INFORMATION SECURITY POLICY

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท เจริญโภคภัณฑ์อาหาร จำกัด (มหาชน) และบริษัทย่อย

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท เจริญโภคภัณฑ์อาหาร จำกัด (มหาชน) และบริษัทย่อย

Information Secuirty Policy

Charoen Pokphand Foods Public Company Limited and Subsidiaries

หลักการ / INTRODUCTION

เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินธุรกิจของบริษัท เจริญโภคภัณฑ์อาหาร จำกัด (มหาชน) และบริษัทย่อย (กลุ่มซีพีเอฟ) ทั้งในเรื่องของการบริหารจัดการ การจัดเก็บข้อมูลและการประมวลผลข้อมูล ทำให้การดำเนินงานมีความสะดวก รวดเร็ว มีประสิทธิภาพและเพิ่มโอกาสแข่งขันในทางธุรกิจได้มากขึ้น อย่างไรก็ตาม การนำเทคโนโลยีเข้ามาใช้อาจนำมาซึ่งความเสี่ยงจากภัยคุกคามหลายรูปแบบ ซึ่งหากไม่มีการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศที่เหมาะสมและรัดกุมเพียงพอ อาจทำให้สารสนเทศเหล่านั้นถูกเปิดเผย แก้ไขเปลี่ยนแปลง ทำลาย หรือสูญหายและอาจส่งผลกระทบต่อการดำเนินธุรกิจ ภาพลักษณ์และชื่อเสียงของกลุ่มซีพีเอฟได้ ผู้บริหารสูงสุดของกลุ่มซีพีเอฟจึงกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อใช้เป็นหลักในการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับการดำเนินงานและวัตถุประสงค์ในการดำเนินธุรกิจ และได้จัดทำมาตรฐานการปฏิบัติงานเรื่องความมั่นคงปลอดภัยด้านสารสนเทศขึ้นและกำหนดให้พนักงานของกลุ่มซีพีเอฟต้องปฏิบัติตามอย่างเคร่งครัด

Information Technology has become an essential role for Charoen Pokphand Foods Public Company Limited and its subsidiaries (CPF Group) in several areas of several business activities such as managing, storing and processing information. Such technology helps workers perform their assignments more efficiently, easily and faster as well as improves competitiveness for CPF Group. Nevertheless, Information Technology system may create grave risks. If mishandled, confidential information may be leaked, modified and lost. As a result of mismanagement of the information technology system, the performance of CPF Group may be impaired and reputation ruined. Chief Executive Officer of CPF Group has formulated this Information Security Policy to serves as a guideline on administering the Information Security Management System (ISMS) and to ensure that the practice of information security management is in accordance with the objectives and processes of CPF Group business and has established this Information Security Standard to be strictly enforced.

ขอบเขต / SCOPE OF POLICY

มาตรฐานการปฏิบัติงานความมั่นคงปลอดภัยด้านสารสนเทศครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยของสารสนเทศของกลุ่มซีพีเอฟ ทั้งที่อยู่ในสถานที่ปฏิบัติงานของกลุ่มซีพีเอฟ หรือของหน่วยงานภายนอกที่เกี่ยวข้อง ครอบคลุมถึง

1. พนักงานและหน่วยงานทั้งหมดของกลุ่มซีพีเอฟ
2. พนักงานและหน่วยงานภายนอกที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับสารสนเทศของกลุ่มซีพีเอฟ

Information security standard covers protecting and maintaining security of CPF Group's information both on the premises and off the premises as well as the following individuals:

1. Employee and all units within CPF Group
2. Outsourced individuals and external parties given access to CPF Group's information assets

นิยาม / DEFINATION

ความมั่นคงปลอดภัยด้านสารสนเทศ	:	การป้องกันสารสนเทศจากภัยคุกคามต่างๆ เพื่อทำให้มั่นใจว่าการดำเนินธุรกิจจะมีความต่อเนื่อง ลดความเสี่ยงทางธุรกิจ รวมถึงเพิ่มผลตอบแทนการลงทุนและโอกาสในการดำเนินธุรกิจของกลุ่มซีพีเอฟ
Information Security	:	Protection of information from a wide range of threats to ensure business continuity, minimize business risks as well as maximize return on investments and business opportunities.
กลุ่มซีพีเอฟ	:	บริษัท เจริญโภคภัณฑ์อาหาร จำกัด (มหาชน) และบริษัทย่อย
CPF Group	:	Charoen Pokphand Foods Public Company Limited and Subsidiaries.
การแจ้งเตือน (การแจ้งเตือนที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ)	:	การแจ้งเตือนเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศจากแหล่งต่างๆ ซึ่งรวมถึง บุคลากร ระบบและข้อมูลที่เปิดเผยต่อสาธารณะ
Alert (Information Security-related alert)	:	Information Security-related notification from various sources, including people, systems, and publicly available information.
การโจมตี	:	ความพยายามที่ได้รับอนุญาต หรือไม่ได้รับอนุญาต ไม่ว่าจะสำเร็จ หรือไม่ ในการทำลาย แก้ไข ปิดการใช้งาน เข้าถึงสินทรัพย์ หรือพยายามเปิดเผย ขโมย หรือใช้สินทรัพย์โดยไม่ได้รับอนุญาต
Attack	:	Successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an asset or any attempt to expose, steal, or make unauthorized use of an asset.
จุดอ่อน หรือช่องโหว่	:	เป็นสาเหตุ หรือข้อบกพร่องที่เป็นช่องทางที่ก่อให้เกิดภัยคุกคาม
Vulnerability	:	Weaknesses that can be exploited by one or more threats.

ทีมตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ	:	ทีมที่ได้รับการแต่งตั้งโดยเจ้าหน้าที่ความมั่นคงปลอดภัยด้านสารสนเทศที่ประกอบด้วยบุคลากรที่มีทักษะและประสบการณ์ที่เพียงพอและได้รับการจัดสรรทรัพยากรและอุปกรณ์อำนวยความสะดวกในการทำงานอย่างเหมาะสม ทำหน้าที่จัดการงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ ไม่ว่าจะเป็นเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ เหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ หรือช่องโหว่
Incident Response Team	:	A team appointed by Information Security Officer and composed of employee with adequate skills and experience and are provided with proper resources and facilities. It is responsible for handling information security case, which could be either events, incident or vulnerabilities.
เทคโนโลยีเชิงปฏิบัติงาน	:	Industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), programmable logic controllers (PLCs), Internet of Things (IoT), Robotics and Automation System และระบบอื่นๆ ที่ทำงานเกี่ยวกับ Industrial Control
Operational Technology	:	Industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), programmable logic controllers (PLCs), Internet of Things (IoT), Robotics and Automation System, and other systems performing industrial control functions.
เป้าหมายด้านข้อมูลของการกู้คืนสภาพ	:	จุดของข้อมูลล่าสุดที่ต้องสามารถนำกลับคืนมาได้เมื่อเกิดความเสียหายต่อระบบสารสนเทศ
Recovery Point Objective (RPO)	:	An acceptable point in time to which information needs to be recovered in the event of damage to the information systems.
เป้าหมายด้านระยะเวลาที่ใช้ในการกู้คืนสภาพ	:	ระยะเวลาสูงสุดที่ยอมรับได้ในการกู้คืนสภาพจากการหยุดชะงักของการปฏิบัติงานทางธุรกิจ การให้บริการ หรือระบบสารสนเทศให้กลับมาให้บริการได้ดังปกติจากจุดที่เกิดความเสียหาย หรือการหยุดชะงักอันเนื่องมาจากเหตุฉุกเฉิน หรือภัยพิบัติ
Recovery Time Objective (RTO)	:	Maximum tolerable period of recovery of disrupted business operation, service delivery or information systems in order to get back to normal

		operations after an incident or a disruption caused by disasters or emergencies.
โปรแกรมที่ไม่ประสงค์ดี	:	โปรแกรม หรือชุดโปรแกรมที่ทำให้สารสนเทศ หรือระบบสารสนเทศเกิดความเสียหายโดยตั้งใจ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) แอดแวร์ (Adware) หรือสปายแวร์ (Spyware) เป็นต้น
Malicious Software	:	A program or a set of programs which intentionally cause damage to information or information system such as Virus, Worm, Trojan, Adware and Spyware.
ภัยคุกคาม	:	เหตุการณ์ หรือสิ่งที่เกิดขึ้นจากภายใน หรือภายนอกและส่งผลเสียต่อทรัพย์สินของกลุ่มซีพีเอฟ
Threat	:	Potential causes which can be originated either internally or externally, as well as adversely affect CPF Group's assets.
เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ	:	เหตุการณ์ที่เกิดกับระบบ บริการ (Services) หรือเครือข่าย ที่บ่งชี้ว่าอาจมีการละเมิดนโยบายการปฏิบัติงานความมั่นคงปลอดภัยด้านสารสนเทศ หรือการล้มเหลวของการควบคุม หรือสถานการณ์ที่ไม่ทราบมาก่อนที่อาจเกี่ยวข้องกับความมั่นคงปลอดภัย ทั้งนี้ เหตุการณ์อาจมี หรือไม่มีผลกระทบกับกลุ่มซีพีเอฟ
Information Security Event	:	Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant. An event may or may not have a potential impact to CPF Group.
เหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ	:	เหตุการณ์เดียว หรือหลายเหตุการณ์ที่เกิดขึ้นอย่างต่อเนื่องโดยไม่เป็นที่ต้องการและไม่ได้คาดการณ์ไว้ ที่มีความเป็นไปได้ที่จะส่งผลกระทบต่อการดำเนินธุรกิจและเป็นอันตรายต่อความมั่นคงปลอดภัยด้านสารสนเทศ อีกนัยหนึ่ง เหตุการณ์ที่มีความเป็นไปได้ที่จะส่งผลกระทบต่อกลุ่มซีพีเอฟจะถูกพิจารณาเพื่อยืนยันว่าเป็นเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ
Information Security Incident	:	Single or a series of unwanted or unexpected events that have a significant probability of compromising business operations and

threatening information security. In other words, an event with potential impact to CPF Group will be considered and confirmed as an Incident.

หน่วยงานภายนอก : หน่วยงาน หรือบุคคลภายนอกที่ดำเนินธุรกิจ หรือให้บริการและอาจได้รับสิทธิเข้าถึงทรัพย์สินของกลุ่มซีพีเอฟ หน่วยงานภายนอกนี้ครอบคลุมดังนี้

(1) ผู้รับจ้างปฏิบัติงานให้กับกลุ่มซีพีเอฟ (Outsourcer) เช่น ผู้รับจ้างผลิตส่วนประกอบสินค้า ผู้รับจ้างผลิตโฆษณา ผู้รับจ้างผลิตบรรจุภัณฑ์ เป็นต้น

(2) ผู้รับจ้างพัฒนาระบบงาน หรือจัดหาวัสดุอุปกรณ์ต่างๆ (Supplier) เช่น ผู้พัฒนาระบบงานควบคุมการผลิต ผู้จำหน่ายอุปกรณ์คอมพิวเตอร์ เป็นต้น

(3) ผู้ให้บริการต่างๆ (Service Provider) เช่น ผู้ติดตั้งและบำรุงรักษาทรัพย์สินต่างๆ
ผู้ให้บริการโครงข่ายสื่อสาร ผู้ให้บริการอินเทอร์เน็ต เป็นต้น

(4) ที่ปรึกษา (Consultant) เช่น ที่ปรึกษาระบบงาน ERP เป็นต้น

(5) บริษัทคู่ค้า (Partner)

(6) หน่วยงานภายนอกอื่นใดที่ได้รับสิทธิเข้าถึงทรัพย์สิน หรือข้อมูลสารสนเทศขององค์กร

External Party : Any external organization or individual who works for CPF Group and is probably provided the access rights to CPF Group's assets. External parties include the following.

(1) Outsourcers – for example component manufacturers, advertising agencies and container manufacturers,

(2) Suppliers – for example developers of production control system and computer equipment distributors,

(3) Service Providers – for example provider responsible for installation and maintenance of assets, communication service provider and Internet Service Provider (ISP),

(4) Consultants – for example consultants for ERP system,

(5) IT Business partner,

(6) Other external parties who access to CPF Group's assets or information.

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

Information Security Policy

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022 เป็นกรอบการทำงานที่ครอบคลุมสำหรับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านสารสนเทศในทุกมิติ ตั้งแต่มาตรการกำกับดูแลขององค์กร (Organizational Controls) มาตรการด้านบุคลากร (People Controls) มาตรการรักษาความปลอดภัยทางกายภาพ (Physical Controls) และมาตรการ ป้องกันที่ขับเคลื่อนด้วยเทคโนโลยี (Technological Controls) มาตรการเหล่านี้ช่วยเสริมสร้างความแข็งแกร่งให้กับแนวทาง ด้านความมั่นคงปลอดภัยขององค์กร ทำให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปได้อย่างมีประสิทธิภาพ พร้อมทั้งรักษาการปฏิบัติตามมาตรฐานที่เกี่ยวข้อง

The Information Security Policy in accordance with ISO/IEC 27001:2022 is a comprehensive framework for managing information security risks in all dimensions. This includes:

(1) Organizational Control
(2) People Controls
(3) Physical Controls
(4) Technological Controls

These controls collectively strengthen the organization's security posture, enabling it to effectively respond to evolving cyber threats while ensuring ongoing compliance.

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย 4 เรื่อง ดังต่อไปนี้

Information Security Policy consists of the following four areas:

1. **มาตรการควบคุมด้านองค์กร (Organization Controls)**

   เพื่อให้มั่นใจว่าองค์กรมีแนวทางที่เป็นระบบและมีประสิทธิภาพในการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งรวมถึงการกำหนดนโยบาย กลยุทธ์และแนวทางที่ชัดเจนในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านสารสนเทศ องค์กรต้องกำหนดบทบาทและความรับผิดชอบต่อความมั่นคงปลอดภัยด้านสารสนเทศ นอกจากนี้ การส่งเสริมวัฒนธรรมและความตระหนักด้านความมั่นคงปลอดภัยภายในองค์กรถือเป็นปัจจัยสำคัญ องค์กรต้องมีการบริหารจัดการซัพพลายเออร์และบุคคลภายนอกอย่างเหมาะสม รวมถึงการปฏิบัติตามกฎหมาย ข้อบังคับและมาตรฐานที่เกี่ยวข้อง ซึ่งมาตรการเหล่านี้จะช่วยให้องค์กรมีการกำกับดูแลด้านความมั่นคงปลอดภัยที่สอดคล้องกับแนวปฏิบัติสากล ลดความเสี่ยงและสนับสนุนการดำเนินธุรกิจอย่างต่อเนื่อง

To ensure that the organization has a systematic and effective approach to managing information security. This includes establishing clear policies, strategies, and guidelines for managing security risks. The organization must define roles and responsibilities at all levels, ensuring accountability for information security. Additionally, fostering security awareness and culture within the organization is crucial. Organizations must also manage suppliers and third parties appropriately and comply with legal, regulatory, and industry-specific requirements. These measures ensure that security governance aligns with international best practices, minimizing risks and supporting business continuity.

2. **มาตรการควบคุมด้านบุคคลากร** (People Controls)

เพื่อให้บุคลากรในองค์กรเข้าใจบทบาทของตนในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งรวมถึงการสรรหาบุคลากรที่มีคุณสมบัติเหมาะสมสำหรับตำแหน่งที่เกี่ยวข้องกับข้อมูลสำคัญ การกำหนดหน้าที่และความรับผิดชอบที่ชัดเจนด้านความมั่นคงปลอดภัยและการให้การฝึกอบรมและการสร้างจิตสำนึกเกี่ยวกับภัยคุกคามทางไซเบอร์ องค์กรต้องมีมาตรการควบคุมการเข้าถึงข้อมูลและการจัดการสิทธิ์ของพนักงานอย่างเหมาะสม เมื่อเริ่มงาน เปลี่ยนตำแหน่ง หรือออกจากงาน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและลดความเสี่ยงที่อาจเกิดขึ้นจากการละเมิดความมั่นคงปลอดภัยของข้อมูลทั้งโดยเจตนาและไม่เจตนา

To ensure that individuals within the organization understand their role in maintaining information security. This involves hiring personnel with appropriate qualifications for roles involving sensitive information, clearly defining security-related responsibilities, and providing employees with training and awareness programs to mitigate cybersecurity threats. Organizations must also implement access control measures and manage privileges appropriately when employees join, change roles, or leave the company. This prevents unauthorized access to information and reduces the risk of intentional or unintentional security breaches.

3. **มาตรการควบคุมด้านกายภาพ** (Physical Controls)

เพื่อปกป้องข้อมูลและทรัพย์สินจากการเข้าถึงโดยไม่ได้รับอนุญาต การโจรกรรม ความเสียหาย หรือภัยธรรมชาติที่อาจเกิดขึ้น องค์กรต้องมีมาตรการควบคุมการเข้าถึงพื้นที่ที่ต้องการความปลอดภัยสูง หรือมีข้อมูลสำคัญ เช่น การใช้บัตรผ่าน ระบบตรวจสอบลายนิ้วมือ หรือใบหน้า หรือกล้องวงจรปิด เป็นต้น นอกจากนี้ ควรมีมาตรการรักษาความปลอดภัยสำหรับอุปกรณ์ที่ใช้ภายนอกองค์กร เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต อีกทั้งองค์กรต้องมีแนวทางที่เหมาะสมในการกำจัด หรือทำลายข้อมูลและอุปกรณ์ที่ไม่ใช้แล้ว เพื่อป้องกันการรั่วไหลของข้อมูลและรักษาการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

To protect information and assets from unauthorized physical access, theft, damage, or natural disasters. Organizations must implement access control mechanisms for secure areas or locations containing critical

information. These controls such as keycard access, biometric authentication, surveillance cameras. Additionally, security measures must be in place for devices used outside the organization to prevent unauthorized access. Secure disposal of obsolete information and devices is also essential to prevent data leakage and maintain compliance with security policies.

4. **มาตรการควบคุมด้านเทคโนโลยี** (Technological Controls)

เพื่อปกป้องข้อมูลและระบบสารสนเทศจากภัยคุกคามทางไซเบอร์ โดยใช้มาตรการทางเทคโนโลยี ซึ่งรวมถึงการกำหนดมาตรการควบคุมการเข้าถึง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต การเข้ารหัสข้อมูลที่สำคัญ เพื่อรักษาความลับของข้อมูลและการรักษาความปลอดภัยของเครือข่ายและช่องทางการสื่อสาร เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ องค์กรต้องมีการตรวจสอบและบันทึกกิจกรรมของระบบอย่างต่อเนื่อง เพื่อให้สามารถตรวจจับและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างรวดเร็ว นอกจากนี้ ควรมีการบริหารจัดการช่องโหว่และอัปเดตซอฟต์แวร์เป็นประจำ เพื่อป้องกันการถูกโจมตีจากผู้ไม่หวังดี อีกทั้งการสำรองข้อมูลและการมีแผนกู้คืนระบบถือเป็นสิ่งสำคัญเพื่อให้มั่นใจว่าธุรกิจสามารถดำเนินต่อไปได้แม้เกิดเหตุการณ์ที่ไม่คาดคิด เช่น การโจมตีทางไซเบอร์ หรือระบบขัดข้อง

To protect information and IT systems from cybersecurity threats using technological measures. This includes enforcing access controls to prevent unauthorized system access, encrypting sensitive data to maintain confidentiality, and securing networks and communication channels from cyber threats. Continuous monitoring and logging of system activities help detect and respond to security incidents promptly. Organizations must also implement vulnerability management and regular software updates to prevent exploitation by attackers. Furthermore, maintaining backups and having a disaster recovery plan ensures business continuity in case of unexpected incidents or cyberattacks.