



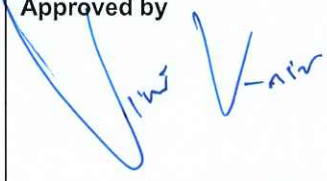


# Guideline on Appropriate Use of Information Technology Resources

Osotspa Public Company Limited and subsidiaries

**DIGITIZATION | SUPPLY CHAIN MANAGEMENT**

Effective 15 April 2023

<p>Prepared by</p>  <p>( Anupas Siriwej ) Head of Digital Service Excellence</p>	<p>Reviewed by</p>  <p>( Pajaree Saengcum ) Head of Digital Technology</p>	<p>Approved by</p>  <p>( Viwat Krisdhasima ) Chief Supply Chain and Digital Officer</p>
---	---	--



Unit / Division :		DIGITIZATION / SUPPLY CHAIN	
Document Type :		Guideline	
Document Number :		P-HM-ITD-001	Revision : 2
Effective Date :		15 April 2023	Page No. : 2 of 4
Reviewed by :		Approved by:	
( Pajaree Saengcum )		( Viwat Krisdhasima )	
Head of Digital Technology		Chief Supply Chain and Digital Officer	

**Subject :** Guideline on Appropriate Use of Information Technology Resources

## 1. Overview

Guideline on Appropriate Use of Information Technology Resources does not intend to impose restrictions in any ways contradicting to Osotspa Public Company Limited ("Osotspa")'s ITIP core values including Integrity, Teamwork, Innovative Thinking, Passion to Win and Sustainable Living. Instead, it intends to guide all employees, who are users of Information Technology (IT) resources, on the responsibility in exercising good judgment regarding appropriate use of IT resources and services in accordance with Osotspa policies and standards, relevant laws and regulations.

## 2. Purpose

The Guideline outlines the acceptable and appropriate use of Osotspa's IT resources and services. Compliance will help protect the employees and Osotspa from actions resulted in damages or regulatory violations, either knowingly or unknowingly, and from exposing Osotspa to risks on cyber-crime, cyber-attack, or network systems and services being compromised.

## 3. Scope

The Guideline applies to all users (e.g., employees, contractors, consultants, temporaries, and other workers) worldwide who are accessible to and/or use Osotpa's IT resources and services.

IT resources and services include, but are not limited to all company owned, leased, licensed, or managed hardware, software, data, systems, email, online/cloud services, and use of the Internet and company network, regardless of the ownership of the computer or device connected to the network.

## 4. Practical Guide

### 4.1 General Use and Ownership

1. Information stored on electronic and computing devices whether owned or leased by Osotspa, the employee or a third party, remains the sole property of Osotspa.
2. Theft, loss or unauthorized disclosure of Osotspa equipment or confidential information must be reported to IT Service Desk within 24 hours.
3. Osotspa's IT resources and services which you have an authorized access should be used only for business purposes to fulfill assigned job duties.
4. Personal use is generally prohibited, unless the usage is incidental and is at reasonable level.
5. You are individually held accountable for all resources assigned to you including the misuse of such resources.
6. You must abide by all applicable laws, including copyright laws and license agreements.
7. For security and network maintenance purposes, certain authorized individuals within Osotspa may monitor equipment, systems and network traffic at any time.



Unit / Division :		DIGITIZATION / SUPPLY CHAIN	
Document Type :		Guideline	
Document Number :		P-HM-ITD-001	Revision : 2
Effective Date :		15 April 2023	Page No. : 3 of 4
Reviewed by :		Approved by:	
( Pajaree Saengcum )		( Viwat Krisdhasima )	
Head of Digital Technology		Chief Supply Chain and Digital Officer	

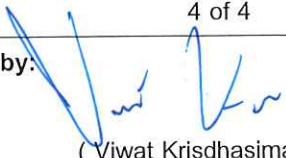
**Subject :** Guideline on Appropriate Use of Information Technology Resources

#### 4.2 Inappropriate Use

The following activities are prohibited:

1. Using IT resources and services for illegal or unlawful activity.
2. Using IT resources and services for any commercial activity for personal gain.
3. Using personal email account, rather than business email account, for business purposes.
4. Accessing IT resources and services without proper authentication procedure or intentionally enable others to do so.
5. Sharing account password to others or allowing others to use your account, either deliberately or through failure to secure its access.
6. Attempting to install, modify, relocate, or remove computing/network equipment, software, or peripherals unless prior notification to IT Service Desk is made and approved.
7. Deliberate activities having, with reasonable likelihood, any of the following characteristics:
  - a) Introduction of malicious programs into the network or computer (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
  - b) Disrupting network, other computer or users, or damaging software or hardware components of a system, including data.
  - c) Degrading performance of the network or system by excessive usage (e.g., sending chain letters or excessive messages, use an excessive amount of network bandwidth, etc.)
  - d) Accessing data of which you are not an intended recipient or logging into a server or account that you are not authorized to access unless these duties are within the scope of regular duties.
  - e) Attempting to access restricted portions of the network, system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
  - f) Using tools that are normally used to assess security or to attack computer systems or networks (e.g., password crackers, vulnerability scanners, data interception, etc.) unless you have been specifically authorized to do so.
  - g) Violating the privacy of other users.
8. Providing trade secrets, confidential, or proprietary information to parties outside Osotspa.
9. Downloading, use, copying, or distribution of copyrighted work or other intellectual property, including but not limited to, software, photographs, graphics, music, film clips, trademarks and logos, unless you have a legal right to do so.
10. Sending or posting message, image, or other material containing offensive, obscene, indecent, aggressive, menacing, harassing, defamatory, intimidating, unlawful, racist and other unethical messages.
11. Sending or posting unsolicited/bulk message (spam), or other advertising material to individuals who did not specifically request such material and not related to Osotspa's activities.



Unit / Division :	DIGITIZATION / SUPPLY CHAIN		
Document Type :	Guideline		
Document Number :	P-HM-ITD-001	Revision :	2
Effective Date :	15 April 2023	Page No. :	4 of 4
Reviewed by :	 ( Pajaree Saengcum ) Head of Digital Technology		
	 ( Viwat Krisdhasima ) Chief Supply Chain and Digital Officer		

**Subject :** Guideline on Appropriate Use of Information Technology Resources

12. Sending or posting message that may harm or tarnish the image, reputation and/or goodwill of Osotspa and/or any of its employees or customers. If expressing beliefs and/or opinions in social media, you may not, explicitly or implicitly, represent yourself as an employee or representative of Osotspa.

In case of doubt or uncertainty, you should consult your supervisor or manager. Violation may lead to disciplinary action, up to and including termination of employment, including possible legal action if involving unlawful activity.

#### 5. Related Policies and Guidelines

- Code of Conduct (Company Asset Policy Statement)
- Information Technology Policy
- Information Safeguarding Guideline
- Personal Data Protection Policy

## Guideline on Appropriate Use of Information Technology Resources

### 1. Overview

Guideline on Appropriate Use of Information Technology Resources does not intend to impose restrictions in any ways contradicting to Osotspa Public Company Limited ("Osotspa")'s ITIPS core values including Integrity, Teamwork, Innovative Thinking, Passion to Win, and Sustainable Living. Instead, it intends to guide all employees, who are users of Information Technology (IT) resources, on the responsibility in exercising good judgment regarding appropriate use of IT resources and services in accordance with Osotspa policies and standards, relevant laws and regulations.

### 2. Purpose

The Guideline outlines the acceptable and appropriate use of Osotspa's IT resources and services. Compliance will help protect the employees and Osotspa from actions resulted in damages or regulatory violations, either knowingly or unknowingly, and from exposing Osotspa to risks on cyber-crime, cyber-attack, or network systems and services being compromised.

### 3. Scope

The Guideline applies to all users (e.g., employees, contractors, consultants, temporaries, and other workers) worldwide who are accessible to and/or use Osotspa's IT resources and services.

IT resources and services include, but are not limited to all company owned, leased, licensed, or managed hardware, software, data, systems, email, online/cloud services, and use of the Internet and company network, regardless of the ownership of the computer or device connected to the network.

### 4. Practical Guide

#### 4.1 General Use and Ownership

1. Information stored on electronic and computing devices whether owned or leased by Osotspa, the employee or a third party, remains the sole property of Osotspa.
2. Theft, loss, or unauthorized disclosure of Osotspa equipment or confidential information must be reported to IT Service Desk within 24 hours.
3. Osotspa's IT resources and services which you have an authorized access should be used only for business purposes to fulfill assigned job duties.
4. Personal use is generally prohibited, unless the usage is incidental and is at reasonable level.
5. You are individually held accountable for all resources assigned to you including the misuse of such resources.
6. You must abide by all applicable laws, including copyright laws and license agreements.
7. For security and network maintenance purposes, certain authorized individuals within Osotspa may monitor equipment, systems and network traffic at any time.

#### 4.2 Inappropriate Use

The following activities are prohibited:

1. Using IT resources and services for illegal or unlawful activity.
2. Using IT resources and services for any commercial activity for personal gain.
3. Using personal email account, rather than business email account, for business purposes.
4. Accessing IT resources and services without proper authentication procedure or intentionally enable others to do so.
5. Sharing account password to others or allowing others to use your account, either deliberately or through failure to secure its access.
6. Attempting to install, modify, relocate, or remove computing/network equipment, software, or peripherals unless prior notification to IT Service Desk is made and approved.
7. Deliberate activities having, with reasonable likelihood, any of the following characteristics:
  - a) Introduction of malicious programs into the network or computer (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
  - b) Disrupting network, other computer or users, or damaging software or hardware components of a system, including data.
  - c) Degrading performance of the network or system by excessive usage (e.g., sending chain letters or excessive messages, use an excessive amount of network bandwidth, etc.)

- d) Accessing data of which you are not an intended recipient or logging into a server or account that you are not authorized to access unless these duties are within the scope of regular duties.
  - e) Attempting to access restricted portions of the network, system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
  - f) Using tools that are normally used to assess security or to attack computer systems or networks (e.g., password crackers, vulnerability scanners, data interception, etc.) unless you have been specifically authorized to do so.
  - g) Violating the privacy of other users.
8. Providing trade secrets, confidential, or proprietary information to parties outside Osotspa.
  9. Downloading, use, copying, or distribution of copyrighted work or other intellectual property, including but not limited to, software, photographs, graphics, music, film clips, trademarks and logos, unless you have a legal right to do so.
  10. Sending or posting message, image, or other material containing offensive, obscene, indecent, aggressive, menacing, harassing, defamatory, intimidating, unlawful, racist and other unethical messages.
  11. Sending or posting unsolicited/bulk message (spam), or other advertising material to individuals who did not specifically request such material and not related to Osotspa's activities.
  12. Sending or posting message that may harm or tarnish the image, reputation and/or goodwill of Osotspa and/or any of its employees or customers. If expressing beliefs and/or opinions in social media, you may not, explicitly or implicitly, represent yourself as an employee or representative of Osotspa.

In case of doubt or uncertainty, you should consult your supervisor or manager. Violation may lead to disciplinary action, up to and including termination of employment, including possible legal action if involving unlawful activity.

#### 5. Related Policies and Guidelines

- Code of Conduct (Company Asset Policy Statement)
- Information Technology Policy
- Information Safeguarding Guideline
- Personal Data Protection Policy

#### 6. User Agreement

I have read, understand, and will abide by the above Guideline. I understand that violations can result in revocation of Osotspa's IT resources and services, and subject me to potential disciplinary and possible legal actions.

Signature: \_\_\_\_\_

Full Name: \_\_\_\_\_

Employee ID: \_\_\_\_\_

Position: \_\_\_\_\_

Department: \_\_\_\_\_

Company: \_\_\_\_\_

Date: \_\_\_\_\_

## แนวปฏิบัติการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ

### 1. บทนำ

แนวปฏิบัติการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศนี้ไม่ได้มีวัตถุประสงค์ในการกำหนดข้อจำกัดที่ขัดแย้งกับค่านิยมองค์กร "ITIPS" ของบริษัท โอเอสเอสพี จำกัด (มหาชน) ("บริษัทฯ") ได้แก่ มีคุณธรรมและมีความรับผิดชอบ การทำงานเป็นทีม ความคิดริเริ่มสร้างสรรค์ มุ่งมั่นคว้าชัยชนะ ยึดมั่นและมีจิตสำนึกด้านความยั่งยืน แต่เพื่อกำหนดแนวปฏิบัติให้พนักงานทุกคนมีความรับผิดชอบและใช้วิจารณญาณในการใช้ทรัพยากรและบริการด้านเทคโนโลยีสารสนเทศให้เป็นไปตามนโยบายและมาตรฐานของบริษัท ตลอดจนกฎหมายและระเบียบข้อบังคับอื่นที่เกี่ยวข้อง

### 2. วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติการใช้ทรัพยากรและบริการด้านเทคโนโลยีสารสนเทศของบริษัทฯ การปฏิบัติตามแนวทางนี้จะช่วยป้องกันพนักงานและบริษัทฯ จากผลการกระทำโดยเจตนาหรือไม่ก็ตาม ที่สร้างความเสียหายหรือฝ่าฝืนกฎระเบียบ และทำให้บริษัทฯ มีความเสี่ยงจากอาชญากรรมและการถูกโจมตีทางไซเบอร์ หรือการที่บริการและระบบเครือข่ายของบริษัทถูกบุกรุก

### 3. ขอบเขต

แนวปฏิบัตินี้มีผลบังคับใช้กับพนักงานทุกคน เช่น พนักงานประจำ พนักงานตามสัญญาจ้าง ที่ปรึกษา พนักงานชั่วคราว และคนงานอื่นๆ ที่เข้าถึง และ/หรือ ใช้ทรัพยากรและบริการด้านเทคโนโลยีสารสนเทศของบริษัทฯ

ทรัพยากรและบริการด้านเทคโนโลยีสารสนเทศ หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ ที่บริษัทฯ เป็นเจ้าของ/เช่า/ได้รับสิทธิการใช้งาน/บริหารจัดการ ข้อมูล ระบบ อีเมล บริการออนไลน์ คลาวด์ การใช้อินเทอร์เน็ตและเครือข่ายของบริษัทฯ โดยเชื่อมต่อจากอุปกรณ์ของบริษัทฯ หรืออุปกรณ์ส่วนตัว เป็นต้น

### 4. แนวปฏิบัติ

#### 4.1 การใช้งานทั่วไปและความเป็นเจ้าของ

1. ข้อมูลของบริษัทฯ ที่ถูกจัดเก็บอยู่ในอุปกรณ์คอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ ทั้งที่เป็นของบริษัทฯ พนักงาน หรือบุคคลที่สาม ยังคงเป็นทรัพย์สินของบริษัทฯ แต่เพียงผู้เดียว

2. ผู้ใช้งานจะต้องแจ้ง IT Service Desk ภายใน 24 ชั่วโมง เมื่ออุปกรณ์หรือข้อมูลที่เป็นความลับของบริษัทฯ ถูกขโมย สูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต
3. ผู้ใช้งานควรใช้ทรัพยากรและบริการด้านเทคโนโลยีสารสนเทศของบริษัทฯ ที่ตัวเองมีสิทธิ์เข้าถึง ในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมายเพื่อวัตถุประสงค์ทางธุรกิจของบริษัทฯ เท่านั้น
4. ห้ามผู้ใช้งานใช้ทรัพยากรและบริการด้านเทคโนโลยีสารสนเทศของบริษัทฯ เพื่อประโยชน์ส่วนตัว เว้นแต่เป็นการใช้งานโดยบังเอิญและสมเหตุสมผล
5. ผู้ใช้งานต้องรับผิดชอบต่อทรัพยากรและบริการด้านเทคโนโลยีสารสนเทศทั้งหมดที่บริษัทฯ จัดให้ รวมถึงผลที่เกิดขึ้นจากการใช้งานในทางที่ผิด
6. ผู้ใช้งานต้องปฏิบัติตามกฎหมายที่บังคับใช้ทั้งหมด เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมถึงกฎหมายลิขสิทธิ์และข้อตกลงสิทธิ์การใช้
7. บริษัทฯ อาจตรวจสอบอุปกรณ์ ระบบ และการรับส่งข้อมูลผ่านเครือข่ายได้ตลอดเวลา เพื่อความมั่นคงปลอดภัยและการบำรุงรักษาเครือข่าย

#### 4.2 การใช้งานที่ไม่เหมาะสม

ห้ามผู้ใช้งานกระทำการหรือดำเนินการใดๆ ที่มีลักษณะดังต่อไปนี้

1. ใช้ทรัพยากรและบริการด้านเทคโนโลยีสารสนเทศเพื่อการกระทำที่ผิดกฎหมายหรือไม่เป็นไปตามกฎระเบียบ
2. ใช้ทรัพยากรและบริการด้านเทคโนโลยีสารสนเทศเพื่อการค้าหรือการแสวงหาผลกำไรในผลประโยชน์ส่วนตัว
3. ใช้อีเมลส่วนตัวเพื่อวัตถุประสงค์ทางธุรกิจของบริษัทฯ
4. เข้าถึงหรือจงใจให้ผู้อื่นเข้าถึงทรัพยากรและบริการด้านเทคโนโลยีสารสนเทศ โดยไม่ผ่านขั้นตอนการยืนยันตัวตนตามที่กำหนดไว้
5. แบ่งปันรหัสผ่านกับผู้อื่น หรืออนุญาตให้ผู้อื่นใช้บัญชีของตัวเอง ไม่ว่าจะโดยเจตนาหรือไม่มีการป้องกันอย่างเหมาะสม
6. พยายามติดตั้ง ปรับเปลี่ยน โยกย้าย หรือถอดถอน อุปกรณ์คอมพิวเตอร์ เครือข่าย ซอฟต์แวร์ หรืออุปกรณ์ต่อพ่วง เว้น

แต่จะมีการแจ้งให้ IT Service Desk ทราบล่วงหน้า และได้รับอนุญาตให้ดำเนินการแล้วเท่านั้น

7. เจตนากระทำการอย่างใดอย่างหนึ่ง ซึ่งมีลักษณะดังต่อไปนี้
  - a) นำโปรแกรมที่ประสงค์ร้าย (มัลแวร์) เข้าสู่เครือข่ายหรือคอมพิวเตอร์ เช่น ไวรัส เวิร์ม ม้าโทรจัน เป็นต้น
  - b) ทำให้เครือข่าย คอมพิวเตอร์ หรือผู้ใช้งานอื่นไม่สามารถใช้งานได้ หรือทำให้ซอฟต์แวร์หรือฮาร์ดแวร์ของระบบรวมถึงข้อมูลเกิดความเสียหาย
  - c) ทำให้เครือข่ายหรือระบบมีประสิทธิภาพลดลงจากการใช้งานที่มากเกินไป เช่น การส่งจดหมายลูกโซ่ การรับส่งข้อมูลที่มากเกินไป เป็นต้น
  - d) เข้าถึงข้อมูลซึ่งตัวเองไม่ใช่ผู้รับที่ตั้งใจไว้ หรือเข้าสู่เซิร์ฟเวอร์หรือบัญชีผู้ใช้ที่ตัวเองไม่ได้ได้รับอนุญาตให้เข้าถึง เว้นแต่จะเป็นการกระทำที่อยู่ในขอบเขตการปฏิบัติหน้าที่ตามปกติ
  - e) พยายามเข้าถึงส่วนที่ถูกป้องกันของเครือข่าย ระบบซอฟต์แวร์ความปลอดภัย หรือแอปพลิเคชันการดูแลระบบอื่นๆ โดยไม่ได้รับอนุญาตจากเจ้าของหรือผู้ดูแลระบบ
  - f) ใช้เครื่องมือสำหรับประเมินความมั่นคงปลอดภัยหรือโจมตีระบบคอมพิวเตอร์หรือเครือข่าย เช่น โปรแกรมถอดรหัสผ่าน โปรแกรมสแกนช่องโหว่ โปรแกรมสกัดกั้นข้อมูล เป็นต้น เว้นแต่จะได้รับอนุญาตเป็นการเฉพาะ
  - g) ละเมิดความเป็นส่วนตัวของผู้ใช้งานอื่น
8. เปิดเผยความลับทางการค้า ข้อมูลที่เป็นความลับ หรือข้อมูลที่เป็นกรรมสิทธิ์ ให้แก่บุคคลภายนอกบริษัท
9. ดาวน์โหลด ใช้ คัดลอก หรือแจกจ่ายงานที่มีลิขสิทธิ์ หรือทรัพย์สินทางปัญญาอื่นๆ รวมถึงแต่ไม่จำกัดเพียง ซอฟต์แวร์ ภาพถ่าย กราฟิก เพลง คลิปภาพยนตร์ เครื่องหมายการค้า และโลโก้ เว้นแต่มีสิทธิ์ตามกฎหมายที่จะทำเช่นนั้น
10. ส่งหรือโพสต์ข้อความ รูปภาพ หรือเนื้อหาอื่นๆ ที่มีข้อความที่ไม่เหมาะสม ลามกอนาจาร หยาบคาย ก้าวร้าว คุกคาม ล่วงละเมิด ทำให้เสื่อมเสียชื่อเสียง ช่มชู้ ผิดกฎหมาย เหยียดเชื้อชาติ และข้อความที่ผิดจรรยาบรรณอื่นๆ
11. ส่งหรือโพสต์ข้อความไม่พึงประสงค์หรือข้อความจำนวนมาก (สแปม) หรือสื่อบริษัทอื่นๆ ให้กับบุคคลที่ไม่ได้ขอรับข้อความหรือสื่อดังกล่าวโดยเฉพาะ และไม่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท

12. ส่งหรือโพสต์ข้อความที่อาจก่อให้เกิดความเสียหายหรือเสื่อมเสียต่อภาพลักษณ์ ชื่อเสียง และ/หรือ ค่าความนิยมของบริษัท และ/หรือ พนักงานหรือลูกค้าของบริษัท หากต้องการแสดงความเชื่อหรือความคิดเห็นของตนเองในสื่อสังคมออนไลน์ ห้ามแสดงตนว่าเป็นพนักงานหรือตัวแทนของบริษัท ไม่ว่าจะโดยชัดแจ้งหรือโดยปริยาย ทั้งนี้ หากพบเห็นข้อความที่คิดว่าไม่เหมาะสม ให้แจ้งหน่วยงานที่เกี่ยวข้องเพื่อดำเนินการต่อไป

หากมีข้อสงสัยหรือเกิดความไม่แน่ใจให้ปรึกษากับหัวหน้างานหรือผู้จัดการ การฝ่าฝืนแนวปฏิบัตินี้อาจนำไปสู่การลงโทษทางวินัยหรือกระทั่งการเลิกจ้าง รวมถึงการดำเนินการทางกฎหมายที่เกี่ยวข้อง

#### 5. นโยบายและแนวปฏิบัติที่เกี่ยวข้อง

- จรรยาบรรณทางธุรกิจ (การปกป้อง ดูแลทรัพย์สิน และรักษาความลับของกลุ่มบริษัท)
- นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- Information Safeguarding Guideline
- นโยบายการคุ้มครองข้อมูลส่วนบุคคล

#### 6. ข้อตกลงผู้ใช้งาน

ข้าพเจ้าได้อ่าน ทำความเข้าใจ และจะปฏิบัติตามแนวปฏิบัติข้างต้นอย่างเคร่งครัด ข้าพเจ้าเข้าใจดีว่าการฝ่าฝืนอาจส่งผลให้ถูกเพิกถอนสิทธิ์การใช้ทรัพยากรและบริการด้านเทคโนโลยีของบริษัท รวมถึงอาจถูกดำเนินการทางวินัยและทางกฎหมายได้

ลงชื่อ: \_\_\_\_\_ ผู้ใช้งาน

ชื่อ-นามสกุล: \_\_\_\_\_

รหัสพนักงาน: \_\_\_\_\_

ตำแหน่ง: \_\_\_\_\_

หน่วยงาน: \_\_\_\_\_

บริษัท: \_\_\_\_\_

วันที่: \_\_\_\_\_