นโยบายพื้นฐานความปลอดภัยของข้อมูล

บริษัท ทรานสตรอน (ไทยแลนด์) จำกัด (บริษัทฯ) มีความมุ่งมั่นในการดำเนินธุรกิจภายใต้มาตรการการรักษาความปลอดภัยของข้อมูล, การรักษาความลับ, ความสมบูรณ์, ความพร้อมใช้งาน รวมถึงปฏิบัติตามกฎระเบียบข้อบังคับเพื่อให้คงอยู่ของวงจรชีวิตการจัดการความปลอดภัยของข้อมูล เพื่อป้องกันภัยคุกคาม การโจมตี การทำลายระบบสารสนเทศ และการจารกรรมข้อมูลทางไซเบอร์ โดยกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล โดยมีสาระสำคัญ ดังนี้

1) ปฏิบัติตามนโยบายด้านความปลอดภัยข้อมูลให้สอดคล้องกับบริษัทฟูจิตสึ (Fujitsu) เพื่อให้เกิดความปลอดภัยของระบบสารสนเทศ ความปลอดภัยของข้อมูลทั้งส่วนรวมและองค์กร
2) มีการประเมินและจัดการความเสี่ยงของระบบสารสนเทศเพื่อป้องกันความมั่งคงปลอดภัยของข้อมูล ตามความถี่ที่เหมาะสมให้ทันท่วงทีและทุกครั้งที่มีการเปลี่ยนแปลง
3) ตอบสนองต่อภัยคุกคามทางด้านความปลอดภัยของข้อมูลอย่างทันท่วงที เพื่อให้บริษัทสามารถดำเนินการด้านเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง พร้อมทั้งลดผลกระทบที่มี ต่อข้อมูลสารสนเทศ หรือเครือข่ายทางสารสนเทศให้น้อยที่สุด เพื่อให้ธุรกิจยังสามารถดำเนินงานได้อย่างต่อเนื่องและสร้างความเชื่อมั่นให้กับลูกค้าหรือผู้มีส่วนได้เสีย
4) การสร้างความรู้ ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยของข้อมูลให้กับบุคลากรในองค์กร โดยคำนึง ถึงความปลอดภัยของข้อมูลเป็นอันดับแรก

Basic Policy of Information Security.

TRANSTRON (THAILAND) CO., LTD (the Company) is committed to conducting business under measures of data security, confidentiality, integrity, availability. and comply with regulatory requirements to sustain the information security management lifecycle. To prevent threats, attacks, destruction of information systems and cyber espionage by establishing information security policies The important points are as follows:

1) Follow the information security policy in accordance with Fujitsu Company to ensure the security of information for public and corporate.
2) Information system risks are assessed and managed to protect information security. according to the appropriate frequency promptly and when any changes.
3) Prompt incidents response to information security threats so that the company can continue to operate information technology along with reducing the impact to system, the business can continue to operate and build confidence among customers or stakeholders.
4) Establishing the knowledge and awareness about Information security to all employees to regarding information security as the priority.

Effective Date: 17 Mar 2023

.....

(Mr. Tezuka Naoto)

President