที่ช่วยเหลือและพัฒนาระบบอย่างต่อเนื่อง
4. การควบคุมข้อมูล: องค์กรสามารถควบคุม และจัดการข้อมูลได้อย่างเต็มที่
5. การรักษาความปลอดภัย: Nextcloud ให้คุณสมบัติการรักษาความปลอดภัยที่หลากหลาย เช่น การเข้ารหัสจากต้นทางถึงปลายทาง (End-to-End Encryption), การตรวจสอบสิทธิ์แบบสองชั้น (Two Factor Authenticate) หรือแม้แต่การตั้งค่าให้สามารถเข้าใช้งานผ่านการตรวจสอบตัวตน (Active Directory) ขององค์กรเพื่อกำหนดสิทธิ์การเข้าใช้งาน
6. ข้อมูลไม่ถูกจัดเก็บภายนอกองค์กร: เนื่องจากบางองค์กรนั้นต้องการรักษาความลับขององค์กร และต้องการบริหารจัดการข้อมูลที่สำคัญด้วยตัวเอง ซึ่ง Nextcloud ที่ตั้งอยู่ภายในพื้นที่ขององค์กรนั้น ๆ ที่ใช้งาน Nextcloud จะแน่ใจได้ว่าข้อมูลทั้งหมดจะอยู่ภายในพื้นที่จัดเก็บขององค์กรเท่านั้น

ข้อเสียของกรณีศึกษา: การใช้งาน Nextcloud เพื่อการจัดเก็บเอกสารในระบบสารสนเทศ

1. การบริหารจัดการ: ต้องการทรัพยากรในการบริหารจัดการ และการดูแลระบบ
2. การรักษาความปลอดภัย: ต้องมีความรู้ และทักษะในการรักษาความปลอดภัยของระบบเอง
3. การตั้งค่า: การตั้งค่า Nextcloud บนเซิร์ฟเวอร์ส่วนตัวอาจต้องใช้ความรู้ด้านเทคนิค
4. การบำรุงรักษา: ผู้ใช้ต้องรับผิดชอบในการอัปเดตและดูแลรักษาซอฟต์แวร์
5. พื้นที่จัดเก็บ: ผู้ใช้ต้องจัดหาพื้นที่เก็บข้อมูลเอง

ข้อเสนอแนะทางการแก้ปัญหาของกรณีศึกษา: การใช้งาน Nextcloud เพื่อการจัดเก็บเอกสารในระบบสารสนเทศ

Nextcloud เป็นแพลตฟอร์มการจัดเก็บข้อมูลบนคลาวด์ และการทำงานร่วมกันแบบโอเพนซอร์สที่ได้รับความนิยม เนื่องจากช่วยให้องค์กรสามารถควบคุมข้อมูลได้อย่างสมบูรณ์ และลดความเสี่ยงจากการพึ่งพาผู้ให้บริการคลาวด์ภายนอก อย่างไรก็ตาม การนำ Nextcloud มาใช้ภายในองค์กรก็มี ความท้าทาย หลายประการ โดยเฉพาะด้าน การบริหารจัดการ, การรักษาความปลอดภัย และการบำรุงรักษา โดยปัจจัยที่ทำให้ Nextcloud ต้องการทรัพยากร และการบริหารจัดการที่สูง คือการที่องค์กรต้อง ติดตั้ง, กำหนดค่า, บำรุงรักษา และดูแลความปลอดภัยของระบบเอง ซึ่งแตกต่างจากบริการคลาวด์สำเร็จรูป เช่น Google Drive หรือ Dropbox ที่ให้บริการแบบครบวงจรและมีการอัปเดตอัตโนมัติ ดังนั้นจากข้อเสียที่ระบุไว้ข้างต้นองค์กรสามารถใช้แนวทางต่อไปนี้เพื่อบรรเทาหรือแก้ไขปัญหาก็พบในการนำ Nextcloud ไปใช้งาน

1. ใช้บริการ Nextcloud แบบบริหารจัดการ (Managed Nextcloud Hosting) ที่มีผู้ให้บริการดูแลระบบให้ทั้งหมด เช่น IONOS Cloud, A2 Hosting
2. ใช้บริการโฮสติ้งที่ใช้เทคโนโลยีคลาวด์คอมพิวติ้งในการจัดการและให้บริการเซิร์ฟเวอร์ (Cloud Hosting) ที่รองรับ Nextcloud เช่น DigitalOcean, Hetzner

แนวทางการใช้งาน Nextcloud สำหรับองค์กรขนาดเล็กและธุรกิจ SME

Nextcloud ไม่ได้เหมาะสมเพียงแค่องค์กรขนาดใหญ่ที่มีทีมไอทีดูแลเท่านั้น แต่ยังสามารถใช้งานได้สำหรับองค์กรขนาดเล็ก และธุรกิจวิสาหกิจขนาดกลางและขนาดย่อม (SME) ที่ต้องการแพลตฟอร์มคลาวด์

ส่วนตัว (Private Cloud) เพื่อการจัดเก็บข้อมูลอย่างปลอดภัยโดยมีต้นทุนต่ำ และสามารถควบคุมข้อมูลได้เอง องค์กรขนาดเล็กก็มีข้อจำกัดด้านทรัพยากรบุคคลและงบประมาณ ทำให้การเลือกใช้โซลูชันคลาวด์จำเป็นต้องคำนึงถึงต้นทุนและความคุ้มค่าในการลงทุน (สมเกียรติ ลิสาทวิวัฒน์, 2557) นอกจากนี้ การศึกษาของ สุขสุดา ขุนราช (2559) ยังระบุว่าการเลือกใช้เทคโนโลยีการประมวลผลแบบกลุ่มเมฆ (Cloud Computing) ในธุรกิจขนาดเล็กควรพิจารณา ความง่ายในการติดตั้งและการดูแลระบบ รวมถึงการรองรับการขยายตัวของธุรกิจในอนาคต ดังนั้นองค์กรวิสาหกิจขนาดกลางและขนาดย่อม (SME) สามารถใช้บริการ Nextcloud แบบบริหารจัดการ (Managed Nextcloud Services) ข้อดีคือ การที่ไม่ต้องติดตั้งและดูแลเซิร์ฟเวอร์เอง ผู้ให้บริการจะดูแลด้านความปลอดภัย และการอัปเดตระบบให้ลดความซับซ้อน และภาระการดูแลระบบสำหรับธุรกิจที่ไม่มีทีมไอที ตัวอย่างผู้ให้บริการ เช่น IONOS Cloud, A2 Hosting IONOS

สรุป

การจัดเก็บข้อมูลบนคลาวด์ และแพลตฟอร์มการทำงานร่วมกันแบบโอเพนซอร์สเป็นทางเลือกที่น่าสนใจสำหรับองค์กรที่ต้องการความยืดหยุ่น และการลดต้นทุน Nextcloud เป็นตัวอย่างแพลตฟอร์มที่สามารถตอบโจทย์ความต้องการดังกล่าวได้อย่างมีประสิทธิภาพ โดยมีข้อดีในด้านความปลอดภัย ความยืดหยุ่น และการสนับสนุนจากชุมชน แม้ว่าจะมีข้อเสียบางประการ เช่น การบริหารจัดการ และการรักษาความปลอดภัยที่ต้องการทรัพยากรและความรู้เฉพาะทาง แต่สำหรับองค์กรที่ต้องการควบคุมดูแลข้อมูลภายในองค์กรถือว่า Nextcloud เป็นเครื่องมือที่เหมาะสมด้วยคุณสมบัติการกำหนดสิทธิ์การเข้าถึงที่ละเอียดอ่อน การเข้ารหัสจากต้นทางถึงปลายทาง (End-to-End Encryption) และระบบตรวจสอบสิทธิ์แบบสองชั้น (Two Factor Authenticate) ซึ่งสามารถรองรับการทำงานร่วมกันทั้งภายใน และภายนอกองค์กรได้อย่างปลอดภัย นอกจากนี้ วิสาหกิจขนาดกลางและขนาดย่อม (SME) ที่ต้องการแพลตฟอร์มคลาวด์ส่วนตัวสามารถพิจารณา Nextcloud ได้โดยเลือกใช้วิธีการติดตั้งที่เหมาะสมกับทรัพยากรที่มีอยู่ หากองค์กรมีทีมไอทีที่สามารถดูแลเซิร์ฟเวอร์ได้ การติดตั้งแบบโฮสต์ด้วยตนเอง (Self-Hosted) อาจเป็นตัวเลือกที่ช่วยลดต้นทุนระยะยาว และให้ความคุ้มค่าสูงสุด อย่างไรก็ตามหากไม่มีทีมไอทีเฉพาะทาง การเลือกใช้บริการ Nextcloud แบบบริหารจัดการ (Managed Nextcloud Hosting) อาจเป็นทางเลือกที่สะดวกกว่า เนื่องจากช่วยลดภาระด้านการดูแลรักษาระบบและความปลอดภัย

ข้อเสนอแนะ

ในอนาคตเทคโนโลยีการจัดเก็บข้อมูลบนคลาวด์ และแพลตฟอร์มการทำงานร่วมกันแบบโอเพนซอร์สจะยังคงเติบโตและพัฒนาอย่างต่อเนื่อง เพื่อตอบสนองความต้องการขององค์กรทุกขนาดตั้งแต่องค์กรขนาดใหญ่ไปจนถึงวิสาหกิจขนาดกลางและขนาดย่อม (SME) โดยองค์กรสามารถประยุกต์ใช้ Nextcloud ในการจัดการข้อมูลได้หลายรูปแบบ เช่น การจัดเก็บและจัดการข้อมูลบัญชีและการเงินในองค์กรขนาดใหญ่ โดยใช้ฟีเจอร์การกำหนดสิทธิ์การเข้าถึงเฉพาะแผนกที่เกี่ยวข้องกับการเข้ารหัสไฟล์ (File Encryption) การบันทึกและติดตามกิจกรรมต่าง ๆ (Audit Log) เพื่อใช้ตรวจสอบข้อมูลการเปลี่ยนแปลง รวมถึงการใช้งานในธุรกิจวิสาหกิจขนาดกลางและขนาดย่อม (SME) สำหรับการจัดเก็บข้อมูลลูกค้า (CRM) เพื่อลดความเสี่ยงในการที่ข้อมูลลูกค้าจะหลุดไปอยู่ในมือคู่แข่ง และยังสามารถเก็บรักษาข้อมูลบนเซิร์ฟเวอร์ขององค์กรเอง เพื่อเพิ่มความน่าเชื่อถือมากยิ่งขึ้น ทั้งนี้ การสนับสนุนจากชุมชนนักพัฒนา และผู้ใช้งานเป็นปัจจัยสำคัญที่ช่วยให้แพลตฟอร์มอย่าง Nextcloud มีการพัฒนาอย่างต่อเนื่อง ซึ่งองค์กรที่เลือกใช้ Nextcloud ควรให้ความสำคัญกับการอัปเดตระบบอยู่เสมอ เพื่อให้มั่นใจว่าแพลตฟอร์มที่ใช้งานอยู่มีความปลอดภัยและมีประสิทธิภาพสูงสุด โดยสำหรับธุรกิจที่ต้องการใช้งาน

แพลตฟอร์มคลาวด์ส่วนตัว (Private Cloud) ควรคำนึงถึงปัจจัยด้านต้นทุน และทรัพยากรที่จำเป็น หากองค์กรมีทีมไอทีที่สามารถดูแลเซิร์ฟเวอร์ได้ การติดตั้งแบบโฮสต์ด้วยตนเอง (Self-Hosted) อาจเป็นทางเลือกที่ดีเพื่อควบคุมต้นทุนระยะยาว และปรับแต่งระบบได้ตามต้องการ แต่หากองค์กรไม่มีทีมไอทีเฉพาะทาง การเลือกใช้บริการ Managed Nextcloud Hosting อาจช่วยให้การใช้งานเป็นไปได้อย่างสะดวก และลดความซับซ้อนในการบริหารจัดการ ดังนั้น องค์กรควรพิจารณาเลือกใช้ Nextcloud ตามขนาดและทรัพยากรของตนเอง เพื่อให้สามารถใช้แพลตฟอร์มนี้ได้อย่างมีประสิทธิภาพสูงสุด และคุ้มค่าต่อการลงทุน

เอกสารอ้างอิง

- จรรยา สาวิถี. (2567). การเปรียบเทียบประสิทธิภาพการทำงานของ การจัดเก็บข้อมูลบนคลาวด์สตอเรจแบบโอเพ่นซอร์สบนเซิร์ฟเวอร์แบบเวอร์ช่วลไลเซชันสำหรับองค์กรธุรกิจ. *วารสารวิชาการ การจัดการเทคโนโลยี มหาวิทยาลัยราชภัฏมหาสารคาม*, 11(1), 7-17.
- แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 (พ.ศ.2566–2570). (2565, 1 พฤศจิกายน).
- ราชกิจจานุเบกษา. เล่ม 139 ตอนพิเศษ 258 ง. หน้า 1.
- มนพ การกล้า, ชุติศักดิ์ เอกเพชร และนัฏฐิณี เจริญสุข. (2565). การพัฒนาระบบจัดเก็บข้อมูลสารสนเทศออนไลน์ เพื่อการบริหารงานของโรงเรียนในเครือข่ายศรีลันตา สังกัดสำนักงานเขตพื้นที่การศึกษาประถมศึกษาจังหวัดกระบี่. *วารสารรัชต์ภาคย์*, 16(46), 197-216.
- สมเกียรติ ลีลาทวิวิฒ. (2557). ปัจจัยขับเคลื่อนการใช้ระบบคลาวด์สำหรับธุรกิจไทยให้ประสบผลสำเร็จ. *วารสารสิทธิปริทรรศน์*, 28(88), 118-144.
- สุขสุดา ขุนราช. (2559). *การศึกษาแนวทางการประยุกต์ใช้เทคโนโลยีคลาวด์ คอมพิวติงในวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) [การค้นคว้าอิสระปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์]*. TU Digital Collections. https://digital.library.tu.ac.th/tu_dc/frontend/Info/item/dc:93625
- Buja, G. A., Wahid, S. D. M., Rahman, T. F. A., Deraman, N. A., Jono, M. N. H. H., & Aziz, A. A. (2021). *Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly. International Journal of Advanced Technology and Engineering Exploration*, 8(76). 511-519. <http://dx.doi.org/10.19101/IJATEE.2020.762185>
- Khosravi, A. (2022, March 3). *Get started with Carbonio, an open source collaboration platform*. Opensource. <https://opensource.com/article/22/3/open-source-collaboration-carbonio>
- Kochovski, A. (2024, November 11). *The risks and benefits of Cloud Storage in 2024*. Cloudwards. <https://www.cloudwards.net/the-risks-and-benefits-of-cloud-storage/>
- Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, 21(15), Article 5119. <https://doi.org/10.3390/s21155119>
- Walkowski, D. (2019, July 08). *What is the CIA Triad?*. F5Labs. <https://www.f5.com/labs/learning-center/what-is-the-cia-triad>