



แบบเสนอโครงการ ประจำปีงบประมาณ พ.ศ. 2569  
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

- ชื่อโครงการ : ระบบรักษาความปลอดภัยเว็บไซต์สำหรับการเรียนรู้ออนไลน์
- หน่วยงานที่รับผิดชอบ : ฝ่ายวิศวกรรมระบบเครือข่าย  
ผู้รับผิดชอบ : นายจันทพงษ์ บุตรลักษณ์
- ความเชื่อมโยงสอดคล้องกับ แผนพัฒนาการศึกษาระดับอุดมศึกษา ฉบับที่ 13 ระยะกลางแผน (พ.ศ. 2568 - 2570)  
ประเด็นยุทธศาสตร์ที่ 4 ความเป็นเลิศด้านการจัดการ (Management Excellence)  
เป้าประสงค์ที่ 2 เป็นมหาวิทยาลัยดิจิทัล (Digital University)  
กลยุทธ์ 4.2.2 ปรับปรุงและพัฒนาระบบเครือข่าย สื่อสารเพื่อสนับสนุนพันธกิจของ มหาวิทยาลัยอย่างยั่งยืน
- ลักษณะโครงการ/กิจกรรม โครงการใหม่  
 โครงการใหม่  โครงการต่อเนื่อง  งานประจำ  งานพัฒนา
- การบูรณาการโครงการ  
 บูรณาการกับการเรียนการสอน  
มจพ. ทั้ง 3 วิทยาเขต  
 บูรณาการกับงานวิจัย  
 บูรณาการกับงานบริการวิชาการ  
 บูรณาการกับงานทำนุบำรุงศิลปวัฒนธรรม  
 อื่นๆ (บูรณาการโครงการระหว่างหน่วยงาน/โครงการ : ระบุชื่อหน่วยงาน/โครงการ ที่มีการบูรณาการ)
- หลักการและเหตุผลของโครงการ  
ในยุคดิจิทัลที่การใช้งานเทคโนโลยีสารสนเทศมีความสำคัญอย่างยิ่งต่อการดำเนินงานขององค์กรต่าง ๆ การบริหารจัดการด้านความปลอดภัยของข้อมูลในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ (KMUTNB) จึงเป็นภารกิจที่มีความสำคัญอย่างยิ่ง สำนักคอมพิวเตอร์ฯ  
ซึ่งเป็นผู้ดูแลโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศภายในมหาวิทยาลัย  
มีหน้าที่รับผิดชอบในการให้บริการระบบแม่ข่ายเสมือน (Virtual Servers) แก่คณะและหน่วยงานต่าง ๆ  
ปัจจุบันมีเครื่องแม่ข่ายเสมือนทั้งสิ้น 130 เครื่อง โดยมีเว็บไซต์ที่ให้บริการอยู่ทั้งหมด 221 เว็บไซต์ เช่น ระบบสารสนเทศเพื่องานทะเบียนนักศึกษา ระบบสารสนเทศทรัพยากรมนุษย์ ระบบจัดการบัญชีผู้ใช้งาน(ICIT

Account) ระบบวารสารมหาวิทยาลัย และเว็บไซต์ของหน่วยงาน เป็นต้น ซึ่งเว็บไซต์เหล่านี้ครอบคลุมถึงระบบข้อมูล การเรียนการสอน งานวิจัย และระบบบริหารจัดการต่าง ๆ  
ที่มีความสำคัญต่อการดำเนินงานของมหาวิทยาลัยอย่างมาก

อย่างไรก็ตาม ปริมาณการใช้งานระบบเว็บแอปพลิเคชันและจำนวนเว็บไซต์ที่เพิ่มขึ้นนี้ ส่งผลให้มหาวิทยาลัยต้องเผชิญกับความเสี่ยงจากการโจมตีทางไซเบอร์มากขึ้นอย่างหลีกเลี่ยงไม่ได้ การโจมตีทางไซเบอร์มีความหลากหลายทั้งในรูปแบบและความซับซ้อน เช่น การโจมตีแบบ SQL Injection, Cross-Site Scripting (XSS), หรือ Distributed Denial of Service (DDoS) ซึ่งสามารถทำให้ระบบเว็บไซต์หรือแอปพลิเคชันไม่สามารถให้บริการได้ การขาดระบบป้องกันที่เหมาะสม อาจทำให้ข้อมูลสำคัญของมหาวิทยาลัยเสี่ยงต่อการถูกขโมย ถูกทำลาย หรือถูกนำไปใช้ในทางที่ไม่เหมาะสม ซึ่งจะส่งผลกระทบต่อชื่อเสียงและความน่าเชื่อถือของมหาวิทยาลัยในระยะยาว

ระบบรักษาความปลอดภัยเว็บแอปพลิเคชันที่ใช้ในปัจจุบันเป็นระบบพื้นฐานที่มีข้อจำกัดในด้านประสิทธิภาพและการรองรับภัยคุกคามที่ซับซ้อนมากขึ้น ระบบดังกล่าวสามารถป้องกันภัยคุกคามได้เพียงบางส่วน แต่ไม่สามารถรับมือกับการโจมตีที่ทันสมัย เช่น การโจมตีด้วยมัลแวร์ที่มีการพัฒนาให้สามารถเจาะช่องโหว่ของระบบได้ง่ายขึ้น นอกจากนี้ ระบบรักษาความปลอดภัยเดิมยังมีข้อจำกัดในการอัปเดตเพื่อรองรับการเปลี่ยนแปลงและการพัฒนาในด้านความปลอดภัย ทำให้ระบบเสี่ยงต่อการถูกโจมตีและสร้างความเสียหายที่ไม่อาจประเมินค่าได้ หากมหาวิทยาลัยไม่สามารถปกป้องข้อมูลและระบบเว็บแอปพลิเคชันได้อย่างมีประสิทธิภาพ อาจก่อให้เกิดความเสียหายทางการเงินอย่างมหาศาลจากการสูญเสียข้อมูลสำคัญ การฟื้นฟูระบบที่เสียหาย รวมถึงการจัดการผลกระทบต่อชื่อเสียงขององค์กร ไม่เพียงเท่านั้น หากเกิดการโจมตีในช่วงเวลาที่มีความสำคัญ เช่น ช่วงการสอบ การลงทะเบียนเรียน หรือการเผยแพร่ผลงานวิจัย อาจส่งผลกระทบต่อประสบการณ์ของนักศึกษาและบุคลากรของมหาวิทยาลัย

รวมถึงทำให้บุคคลภายนอกที่ต้องการเข้าถึงข้อมูลของมหาวิทยาลัยเกิดความไม่พึงพอใจและสูญเสียความเชื่อมั่นในระบบการให้บริการของมหาวิทยาลัย

ด้วยเหตุนี้ สำนักคอมพิวเตอร์ฯ จึงมีความจำเป็นที่จะต้องจัดซื้อระบบรักษาความปลอดภัยเว็บแอปพลิเคชันใหม่ในรูปแบบของ Web Application Firewall (WAF) เพื่อทดแทนระบบเดิมที่ไม่สามารถตอบสนองความต้องการด้านความปลอดภัยได้อย่างมีประสิทธิภาพอีกต่อไป โดยอุปกรณ์ Web Application Firewall (WAF) ที่จัดหามาใหม่จะมีความสามารถในการป้องกันและกรองการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ รองรับการกรองข้อมูลด้วยความเร็ว 1Gbps ซึ่งเพียงพอสำหรับการใช้งานในปัจจุบันและสามารถขยายตัวในอนาคต การจัดหา WAF ใหม่ไม่เพียงแต่เป็นการปรับปรุงความปลอดภัยให้กับเว็บแอปพลิเคชันของมหาวิทยาลัยเท่านั้น แต่ยังเป็นการลงทุนที่คุ้มค่าในการปกป้องข้อมูลสำคัญของมหาวิทยาลัยในระยะยาว นอกจากนี้ การเปลี่ยนระบบรักษาความปลอดภัยให้ทันสมัยยังช่วยให้มหาวิทยาลัยสามารถรักษามาตรฐานการให้บริการข้อมูลที่มีความปลอดภัยและน่าเชื่อถือ ตลอดจนสร้างความมั่นใจให้กับผู้ใช้บริการทุกกลุ่ม

## 7. วัตถุประสงค์

7.1 เพื่อจัดหาระบบรักษาความปลอดภัยเว็บไซต์ทดแทนของเดิม

## 8. ตัวชี้วัดความสำเร็จระดับโครงการ (Output/Outcome) และ ค่าเป้าหมาย (ระบุหน่วยนับ)

ตัวชี้วัดความสำเร็จ	หน่วยนับ	ค่าเป้าหมาย
ปริมาณการใช้งาน(Throughput) สำหรับรักษาความปลอดภัยเว็บไซต์	Gbps	1

## 9. กลุ่มเป้าหมาย (ระบุกลุ่มเป้าหมายและจำนวนกลุ่มเป้าหมายที่เข้าร่วมโครงการ)

เว็บไซต์ทั้งหมดที่อยู่ภายใต้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน และบริการพื้นที่เว็บไซต์

## 10. ขั้นตอนการดำเนินการ :

ขั้นตอนการดำเนินการ	พ.ศ. 2568				พ.ศ. 2569							
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
1. ออกแบบ จัดทำข้อกำหนดคุณลักษณะเฉพาะ												
2. จัดซื้อ จัดจ้างและติดตั้ง												
3. สรุปผลและรายงานผลตามตัวชี้วัด												

## 11. ระยะเวลาดำเนินงาน : เริ่มต้น 1 ตุลาคม 2568 สิ้นสุด 31 มกราคม 2569

12. ประมาณการงบประมาณที่ใช้ : 3,940,000.00 บาท ( สามล้านเก้าแสนสี่หมื่นบาทถ้วน )

13. แหล่งเงิน/ประเภทงบประมาณที่ใช้/แผนงาน

งบประมาณแผ่นดิน

แผนงาน :

แผนงานบริหารการศึกษา

14. ประมาณการค่าใช้จ่าย : ( หน่วย : บาท )

ประเภทรายจ่าย	รวม	ไตรมาส 1	ไตรมาส 2	ไตรมาส 3	ไตรมาส 4
	แผนการใช้จ่าย	แผนการใช้จ่าย	แผนการใช้จ่าย	แผนการใช้จ่าย	แผนการใช้จ่าย
1. งบลงทุน					
1.1. ค่าครุภัณฑ์	3,940,000.00	3,940,000.00	-	-	-
รวมเงินงบประมาณ	3,940,000.00	3,940,000.00	-	-	-

15. ประโยชน์ที่คาดว่าจะได้รับ

15.1 ได้ระบบรักษาความปลอดภัยเว็บไซต์ตัวใหม่เพื่อทดแทนระบบเดิม

ลงชื่อ .....

( นายจันทพงษ์ บุตรลักษณ์ )

ผู้รับผิดชอบโครงการ

วันที่ ...../...../.....