https://so19.tci-thaijo.org/index.php/CUASTJournal

การใช้แอ็กทีฟ ไดเรกทอรีในการยืนยันตัวตนและกำหนดสิทธิ์ผู้ใช้งานสำหรับระบบสารสนเทศโรงพยาบาล

วิภาวี รื่นจิตต์*

คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล กรุงเทพมหานคร 10700

*อีเมลของผู้ประพันธ์บรรณกิจ: Wipawee.rue@mahidol.ac.th

บทคัดย่อ

ในยุคแห่งความก้าวหน้าทางเทคโนโลยีสารสนเทศ ปฏิเสธไม่ได้เลยว่าการบริหารงานต่าง ๆ ขององค์กรในปัจจุบันล้วนขับเคลื่อนด้วยเทคโนโลยีสารสนเทศ การบริหารงานโรงพยาบาลก็เช่นเดียวกัน ซึ่งระบบสารสนเทศโรงพยาบาลนั้นเป็นระบบที่มีขนาดใหญ่ ประกอบด้วยระบบสารสนเทศย่อย ๆ หลายระบบ ทำงานสอดประสานสนับสนุน เชื่อมต่อข้อมูลเข้าด้วยกัน ตลอดจนมีผู้ใช้งานที่เกี่ยวข้องเป็นจำนวนมาก ทั้งภายในหน่วยงานและต่างหน่วยงาน ดังนั้นการเข้าใช้งานระบบสารสนเทศในโรงพยาบาลต้องมีการตรวจสอบยืนยันตัวตนและจัดการสิทธิ์การเข้าถึงข้อมูลที่มีความสำคัญเพื่อรักษาความปลอดภัยและความเป็นส่วนตัวของผู้ใช้งาน

ระบบ Active Directory เป็นเครื่องมือที่มีประสิทธิภาพในการจัดการและควบคุมการเข้าถึงข้อมูลในระบบสารสนเทศโรงพยาบาล โดยมีบทบาทสำคัญในการจัดการการยืนยันตัวตนและการกำหนดสิทธิ์ผู้ใช้งาน เช่น การกำหนดสิทธิ์ในการเข้าถึงเอกสารทางการแพทย์ การตรวจสอบสิทธิ์ในการเข้าถึงแฟ้มข้อมูลของผู้ป่วย และการจัดการสิทธิ์การเข้าถึงระบบโดยรวม ด้วยความสามารถในการจัดการและควบคุมอย่างมีประสิทธิภาพ Active Directory จึงเป็นเครื่องมือที่สำคัญในการป้องกันการเข้าถึงข้อมูลที่ไม่เหมาะสมและช่วยให้ระบบสารสนเทศโรงพยาบาลมีความปลอดภัยและเชื่อถือได้ในการใช้งาน

คำสำคัญ: แอ็กทีฟ ไดเรกทอรี เอดี การยืนยันตัวตน การกำหนดสิทธิ์ ระบบสารสนเทศโรงพยาบาล

Received 10 กุมภาพันธ์ 2567, Revised: 22 เมษายน 2567, Accepted: 07 พฤษภาคม 2567

Utilizing Active Directory for Authentication and Authorization in Hospital Information System

Wipawee Ruenchit

Faculty of Medicine Siriraj Hospital, Mahidol University, Bangkok 10700, Thailand

*Corresponding author's e-mail: Wipawee.rue@mahidol.ac.th

Abstract

In the era of information technology advancement, it cannot be denied that today's organizations are driven by information technology. The hospital information system is a large system consisting of several subsystems that collaborate, support, and connect data, with a large number of users involved. Therefore, access to hospital information systems requires authentication and authorization for accessing data to maintain the safety and privacy of users.

Active Directory is an effective tool for managing and controlling access within hospital information systems, playing a crucial role in authentication and authorization processes, such as determining access to medical documents. With its effective management and control capabilities, Active Directory is an essential tool for preventing inappropriate access to information and ensuring hospital information systems are safe and reliable for use.

Keywords: Active Directory, AD, Authentication, Authorization, Hospital Information System

บทนำ

สมาคมเวชสารสนเทศไทย (2564) กล่าวว่า ในปัจจุบัน มีการนำเทคโนโลยีดิจิทัลมาใช้ในการปรับปรุงบริการในโรงพยาบาลมากขึ้น ประกอบกับสถานการณ์ทั่วไปในโลกแสดงให้เห็นว่า เทคโนโลยีดิจิทัลทำให้เกิดการล่มสลาย (Disruption) ขององค์การต่าง ๆ ที่ไม่สามารถปรับตัวให้รองรับได้อย่างมากมาย นอกจากนั้น ยังเกิดภัยคุกคามใหม่ ๆ ทางด้านไซเบอร์ (Cybersecurity) ที่เป็นปัจจัยเร่งให้เกิดกระบวนการปรับเปลี่ยนไปสู่ดิจิทัล (Digital Transformation) ดังนั้นเพื่อให้โรงพยาบาลก้าวทันยุคสมัยแห่งการเปลี่ยนแปลงนี้ การบริการของโรงพยาบาลจำเป็นต้องได้รับการสนับสนุนด้านข้อมูลและการบริหารจัดการข้อมูลที่สามารถปรับเปลี่ยนและแสดงผลได้หลากหลายรูปแบบ เพื่ออำนวยความสะดวกในการรายงานผล ความรวดเร็ว ความถูกต้อง การบูรณาการ การปรับปรุงบริการประสิทธิภาพ สำหรับให้บริการด้านการดูแลสุขภาพ (Sinaga *et al.*, 2024) จึงจำเป็นต้องมีการปรับปรุงระบบการทำงานขององค์กร โดยการจัดให้มีระบบสารสนเทศต่าง ๆ ที่เหมาะสม ช่วยอำนวยความสะดวก ลดข้อผิดพลาด สนับสนุนการทำงาน เกิดเป็นภาพการขับเคลื่อนองค์กรด้วยระบบสารสนเทศโรงพยาบาล

ระบบสารสนเทศโรงพยาบาล หรือ HIS (Hospital Information System) เป็นการใช้เทคโนโลยีสารสนเทศ (IT) เข้ามาเป็นเครื่องมือในการจัดการฐานข้อมูลขนาดใหญ่ (Big Data) เพื่อให้แพทย์ พยาบาล หรือบุคลากรที่เกี่ยวข้อง สามารถเข้าถึงข้อมูลสุขภาพของผู้ป่วยได้ทั้งจากฐานข้อมูลของโรงพยาบาลหรือจากสถานสุขภาพอื่น ๆ เพื่อวางแผนการรักษา ประเมินรูปแบบการดูแลผู้ป่วยได้อย่างรวดเร็ว รวมถึงการดำเนินงานของแต่ละแผนกภายในโรงพยาบาล ให้เกิดการทำงานที่มีประสิทธิภาพและประสานงานกันได้อย่างเป็นระบบ (HOCCO, 2023) เช่น ระบบการรักษาพยาบาล ระบบตรวจทางห้องปฏิบัติการ ระบบเอกซ์เรย์ ระบบโภชนาการ ระบบบำรุงรักษา ระบบเภสัชกรรม ระบบสังคมสงเคราะห์ ระบบงานคลัง ระบบบุคลากร เป็นต้น ภายใต้ระบบหลัก ๆ เหล่านี้ก็มีระบบย่อยต่าง ๆ อีกมากที่เกี่ยวข้อง

เมื่อพิจารณาลึกลงไปจะเห็นว่า ระบบการทำงานบางอย่างมีความเฉพาะเจาะจง สำหรับเจ้าหน้าที่บางกลุ่ม ดังนั้นการเข้าใช้งานระบบต่าง ๆ ข้างต้น ผู้ใช้งานทุกคนไม่จำเป็น/ไม่ควรได้รับสิทธิ์ให้เข้าใช้งานได้ทุกระบบของโรงพยาบาล และการเข้าถึงข้อมูลของแต่ละคนในแต่ละระบบก็อาจจะไม่เหมือนกันอีกด้วย เพราะแต่ละคนมีบทบาทตำแหน่งหน้าที่ ภาระงานที่แตกต่างกัน และก่อนที่ผู้ใช้งานจะใช้งานระบบใด ๆ ก็ตามได้นั้น จะต้องตรวจสอบและยืนยันให้ได้ว่าเป็นบุคลากรขององค์กรนั้นจริง เมื่อองค์กรมีขนาดเล็ก ระบบไม่เยอะ การบริหารงานเหล่านี้พอที่จะสามารถให้ผู้ดูแลระบบแต่ละระบบดูแลและบริหารจัดการได้ด้วยตนเอง แต่เมื่อองค์กรมีขนาดใหญ่ขึ้น ความซับซ้อนของการบริหารจัดการทรัพยากรก็มีแนวโน้มที่จะเพิ่มขึ้นตามไปด้วย องค์กรจึงจำเป็นต้องเร่งยกระดับมาตรฐานการดูแลระบบของตน นำมาซึ่งความสำคัญของการนำระบบ Active Directory มาช่วยให้ผู้ดูแลระบบสามารถบริหารจัดการบัญชีผู้ใช้งาน กำหนดสิทธิ์การเข้าถึงข้อมูลและตรวจสอบกิจกรรมต่าง ๆ ในระบบได้อย่างมีประสิทธิภาพและมีความปลอดภัยมากยิ่งขึ้น

การยืนยันตัวตนและการกำหนดสิทธิ์ผู้ใช้งานคืออะไร แตกต่างกันอย่างไร ทำไมจึงสำคัญ

การยืนยันตัวตน (Authentication) หรือเรียกสั้น ๆ ว่า “AuthN” คือ การยืนยันตัวตนเมื่อเราเข้าใช้งานเว็บไซต์ แอปพลิเคชันหรือระบบใดก็ตามบนโลกออนไลน์หรือกล่าวโดยง่ายคือการล็อกอิน (Log-in) นั่นเอง เช่น การ

เข้าสู่ระบบอีเมล (E-mail), การเข้าสู่ระบบอินเทอร์เน็ต (Internet) และการเข้าสู่ระบบโซเชียลมีเดีย (Social media) ต่าง ๆ เพื่อเป็นการยืนยันตัวตนว่าเราคือคน ๆ นี้ และกำลังใช้บริการต่าง ๆ ในฐานะคนนี้ (Phothiin, 2021) ซึ่งสอดคล้องกับที่ Magnusson (2023) กล่าวว่า การยืนยันตัวตนเป็นกระบวนการที่ใช้สำหรับตรวจสอบผู้ใช้งานหรืออุปกรณ์ก่อนที่จะอนุญาตให้เข้าถึงระบบหรือทรัพยากร

การกำหนดสิทธิ์ (Authorization) หรือเรียกสั้น ๆ ว่า "AuthZ" คือ การรักษาความปลอดภัยที่ระบุและกำหนดค่าระดับการเข้าถึงหรือสิทธิ์ของผู้ใช้ผ่านตัวตนที่ทำการล็อกอิน (Log-in) เข้ามาในระบบ มีสิทธิ์หรือบทบาทหน้าที่ตามที่ได้รับอนุญาตหรือตามที่กำหนดไว้หรือไม่ ซึ่งบุคคลที่มีหน้าที่แตกต่างกัน ย่อมมีสิทธิ์หรือบทบาทในการเข้าถึงระบบหรือข้อมูลที่แตกต่างกันไป ยกตัวอย่าง การกำหนดสิทธิ์ในระบบองค์กร เป็นการระบุว่าพนักงานคนไหนสามารถเข้าถึงหรือใช้ข้อมูลของบริษัทและสามารถกำหนดเพิ่มเติมได้อีกว่า ข้อมูลใดที่พนักงานคนนั้นสามารถดูหรือใช้งานได้ นอกจากนี้ผู้ใช้งานสามารถอยู่ในกลุ่มการอนุญาตได้มากกว่าหนึ่งกลุ่ม โดยที่ผู้ดูแลระบบสามารถเปลี่ยนแปลงการอนุญาตผู้ใช้งานนี้ได้ตลอดเวลา (Kron, 2022)

ความแตกต่างระหว่างการยืนยันตัวตนและการกำหนดสิทธิ์ แม้ว่าการยืนยันตัวตนและการกำหนดสิทธิ์จะถือเป็นหลักการพื้นฐานของการรักษาความปลอดภัยและสร้างความน่าเชื่อถือให้แก่ระบบที่มักจะถูกนำมาใช้ควบคู่กันเพื่อบรรลุเป้าหมายในการปกป้องข้อมูลที่เป็นความลับไม่ให้ตกไปอยู่ในมือของผู้ไม่ประสงค์ดี และเรามักจะได้ยินสองคำนี้ปรากฏร่วมกันเสมอ แต่ทั้งสองมีหลักการและจุดประสงค์ ตลอดจนกระบวนการทำงานที่แตกต่างกัน ดังตารางต่อไปนี้

ตารางที่ 1. ความแตกต่างการยืนยันตัวตน (Authentication) และการกำหนดสิทธิ์ (Authorization)

	การยืนยันตัวตน (Authentication)	**การกำหนดสิทธิ์ (Authorization)**
1. จุดประสงค์	มุ่งค้นหาและตรวจสอบ เพื่อระบุตัวตนว่าคุณคือใครในระบบ ?	มุ่งเน้นตรวจสอบว่าคุณสามารถทำอะไรได้บ้างในระบบ ?
2. กระบวนการทำงาน	กระบวนการยืนยันตัวตน เป็นการใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) รหัสพินแบบใช้ครั้งเดียว (One-time pins) ข้อมูลไบโอเมตทริกซ์[1] หรือข้อมูลอื่น ๆ ที่ผู้ใช้ป้อนเข้าสู่ระบบ (SailPoint, 2023)	กระบวนการกำหนดสิทธิ์ เป็นการกำหนดโดยนโยบายขององค์กรว่าผู้ใช้งานควรจะได้รับสิทธิ์นั้น ๆ หรือไม่ตามกฎและนโยบาย ซึ่งเป็นการกำหนดค่าและควบคุมโดยผู้ดูแลระบบ
3. ลำดับการทำงาน	กระบวนการยืนยันตัวตนเป็นขั้นตอนแรกของการตรวจสอบสิทธิ์ ดังนั้นกระบวนการนี้จะเป็นกระบวนการที่เกิดขึ้นก่อนเสมอ	กระบวนการตรวจสอบสิทธิ์จะเกิดหลังจากกระบวนการยืนยันตัวตนดำเนินการเสร็จเรียบร้อยแล้ว

[1] ไบโอเมตทริกซ์ คือ ลักษณะของมนุษย์ที่สร้างเอกลักษณ์ของแต่ละบุคคล เช่น ลักษณะบนใบหน้า ดวงตา ลายนิ้วมือ เป็นต้น

	การยืนยันตัวตน (Authentication)	**การกำหนดสิทธิ์ (Authorization)**
4. การมองเห็นและการเปลี่ยนแปลง	ผู้ใช้งานสามารถเห็นข้อมูลที่ตนเองกรอกและสามารถทำการเปลี่ยนแปลงได้ด้วยตนเอง เช่น การเปลี่ยนรหัสผ่าน เป็นต้น	ผู้ใช้งานไม่สามารถมองเห็นและไม่สามารถแก้ไขได้ด้วยตนเอง องค์กรหรือหน่วยงานเป็นผู้ควบคุมและกำหนดสิทธิ์ให้
5. สถานการณ์ตัวอย่าง	แพทย์ของโรงพยาบาลศิริราชกรอกชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเข้าระบบเวชระเบียนผู้ป่วย โดยก่อนที่จะเข้าสู่ระบบนั้นระบบจะทำการยืนยันตัวตน ก่อนอนุญาตหรือไม่อนุญาตให้เข้าสู่ระบบ	การกำหนดสิทธิ์จะระบุไว้อย่างชัดเจนว่าข้อมูลใดที่แพทย์ ได้รับอนุญาตให้เข้าถึงได้บนระบบเวชระเบียนผู้ป่วย เช่น การเข้าถึงประวัติผู้ป่วย ประวัติใบสั่งยา เป็นต้น

กล่าวโดยสรุป **การยืนยันตัวตนและการกำหนดสิทธิ์ผู้ใช้งานของระบบสารสนเทศโรงพยาบาล** จึงเป็นกระบวนการสำหรับพิสูจน์และยืนยันตัวตน ตลอดจนตรวจสอบสิทธิของผู้ใช้งาน เพื่อเข้าถึงข้อมูลหรือระบบต่าง ๆ ของโรงพยาบาล โดยควบคุมการเข้าถึงข้อมูลตามสิทธิและบทบาท ภาระงาน เท่าที่จำเป็น ซึ่งถือเป็นการคุ้มครองข้อมูลส่วนบุคคล สร้างความน่าเชื่อถือ และรักษาความปลอดภัยให้กับระบบสารสนเทศ

Active Directory เครื่องมือสำหรับการยืนยันตัวตนและการกำหนดสิทธิ์ผู้ใช้งาน

ปัจจุบันความปลอดภัยของข้อมูลเป็นเรื่องสำคัญอย่างมากสำหรับองค์กร การยืนยันตัวตนและการกำหนดสิทธิ์ผู้เข้าใช้งานระบบสารสนเทศเป็นกลยุทธ์และกระบวนการขั้นพื้นฐานที่หน่วยงานหรือองค์กรจะต้องจัดให้มี ทั้งนี้เครื่องมือยอดนิยมที่มีประสิทธิภาพสำหรับบริหารจัดการงานในด้านนี้ คือ ระบบ Active Directory หรือ “AD”

ระบบ Active Directory เป็นโครงสร้างระบบจัดการผู้ใช้งานและความปลอดภัยของ Windows Server ที่พัฒนาโดย บริษัท Microsoft ซึ่งมีไว้เพื่อใช้ในการจัดการและควบคุมการเข้าถึงและการใช้งานทรัพยากรบนเครือข่าย (Chai and Gillis, 2021) โดย AD จะเป็นศูนย์กลางของการทำหน้าที่จัดเก็บข้อมูลต่าง ๆ เช่น บัญชีผู้ใช้งาน กลุ่มผู้ใช้งาน (Group) เครื่องคอมพิวเตอร์ (Computer) เป็นต้น

สุจิตรา (2560) กล่าวว่า Active Directory (AD) เป็นระบบที่ได้รับการออกแบบตามมาตรฐานของ Internet Technology รองรับการค้นหาทรัพยากรต่าง ๆ บนเครือข่ายขนาดใหญ่ ช่วยให้ผู้ดูแลระบบสามารถบริหารจัดการเครือข่ายที่ซับซ้อนจากศูนย์กลางได้อย่างสะดวก โดย AD เป็นการทำงานร่วมกันระหว่าง DNS (Domain Naming System)[2] และ LDAP (Lightweight Directory Access Protocol)[3] ทำให้สามารถติดต่อเชื่อมโยง (interoperability) กับไดเรกทอรีเซอร์วิสอื่น ๆ ได้อย่างมีประสิทธิภาพ โดยมีโครงสร้าง 2 ลักษณะ คือ ทางกายภาพ

[2] DNS (Domain Naming System หรือ Domain Name Server) คือ ระบบที่มีไว้สำหรับบริหารจัดการข้อมูลของชื่อโดเมนเนม (Domain Name) และทำหน้าที่ในการแปลงชื่อโดเมนเนมดังกล่าวเป็นหมายเลขไอพีแอดเดรส (IP Address)

[3] LDAP คือ โปรโตคอลที่ใช้ในการค้นหาและเข้าถึงข้อมูลต่าง ๆ ได้อย่างรวดเร็วด้วยโครงสร้างแบบ Directory

(Physical Structure) และทางลอจิคัล (Logical Structure) การทำงานของ AD สามารถแบ่งการทำงานออกเป็น 2 ส่วนด้วยกันเพื่อแยกประเภทการใช้งานดังนี้

ส่วนประกอบของ Active Directory

1. ส่วน Services เรียกว่า Active Directory Service เป็นส่วนประกอบที่ทำหน้าที่ให้บริการในส่วนของผู้บริหารระบบ เช่น การสร้างหรือลบรายชื่อผู้ใช้งาน การเปลี่ยนรหัสผ่าน การกำหนดนโยบายของกลุ่ม (Group Policy) และการให้บริการที่สนับสนุนผ่านบริการระบบเครือข่าย โดยสามารถสนับสนุนทั้ง Domain Naming System (DNS) และ Lightweight Directory Access Protocol (LDAP)

2. ส่วน Database เรียกว่า Active Directory Database เป็นฐานข้อมูลสำหรับใช้ในการเก็บไดเรกทอรีบนระบบเครือข่าย เช่น บัญชีรายชื่อและคุณลักษณะของผู้ใช้ กลุ่มผู้ใช้ รายชื่อ และคุณสมบัติของทรัพยากรต่าง ๆ ในการจัดเก็บรายชื่อและคุณสมบัติของทรัพยากรบนระบบเครือข่ายไว้ในฐานข้อมูล Active Directory (AD) จะช่วยให้ผู้ใช้งานสามารถค้นหาและเรียกใช้ทรัพยากรนั้นได้ง่ายและรวดเร็วขึ้น

หน้าที่หลักของ Active Directory

Simister (2024) กล่าวว่า Active Directory เป็นเครื่องมืออันทรงพลังที่มีคุณประโยชน์อย่างมากต่อองค์กร ช่วยให้การทำงานง่ายขึ้นทั้งในส่วนของ ผู้ดูแลระบบ ผู้ใช้งานระบบ รวมถึงการปรับปรุงด้านความปลอดภัยด้วยการควบคุมการเข้าถึงทรัพยากรบนเครือข่าย ทั้งนี้หน้าที่หลักของ Active Directory ที่สำคัญ 3 ประการ คือ

1.การยืนยันตัวตน : Active Directory ใช้เพื่อตรวจสอบสิทธิ์ผู้ใช้ คอมพิวเตอร์ และทรัพยากรอื่น ๆ บนเครือข่าย ซึ่งหมายความว่า AD จะตรวจสอบตัวตนของผู้ใช้หรืออุปกรณ์ก่อนที่จะอนุญาตให้เข้าถึงทรัพยากรเครือข่าย

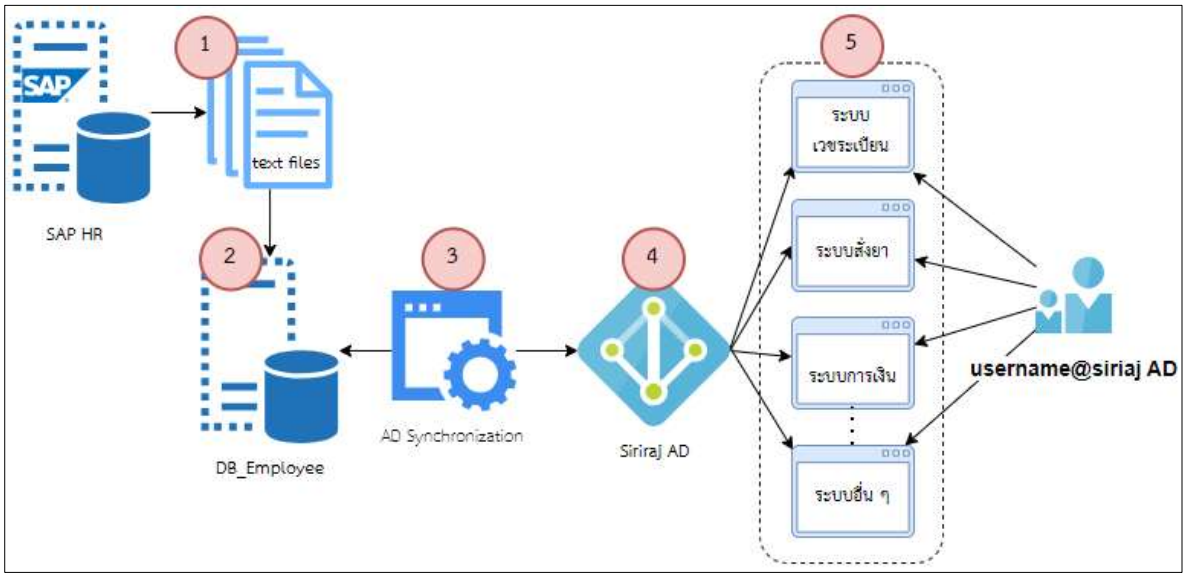
2.การกำหนดสิทธิ์ : เมื่อผู้ใช้หรืออุปกรณ์ได้รับการรับรองความถูกต้องแล้ว AD จะถูกใช้เพื่ออนุญาตการเข้าถึงทรัพยากรเฉพาะบนเครือข่าย ทำได้โดยการกำหนดสิทธิ์ให้กับผู้ใช้งานและกลุ่มของผู้ใช้งาน ซึ่งกำหนดสิ่งที่พวกเขาได้รับอนุญาตให้ทำบนเครือข่าย

3.บริการไดเรกทอรี : Active Directory ยังเป็นบริการไดเรกทอรี ซึ่งหมายความว่าจะจัดเก็บและจัดการข้อมูลเกี่ยวกับทรัพยากรเครือข่าย เช่น ผู้ใช้ คอมพิวเตอร์ และแอปพลิเคชัน ข้อมูลนี้สามารถใช้เพื่อจัดการและค้นหาทรัพยากรบนเครือข่าย

ด้วยความสามารถที่กล่าวมานี้ทำให้ Active Directory เป็นเครื่องมือที่สำคัญและมีประสิทธิภาพสำหรับองค์กรที่นิยมเลือกมาใช้งาน เพื่อบริหารจัดการควบคุมทรัพยากรและผู้ใช้บนเครือข่ายองค์กรในลักษณะที่ปลอดภัยและมีประสิทธิภาพสูงสุด

แนวทางการนำ Active Directory มาใช้งานกับระบบสารสนเทศโรงพยาบาล

เนื่องด้วยคณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ตระหนักถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล ที่มิใช่ว่าใครก็ได้จะสามารถเข้าถึงข้อมูลระบบสารสนเทศโรงพยาบาล กอปรกับการที่โรงพยาบาลศิริราช มีระบบสารสนเทศไม่น้อยกว่า 200 ระบบสำหรับบริหารงานจัดการด้านต่าง ๆ และมีแนวโน้มที่จะเพิ่มมากขึ้น ดังนั้นองค์กรจึงได้เกิดแนวคิดนำระบบ Active Directory หรือ “AD” มาใช้เป็นศูนย์กลางในการยืนยันตัวตนเพื่อควบคุมสิทธิ์การเข้าใช้งานระบบสารสนเทศของโรงพยาบาลศิริราช โดยมีโครงสร้างพื้นฐานการทำงานหลัก ๆ ซึ่งในที่นี้ผู้เขียนจะขอกล่าวถึงเฉพาะภาพกรอบแนวทางการทำงานโดยรวมเท่านั้น จะไม่ลงรายละเอียดทางเทคนิคมากจนเกินไป ดังภาพต่อไปนี้



ภาพที่ 1. โครงสร้างพื้นฐานของการนำ AD มาบูรณาการใช้งานร่วมกับระบบสารสนเทศของโรงพยาบาลศิริราช

1. ส่วนของ SAP HR[4] และการส่งออก text files เนื่องจากโรงพยาบาลศิริราชใช้ระบบ SAP HR ในการบริหารจัดการทรัพยากรบุคคล ที่ครอบคลุมทั้งการจ้างงาน เงินเดือนพนักงาน มีการเก็บรวมรวมข้อมูลประวัติการบรรจุและการพ้นสภาพพนักงาน โครงสร้างการบริหารงานตามผังองค์กร จึงก่อให้เกิดแนวคิดการนำข้อมูลจากระบบ SAP HR มาเป็นข้อมูลตั้งต้นสำหรับการสร้างบัญชีผู้ใช้งาน (Account) บนระบบ AD โดยอัตโนมัติ โดยกำหนดให้ระบบ SAP HR ส่งออกข้อมูลที่จำเป็นสำหรับการสร้างบัญชีผู้ใช้งานในรูปของ text files ได้แก่ 1. ข้อมูลผังโครงสร้างการบริหารงานขององค์กร 2. ข้อมูลส่วนบุคคลของพนักงาน เช่น ชื่อ-นามสกุล หน่วยงานที่สังกัด หน้าที่ตามตำแหน่งงาน เป็นต้น 3. ภาระงานที่ได้รับมอบหมายภายใต้หน่วยงาน เช่น หัวหน้างาน เจ้าหน้าที่ รองคณบดี เป็นต้น ซึ่งส่วนนี้เป็นส่วนสำคัญลำดับแรกที่ต้องมีการหารือร่วมกันเพื่อออกแบบโครงสร้างข้อมูลของบุคลากรที่เหมาะสมและสอดคล้องกับโครงสร้างขององค์กร

[4] SAP HR เป็นชื่อโมดูลหนึ่งในระบบ SAP ERP (Enterprise Resource Planning) ใช้สำหรับบริหารจัดการทรัพยากรบุคคลขององค์กร

2. ส่วนของ DB_Employee[5] คือ ส่วนที่รองรับการแปลงค่าจาก text files ที่ส่งออกจากระบบ SAP HR ให้อยู่ในรูปฐานข้อมูล (Database) ที่แสดงความสัมพันธ์เชื่อมโยงข้อมูลกันระหว่างแต่ละ text files เพื่อความสะดวกในการนำไปใช้งานหรือพัฒนาต่อยอด

3. ส่วนของ AD Synchronization ทำหน้าที่ตรวจสอบการเปลี่ยนแปลงข้อมูลของบุคลากร (User Object) ที่แตกต่างระหว่าง Siriraj AD กับข้อมูลบุคลากรในฐานข้อมูล DB_Employee เมื่อพบข้อมูลที่มีความแตกต่างกันจะทำการเปลี่ยนแปลง (Update) หรือสร้าง (Create) ข้อมูลนั้น ๆ ให้เป็นปัจจุบัน เช่น บุคลากรมีการเปลี่ยนแปลงตำแหน่งงาน เปลี่ยนแปลงหน่วยงานที่สังกัด เปลี่ยนแปลงข้อมูลส่วนบุคคลต่าง ๆ หรือสร้างข้อมูลของบุคลากรที่ได้รับการบรรจุใหม่ เป็นต้น

4. ส่วนของ Siriraj AD[6] เป็นส่วนของ AD ที่ได้ทำการติดตั้งและกำหนดค่าไว้เรียบร้อยแล้ว ซึ่งมีข้อมูลบุคลากร (User Object) ที่สังกัดภายใต้หน่วยงานต่าง ๆ ของศิริราช รวมถึงสิทธิ์ของบุคลากรในการเข้าถึงระบบหรือทรัพยากรต่าง ๆ ที่นโยบายขององค์กรกำหนดไว้ให้

5. ส่วนของ ระบบสารสนเทศโรงพยาบาลต่าง ๆ ที่ทำการเชื่อมโยงกับระบบ Siriraj AD ส่วนนี้นับเป็นส่วนสำคัญอีกส่วนหนึ่งที่ผู้พัฒนาและออกแบบระบบจะต้องศึกษาและทำความเข้าใจวิธีการในการเชื่อมโยงกับระบบ AD ตลอดจนถึงเข้าใจโครงสร้างพื้นฐานของข้อมูลบุคลากรที่ถูกจัดไว้บนระบบ AD โดยเนื้องานหลัก ๆ ที่เกี่ยวข้องมีดังนี้

- **ด้านนโยบายขององค์กร** หลังจากที่ได้จัดวางโครงสร้างระบบ AD ขององค์กรเรียบร้อย ควรกำหนดนโยบายและประกาศใช้อย่างชัดเจนว่าระบบใดที่พัฒนาขึ้นมาใหม่ต้องเชื่อมโยงกับระบบ AD ทุกระบบ ระบุความสำคัญทั้งทางด้านธุรกิจและด้านความปลอดภัย

- **ด้านการวิเคราะห์และออกแบบระบบ** สำหรับระบบที่จะดำเนินการพัฒนาผู้ทำหน้าที่วิเคราะห์และออกแบบระบบ ต้องทำความเข้าใจโครงสร้างทางธุรกิจขององค์กร เช่น ผู้ใช้งานทั้งหมดของระบบอยู่หน่วยงานใด มีตำแหน่งอะไรบ้าง และสามารถที่จะเข้าใช้งานส่วนใดของระบบ เป็นต้น เพื่อเป็นการออกแบบการจัดกลุ่มผู้ใช้งานและการกำหนดสิทธิ์ให้สอดคล้องกับข้อมูลของระบบ AD

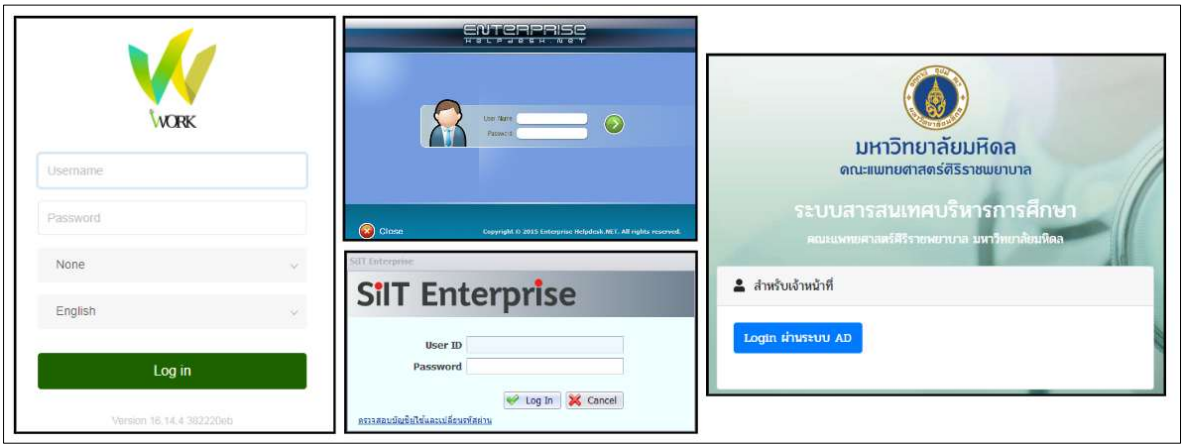
[5] DB_Employee ชื่อสมมุติของฐานข้อมูลที่ใช้สำหรับเก็บข้อมูลของบุคลากรของโรงพยาบาลศิริราช

[6] Siriraj AD ชื่อสมมุติของระบบ Active Directory ที่โรงพยาบาลศิริราชจัดตั้งขึ้น

ตารางที่ 2. การออกแบบการจัดกลุ่มผู้ใช้งานและการกำหนดสิทธิ์ของ AD ให้สอดคล้องกับโครงสร้างทางธุรกิจขององค์กร

1.แบบฟอร์มการกำหนดเงื่อนไข Role Group ตามผังองค์กร				
หน้าที่รับผิดชอบของระบบ (Role ของ Application)	**กลุ่ม user ที่ต้องการ (คำอธิบายอย่างย่อ)**	**รายการที่ต้องกรอก**	**ค่าที่กรอก**	**หมายเหตุ**
		สังกัดหน่วยงาน ระดับ 1	**คณะแพทยศาสตร์ศิริราชพยาบาล**	
		สังกัดหน่วยงาน ระดับ 2		
		สังกัดหน่วยงาน ระดับ 3		
		สังกัดหน่วยงาน ระดับ 4		
		สังกัดหน่วยงาน ระดับ 5		
		ภาระงาน(Duty)		
		ลักษณะงาน (Job)		
		ตำแหน่งงาน (Position)		
2.แบบฟอร์มการกำหนดเงื่อนไข Role Group แบบ Manual (เลือกรายบุคคล)				
หน้าที่รับผิดชอบของระบบ (Role ของ Application)	**กลุ่ม user ที่ต้องการ**	**รายการที่ต้องกรอก**	**ค่าที่กรอก**	**หมายเหตุ**
	ไม่ต้องระบุ	**บุคลากร (Employee)**	**ระบุชื่อ - นามสกุล**	

- **ด้านการพัฒนาระบบเพื่อเชื่อมต่อ AD** ผู้พัฒนาระบบเมื่อตัดสินใจเลือกภาษาโปรแกรมใดในการพัฒนาระบบต้องศึกษาวิธีการเชื่อมต่อ AD ของแต่ละภาษาโปรแกรม ซึ่งแต่ละภาษามีวิธีการที่แตกต่างกันไป



ภาพที่ 2. ตัวอย่างระบบสารสนเทศของโรงพยาบาลศิริราชที่ทำการเชื่อมโยงกับ AD

ดังนั้นเมื่อแต่ละระบบยึดหลักแนวทางการดำเนินการตามนี้ ส่งผลให้ระบบสารสนเทศของโรงพยาบาลที่เกิดขึ้นมาใหม่สามารถตรวจสอบและบริหารงานจัดการสิทธิ์ได้จากส่วนกลาง อีกทั้งผู้ใช้งานสามารถใช้บัญชีผู้ใช้งานและรหัสผ่านเดียวกันได้ ก่อให้เกิดความสะดวก สร้างความพึงพอใจ ให้กับผู้ใช้งาน

ผลการนำ Active Directory มาใช้งานกับระบบสารสนเทศโรงพยาบาล

การนำระบบ AD เข้ามาใช้งานในระบบสารสนเทศโรงพยาบาลเพื่อบริหารจัดการด้านการยืนยันตัวตนและการกำหนดสิทธิ์ผู้ใช้งาน ทำให้การจัดการด้านยืนยันตัวตนและการรับรองตัวตน ตลอดจนถึงสิทธิ์ ได้รับการบริหารจัดการอย่างมีประสิทธิภาพ เป็นระบบและมีความปลอดภัย โดยเมื่อพิจารณาทำการเปรียบเทียบระหว่างระบบสารสนเทศโรงพยาบาลที่ยังไม่ได้เชื่อมต่อ AD กับระบบสารสนเทศของโรงพยาบาลที่เชื่อมต่อ AD พบว่าปัญหาต่าง ๆ ได้รับการแก้ไขเมื่อทำการเชื่อมต่อ AD มีดังนี้

ตารางที่ 3. เปรียบเทียบปัญหาที่ได้รับการแก้ไขเมื่อระบบสารสนเทศโรงพยาบาลเชื่อมต่อกับ AD

ลำดับ	ปัญหาที่พบกับระบบสารสนเทศโรงพยาบาลที่ยังไม่ได้เชื่อมต่อ AD	ปัญหาที่ได้รับการแก้ไขเมื่อระบบสารสนเทศโรงพยาบาลเชื่อมต่อ AD
1	ข้อมูลผู้ใช้งานไม่ได้ถูกปรับปรุงให้เป็นปัจจุบันตามการเปลี่ยนแปลงจากหน่วยงานทรัพยากรบุคคล มีโอกาสทำให้ข้อมูลรั่วไหล เมื่อผู้เข้าใช้งานระบบพ้นสภาพการเป็นพนักงาน	ข้อมูลผู้ใช้งานได้รับการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ ตามการเปลี่ยนแปลงจากหน่วยงานทรัพยากรบุคคล เมื่อผู้ใช้งานพ้นสภาพการเป็นพนักงาน จะไม่สามารถเข้าระบบได้โดยอัตโนมัติ
2	ผู้ใช้งานมีการเปลี่ยนตำแหน่งหรือโยกย้ายหน่วยงานที่ตนเองสังกัดไปแล้ว แต่พบว่ารหัสผู้ใช้งานที่มีอยู่สามารถเข้าถึงระบบของ	ระบบสามารถกำหนดนโนบายการให้สิทธิ์ผู้ใช้งาน ในระดับตำแหน่ง/หน่วยงานได้ เมื่อผู้ใช้งานมีการเปลี่ยนแปลงสังกัดหน่วยงาน จะไม่สามารถเข้าระบบที่ได้กำหนดสิทธิ์เหล่านี้ไว้โดยอัตโนมัติ

ลำดับ	ปัญหาที่พบกับระบบสารสนเทศโรงพยาบาลที่ยังไม่ได้เชื่อมต่อ AD	ปัญหาที่ได้รับการแก้ไขเมื่อระบบสารสนเทศโรงพยาบาลเชื่อมต่อ AD
	หน่วยงานเดิมได้ ทั้งที่ระบบกำหนดให้เฉพาะคนในหน่วยงานเข้าใช้งานได้เท่านั้น	
3	ผู้ใช้งานที่มีสิทธิ์เข้าใช้งานระบบสารสนเทศโรงพยาบาลได้หลายระบบ หรือบางท่านอาจมีสิทธิ์ถึง 10 ระบบ ทำให้ต้องจดจำบัญชีผู้ใช้งานและรหัสผ่านของแต่ละระบบ ทำให้เกิดความยุ่งยาก ซับซ้อนในการจดจำ และบางท่านเลือกที่จะจดใส่กระดาษ ซึ่งส่งผลให้เกิดช่องโหว่ในการรักษาความปลอดภัยของข้อมูลตามมา	ช่วยลดปัญหาการจดจำบัญชีผู้ใช้งานและรหัสผ่าน เพราะระบบที่เชื่อม AD จะใช้บัญชีผู้ใช้งานและรหัสผ่านเดียวกัน ทำให้เกิดความสะดวก รวดเร็ว ง่ายต่อการจดจำ เมื่อจะเข้าระบบใดก็ไม่ต้องเสียเวลาคิดว่าระบบนี้ใช้บัญชีและรหัสผ่านอะไร
4	การบริหารจัดการข้อมูลผู้ใช้งานไม่ได้รวมอยู่ที่จุดศูนย์กลาง ต้องอาศัยผู้ดูแลระบบแต่ละระบบบริหารจัดการเอง ไม่ว่าจะเป็นการตรวจสอบรหัสผู้ใช้งานหรือการแก้ไขรหัสผ่าน ทำให้ยากต่อการให้บริการแก้ไขปัญหาจากส่วนกลาง	ระบบสารสนเทศที่ทำการเชื่อมต่อกับระบบ AD การบริหารจัดการข้อมูลสามารถทำได้จากส่วนกลาง สามารถตรวจรหัสผู้ใช้งานและทำการเปลี่ยนรหัสผ่านได้จากระบบกลาง ทำให้สะดวกต่อการให้บริการ เพราะไม่ต้องไล่สอบถามและแก้ไขปัญหาทีละระบบ

เมื่อทำการศึกษาและเปรียบเทียบกับบทความหรืองานวิจัยต่าง ๆ ที่ผ่านมา ได้ผลลัพธ์สอดคล้องไปในทิศทางเดียวกันกับบทความหรืองานวิจัยหลาย ๆ งาน เช่น งานของ นิธิ และ อิศรา (2562) เรื่อง การยกระดับองค์กรด้วยระบบ Active Directory โดยกล่าวถึงการนำระบบ Active Directory เข้ามาประยุกต์ใช้ให้สอดคล้องกับการดำเนินการขององค์กร เพิ่มประสิทธิภาพและลดความยุ่งยากในการบริหารจัดการบัญชีและรหัสผ่านของผู้ใช้งาน นอกจากนี้ยังสอดคล้องกับงานวิจัยเรื่อง การยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต ของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช (เอกชัย, 2566) โดยศึกษาการพัฒนาระบบยืนยันตัวบุคคลโดยใช้ Active Directory Domain Services ในการจัดการและควบคุมการใช้งานทรัพยากรบนเครือข่าย ผลจากการพัฒนาทำให้หน่วยงานมีระบบสำหรับยืนยันตัวบุคคลในการเข้าใช้งานอินเทอร์เน็ต สามารถกำกับดูแล ผู้ใช้งานและการสื่อสารได้อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย

ข้อดีของการนำ Active Directory มาใช้งานกับระบบสารสนเทศโรงพยาบาล

การนำระบบ AD มาใช้งานในระบบสารสนเทศของโรงพยาบาลมีข้อดีด้วยกันหลายประการ ซึ่งข้อดีหลัก ๆ ที่เห็นได้ชัดเจนมีดังนี้

1. ด้านการจัดการบัญชีและสิทธิ์ของผู้ใช้งาน ช่วยลดความยุ่งยากในการบริหารจัดการบัญชีและรหัสผ่าน ผู้ใช้งานสามารถเข้าระบบสารสนเทศโรงพยาบาลด้วยบัญชีและรหัสผ่านเดียวกัน การสร้าง ปรับปรุงและลบบัญชีผู้ใช้ตลอดจนถึงการจัดการสิทธิ์ทำได้จากส่วนกลาง ทำให้สะดวกต่อการดูแลและให้บริการแก่ผู้ใช้งาน

2. ด้านความปลอดภัยของข้อมูล ระบบจะทำหน้าที่ตรวจสอบตัวตนของผู้ใช้งานและการให้สิทธิ์เข้าถึงทรัพยากรต่าง ๆ ขององค์กร ตามที่กำหนดไว้ ซึ่งจะช่วยป้องกันการเข้าถึงข้อมูลและทรัพยากรโดยที่ไม่ได้รับอนุญาต ถือเป็นการปกป้องและรักษาความลับของข้อมูล

3. ด้านประสิทธิภาพการทำงาน จากการที่ระบบ AD สามารถควบคุมบริหารจัดการบัญชี รหัสผ่าน และสิทธิ์การเข้าถึงทรัพยากรต่าง ๆ ได้จากส่วนกลาง ทำให้ผู้ดูแลระบบตรวจสอบและค้นหาข้อมูลได้อย่างรวดเร็ว การแก้ไขปัญหาใช้เวลาไม่นาน ผู้ใช้งานสามารถเข้าใช้งานระบบสารสนเทศโรงพยาบาลและปฏิบัติงานต่อได้อย่างราบรื่น ส่งผลต่อการให้บริการผู้ป่วย/ผู้รับบริการเป็นไปอย่างมีประสิทธิภาพ

ข้อเสียของการนำ Active Directory มาใช้งานกับระบบสารสนเทศโรงพยาบาล

ระบบหรือเครื่องมือใด ๆ เมื่อมีข้อดีย่อมมีข้อเสีย AD ก็เช่นเดียวกัน แม้จะเป็นระบบที่มีความสำคัญ มีการใช้งานอย่างกว้างขวาง แต่ก็มีข้อเสียอยู่บางประการ ดังนั้นก่อนที่จะนำมาใช้งานควรพิจารณาข้อเสียเหล่านี้ด้วย

1. ความซับซ้อนและความยากในการติดตั้ง การติดตั้งและการกำหนดปรับปรุงค่าต่าง ๆ ของ Active Directory มีความซับซ้อน ดังนั้นต้องการผู้ที่มีความรู้ ความเข้าใจการทำงานของระบบเพื่อดำเนินการปรับปรุง

2. การบำรุงและการดูแลรักษา หลังจากการติดตั้งและกำหนดปรับปรุงค่าต่าง ๆ แล้ว ระบบ AD ยังต้องได้รับการบำรุงดูแลรักษาอย่างสม่ำเสมอ โดยเฉพาะด้านความปลอดภัยซึ่งเป็นสิ่งสำคัญมาก เพราะเป็นที่รวบรวมข้อมูลสำคัญที่เกี่ยวกับผู้ใช้งาน หากดูแลได้ไม่ทั่วถึง อาจเกิดเป็นช่องโหว่ สามารถถูกนำมาใช้ประโยชน์ที่ไม่เหมาะสมหรือถูกโจมตีได้

3. ค่าใช้จ่ายที่มีแนวโน้มจะเพิ่มขึ้น นอกเหนือจากการลงทุนด้านซอฟต์แวร์และฮาร์ดแวร์ ตลอดจนทรัพยากรอื่น ๆ ที่เกี่ยวข้องในระยะเริ่มต้นแล้ว ยังมีเรื่องของการอัปเกรดทรัพยากรต่าง ๆ ที่จะเกิดขึ้นในอนาคตซึ่งส่งผลให้องค์กรหรือหน่วยงานมีค่าใช้จ่ายเพิ่มมากขึ้น

ข้อเสนอแนะการนำ Active Directory มาใช้งานกับระบบสารสนเทศโรงพยาบาล

ระบบ Active Directory (AD) เป็นระบบที่มีความสำคัญ ดังนั้นก่อนที่จะทำการติดตั้งองค์กรหรือหน่วยงานควรพิจารณาข้อเสนอแนะดังต่อไปนี้ อย่างรอบคอบเพื่อให้การใช้งานเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

1. ก่อนการตัดสินใจที่จะทำการติดตั้ง ควรพิจารณาความคุ้มค่าในการนำ AD ไปใช้งานในธุรกิจหรือองค์กร เพราะการติดตั้งมีค่าใช้จ่ายทั้งในด้านซอฟต์แวร์ ฮาร์ดแวร์ ตลอดจนถึงการลงทุนสร้างองค์ความรู้และพัฒนาบุคลากรสำหรับบำรุงดูแลรักษา

2. ควรทำการวางโครงสร้างของระบบให้เหมาะสมกับองค์กรของตนเอง ก่อนที่จะทำการติดตั้ง เพราะแต่ละหน่วยงานแต่ละองค์กรย่อมมีรูปแบบลำดับชั้นการบริหารจัดการที่ไม่เหมือนกัน

3. สำหรับองค์กรหรือหน่วยงานที่ไม่มีประสบการณ์การใช้งานระบบ AD หรือยังไม่มีระบบ AD ของหน่วยงานและอยู่ระหว่างพิจารณาตัดสินใจ ควรจัดหาที่ปรึกษาหรือผู้เชี่ยวชาญเพื่อให้คำแนะนำ

บทสรุป

ในการศึกษาการนำระบบ Active Directory หรือ AD เข้ามาใช้งานในองค์กรโดยการบูรณาการเข้ากับระบบสารสนเทศของโรงพยาบาลเดิมที่มีอยู่ และมุ่งขยายขอบเขตให้ทุกระบบที่พัฒนาขึ้นมาใหม่เชื่อมต่อกับระบบ AD เพื่อใช้เป็นศูนย์กลางด้านการบริหารจัดการบัญชีผู้ใช้งาน สำหรับการยืนยันตัวตนและการกำหนดสิทธิ์ผู้ใช้งาน พบว่าสามารถช่วยให้องค์กรสามารถบริหารจัดการทรัพยากรและผู้ใช้งานเป็นไปอย่างมีระบบและปลอดภัย ช่วยลดความซับซ้อนในการดูแลรักษา เพิ่มเสถียรภาพและประสิทธิภาพในการทำงานให้กับองค์กรได้เป็นอย่างดี

อย่างไรก็ตามการพิจารณานำระบบ AD มาใช้ภายในองค์กร โดยเฉพาะอย่างยิ่งองค์กรที่มีขนาดใหญ่ มีระบบสารสนเทศที่ใช้งานเป็นจำนวนมาก ถือเป็นความท้าทายขององค์กร ที่ต้องอาศัยการวางแผนการติดตั้งและวางโครงสร้างของระบบ AD โดยต้องมีการหารือแนวทางการปรับปรุง/เปลี่ยนแปลงระบบงามเดิมให้พร้อมรองรับการเชื่อมต่อ เริ่มตั้งแต่กระบวนการวิเคราะห์ออกแบบระบบ การพัฒนาระบบ ตลอดจนรูปแบบพฤติกรรมการใช้งานที่มีการเปลี่ยนแปลงไป ซึ่งสิ่งเหล่านี้ต้องมีการเตรียมความพร้อมและอาศัยความร่วมมือจากทุกคน/ทุกหน่วยงาน เพื่อให้การนำระบบ AD มาใช้ยืนยันตัวตนและกำหนดสิทธิ์ผู้ใช้งานของระบบสารสนเทศโรงพยาบาล เป็นไปอย่างมีประสิทธิภาพและยั่งยืน

กิตติกรรมประกาศ

บทความทางวิชาการฉบับนี้สำเร็จสมบูรณ์ได้จากการสนับสนุนจากฝ่ายสารสนเทศ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ที่ได้เล็งเห็นความสำคัญของการนำระบบ AD เข้ามาใช้งานในระบบสารสนเทศโรงพยาบาลเพื่อยกระดับการบริหารจัดการด้านการยืนยันตัวตนและการกำหนดสิทธิ์ผู้ใช้งาน เพื่อเพิ่มประสิทธิภาพความยืดหยุ่น ในการดำเนินงานและควบคุมความปลอดภัยของระบบให้เพิ่มมากยิ่งขึ้น ผู้เขียนขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

เอกสารอ้างอิง

นิธิ ภัทรปิติตานนท์ และ อิศรา แย้มงามเหลือ. (2562). การยกระดับองค์กรด้วยระบบ Active Directory. *วารสาร Mahidol R2R e-Journal, 6*(2), 1–8.

สมาคมเวชสารสนเทศไทย. (2564). *กรอบการพัฒนาคุณภาพเทคโนโลยีสารสนเทศโรงพยาบาล.* [ออนไลน์]. เข้าถึงได้จาก https://tmi.or.th/wp-content/uploads/2021/12/HospitalIT_QualityImproveFramework_V2.pdf (สืบค้นเมื่อ กุมภาพันธ์ 2567).

สุจิตรา ยอดเสน่หา. (2560). *การประยุกต์ใช้ระบบยืนยันตัวตนเพียงครั้งเดียวในการบริหารจัดการห้องเรียนออนไลน์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.* [ออนไลน์]. เข้าถึงได้จาก http://www.repository.rmutt.ac.th/dspace/handle/123456789/2855 (สืบค้นเมื่อ มกราคม 2567).

เอกชัย แก้วเรืองฤทธิ์. (2566). *การยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต ของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช.* [ออนไลน์]. เข้าถึงได้จาก https://ddc.moph.go.th/uploads/ckeditor2//files/3.การยืนยันตัวบุคคล_เอกชัย_สคร11.pdf (สืบค้นเมื่อ มีนาคม 2567).

Chai, W., & Gillis, A. S. (2021). *Active directory*. [Online]. Available: https://www.techtarget.com/searchwindowsserver/definition/Active-Directory (Retrieved October 2023).

HOCCO. (2023). *ระบบ HIS คืออะไร ทำไมโรงพยาบาลต้องมี* [ดูประโยชน์และการใช้งาน]. [Online]. Available: https://hocco.co/blog/what-is-his-systems/ (Retrieved September 2023).

Kron. (2022). *What is AAA* (Authentication, Authorization & Accounting)?. [Online]. Available: https://krontech.com/what-is-aaa-authentication-authorization-accounting (Retrieved March 2024).

Magnusson, A. (2023). *The definitive guide to authentication*. [Online]. Available: https://www.strongdm.com/authentication (Retrieved August 2023).

Phothiin, P. (2021). *Authentication และ Authorization คืออะไร? ต่างกันอย่างไร?*. [Online]. Available: https://monsterconnect.co.th/authentication-vs-authorization/ (Retrieved September 2023).

SailPoint. (2023). *What is the difference between authentication and authorization?*. [Online]. Available: https://www.sailpoint.com/identity-library/difference-between-authentication-and-authorization/ (Retrieved October 2023).

Simister, A. (2024). *What is Active Directory and how does it work?.* [Online]. Available: https://www.lepide.com/blog/what-is-active-directory-and-how-does-it-work/ (Retrieved March 2024).

Sinaga, R. N., Mitra, & Saputra, K. (2024). Implementation of hospital management information system for optimizing healthcare service operations at a hospital. *Viva Medika: Jurnal Kesehatan, Kebidanan Dan Keperawatan, 17*(1), 164–173. https://doi.org/10.35960/vm.v17i1.1329