SITEM MAGAZINE

ISSUE 3/2025

EDITORIAL

ในโลกที่ทุกสิ่งขับเคลื่อนด้วยข้อมูลและเทคโนโลยี ความมั่นคงปลอดภัยไม่ได้จำกัดอยู่แค่การปกป้องกำแพงทางกายภาพอีกต่อไป แต่ขยายไปสู่มิติของไซเบอร์สเปซ ซึ่งเป็นสมรภูมิใหม่ที่มองไม่เห็นแต่มีผลกระทบมหาศาล

นิตยสารของเราในฉบับนี้ จะพาคุณไปเจาะลึกภัยคุกคามทางไซเบอร์ที่กำลังเปลี่ยนโฉมไปในประเทศไทย การโจมตีไม่ได้มุ่งเป้าที่ผลกำไรทางการเงินอีกต่อไป แต่เป็นการแสดงออกทางอุดมการณ์ของกลุ่ม Hacktivist ซึ่งใช้เครื่องมือทางวิศวกรรมอันซับซ้อนอย่างการโจมตี DDoS หรือการทำ Deface เพื่อสร้างแรงกระเพื่อมทางสังคมและทำลายความน่าเชื่อถือขององค์กรภาครัฐและโครงสร้างพื้นฐานสำคัญ

อย่างไรก็ตาม ความท้าทายนี้ไม่ได้ไร้ทางออก วิศวกรรมได้เข้ามามีบทบาทสำคัญในการสร้างเกราะป้องกันที่แข็งแกร่ง เราจะสำรวจนวัตกรรมและโซลูชันด้าน Data Center ที่เป็นหัวใจสำคัญของระบบข้อมูลภาครัฐ เช่น โครงการปรับปรุงและก่อสร้างศูนย์ข้อมูลแห่งใหม่ของกรมการปกครอง ซึ่งสะท้อนให้เห็นถึงความจำเป็นในการยกระดับมาตรฐานโครงสร้างพื้นฐานให้ทันสมัยและปลอดภัยจากความเสี่ยงต่างๆ

นอกจากนี้ เรายังจะเจาะลึกเบื้องหลังความสำเร็จของ AI Transformation ซึ่งเป็นก้าวต่อไปของยุคดิจิทัล โดยเน้นย้ำถึงความสำคัญของ Data Governance และ AI Governance ซึ่งเป็น "เชื้อเพลิง" และ "กฎจราจร" ที่ทำให้ AI ทำงานได้อย่างมีประสิทธิภาพ ปลอดภัย และมีธรรมาภิบาล

สุดท้าย เราจะพาไปทำความรู้จักกับนโยบาย SITEM NEXT SUSTAINABILITY ที่พิสูจน์ให้เห็นว่าความรับผิดชอบต่อสังคมและสิ่งแวดล้อมนั้นไม่ใช่แค่เรื่องของการทำ CSR ทั่วไป แต่คือการผสานหลักการทางวิศวกรรมเข้ากับความยั่งยืน ตั้งแต่การเลือกใช้วัสดุ การบริหารจัดการทรัพยากร ไปจนถึงการสร้างบุคลากรและชุมชนให้เติบโตไปพร้อมกัน

ในทุกวิกฤตย่อมมีโอกาส การทำความเข้าใจภัยคุกคามและการใช้หลักวิศวกรรมที่ชาญฉลาดในการสร้างระบบที่ยืดหยุ่นและปลอดภัย จะเป็นกุญแจสำคัญสู่ความสำเร็จในอนาคต

In a world where everything is driven by data and technology, security is no longer confined to the protection of physical walls. It has expanded into the dimension of cyberspace, a new, invisible battlefield with immense implications.

In this issue, our magazine will delve into the evolving landscape of cyber threats in Thailand. Attacks no longer target financial gain; instead, they are a form of ideological expression by Hacktivist groups. These groups use sophisticated engineering tools, such as DDoS and defacement attacks, to create social disruption and undermine the credibility of government organizations and critical infrastructure.

However, these challenges are not insurmountable. Engineering plays a vital role in building a robust defense. We will explore innovations and solutions in Data Centers, the very heart of government data systems. This includes the Department of Provincial Administration's project to upgrade and construct new data centers, which reflects the imperative to modernize foundational infrastructure and secure it against various risks.

Furthermore, we will take a deeper look behind the success of AI Transformation, the next step in the digital era. We will emphasize the critical importance of Data Governance and AI Governance, which serve as the "fuel" and "traffic rules" that enable AI to operate efficiently, securely, and with integrity.

Finally, we will introduce you to the SITEM NEXT SUSTAINABILITY policy, which proves that social and environmental responsibility is not merely a matter of typical CSR. It is the integration of engineering principles with sustainability, from material selection and resource management to fostering the growth of both personnel and communities.

In every crisis, there lies an opportunity. Understanding these threats and applying intelligent engineering principles to build resilient and secure systems will be the key to future success.

CONTENT

จาก Digital สู่ AI transformation ยุทธศาสตร์ธรรมาภิบาลข้อมูล

โดย ดร.กำพล อดิเรกสมบัติ CEO Athentic Consulting

จากยุค Digital สู่ยุค AI Transformation การเปลี่ยนแปลงครั้งสำคัญนี้กำลังเข้ามาขับเคลื่อนทั้งภาคธุรกิจและภาครัฐให้ก้าวไปข้างหน้าอย่างที่ไม่เคยมีมาก่อน หลายองค์กรต่างมุ่งใช้ศักยภาพของ AI เพื่อเพิ่มประสิทธิภาพและสร้างสรรค์นวัตกรรมใหม่ ๆ เพื่อมอบประสบการณ์ที่ดียิ่งขึ้นให้แก่ลูกค้า แต่เบื้องหลังความน่าตื่นเต้นของ AI ที่เราเห็นกันนั้นมีรากฐานสำคัญที่ไม่ควรมองข้าม นั่นคือ ข้อมูล AI Transformation กำลังเป็นประเด็นที่ทางภาครัฐและเอกชนให้ความสนใจเป็นอย่างมาก หลายหน่วยงานกำลังเร่งรีบที่จะใช้พลังแห่งการเปลี่ยนแปลงของ AI เพื่อเพิ่มประสิทธิภาพในการทำงานแบบที่หลายๆ ภูรูด้านเทคโนโลยีบอกว่าจะเป็นการเพิ่มแบบที่ไม่เคยมีมาก่อน แบบที่เรียกว่าสร้างประสบการณ์ลูกค้าที่เป็นส่วนตัวและนวัตกรรมก้าวล้ำ แต่ภายใต้พื้นผิวที่น่าตื่นเต้นของ Algorithm และ Neural Network มีรากฐานที่สำคัญไม่แพ้กันคือ **เรื่องข้อมูล** ยกตัวอย่างให้เห็นความสำคัญของข้อมูลง่ายง่ายก็คือ คำว่า ChatGPT : GTP ย่อมาจาก Generative Pre-Trainer Transformer ซึ่งเป็นหนึ่งใน Large language model ที่ถูกเทรนหรือสอนด้วยข้อมูลที่เป็น Text จำนวนมหาศาล การจะมี AI transformation ที่มีประสิทธิภาพได้จำเป็นต้องมีรากฐานที่แข็งแกร่งจาก Data Transformation ในองค์กรด้วย เพื่อให้เห็นภาพหากเราเปรียบเทียบ ai เป็นรถแข่งสมรรถภาพ Algorithm คือเครื่องยนต์ทรงพลังที่มีความเร็วและความคล่องตัวที่น่าทึ่งแต่หากไม่มีเชื้อเพลิงที่เหมาะสม รถก็จะกระตุกและดับลงในที่สุด ยกตัวอย่างรถแข่ง Formula แม้ใช้น้ำมันเบนซิน ก็เป็นเบนซินชนิดพิเศษกว่า ซึ่งประกอบด้วยน้ำมันเบนซิน 90% และเอทานอลหมุนเวียน 10% ที่เรียกว่า E10 นี่เป็นก้าวสำคัญสู่ความยั่งยืนที่มากขึ้น ดังนั้นโลกของ AI เชื้อเพลิงนั้นคือข้อมูลโดยคุณภาพ การเข้าถึงความสมบูรณ์ของข้อมูลนั้นมีความมีความสำคัญอย่างยิ่ง

ถ้าธรรมมาภิบาลข้อมูล หรือ Data Governance คือกฎระเบียบที่ทำให้ได้มาซึ่งข้อมูลหรือน้ำมันพร้อมใช้

ธรรมมาภิบาล AI (AI Governance) ก็คือกฎระเบียบกติกาที่จะทำให้การใช้รถเป็นไปอย่าง มั่นคงปลอดภัย ผมขออนุญาตเปรียบเทียบการขับเคลื่อน Data and AI Transformation คล้ายกับการจะสร้างรถประเภทต่างๆ เพื่อให้ใช้วิ่งบนท้องถนน ซึ่งเราจำเป็นต้องมีทั้งรถยนต์ (AI matching learning), น้ำมัน (ข้อมูล), ถนน (โครงสร้างพื้นฐานด้านข้อมูล เช่น Data Center, ระบบสาย Cable ส่งข้อมูล, กติกามารยาทด้านการจราจร (AI Governance) รวมถึงมาตรฐานการผลิตและการใช้น้ำมัน (Data Governance) และคนขับ (ทรัพยากรมนุษย์ที่มีทักษะและปฏิบัติตามกฎ)

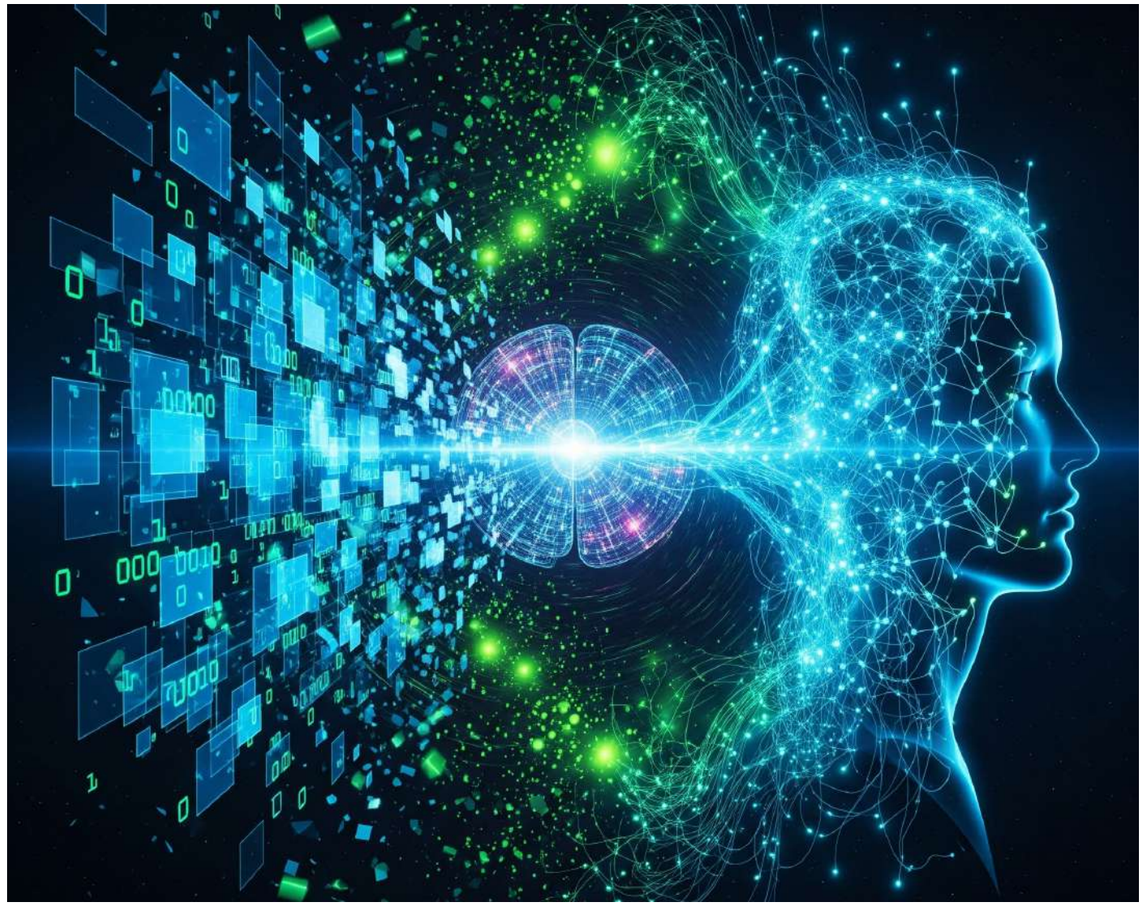
แล้วอะไรเป็นตัวช่วยให้สิ่งต่างๆเกิดขึ้นได้ ผมมองว่ามี 3 ปัจจัยสำคัญดังนี้

1. ยุทธศาสตร์ข้อมูล	2. ธรรมาภิบาลข้อมูล	3. ธรรมาภิบาล AI (AI Algorithm)
จะเข้ามาช่วยเราเลือกทั้งน้ำมัน(ข้อมูล) รถยนต์ (AI / Machine Learning) ที่เหมาะสมกับงบประมาณและทรัพยากรที่มีใช้งานได้ถูกประเภทและตอบโจทย์องค์กรได้	ช่วยให้ได้มาซึ่งน้ำมันที่ถูกประเภท พร้อมใช้ทั้งในปัจจุบันและไม่ทำให้เครื่องพังในภายหลัง โดยถ้าเกิดเหตุการณ์ที่ใช้น้ำมันผิดประเภทหรือน้ำมันที่ไม่มีมาตรฐานก็จะต้องมีผู้รับผิดชอบ	จะเป็นกฎกติกามารยาทมาตรฐานในการสร้างรถยนต์และขับเคลื่อนบนท้องถนนอย่างมั่นคงปลอดภัย ไม่ใช่ว่าใครอยากจะสร้างรถแบบไหนก็ได้ออกมาขับขี่ยังไงก็ได้ สร้างปัญหามลภาวะโดยไม่ต้องรับผิดชอบกับคนที่ตามมา

กระแส AI กำลังสร้างความต้องการมหาศาลในการใช้ข้อมูลคุณภาพสูง Algorithm ของ AI เรียนรู้และปรับปรุงโดยการระบุรูปแบบและความสัมพันธ์ภายในชุดข้อมูลขนาดใหญ่ (Big Data) ยิ่งข้อมูลที่ใช้ฝึกฝนโมเดล AI มีความเกี่ยวข้องหลากหลายและมีคุณภาพสูงมากเท่าใด โมเดลนั้นก็จะยิ่งมีความแม่นยำน่าเชื่อถือและมีคุณค่ามากขึ้นเท่านั้น

ตัวอย่างเช่น AI ที่ได้รับการป้อนข้อมูลประวัติการซื้อของลูกค้า พฤติกรรมการเรียกดู และข้อมูลประชากรที่ครอบคลุม ที่ผ่านกระบวนการสร้างคุณภาพข้อมูลมาแล้ว AI ตัวนี้จะสามารถให้คำแนะนำที่เป็นส่วนตัวและมีประสิทธิภาพสูง ซึ่งจะช่วยเพิ่มยอดขายและความภักดีของลูกค้า ในทางกลับกันการฝึกฝนเครื่องมือเดียวกันด้วยข้อมูลที่ไม่สมบูรณ์ ไม่ถูกต้อง หรือมีอคติ จะนำไปสู่คำแนะนำที่ผิดพลาด ซึ่งจะกัดกร่อนความไว้วางใจของลูกค้าและขัดขวางการเติบโตของธุรกิจ

การเข้ามามีส่วนร่วมของ AI ในฟังก์ชันทางธุรกิจและบริการภาครัฐต่างๆ ขยายความจำเป็นในการมีแนวทางเชิงกลยุทธ์ในการจัดการข้อมูล ตั้งแต่การวิเคราะห์เชิงคาดการณ์เพื่อคาดการณ์แนวโน้มของตลาด ไปจนถึงการประมวลผลด้านภาษาที่ขับเคลื่อน Chatbot ที่ซับซ้อน แอพพลิเคชั่น AI แต่ละรายการล้วนต้องพึ่งพาข้อมูลประเภทและรูปแบบเฉพาะอย่างมาก



ยุทธศาสตร์ข้อมูลที่ช่วยให้ AI Transformation ตอบโจทย์องค์กรและจับต้องได้จริง

เปรียบได้เหมือนกับเราสามารถเลือกน้ำมันที่ถูกประเภทเพื่อนำไปใช้กับรถยนต์ที่เราอยากได้และใช้ได้จริง ธรรมาภิบาลข้อมูลในฐานะรากฐานสำคัญและรั้วกั้น สร้างความมั่นใจในความน่าเชื่อถือและการปฏิบัติตามกฎระเบียบ โดยเรื่องของยุทธศาสตร์และธรรมาภิบาลข้อมูล ไม่ใช่หน่วยงานที่เป็นอิสระต่อกัน แต่เป็นสองด้านของเหรียญเดียวกัน โดยยุทธศาสตร์ข้อมูลที่ชัดเจนให้อะไรและทำไมของการใช้ข้อมูลสำหรับ AI Transformation ในขณะที่ธรรมาภิบาลที่แข็งแกร่งกำหนด อย่างไร และ ใคร

เพื่อให้มั่นใจถึงการนำไปใช้อย่างมีความรับผิดชอบและมีประสิทธิภาพ

เพื่อให้เห็นภาพ ผมขออนุญาตยกตัวอย่าง Use case สถาบันการเงินที่ใช้ AI ในการตรวจจับการฉ้อโกง ยุทธศาสตร์ข้อมูลจะระบุข้อมูลการทำธุรกรรมที่เกี่ยวข้อง โปรไฟล์ลูกค้าและรูปแบบการฉ้อโกงในอดีต ในขณะที่กรอบธรรมาภิบาลข้อมูลจะกำหนดกระบวนการทำงานที่เข้มงวดสำหรับการเข้าถึงและปกปิดข้อมูลลูกค้าที่ละเอียดอ่อน เพื่อให้มั่นใจถึงการปฏิบัติตามกฎระเบียบด้านความเป็นส่วนตัว นอกจากนี้ยังใช้กลไกการตรวจสอบจากอคติ เพื่อป้องกันไม่ให้ AI ติดตามธุรกรรมอย่างไม่ยุติธรรม โดยอิงจากลักษณะที่ได้รับการคุ้มครอง

สร้างข้อมูลในฐานะสินทรัพย์เชิงกลยุทธ์เพื่อความสำเร็จของ AI Transformation

การแข่งขันเพื่อนำ AI มาใช้ในการดำเนินงาน ไม่ว่าจะเป็นภาครัฐหรือภาคเอกชน การปฏิบัติต่อข้อมูลในฐานะสินทรัพย์เชิงกลยุทธ์ โดยมียุทธศาสตร์ข้อมูลที่แข็งแกร่งและธรรมาภิบาลที่มั่นคงเป็นรากฐาน จะได้รับความได้เปรียบทางการแข่งขันที่สำคัญ หน่วยงานจะสามารถเติมพลังให้กับ AI ด้วยข้อมูลคุณภาพสูงที่น่าเชื่อถือ นำไปสู่ข้อมูลเชิงลึก (Data Insight) ที่แม่นยำยิ่งขึ้น การคาดการณ์ที่น่าเชื่อถือและท้ายที่สุดคือมูลค่าทางธุรกิจหรือประโยชน์ที่มากขึ้น

การเพิกเฉยต่อรากฐานที่สำคัญนี้ ก็เหมือนกับการสร้างตึกสูงบนทราย ยิ่งคุณตั้งเป้าหมายสูงเท่าไหร่ ความเสี่ยงก็ยิ่งมากขึ้นเท่านั้น

From Digital to AI Transformation: The Strategic Role of Data Governance

By Dr. Kamphon Adireksombat, CEO, Athentic Consulting

From the digital era to the era of AI Transformation, this significant shift is driving businesses and governments forward like never before. Many organizations are focused on using the potential of AI to enhance efficiency and create new innovations, aiming to deliver better experiences for customers. However, behind the exciting facade of AI lies a crucial, often overlooked, foundation: data.

AI Transformation has become a major topic of interest for both public and private sectors. Many agencies are rushing to harness the power of AI to boost operational efficiency to unprecedented levels, as many technology gurus predict, creating personalized customer experiences and groundbreaking innovations. But beneath the exciting surface of algorithms and neural networks, there is an equally important foundation: data.

A simple example to illustrate the importance of data is ChatGPT. GPT stands for Generative Pre-trained Transformer, one of the large language models trained on a massive amount of text data.

For an effective AI transformation, a strong foundation from the organization's data transformation is essential. To put it in perspective, if we compare AI to a high-performance race car, the algorithm is the powerful engine with incredible speed and agility. But without the right fuel, the car will sputter and eventually stall.

For example, a Formula 1 race car uses a special type of gasoline, a mix of 90% gasoline and 10% renewable ethanol, known as E10. This is a significant step toward greater sustainability. In the world of AI, the fuel is data. The quality, accessibility, and completeness of this data are absolutely critical.

If data governance is the set of rules that ensures the availability of ready-to-use data (the fuel), then AI governance is the set of rules and regulations that ensures the car is used safely and securely.

I'd like to compare the journey of Data and AI Transformation to building different types of cars to be driven on the road. We need a car (AI/machine learning), fuel (data), roads (data infrastructure like data centers and data transmission cables), traffic rules (AI governance), as well as standards for production and fuel use (data governance), and a driver (human resources with skills and compliance).

So, what helps all of these things happen? I see three key factors :

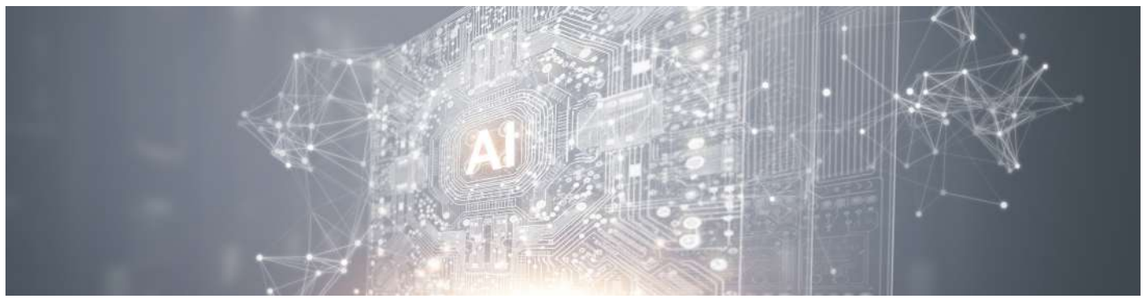
Data Strategy	Data Governance	AI Governance (AI Algorithm)
This helps us choose the right fuel (data) and car (AI/machine learning) based on our budget and resources. It ensures that the tools are used for the right purposes and meet the organization's goals.	This helps us obtain the right type of fuel that is ready to use now and won't damage the engine later. If an incident occurs where the wrong or substandard fuel is used, someone must be held accountable.	This establishes the rules, standards, and etiquette for building and driving cars on the road safely and securely. It prevents anyone from building any type of car they want and driving it however they please, creating pollution without being held responsible for the consequences.

The AI boom is creating an enormous demand for high-quality data. AI algorithms learn and improve by identifying patterns and relationships within large datasets. The more relevant, diverse, and high-quality the data used to train an AI model, the more accurate, reliable, and valuable that model becomes.

For example, an AI fed with comprehensive customer purchase history, browsing behavior, and demographic data that has undergone a data quality process can provide highly effective, personalized recommendations, which can boost sales and customer loyalty. Conversely, training the same tool with incomplete, incorrect, or biased data will lead to flawed recommendations, eroding customer trust and hindering business growth. The increasing integration of AI into various business functions and government services amplifies the need for a strategic approach to data management. From predictive analytics to forecast market trends to complex language processing driving sophisticated chatbots, each AI application relies heavily on specific data types and formats.

A data strategy that makes AI transformation tangible and aligned with organizational goals is like being able to choose the right fuel for the specific car you want and can actually use. Data governance, as a crucial foundation and a safeguard, ensures reliability and compliance. Data strategy and data governance are not independent entities; they are two sides of the same coin. A clear data strategy outlines the "what" and "why" of data use for AI transformation, while a robust governance framework defines the "how" and "who" to ensure responsible and effective implementation.

To illustrate, consider a use case of a financial institution using AI for fraud detection. The data strategy would identify relevant transaction data, customer profiles, and historical fraud patterns. Meanwhile, the data governance framework would establish strict processes for accessing and anonymizing sensitive customer information to ensure compliance with privacy regulations. It would also use bias detection mechanisms to prevent the AI from unfairly flagging transactions based on protected characteristics.



Treating Data as a Strategic Asset for Successful AI Transformation

In the race to implement AI across both public and private sectors, organizations that treat data as a strategic asset—with a strong data strategy and robust governance as the foundation—will gain a significant competitive advantage. These entities can power their AI with reliable, high-quality data, leading to more accurate insights, trustworthy predictions, and ultimately, greater business value or public benefit.

Ignoring this critical foundation is like building a tall skyscraper on sand. The higher you aim, the greater the risk.

ศูนย์เทคโนโลยีสารสนเทศกรมการปกครอง

หัวใจสำคัญของระบบทะเบียนราษฎร์

กรมการปกครองมีบทบาทสำคัญอย่างยิ่งในการบริหารจัดการฐานข้อมูลทะเบียนกลางของประเทศ ทั้งทะเบียนราษฎร บัตรประจำตัวประชาชน และงานทะเบียนอื่นๆ ซึ่งเป็นโครงสร้างพื้นฐานสำคัญด้านข้อมูลภาครัฐที่ต้องพร้อมใช้งานตลอดเวลา เพื่อรองรับการเชื่อมโยงกับหน่วยงานภาครัฐและเอกชน รวมถึงการให้บริการประชาชนทั่วประเทศ

ปัจจุบันการบริหารจัดการข้อมูลของกรมการปกครองอาศัย Data Center หลัก 2 แห่ง คือที่ คลอง 9 จังหวัดปทุมธานี และ วังไชยา (นางเลิ้ง) กรุงเทพมหานคร ซึ่งทั้งสองแห่งถูกออกแบบมาให้สามารถสลับบทบาทเป็นศูนย์ข้อมูลหลัก (Data Center: DC Site) และ ศูนย์สำรองข้อมูล (Disaster Recovery Site : DR Site) ได้โดยสลับการทำงานทุก 6 เดือน เพื่อให้ระบบมีความต่อเนื่องและเสถียร

ความท้าทายและจุดเสี่ยงที่ต้องแก้ไข

แม้จะมีการใช้งาน Data Center ทั้งสองแห่ง แต่ก็มีความจำเป็นเร่งด่วนที่ต้องปรับปรุง โดยเฉพาะ Data Center ที่วังไชยา ซึ่งเป็นอาคารเก่าที่มีความเสี่ยงสูงเนื่องจาก

- ความเสี่ยงด้านที่ตั้งและอาคาร: อาคารเป็นโครงสร้างเก่าแก่และตัว Data Center ตั้งอยู่ในชั้นใต้ดินของอาคารจอดรถ ทำให้มีความเสี่ยงสูงจากสถานการณ์น้ำท่วม
- ไม่เป็นไปตามมาตรฐานสากล: Data Center ปัจจุบันไม่เป็นไปตามมาตรฐานสากลที่ควรจะเป็น ซึ่งส่งผลต่อความมั่นคงปลอดภัยของข้อมูล
- ผลกระทบต่อสิ่งแวดล้อม: ระบบเครื่องกำเนิดไฟฟ้าสำรองก่อให้เกิดมลพิษทางเสียงและควันดำ ซึ่งส่งผลกระทบโดยตรงต่อประชาชนที่พักอาศัยในพื้นที่ใกล้เคียง

เพื่อแก้ไขปัญหาเหล่านี้และปฏิบัติตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างเคร่งครัด กรมการปกครองจึงมีแผนก่อสร้าง Data Center แห่งใหม่ที่ได้มาตรฐาน

แผนการพัฒนา Data Center แห่งใหม่: ยกระดับความมั่นคงปลอดภัยของข้อมูลภาครัฐ

กรมการปกครองได้พิจารณาสถานที่ที่เหมาะสมเพื่อก่อสร้าง Data Center แห่งใหม่ ซึ่งจะเป็นอาคารเฉพาะกิจด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยให้ความสำคัญกับปัจจัยต่างๆ ทั้งสถานที่ตั้ง สภาพแวดล้อม และเทคโนโลยีที่ทันสมัย เพื่อให้เป็นไปตามมาตรฐานสากล

อาคาร Data Center แห่งใหม่นี้จะได้รับการออกแบบตามมาตรฐาน Uptime Institute TIER III: Concurrently Maintainable Site Infrastructure ซึ่งหมายความว่า ระบบสามารถบำรุงรักษาได้โดยไม่มีผลกระทบต่อการทำงานโดยรวม ทำให้สามารถซ่อมบำรุงได้โดยที่ระบบยังคงให้บริการได้ตามปกติ

อาคารใหม่นี้ก่อสร้างบนพื้นที่ 3,200 ตารางเมตร สูง 4 ชั้น พร้อมทั้งมีระบบสนับสนุน Data Center ที่ครบครัน และมีพื้นที่สำหรับห้องทำงานและห้องประชุมเพื่อรองรับสถานการณ์ต่างๆ ในอนาคต

ศูนย์ข้อมูลที่แข็งแกร่ง เปรียบเสมือนหัวใจของระบบทะเบียนราษฎรทั่วประเทศ ทำให้การบริหารจัดการ "ข้อมูลทะเบียนราษฎร" เป็นไปอย่างรวดเร็วและแม่นยำ ทุกครั้งที่ไปใช้บริการ ไม่ว่าจะเป็นการทำบัตรประชาชน การแจ้งเกิด หรือการแจ้งย้ายที่อยู่ เจ้าหน้าที่สามารถเรียกดูข้อมูลได้ทันทีจากฐานข้อมูลกลาง ทำให้ไม่ต้องรอนาน นอกจากนี้เมื่อข้อมูลมีความถูกต้องและเป็นปัจจุบันอยู่ในระบบแล้ว ข้อมูลนั้นจะถูกเชื่อมต่อไปยังหน่วยงานอื่นๆ โดยอัตโนมัติ ทำให้ไม่ต้องเสียเวลาเตรียมเอกสารชุดเดิม ซ้ำๆ เพื่อไปยื่นที่หน่วยงานอื่นอีกต่อไป ไม่ว่าจะเป็นการติดต่อกับโรงพยาบาล สถาบันการเงิน หรือแม้แต่การลงทะเบียนรับสวัสดิการของรัฐ ทั้งหมดนี้คือการลดขั้นตอนที่ยุ่งยากในชีวิตประจำวัน

SITEM ผู้อยู่เบื้องหลังของการเป็นผู้บริหารจัดการโครงการนี้ เพราะเป้าหมายของกรมการปกครองไม่ได้หยุดอยู่แค่การออกเอกสาร แต่คือการทำให้ชีวิตของประชาชนง่ายขึ้น สะดวกขึ้น และปลอดภัยจากความยุ่งยากต่างๆ

The Department of Provincial Administration's Information Technology Center

The Heart of the Civil Registration System

The Department of Provincial Administration (DOPA) plays a crucial role in managing the country's central registration database, including civil registration, national ID cards, and other registration services. This serves as essential government data infrastructure that must be constantly available to support connections with public and private agencies and to provide services to citizens nationwide.

Currently, DOPA's data management relies on two main data centers: one in Khlong Sam, Pathum Thani province, and another in Wang Chaiya (Nang Loeng), Bangkok. Both are designed to function as either the primary Data Center (DC Site) or the Disaster Recovery Site (DR Site), with their roles switching every six months to ensure system continuity and stability.

Challenges and Risks That Need to Be Addressed

Despite using both data centers, there is an urgent need for improvement, particularly for the Wang Chaiya Data Center, which is an old building with significant risks due to

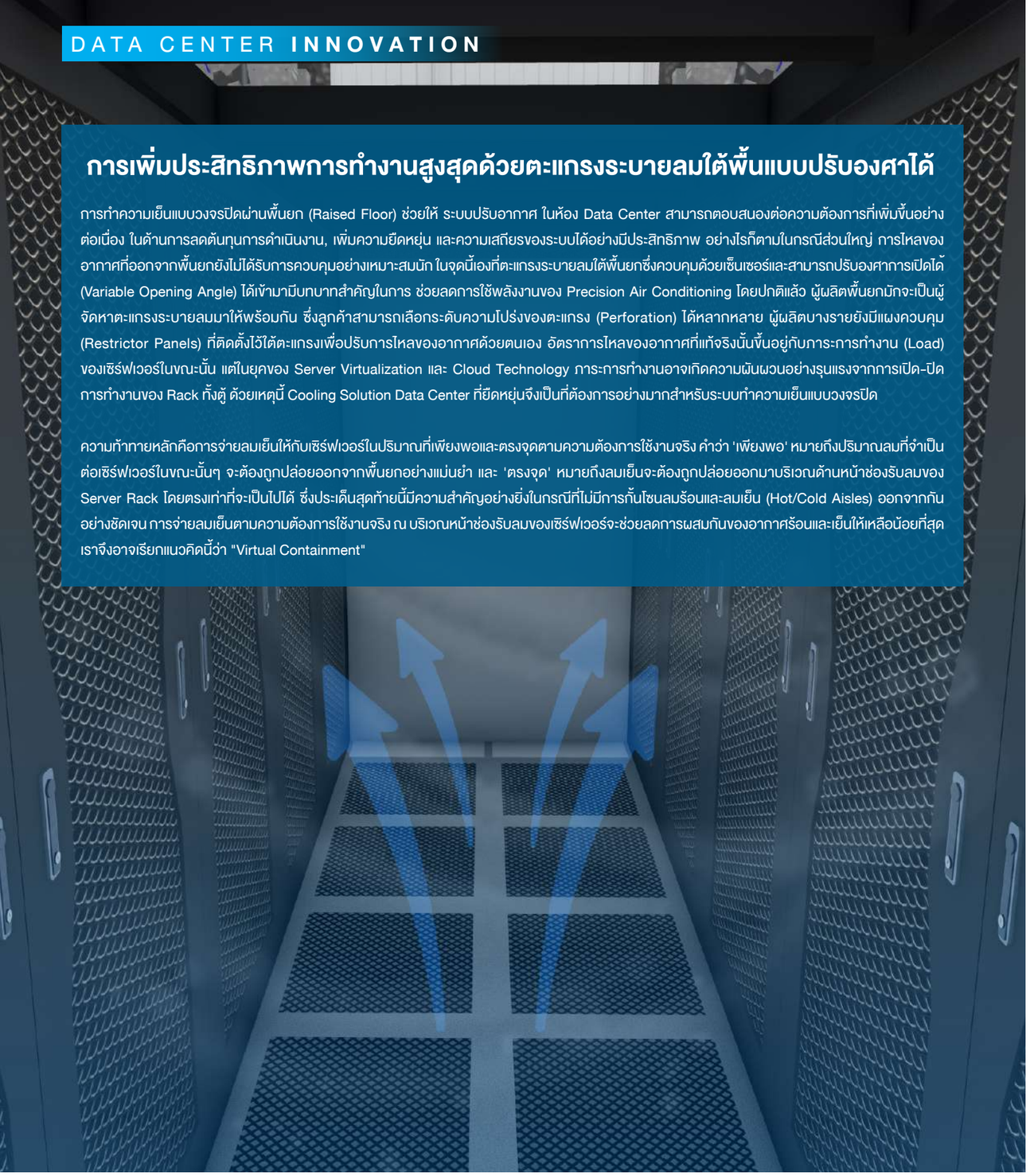
- **Location and building risks** : The building is an old structure, and the data center is located in the basement of the parking garage,making it highly vulnerable to flooding.
- **Failure to meet international standards** : The current data center does not meet international standards, which affects data security.
- **Environmental impact** : The backup generator system produces noise and black smoke, directly impacting residents in the nearby area. To resolve these issues and strictly comply with the Cybersecurity Act, DOPA has planned to construct a new, standardized data center.

New Data Center Development Plan: Elevating Government Data Security

DOPA has identified a suitable location for a new data center, which will be a purpose-built building for information and communication technology. It will prioritize location, environment, and modern technology to meet international standards. This new data center will be designed to the Uptime Institute TIER III: Concurrently Maintainable Site Infrastructure standard. This means the system can be maintained without affecting overall operations, allowing for repairs while the system remains fully functional. The new, four-story building will be built on a 3,200-square-meter plot, complete with comprehensive data center support systems and dedicated office and meeting spaces to handle future situations.

A robust data center is the heart of the nationwide civil registration system, ensuring that civil registration data is managed quickly and accurately. Every time a person uses a service—whether it's getting a national ID card, registering a birth, or reporting a change of address—officials can instantly access data from the central database, reducing wait times. Furthermore, once the data is accurate and up-to-date in the system, it is automatically linked to other agencies, eliminating the need to repeatedly prepare the same documents for different government offices, such as hospitals, financial institutions, or even for registering for government welfare. This all helps to streamline people's daily lives.

SITEM is the company behind the project management. DOPA's goal isn't just about issuing documents but about making citizens' lives easier, more convenient, and free from complications.

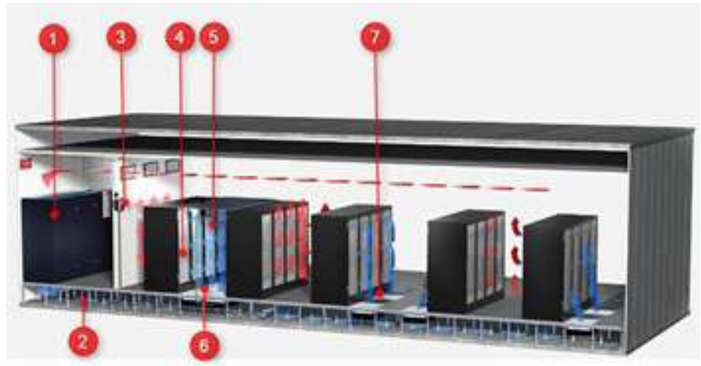


การเพิ่มประสิทธิภาพการทำงานสูงสุดด้วยตะแกรงระบายลมใต้พื้นแบบปรับองศาได้

การทำความเย็นแบบวงจรปิดผ่านพื้นยก (Raised Floor) ช่วยให้ ระบบปรับอากาศ ในห้อง Data Center สามารถตอบสนองต่อความต้องการที่เพิ่มขึ้นอย่างต่อเนื่อง ในด้านการลดต้นทุนการดำเนินงาน, เพิ่มความยืดหยุ่น และความเสถียรของระบบได้อย่างมีประสิทธิภาพ อย่างไรก็ตามในกรณีส่วนใหญ่ การไหลของอากาศที่ออกจากพื้นยกยังไม่ได้รับการควบคุมอย่างเหมาะสมนัก ในจุดนี้เองที่ตะแกรงระบายลมใต้พื้นยกซึ่งควบคุมด้วยเซ็นเซอร์และสามารถปรับองศาการเปิดได้ (Variable Opening Angle) ได้เข้ามามีบทบาทสำคัญในการ ช่วยลดการใช้พลังงานของ Precision Air Conditioning โดยปกติแล้ว ผู้ผลิตพื้นยกมักจะเป็นผู้จัดหาตะแกรงระบายลมมาให้พร้อมกัน ซึ่งลูกค้าสามารถเลือกระดับความโปร่งของตะแกรง (Perforation) ได้หลากหลาย ผู้ผลิตบางรายยังมีแผงควบคุม (Restrictor Panels) ที่ติดตั้งไว้ใต้ตะแกรงเพื่อปรับการไหลของอากาศด้วยตนเอง อัตราการไหลของอากาศที่แท้จริงนั้นขึ้นอยู่กับภาระการทำงาน (Load) ของเซิร์ฟเวอร์ในขณะนั้น แต่ในยุคของ Server Virtualization และ Cloud Technology ภาระการทำงานอาจเกิดความผันผวนอย่างรุนแรงจากการเปิด-ปิดการทำงานของ Rack ทั้งตู้ ด้วยเหตุนี้ Cooling Solution Data Center ที่ยืดหยุ่นจึงเป็นที่ต้องการอย่างมากสำหรับระบบทำความเย็นแบบวงจรปิด

ความท้าทายหลักคือการจ่ายลมเย็นให้กับเซิร์ฟเวอร์ในปริมาณที่เพียงพอและตรงจุดตามความต้องการใช้งานจริง คำว่า 'เพียงพอ' หมายถึงปริมาณลมที่จำเป็นต่อเซิร์ฟเวอร์ในขณะนั้นๆ จะต้องถูกปล่อยออกจากพื้นยกอย่างแม่นยำ และ 'ตรงจุด' หมายถึงลมเย็นจะต้องถูกปล่อยออกมาบริเวณด้านหน้าช่องรับลมของ Server Rack โดยตรงเท่าที่จะเป็นไปได้ ซึ่งประเด็นสุดท้ายนี้มีความสำคัญอย่างยิ่งในกรณีที่ไม่มีการกั้นโซนลมร้อนและลมเย็น (Hot/Cold Aisles) ออกจากกันอย่างชัดเจน การจ่ายลมเย็นตามความต้องการใช้งานจริง ณ บริเวณหน้าช่องรับลมของเซิร์ฟเวอร์จะช่วยลดการผสมกันของอากาศร้อนและเย็นให้เหลือน้อยที่สุด เราจึงอาจเรียกแนวคิดนี้ว่า "Virtual Containment"

STULZ ซึ่งเป็นผู้นำด้าน Precision Air Conditioning และเป็นที่รู้จักในนาม STULZ Thailand และ STULZ Siam ขอนำเสนอโซลูชัน AirModulator ที่ตอบโจทย์การใช้งานหลากหลายรูปแบบ ด้วยขนาดมาตรฐาน 600 x 600 มม. ทำให้สามารถติดตั้งร่วมกับพื้นยกที่มีจำหน่ายทั่วไปในท้องตลาดได้ทันที องศาการเปิดของบานเกล็ด (Damper) สามารถปรับเปลี่ยนได้ตามความต้องการผ่านระบบบริหารจัดการอาคาร (BMS) หรือผ่านชุดควบคุมของ AirModulator โดยอ้างอิงจากค่าอุณหภูมิหรือความแตกต่างของแรงดัน (Pressure Difference) และในกรณีที่เกิดไฟฟ้าดับ บานเกล็ดจะเปิดออกโดยอัตโนมัติด้วยสปริง (Return Spring) ตัวอุปกรณ์ทั้งหมดถูกประกอบอย่างสมบูรณ์พร้อมตะแกรงที่ออกแบบตามหลักอากาศพลศาสตร์ (Flow Optimized Grille) จึงมั่นใจได้ในความแข็งแรงทนทานต่อแรงกระทำต่างๆ เช่น รถยกของ เป็นต้น



1.Precision Cooling Units / เครื่อง ควบคุม อุณหภูมิ และ ความชื้น
2.พื้นยก (Raised Floor)
3.เซ็นเซอร์วัดความต่างของแรงดัน (ห้อง/พื้นยก)
4.ระบบกักเก็บความเย็น / การกั้นโซนลมเย็น (Containment System/Cold Aisle Enclosure)
5.เซ็นเซอร์วัดความต่างของแรงดัน (โซนลมเย็น/ห้อง)
6.ตะแกรงระบายลมควบคุมด้วยแรงดันหรือ BMS
7.ตะแกรงระบายลมควบคุมด้วยอุณหภูมิหรือ BMS

ข้อควรพิจารณาพิเศษสำหรับระบบกักเก็บความเย็น (Containment System)

ในทางอุดมคติ แรงดันสถิต (Static Pressure) ในพื้นยกที่สร้างขึ้นโดย Precision Air STULZ ควรถูกรักษาให้คงที่อยู่เสมอผ่าน ระบบควบคุมอุณหภูมิและความชื้น ในกรณีนี้ตัวตรวจจับความต่างของแรงดันที่กระจายอยู่ใต้พื้นยกจะส่งสัญญาณควบคุมไปยังเครื่องปรับอากาศห้องเซิร์ฟเวอร์ เพื่อปรับความเร็วของพัดลม ให้เหมาะสม

หากภาระความร้อน (Heat Load) ของเซิร์ฟเวอร์เพิ่มสูงขึ้น ก็จำเป็นต้องใช้ปริมาณลมเพื่อการระบายความร้อนมากขึ้น ส่งผลให้ความต่างของแรงดัน (ห้อง/พื้นยก) เปลี่ยนแปลงไป ซึ่งข้อมูลนี้จะถูกใช้เพื่อควบคุมการปล่อยลมเย็นสำหรับ แอร์ ห้อง server ทั้งหมด

เมื่อมีการใช้ระบบ Containment ใน Data Center ซึ่งมีการแบ่งโซนลมร้อนและลมเย็นออกจากกันอย่างชัดเจนด้วยผนังหรือฉากกั้น ห้องเซิร์ฟเวอร์ขนาดใหญ่จะถูกแบ่งออกเป็นหลายๆ โซนย่อยที่มีภาระการทำงานแตกต่างกันอย่างมาก หากโซนย่อยเหล่านี้รับลมเย็นจากพื้นยกเดียวกัน แรงดันภายในแต่ละโซนจะสามารถรักษาให้คงที่ได้ ก็ต่อเมื่อมีกลไกควบคุมความต่างของแรงดันอีกชุดหนึ่ง (โซนลมเย็น/ห้อง) ทำงานร่วมกับตะแกรงระบายลมที่ปรับระดับได้

ข้อมูลเพิ่มเติม: การทำความเย็นแบบวงจรปิดใน Data Center

โดยส่วนใหญ่แล้ว เซิร์ฟเวอร์ใน Data Center จะใช้หลักการทำความเย็นแบบวงจรปิด (Closed-Circuit Cooling) อากาศร้อนที่ถูกปล่อยออกมาจากเซิร์ฟเวอร์จะถูกทำให้เย็นลงอีกครั้งโดย Precision Air Conditioning หรือที่เรียกกันว่า แอร์ควบคุมความชื้น

โดยปกติแล้ว Server Rack ใน Data Center จะถูกจัดวางในรูปแบบของ Hot Aisle/Cold Aisle ซึ่งเป็นการวางสลับแถวระหว่างโซนลมร้อนและโซนลมเย็น ช่องรับลมของ Server Rack จะหันหน้าเข้าหากันในฝั่ง Cold Aisle และช่องระบายลมร้อนจะหันออกทางฝั่ง Hot Aisle อากาศจาก Hot Aisle จะถูกดูดกลับไปยัง แอร์ stulz เพื่อทำความเย็นให้ได้อุณหภูมิตามที่เซิร์ฟเวอร์ต้องการ จากนั้นอากาศเย็นจะถูกส่งผ่านพื้นยกไปยัง Cold Aisle และถูกปล่อยออกมาด้านหน้าเซิร์ฟเวอร์ผ่านตะแกรงระบายลมนั่นเอง หากคุณกำลังพิจารณา การออกแบบ แอร์ ห้อง server หรือต้องการ ติดตั้ง แอร์ ห้อง server การทำความเข้าใจหลักการนี้เป็นสิ่งสำคัญอย่างยิ่ง รวมถึงการ คำนวณ แอร์ ห้อง server ให้เหมาะสมกับภาระงานก็เป็นปัจจัยที่ไม่ควรมองข้าม เพื่อเพิ่มประสิทธิภาพของ Precision Cooling Units สามารถใช้ระบบที่เรียกว่า Containment Systems เพื่อป้องกันไม่ให้อากาศเย็นผสมกับอากาศร้อนได้ การแยกกระแสลมนี้จะช่วยให้ เครื่องควบคุมอุณหภูมิและ ความชื้น หรือปรับอากาศควบคุมความชื้น ทำงานโดยมีผลต่างของอุณหภูมิที่เหมาะสมที่สุด ซึ่งส่งผลให้ประหยัดพลังงานได้มากขึ้น

Maximizing Performance with Variable Opening Angle Underfloor Grilles

Closed-circuit cooling through a raised floor helps a data center's air conditioning system efficiently meet the ever-increasing demands for reduced operational costs, increased flexibility, and system stability. However, in most cases, the airflow exiting the raised floor is not adequately controlled.

This is where a sensor-controlled underfloor grille with a variable opening angle plays a crucial role in helping to reduce the energy consumption of a Precision Air Conditioning unit. Typically, raised floor manufacturers also supply the air grilles, which come with various perforation levels. Some manufacturers also provide manual restrictor panels installed beneath the grille to adjust airflow. The actual airflow rate depends on the server load at any given time. However, in the age of Server Virtualization and Cloud Technology, the load can fluctuate wildly as entire racks are turned on or off. For this reason, flexible data center cooling solutions are in high demand for closed-circuit cooling systems.

The main challenge is to supply servers with a sufficient and targeted amount of cool air based on their actual needs. The word 'sufficient' means the exact amount of air needed for the current server load must be released from the raised floor. 'Targeted' means the cool air must be released as directly as possible in front of the server rack's air intake vents. This last point is especially critical in cases where hot/cold aisles are not clearly separated. Supplying cool air according to actual demand at the server's air intake helps minimize the mixing of hot and cold air, a concept that can be called "Virtual Containment."

STULZ, a leader in Precision Air Conditioning, known as STULZ Thailand and STULZ Siam, offers the AirModulator solution, which meets a wide range of needs. With its standard size of 600 x 600 mm, it can be installed with most raised floors available on the market.

The damper's opening angle can be adjusted as needed via a Building Management System (BMS) or the AirModulator's own controller, based on temperature or pressure difference values. In the event of a power outage, the damper automatically opens with a return spring. The entire unit is fully assembled with an aerodynamically designed grille, ensuring high durability against various forces, such as forklifts.

1.Precision Cooling Units / Temperature and Humidity Control
2.Raised Floor
3.Pressure Difference Sensor (Room/Raised Floor)
4.Containment System/Cold Aisle Enclosure
5.Pressure Difference Sensor (Cold Aisle/Room)
6.Pressure- or BMS-Controlled Air Grille
7.Temperature- or BMS-Controlled Air Grille

Special Considerations for Containment Systems

Ideally, the static pressure in the raised floor created by the STULZ Precision Air unit should always be kept constant through the Temperature and Humidity Control System. In this case, pressure difference sensors distributed under the raised floor send control signals to the server room air conditioners to adjust fan speed as needed.

If the server's heat load increases, more air is needed for cooling, causing a change in the pressure difference (room/raised floor). This information is then used to control the cool air supply for all server room air conditioners.

When a Containment System is used in a data center to clearly separate hot and cold aisles with walls or partitions, a large server room is divided into several smaller zones with vastly different loads. If these sub-zones draw cool air from the same raised floor, the pressure within each zone can only be kept constant if another set of pressure difference control mechanisms (cold aisle/room) works in tandem with the adjustable air grilles.

Additional Information

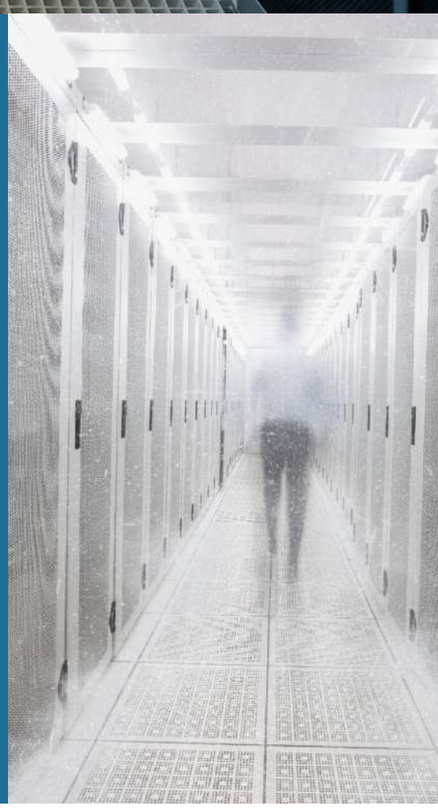
Closed-Circuit Cooling in Data Centers

Most data centers use a closed-circuit cooling principle. Hot air expelled from servers is cooled again by Precision Air Conditioning, also known as a humidity-controlled air conditioner.

Typically, server racks in a data center are arranged in a Hot Aisle/Cold Aisle layout, which involves alternating rows of hot and cold zones. The server rack's air intake vents face each other in the cold aisle, and the hot air exhaust vents face the hot aisle. Air from the hot aisle is drawn back into the STULZ air conditioner to be cooled to the temperature required by the servers. The cool air is then delivered through the raised floor to the cold aisle and released in front of the servers via the air grilles.

If you are considering a server room air conditioner design or need to install a server room air conditioner, understanding this principle is crucial. It is also essential to correctly calculate the server room air conditioner needs for the workload. To increase the efficiency of Precision Cooling Units, a system called Containment Systems can be used to prevent cool air from mixing with hot air. This airflow separation allows the Temperature and Humidity Control System to operate with the optimal temperature difference, resulting in greater energy savings

ที่มา บทความ โดย Uwe Kudszus



ภัยคุกคามไซเบอร์
แนวโน้มใหม่จากกลุ่ม Hacktivist ในช่วงต้นปี 2025

ในช่วงต้นปี 2025 ที่ผ่านมา วงการไซเบอร์ในประเทศไทยได้เผชิญกับคลื่นการโจมตีครั้งใหม่จากกลุ่มแฮกเกอร์หลายกลุ่มที่ประกาศตัวเป็น "Hacktivist" หรือนักเคลื่อนไหวทางการเมืองผ่านการแฮก กลุ่มเหล่านี้ไม่ได้มุ่งหวังผลประโยชน์ทางการเงิน แต่ต้องการสร้างแรงกระเพื่อมทางการเมืองและสังคม โดยพุ่งเป้าไปที่หน่วยงานภาครัฐและโครงสร้างพื้นฐานสำคัญของประเทศ

กลุ่มแฮกเกอร์ผู้เป็นภัยคุกคามใหม่ กลุ่มแฮกเกอร์ที่น่าจับตามอง ได้แก่ BL4CK CYB3R, NXBBSEC, H3C4KEDZ, K0LzSec, khmerghost และ ANONSEC-KH แม้แต่ละกลุ่มจะมีชื่อเรียกต่างกัน แต่มีเป้าหมายและเทคนิคการโจมตีที่คล้ายคลึงกัน คือการใช้การแฮกเป็นเครื่องมือในการแสดงออกทางการเมือง โดยเฉพาะในช่วงที่มีความขัดแย้งระหว่างประเทศ หนึ่งในเหตุการณ์ที่โดดเด่นคือการโจมตีแบบ DDoS (Distributed Denial-of-Service) ครั้งใหญ่ต่อเว็บไซต์ของรัฐบาลไทย ซึ่งกลุ่ม BL4CK CYB3R อ้างว่าเป็นผู้ลงมือ โดยใช้เครื่องมือที่มีชื่อว่า FoxC2 ซึ่งสามารถส่งคำร้องไปยังเซิร์ฟเวอร์เป้าหมายได้มากถึง 30,000 ครั้งต่อวินาที นอกจากนี้ยังมีการเผยแพร่ข้อความโจมตีเชิงการเมืองผ่านช่องทางสื่อสังคมออนไลน์ เช่น Telegram เพื่อสร้างกระแส

ในขณะที่กลุ่มอื่นๆ อย่าง NXBBSEC และ H3C4KEDZ มักจะใช้วิธี deface หรือการเปลี่ยนหน้าเว็บไซต์ของหน่วยงานรัฐ เพื่อโพสต์ข้อความเชิงชาตินิยมและสร้างความวุ่นวายบนโลกออนไลน์ ส่วนกลุ่มอย่าง K0LzSec และ khmerghost ก็มีแนวทางใกล้เคียงกัน โดยเล็งเป้าไปที่เว็บไซต์ของรัฐและระบบเครือข่ายขององค์กรต่างประเทศ เพื่อสื่อสารอุดมการณ์ทางการเมืองของตน

การโจมตีที่ไม่ได้หวังผลทางการเงิน

ลักษณะการโจมตีของกลุ่มเหล่านี้ชี้ให้เห็นถึงเป้าหมายที่เปลี่ยนไป พวกเขาไม่ได้ต้องการเงิน แต่ต้องการ สร้างความเสียหายทางภาพลักษณ์ ให้กับหน่วยงานภาครัฐของไทย และแสดงออกถึงความขัดแย้งทางอุดมการณ์ โดยเฉพาะในช่วงที่มีประเด็นทางการเมืองระหว่างประเทศ การเกิดขึ้นของกลุ่มแฮกเกอร์ประเภทนี้สะท้อนให้เห็นถึงภัยคุกคามทางไซเบอร์ในภูมิภาคอาเซียนที่กำลังพัฒนาไปอีกขั้น นั่นคือการผสานแนวคิดชาตินิยมเข้ากับเทคนิคการแฮกที่ซับซ้อน ทำให้หน่วยงานภาครัฐและองค์กรในไทยต้องเฝ้าระวังอย่างใกล้ชิดและยกระดับมาตรการป้องกันระบบสารสนเทศให้แข็งแกร่งยิ่งขึ้น

การป้องกันที่สำคัญที่สุด : Cyber Security

เพื่อรับมือกับภัยคุกคามเหล่านี้ การเสริมความแข็งแกร่งด้าน Cyber Security จึงเป็นสิ่งจำเป็นอย่างยิ่ง หน่วยงานต่างๆ ควรทบทวนและอัปเดตระบบรักษาความปลอดภัยอยู่เสมอ เพื่อป้องกันการโจมตีที่อาจเกิดขึ้นได้ตลอดเวลา

แนวทางการป้องกันภัยคุกคามทางไซเบอร์จากแฮกเกอร์

ภัยคุกคามทางไซเบอร์เป็นเรื่องใกล้ตัวที่ทุกคนควรให้ความสำคัญ ไม่ว่าจะเป็นบุคคลทั่วไปหรือองค์กร การป้องกันที่ดีที่สุดคือการสร้างความตระหนักและปฏิบัติตามแนวทางที่รัดกุมอย่างสม่ำเสมอ

สำหรับบุคคลทั่วไป

- รหัสผ่านที่รัดกุมและแตกต่าง: สร้างรหัสผ่านที่ซับซ้อนโดยผสมตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลข และสัญลักษณ์ และไม่ใช้รหัสผ่านเดียวกันซ้ำกันในหลายบัญชี
- เปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (MFA) : การใช้ MFA ช่วยเพิ่มความปลอดภัยอีกชั้นหนึ่ง โดยต้องยืนยันตัวตนผ่านช่องทางที่สอง เช่น รหัสผ่านที่ส่งไปยังโทรศัพท์มือถือ หรือแอปพลิเคชัน
- ระมัดระวังการคลิกลิงก์และไฟล์แนบ: ตรวจสอบความน่าเชื่อถือของอีเมลหรือข้อความก่อนคลิกลิงก์หรือดาวน์โหลดไฟล์แนบ โดยเฉพาะจากแหล่งที่ไม่รู้จัก เพราะอาจเป็นอีเมลฟิชชิ่ง (Phishing) ที่พยายามหลอกเอาข้อมูล
- อัปเดตซอฟต์แวร์สม่ำเสมอ: ตรวจสอบให้แน่ใจว่าระบบปฏิบัติการและแอปพลิเคชันต่างๆ ของคุณได้รับการอัปเดตอยู่เสมอ เพื่อปิดช่องโหว่ด้านความปลอดภัยที่แฮกเกอร์อาจใช้เป็นช่องทางในการโจมตี
- ติดตั้งโปรแกรมป้องกันไวรัสและไฟร์วอลล์: ใช้ซอฟต์แวร์ป้องกันไวรัสที่เชื่อถือได้และเปิดใช้งานไฟร์วอลล์ เพื่อช่วยตรวจจับและบล็อกมัลแวร์ (Malware) หรือการเข้าถึงที่ไม่ได้รับอนุญาต
- สำรองข้อมูลเป็นประจำ: หมั่นสำรองข้อมูลสำคัญเก็บไว้ในอุปกรณ์ภายนอกหรือระบบคลาวด์ เพื่อป้องกันข้อมูลสูญหายจากเหตุการณ์ต่างๆ เช่น การโจมตีด้วย Ransomware

สำหรับองค์กร

- สร้างนโยบายความปลอดภัยที่ชัดเจน: กำหนดกฎระเบียบและแนวปฏิบัติที่ชัดเจนเกี่ยวกับความปลอดภัยทางไซเบอร์ให้พนักงานทุกคนทราบ
- ฝึกอบรมพนักงานอย่างสม่ำเสมอ: จัดการฝึกอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามต่างๆ เช่น ฟิชชิ่ง และสอนวิธีรับมืออย่างถูกต้อง
- ใช้เครื่องมือรักษาความปลอดภัยที่ทันสมัย: ลงทุนในเทคโนโลยีและเครื่องมือรักษาความปลอดภัยขั้นสูง เช่น Intrusion Detection/Prevention Systems (IDS/IPS) และ Security Information and Event Management (SIEM)
- ทดสอบความปลอดภัยของระบบเป็นประจำ: ดำเนินการทดสอบเจาะระบบ (Penetration Testing) และประเมินช่องโหว่ (Vulnerability Assessment) เพื่อค้นหาจุดอ่อนในระบบและแก้ไขก่อนที่แฮกเกอร์จะค้นพบ
- วางแผนรับมือเหตุการณ์: จัดทำแผนการรับมือเหตุการณ์โจมตีทางไซเบอร์ (Incident Response Plan) ที่ชัดเจน เพื่อให้สามารถตอบสนองได้อย่างรวดเร็วและลดความเสียหายให้เหลือน้อยที่สุด
- จำกัดสิทธิ์การเข้าถึงข้อมูล: กำหนดสิทธิ์การเข้าถึงข้อมูลของพนักงานตามความจำเป็นของแต่ละตำแหน่งงาน (Principle of Least Privilege) เพื่อลดความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

การป้องกันภัยคุกคามทางไซเบอร์ไม่สามารถทำได้เพียงครั้งเดียว แต่ต้องเป็นกระบวนการต่อเนื่องที่ต้องมีการตรวจสอบและปรับปรุงอยู่เสมอ เพื่อให้ระบบมีความปลอดภัยและพร้อมรับมือกับภัยคุกคามที่เปลี่ยนแปลงไปตลอดเวลา บริษัท ไซโนริตี้ จำกัด (Sinority Co., Ltd.) เป็นบริษัทที่ปรึกษาด้านความปลอดภัยทางไซเบอร์ (Cybersecurity) ให้บริการโซลูชันและคำแนะนำด้านความปลอดภัยทางไซเบอร์แก่ธุรกิจหลากหลายขนาด เพื่อให้มั่นใจว่าข้อมูลและระบบของคุณจะปลอดภัยจากการโจมตีทางไซเบอร์ที่นับวันจะมีความซับซ้อนมากขึ้น

Cyber Threats: New Trends from Hacktivist Groups in Early 2025

In early 2025, the cybersecurity community in Thailand faced a new wave of attacks from several hacking groups that have declared themselves as "Hacktivists" or political activists who operate through hacking. These groups are not seeking financial gain; instead, they aim to create political and social ripples by targeting government agencies and critical national infrastructure.

The New Hacking Threat: Noteworthy Hacktivist Groups

The hacking groups to watch are BL4CK CYB3R, NXBBSEC, H3C4KEDZ, K0LzSec, Khmer ghost, and ANONSEC-KH. Although each group has a different name, they share similar goals and attack techniques: using hacking as a tool for political expression, especially during times of international conflict.

One notable incident was a massive DDoS (Distributed Denial-of-Service) attack on Thai government websites, which the BL4CK CYB3R group claimed responsibility for. They used a tool called FoxC2, which can send up to 30,000 requests per second to the target server. They also spread political messages through social media channels like Telegram to create public buzz.

Meanwhile, other groups like NXBBSEC and H3C4KEDZ often use deface attacks to alter government websites, posting nationalist messages to cause online disruption. Groups such as K0LzSec and Khmer ghosts follow a similar approach, targeting government websites and the networks of foreign organizations to communicate their political ideologies.

Attacks Not Aiming for Financial Gain

The nature of these attacks shows a shift in objectives. The groups are not after money but want to cause reputational damage to Thai government agencies and express ideological conflicts, particularly during periods of international political tension. The emergence of these hacktivist groups reflects a new stage in cyber threats in the ASEAN region, the combination of nationalist ideas with sophisticated hacking techniques. This makes it essential for government agencies and organizations in Thailand to be vigilant and strengthen their information system security measures.

The Most Important Defense: Cyber Security

To counter these threats, strengthening cybersecurity is crucial. Agencies should regularly review and update their security systems to prevent potential attacks at all times.

Cyber Threat Prevention Guidelines for Hackers

Cyber threats are a serious issue that everyone, from individuals to organizations, should prioritize. The best defense is to build awareness and consistently follow strict guidelines

For Individuals

- Create strong and unique passwords: Use complex passwords that mix uppercase and lowercase letters, numbers, and symbols. Do not reuse the same password across multiple accounts.
- Enable multi-factor authentication (MFA): Using MFA adds an extra layer of security, requiring you to verify your identity through a second channel, such as a code sent to your mobile phone or an authentication app.
- Be cautious when clicking links and attachments: Before clicking links or downloading attachments, check the credibility of the email or message, especially from unknown sources. This could be a phishing email attempting to trick you into giving away your information.
- Update software regularly: Make sure your operating systems and applications are always updated to patch security vulnerabilities that hackers might exploit.
- Install antivirus software and a firewall: Use reliable antivirus software and enable your firewall to help detect and block malware or unauthorized access.
- Back up your data regularly: Back up important data to an external device or a cloud system to prevent data loss from incidents like ransomware attacks.

For Organizations

- Establish clear security policies: Set clear rules and practices regarding cybersecurity for all employees.
- Provide regular employee training: Conduct training to raise awareness of threats like phishing and teach employees how to respond correctly.
- Use modern security tools: Invest in advanced security technologies and tools like Intrusion Detection/Prevention Systems (IDS/IPS) and Security Information and Event Management (SIEM).
- Regularly test system security: Perform penetration testing and vulnerability assessments to find and fix system weaknesses before hackers can discover them.
- Create an incident response plan: Develop a clear cyberattack incident response plan to ensure you can respond quickly and minimize damage.
- Limit data access rights: Grant employees data access rights only as needed for their job roles (the Principle of Least Privilege) to reduce the risk of unauthorized data access.

Cyber threat prevention is not a one-time task but a continuous process that requires regular review and improvement to keep systems secure and ready to face ever-changing threats. Sinority Co., Ltd. is a cybersecurity consulting firm that provides cybersecurity solutions and advice to businesses of all sizes, ensuring that your data and systems are safe from increasingly complex cyberattacks.

เก็บตกภาพบรรยากาศภายในงาน WUNCA ครั้งที่ 45

กลุ่มบริษัท ไซเท็ม (SITEM) ผู้ให้บริการโซลูชันด้านเทคโนโลยีสารสนเทศชั้นนำของประเทศไทย เข้าร่วมเป็นส่วนหนึ่งในการผลักดันนวัตกรรมเพื่อสนับสนุนการศึกษา กับงาน "การดำเนินกิจกรรมบนระบบเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา" หรือ WUNCA ครั้งที่ 45 (45th Workshop On Uninet Network And Computer Applications) ซึ่งเป็นงานใหญ่ประจำปีของวงการเครือข่ายสารสนเทศเพื่อการศึกษา โดยจัดขึ้นระหว่างวันที่ 3-5 กันยายน 2568 ณ มหาวิทยาลัยศรีนครินทรวิโรฒ ประสานมิตร

การเข้าร่วมงานในครั้งนี้ไม่เพียงแต่ตอกย้ำถึงศักยภาพของ SITEM ในฐานะผู้นำด้านเทคโนโลยีเท่านั้น แต่ยังสะท้อนให้เห็นถึงความมุ่งมั่นของบริษัทในการสนับสนุนและเป็นส่วนหนึ่งของการพัฒนาประเทศอย่างยั่งยืน

Highlights from WUNCA 45TH

SITEM Group, a leading IT solutions provider in Thailand, proudly participated in the 45th Workshop on UniNet Network and Computer Applications (WUNCA). This major annual event for the educational information network community was held from September 3-5, 2025, at Srinakharinwirot University, Prasarnmit Campus.

By joining this event, SITEM demonstrated its commitment to driving innovation and supporting the advancement of education. The company's participation not only reinforced its position as a technology leader but also highlighted its dedication to contributing to Thailand's sustainable development.

SITEM **ESG**

SITEM NEXT
SUSTAINABILITY

SITEM เราเชื่อว่าความสำเร็จที่แท้จริงไม่ได้จำกัดอยู่แค่การเติบโตทางธุรกิจเท่านั้น แต่คือการสร้างโลกที่ดีขึ้นและยั่งยืนขึ้นเพื่อทุกคน ความมุ่งมั่นในความรับผิดชอบต่อสังคมขององค์กร (CSR) เป็นส่วนสำคัญของตัวตนของเรา ซึ่งสะท้อนให้เห็นในนโยบาย 12 ข้อต่อไปนี้ที่ชี้นำการกระทำและขับเคลื่อนการเปลี่ยนแปลงเชิงบวกของเรา เราทุ่มเทที่จะสร้างผลกระทบที่ยั่งยืน เพื่อให้มั่นใจว่าอนาคตจะสดใสขึ้นสำหรับสิ่งแวดล้อม ชุมชน และโลกของเรา

SITEM, we believe that true success goes beyond business growth. It's about building a better, more sustainable world for everyone. Our commitment to corporate social responsibility (CSR) is an integral part of our identity, reflected in the following 12 policies that guide our actions and drive positive change. We are dedicated to creating a lasting impact, ensuring a brighter future for our environment, our communities, and our planet.

01
ออกแบบอย่างยั่งยืน
สร้างสรรค์สิ่งแวดล้อมที่คำนึงถึงวัสดุและพลังงานที่เป็นมิตร
Sustainable Design
Creating an environment that considers eco-friendly materials and energy.

02
หยุดใช้สารทำลายชั้นบรรยากาศ
เพื่ออนาคตที่เป็นมิตรต่อสิ่งแวดล้อม
Stop Using Ozone-Depleting Substances
For a More Eco-Friendly Future.

03
พลิกโฉมขยะเป็นขุมทรัพย์
เพื่อโลกที่ดีกว่า
Transforming Waste into Treasure
for a Better World.

04
มุ่งสู่โลกไร้กระดาษ
ลดการใช้ 50% ภายในปี 2570
Striving for a Paperless World
50% Reduction in Use by 2027.

05
แบ่งปันความรู้ ลดความเหลื่อมล้ำ
เพื่อประโยชน์ที่ยั่งยืน
Sharing Knowledge, Reducing Inequality
for Sustainable Benefits.

06
สร้างสรรค์สังคมที่เท่าเทียม
เคารพในศักดิ์ศรีมนุษย์ชน ปราศจากการเลือกปฏิบัติ
Creating an Equal Society
Respecting Human Dignity, Free from Discrimination.

07
จุดประกายอนาคต
มอบทุนการศึกษา สู่โอกาสที่ไม่สิ้นสุด
Igniting the Future
Providing Scholarships for Endless Opportunities.

08
สร้างบุคลากรคุณภาพ
มอบความรู้ สร้างโอกาสอาชีพเพื่ออนาคต
Developing Quality Personnel
Providing Knowledge, Creating Career Opportunities for the Future.

09
ของเหลือใช้ ไม่เหลือทิ้ง
สร้างสรรค์คุณค่าจากวัสดุเหลือใช้เพื่อชุมชน
Nothing Wasted, Everything Reused
Creating Value from Used Materials for the Community.

10
เสริมสร้างความปลอดภัย
ฝึกอบรมดับเพลิงและติดตั้งอุปกรณ์ให้ชุมชน
Enhancing Safety
Providing Firefighting Training and Equipment to Communities.

11
พลังแห่งการมีส่วนร่วม ขับเคลื่อน CSR
The Power of Participation Driving CSR

12
ยึดมั่นความโปร่งใส
ปลอดทุจริต ดำเนินธุรกิจตามกฎหมาย
Committed to Transparency
Free from Corruption, Operating Business According to the Law.

SITEM GROUP

PRO PROFESSIONAL | CORP CORPORATION | FM FACILITY MANAGEMENT | AVS AUDIO AND VISUAL SOLUTIONS | ST ENGINEERING AND SERVICE

88/14 Thetsabansongkhor Rd., Ladyao, Chatujak, Bangkok 10900
Call Center (24 Hrs.) +662 591 5000 | Fax : +662 589 2190 | www.sitemgroup.com

SITEM