การประสานงานในการเปิดเผยข้อบกพร่อง หรือ ช่องโหว่ทาง Cyber Security

***AIS** ให้ความสำคัญในความปลอดภัยของข้อมูลและระบบโครงสร้างพื้นฐานเป็นอันดับสูงสุด และมีความยินดีเปิดรับความประสงค์ดีของกลุ่มผู้เชี่ยวชาญทาง **Cyber Security** ที่จะรายงานข้อบกพร่อง หรือ ช่องโหว่ทาง **Cyber Security** ของเรา ดังนั้นเพื่อให้การรายงานข้อมูลดังกล่าวเป็นไปอย่างถูกต้องและมีประสิทธิภาพ ขอให้ท่านดำเนินการตามคำแนะนำในการรายงานข้อบกพร่อง หรือ ช่องโหว่ทาง **Cyber Security** ดังรายละเอียดด้านล่างนี้*

*ทั้งนี้ **AIS** ไม่มีนโยบายจะเสนอ **Bug Bounty Program** หรือ ค่าตอบแทนสำหรับการเปิดเผยข้อบกพร่องหรือช่องโหว่สำหรับผู้รายงาน อย่างไรก็ตาม **AIS** จะจดจำและขอขอบคุณในความปรารถนาดีนี้ของท่าน*

การรายงานข้อบกพร่อง หรือ ช่องโหว่ทาง Cyber Security (Report Submission)

*ข้อมูลข้อบกพร่อง หรือ ช่องโหว่ทาง **Cyber Security** เป็นข้อมูลที่มีความสำคัญ ท่านสามารถส่งรายงานมาที่อีเมล vulnerability@ais.co.th โดยการเข้ารหัสข้อมูลด้วย **PGP Public Key** ของเรา*

*ขอให้ท่านกรอกข้อมูลดังต่อไปนี้ ในรายงานข้อบกพร่อง หรือ ช่องโหว่ทาง **Cyber Security***

- *ชื่อ ชื่อบริษัท และข้อมูลติดต่อ*
- *ระบบที่ได้รับผลกระทบ*
- *รายละเอียดโดยสรุปของข้อบกพร่อง หรือ ช่องโหว่ความปลอดภัยที่ท่านพบ*
- *รายละเอียดข้อมูลสนับสนุนเชิงเทคนิค โดยอธิบาย หรือ แนบตัวอย่างการทดสอบระบบที่พบ เช่น **exploit** หรือ **attack code, packet captures, screen captures** รวมถึงขั้นตอนในการทดสอบระบบ*
- *แผนในการเปิดเผยข้อมูลนี้ (ถ้ามี)*

แนวทางความร่วมมือในการรายงานข้อบกพร่อง หรือ ช่องโหว่ทาง Cyber Security

- *บริษัทจะทำการตรวจสอบรายงานที่ท่านแจ้งมาโดยเร็วที่สุด*
- *ขอให้ท่านหลีกเลี่ยงการกระทำใดก็ตามที่จะเป็นการละเมิด ทำลาย เปลี่ยนแปลงข้อมูล หรือ ทำให้การให้บริการขัดข้อง รวมถึงการใช้เครื่องมือประเภท **Vulnerability Scanning Tools***
- *ขอให้ท่านระมัดระวังและจำกัดปริมาณข้อมูลที่ท่านใช้ให้น้อยที่สุดในการทำ **Proof Of Concept (POC)***
- *ขอให้ท่านไม่จัดเก็บ เผยแพร่ เข้าควบคุม หรือ ทำลายข้อมูลของบริษัท หรือ ข้อมูลลูกค้าของ **AIS** และหากมีการยุ่งเกี่ยว หรือ เข้าถึงข้อมูลที่ระบุตัวบุคคลได้ หรือ **Personally Identifiable Information (PII)** ท่านต้องหยุดการกระทำเหล่านั้นและลบข้อมูลเหล่านั้นออกจากระบบของท่านทันที*
- *ขอให้ท่านไม่วาง **Backdoor** บนระบบ หรือกระทำการอื่นใดที่ก่อให้เกิดข้อบกพร่องหรือช่องโหว่แก่ระบบ*
- *บริษัทจะเก็บข้อมูลทั้งหมดเป็นความลับและจะประสานงานกับท่าน เพื่อวิเคราะห์สาเหตุของปัญหาและหาแนวทางแก้ไขปัญหาโดยเร็วที่สุด*

- *หลังจากการประเมินหากพบว่าเป็นข้อบกพร่อง หรือ ช่องโหว่ทาง **Cyber Security** บริษัทจะดำเนินการเข้าควบคุม เตรียมการรับมือ และแจ้งแก่ผู้เกี่ยวข้องทั้งหมดเท่าที่จำเป็นบนพื้นฐานของความเสี่ยงที่เกี่ยวข้องกับข้อบกพร่อง หรือ ช่องโหว่นี้*
- *บริษัทขอให้ท่านไม่ทำการเปิดเผยข้อมูลใด ๆ ต่อสาธารณะ หรือ เผยแพร่ข้อมูลไปยังบุคคลที่สามจนกว่าเราจะสามารถเข้าใจถึงผลกระทบและดำเนินการปิดความเสี่ยงเหล่านั้นเสร็จสิ้นแล้ว*

สำหรับการกระทำอื่นใดที่ขัดต่อแนวทางฯ ข้างต้นจะถือว่าเป็นความไม่ประสงค์ดีต่อบริษัท

*สิ่งที่อยู่นอกขอบเขตการรายงานข้อบกพร่อง หรือ ช่องโหว่ทาง **Cyber Security***

*สิ่งที่อยู่นอกขอบเขตการรายงานข้อบกพร่อง หรือ ช่องโหว่ทาง **Cyber Security** ในระบบของบริษัท ได้แก่*

1. *การทดสอบระดับ **Physical***
2. ***Social Engineering***
3. ***Phishing***
4. ***Denial of Service Attacks***
5. *การโจมตีเพื่อให้ทรัพยากรของระบบไม่เพียงพอ*
6. *การใช้เทคนิคประเภท **Brute Force***

***AIS** ไม่สนับสนุนและไม่ยินยอมให้บุคคลกระทำการใด ๆ ที่เป็นการละเมิดต่อกฎหมาย*

ทางบริษัทขอขอบพระคุณท่านที่สละเวลาในการรายงานและช่วยให้เราสามารถปรับปรุงระบบของบริษัทให้มั่นคงและปลอดภัยยิ่งขึ้น