<u>แนวทางการรายงานความเป็นไปได้ของข้อบกพร่องหรือช่องโหว่ของความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)</u>

บริษัทฯ มีความยินดีเป็นอย่างยิ่งในการรับรายงานความเป็นไปได้ของข้อบกพร่องหรือช่องโหว่ทาง Cyber Security ของบริษัทฯ

เพื่อให้การรายงานข้อมูลเป็นไปอย่างถูกต้องและมีประสิทธิภาพ บริษัทฯ ขอให้ท่านปฏิบัติตามแนวทางดังต่อไปนี้ โดยบริษัทฯ ขอเรียนแจ้งให้ท่านทราบว่า บริษัทฯ ไม่มีนโยบายมอบค่าตอบแทนให้แก่ผู้รายงาน และขอขอบคุณในความปรารถนาดีของท่านมา ณ ที่นี้

ในกรณีที่ท่านพบความเป็นไปได้ของข้อบกพร่องหรือช่องโหว่ทาง Cyber Security ท่านสามารถส่งรายงานทางอีเมล Vulnerability@truecorp.co.th โดยแจ้งรายละเอียดดังต่อไปนี้

- ชื่อ และข้อมูลติดต่อของท่าน
- ระบบที่ได้รับผลกระทบ โดยสรุปข้อบกพร่องหรือช่องโหว่ทาง Cyber Security ที่ตรวจพบ
- รายละเอียดข้อมูลสนับสนุนเชิงเทคนิค โดยอธิบายหรือแนบตัวอย่างการทดสอบระบบที่พบ เช่น Exploit หรือ Attack code, Packet captures, Screen captures รวมถึงขั้นตอนในการทดสอบระบบ

บริษัทฯ จะดำเนินการตรวจสอบรายงานของท่าน และประสานงานกับท่านเพื่อวิเคราะห์สาเหตุของปัญหาและหาแนวทางแก้ไขโดยเร็วที่สุด โดยข้อมูลทั้งหมดของท่านจะถูกเก็บเป็นความลับ

ทั้งนี้ เพื่อป้องกันไม่ให้เกิดการละเมิดนโยบายคุ้มครองข้อมูลส่วนบุคคลและนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของบริษัทฯ บริษัทฯ ขอความร่วมมือจากท่านในการรายงานความเป็นไปได้ของข้อบกพร่องหรือช่องโหว่ทาง Cyber Security โดยปฏิบัติตามแนวทางดังต่อไปนี้

- หลีกเลี่ยงการกระทำใด ๆ ที่จะเป็นการละเมิด ทำลาย เปลี่ยนแปลงข้อมูล หรือทำให้การให้บริการขัดข้อง รวมถึงการใช้เครื่องมือประเภท Vulnerability Scanning Tools
- ระมัดระวังและจำกัดปริมาณข้อมูลที่ท่านใช้ในการทำ Proof Of Concept (POC) ให้น้อยที่สุด
- ไม่จัดเก็บ เผยแพร่ เข้าควบคุม หรือทำลายข้อมูลของบริษัทฯหรือข้อมูลผู้ใช้บริการของบริษัทฯ
- ในกรณีที่มีการเข้าถึงข้อมูลที่สามารถระบุตัวบุคคลได้ (Personally Identifiable Information : PII) ท่านต้องหยุดการกระทำดังกล่าวและลบข้อมูลข้างต้นออกจากระบบของท่านทันที
- ไม่วาง Backdoor บนระบบ หรือกระทำการอื่นใดที่ก่อให้เกิดข้อบกพร่องหรือช่องโหว่แก่ระบบ
- รักษาข้อมูลทั้งหมดที่เกี่ยวข้องกับข้อบกพร่องหรือช่องโหว่ทาง Cyber Security เป็นความลับและไม่เปิดเผยข้อมูลใด ๆ ต่อสาธารณะ หรือเผยแพร่ข้อมูลให้แก่บุคคลภายนอก

ทั้งนี้ บริษัทฯ ไม่สนับสนุนและไม่ยินยอมให้มีการกระทำการใด ๆ ที่ขัดต่อกฎหมาย การกระทำอื่นใดที่ขัดต่อแนวทางดังกล่าวจะถือเป็นความการสร้างความเสียหายให้แก่บริษัทฯ และบริษัทฯ มีสิทธิในการดำเนินการทางกฎหมายต่อผู้ที่เกี่ยวข้อง

การกระทำที่ถือเป็นการสร้างความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศของบริษัทฯ และการกระทำดังกล่าวไม่ถือว่าอยู่ในขอบเขตการดำเนินการเพื่อรายงานความเป็นไปได้ของข้อบกพร่องหรือช่องโหว่ทาง Cyber Security ได้แก่

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

เมื่อหน่วยงานได้ประเมินข้อบกพร่องหรือช่องโหว่ทาง Cyber Security แล้ว จะดำเนินการแจ้งผู้เกี่ยวข้องทั้งหมดเพื่อแก้ไขและปรับปรุงโครงสร้างพื้นฐานโดยเร็วที่สุดต่อไป ทั้งนี้ บริษัทฯ ขอขอบคุณท่านที่สละเวลาในการรายงานอันเป็นผลให้บริษัทฯ สามารถปรับปรุงระบบให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น