Term of Use

SAFE Cloud

บริษัท สามารถ อินโฟเนต จำกัด

1. **นิยาม/ความหมาย (Definitions)**

บริษัทฯ หมายถึง บริษัท สามารถ อินโฟเนต จำกัด

ผู้ให้บริการ (Cloud Service Provider) หมายถึง บริษัทฯ ผู้ให้บริการ Cloud Computing หรือบริการ SAFE Cloud ที่ให้บริการในรูปแบบ Infrastructure as a Service (IaaS) โดยมีศูนย์ให้บริการ (Geographical Location) ตั้งอยู่ใน จังหวัดกรุงเทพมหานครและนนทบุรี ประเทศไทย

ผู้ให้บริการ (Cloud Service Provider) ดำเนินการตามข้อกำหนดด้านกฎหมายและระเบียบข้อบังคับทั้งภายในและภายนอก ประกอบด้วย ประกาศ /พรบ. /คำสั่ง สำนักงาน หน่วยงานกำกับดูแล, มาตรฐาน ISO 27001, CSA Security, Trust & Assurance Registry (STAR) เป็นการสร้างความมั่นคงปลอดภัยและการให้บริการและเพื่อเสริมสร้างความมั่นคงปลอดภัยและคุณภาพการให้บริการที่ได้มาตรฐานแก่ผู้ใช้บริการ

บริการ SAFE Cloud หมายถึง บริการโครงสร้างพื้นฐานในรูปแบบเสมือน (Virtualization) ที่ช่วยให้ผู้ใช้บริการสามารถกำหนดและบริหารจัดการทรัพยากรได้ตามความต้องการ เช่น การเพิ่ม/ลดขนาดของ CPU, Hard Disk, RAM หรือการติดตั้งระบบปฏิบัติการและซอฟต์แวร์ที่แตกต่างกัน เป็นต้น

ผู้ใช้บริการ (Cloud Customer) หมายถึง ลูกค้าที่ใช้บริการ Cloud Computing หรือบริการ SAFE Cloud ของบริษัทฯ

1. **ข้อมูล (Data)** หมายถึง ข้อมูลสารสนเทศที่ผู้ใช้บริการสร้างขึ้นระหว่างการใช้งานบริการ SAFE Cloud หรือข้อมูลที่บริษัทฯ จัดเตรียมให้ผู้ใช้บริการ ก่อนหรือระหว่างการใช้งานบริการ เช่น Virtual Machine Image, Backup Virtual Machine Image, Snapshot Virtual Machine Image เป็นต้น

เหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) หมายถึง สถานการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ใช้บริการหรือผู้ให้บริการ

จุดอ่อน (Weakness) หมายถึง ข้อบกพร่องหรือสถานการณ์ที่ยังไม่ก่อให้เกิดปัญหาด้านความมั่นคงปลอดภัยของสารสนเทศในขณะนี้ แต่หากไม่ได้รับการแก้ไข อาจนำไปสู่เหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Information Security Incident) ในอนาคต

2. หน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security roles and responsibility) ของผู้ใช้บริการ

2.1 ผู้ใช้บริการมีหน้าที่รับผิดชอบในการดูแลและรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บอยู่ภายใน Virtual Machine

2.2 ผู้ใช้บริการต้องดูแลรักษาความมั่นคงปลอดภัยของ Virtual Machine ที่ใช้จัดเก็บ Customer Data ทั้งนี้ บริษัทฯ จะรับผิดชอบการสำรองข้อมูลของ Virtual Machine ตามข้อตกลงที่ได้ตกลงร่วมกันเท่านั้น

2.3 ผู้ใช้บริการควรใช้มาตรการควบคุมด้านความมั่นคงปลอดภัยที่เหมาะสมกับข้อมูลสำคัญ เช่น การเข้ารหัสข้อมูล (Data Encryption) หรือ การเพิ่มความแข็งแกร่งให้กับระบบปฏิบัติการ (OS Hardening) เป็นต้น

2.4 บริการ SAFE Cloud มีการจัดเตรียมมาตรการควบคุมการเข้าถึง Virtual Machine ผ่านเครือข่ายด้วย Firewall ผู้ใช้บริการสามารถร้องขอเพื่อปรับปรุง Firewall Rules ได้ภายหลังจากเริ่มต้นใช้งาน ทั้งนี้ ผู้ใช้บริการต้องรับผิดชอบในการดูแลรักษาความมั่นคงปลอดภัยด้านเครือข่าย (Network Security) ภายในของ Virtual Machine ด้วยตนเอง อย่างไรก็ตามบริษัทฯ แนะนำให้ผู้ใช้บริการใช้มาตรการควบคุมด้านความมั่นคงปลอดภัยทางเครือข่ายที่เหมาะสม เช่น การใช้การเข้ารหัสข้อมูลสำหรับบริการ Remote Administration (SSH), การควบคุมการเข้าถึงพอร์ตด้วย OS Firewall หรือ Personal Firewall หรือ การเลือกใช้ Protocol ที่มีการเข้ารหัสสำหรับการรับส่งข้อมูลที่สำคัญ (HTTPS, SFTP หรือ SMTPS) เป็นต้น

2.5 ผู้ใช้บริการควรเปลี่ยนรหัสผ่านที่ปลอดภัยของบัญชีผู้ใช้ระบบปฏิบัติการ และบัญชีผู้ใช้ของระบบบริหารจัดการ Virtual Machine (SAFE Cloud) ทันทีที่ได้รับจากบริษัทฯ เมื่อเริ่มต้นใช้บริการ SAFE Cloud

2.6 การบริหารจัดการบัญชีผู้ใช้ หรือ สิทธิ์การเข้าถึงระบบปฏิบัติการ (User and Privilege Management) และบัญชีผู้ใช้ของระบบบริหารจัดการ Virtual Machine (SAFE Cloud) ถือเป็นความรับผิดชอบของผู้ใช้บริการเอง โดย

บริษัทฯ จะไม่รับผิดชอบในการเข้าถึงหรือบริหารจัดการบัญชีของผู้ใช้บริการ ทั้งนี้ เพื่อให้ระบบและข้อมูลของผู้ใช้บริการมีความมั่นคงปลอดภัย ควรดำเนินการลงทะเบียน ยกเลิก และทบทวนบัญชีผู้ใช้งานอย่างสม่ำเสมอ

2.7 ผู้ใช้บริการต้องจัดเก็บและควบคุมการเข้าถึง ข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่อยู่ภายใน Virtual Machine ให้มีความมั่นคงปลอดภัยและสอดคล้องตามที่กฎหมาย พรบ.คอมพิวเตอร์ กำหนดไว้

2.8 ผู้ใช้บริการต้องดำเนินการ เทียบสัญญาณเวลา (Time Synchronization) ของ Virtual Machine กับแหล่งสัญญาณเวลาที่ได้รับมาตรฐานและมีความน่าเชื่อถือ หากผู้ใช้บริการต้องการข้อมูลเพิ่มเติมเกี่ยวกับการเทียบสัญญาณเวลาสามารถติดต่อผ่านช่องทาง technical_service@samartinfonet.co.th หรือ Call Center: 0-2026-6578

2.9 ผู้ใช้บริการควรใช้เครื่องมือที่สามารถสแกนหาช่องโหว่ด้านความปลอดภัยของ Virtual Machine เพื่อให้แน่ใจว่าไม่มีความเสี่ยงที่อาจถูกโจมตี หากตรวจพบช่องโหว่ที่อาจทำให้ระบบเกิดปัญหาหรือเสี่ยงต่อการถูกโจมตี ผู้ใช้บริการมีหน้าที่ต้องดำเนินการแก้ไขเอง หรือหากไม่สามารถดำเนินการเองได้ ให้แจ้งมายังบริษัทฯ เพื่อให้ช่วยแก้ไขผ่านช่องทาง technical_service@samartinfonet.co.th หรือ Call Center: 0-2026-6578

2.10 ผู้ใช้บริการสามารถแจ้ง เหตุการณ์ด้านความมั่นคงปลอดภัย หรือ จุดอ่อนด้านความมั่นคงปลอดภัย ที่เกิดจากการใช้บริการ SAFE Cloud ผ่านช่องทาง technical_service@samartinfonet.co.th หรือ Call Center: 0-2026-6578 และบริษัทฯ จะดำเนินการตอบรับและแก้ไขปัญหาภายในระยะเวลาที่เหมาะสม

2.11 หากผู้ใช้บริการต้องการให้บริษัทฯดำเนินการจัดส่ง Log File ที่อยู่ภายใต้ความรับผิดชอบของบริษัทฯ ผู้ใช้บริการสามารถแจ้งรายละเอียดคำขอผ่านช่องทาง technical_service@samartinfonet.co.th หรือ Call Center: 0-2026-6578

2.12 ในกรณีที่บริษัทฯ มีการเปลี่ยนแปลงระบบภายใต้บริการ SAFE Cloud ซึ่งอาจส่งผลกระทบต่อการใช้งาน Virtual Machine ของผู้ใช้บริการ บริษัทฯ จะทำการแจ้งให้ทราบล่วงหน้าก่อนการดำเนินการผ่านช่องทาง technical_service@samartinfonet.co.th หรือ Call Center: 0-2026-6578

2.13 การบริหารจัดการผู้ให้บริการภายนอก (Supplier of Customer) เป็นความรับผิดชอบของผู้ใช้บริการเอง โดยผู้ใช้บริการต้องกำกับดูแลและควบคุมการดำเนินงานของ Supplier เสมือนเป็นหน้าที่ของตนเอง โดยต้องได้รับอนุญาตจากผู้ใช้บริการก่อนดำเนินการ และผลจากการดำเนินการทั้งหมดถือเป็นความรับผิดชอบของผู้ใช้บริการ

3. การบริหารจัดการความมั่นคงปลอดภัยของข้อมูล (Data Management)

3.1 ผู้ใช้บริการสามารถร้องขอ ไฟล์เอกสารที่เกี่ยวข้องกับบริการ SAFE Cloud ได้ ได้แก่ PDF แต่ถ้าหากต้องการเอกสารในรูปแบบไฟล์อื่น ๆ สามารถส่งคำขอเพิ่มเติมได้

3.2 หากผู้ใช้บริการต้องการ Export หรือ Import ข้อมูลในรูปแบบไฟล์อิเล็กทรอนิกส์ ผู้ใช้บริการต้องแจ้งรายละเอียดเกี่ยวกับ วิธีการและรูปแบบไฟล์ที่ต้องการ ให้บริษัทฯ ทราบล่วงหน้า

3.3 ผู้ใช้บริการควรพิจารณากำหนดระดับชั้นความลับของข้อมูลหรือ ติดป้ายแสดงระดับความสำคัญของข้อมูล ที่อยู่ในรูปแบบเอกสารและไฟล์อิเล็กทรอนิกส์ เพื่อป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลของผู้ใช้บริการ

4. การทำลายข้อมูล (Information/Data Disposal)

4.1 ข้อมูลในรูปแบบ Virtual Machine Image ของผู้ใช้บริการจะถูกทำลายโดยบริษัทฯ ตามกระบวนการที่มีมาตรฐานความมั่นคงปลอดภัยสูง ทั้งนี้ภายหลังจากการทำลายข้อมูลแล้ว จะไม่สามารถกู้คืนได้

4.2 ข้อมูลบัญชีผู้ใช้ (User Account) ในระบบบริหารจัดการ Virtual Machine (SAFE Cloud) ที่ผู้ใช้บริการสร้างขึ้นระหว่างการใช้บริการ จะถูกลบออกจากบริการ SAFE Cloud โดยสมบูรณ์ และไม่สามารถใช้บริการบัญชีดังกล่าวได้

4.3 ในกรณีที่มีการยกเลิกการใช้บริการ ผู้ใช้บริการต้องแจ้งให้บริษัทฯ ทราบล่วงหน้าเพื่อกำหนดระยะเวลาในการ ปิด Virtual Machine และระยะเวลาการเก็บรักษาข้อมูล Virtual Machine หลังจากสิ้นสุดระยะเวลาที่กำหนด บริษัทฯ จะดำเนินการ **ทำลายข้อมูลทั้งหมดของผู้ใช้บริการ** ตามกระบวนการที่ได้กำหนดไว้ หากไม่มีการแจ้งระยะเวลาที่ชัดเจน บริษัทฯ **จะเก็บรักษาข้อมูลของผู้ใช้บริการไว้เป็นระยะเวลา 30 วัน** นับจากวันที่ยกเลิกบริการ

5. ลิขสิทธิ์การใช้งานระบบปฏิบัติการและโปรแกรมประยุกต์

5.1 บริการ SAFE Cloud จะเตรียมระบบปฏิบัติการ และโปรแกรมประยุกต์ที่มีลิขสิทธิ์ถูกต้องให้กับผู้ใช้บริการที่ร้องขอ โดยเป็นไปตามที่ตกลงกับบริษัทฯ

5.2 ผู้ใช้บริการต้องไม่ละเมิดลิขสิทธิ์ของ ระบบปฏิบัติการ และ โปรแกรมประยุกต์ ที่บริษัทฯ จัดเตรียมให้

5.3 ผู้ใช้บริการควรมีมาตรการควบคุม โปรแกรมประยุกต์ที่ใช้งาน และควรทบทวนการใช้งานโปรแกรมประยุกต์เป็นประจำ เพื่อให้เป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยและข้อกำหนดที่เกี่ยวข้อง

5.4 ผู้ใช้บริการต้อง ไม่ติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์ หรือโปรแกรมที่อาจก่อให้เกิดผลกระทบต่อการให้บริการของบริษัทฯ การดักจับข้อมูล (Sniffing Tools) การลักลอบถอดรหัสผ่าน การปลอมแปลงข้อมูลคอมพิวเตอร์ การพยายามเข้าถึงระบบสารสนเทศโดยมิชอบ (Unauthorized Access) หรือรบกวนการทำงานของเครือข่าย (Network Disruptive Software) กรณีที่การใช้งานโปรแกรมประยุกต์ใด ๆ ที่ส่งผลกระทบต่อบริษัทฯ และก่อให้เกิดความเสียหายต่อการให้บริการ ทรัพย์สินของบริษัทฯ ผู้ใช้บริการต้องรับผิดชอบค่าเสียหายทั้งหมดที่เกิดขึ้น

5.5 การจัดการและดูแลลิขสิทธิ์ของระบบปฏิบัติการหรือโปรแกรมประยุกต์อื่น ๆ ที่ผู้ใช้บริการติดตั้งเพิ่มเติมบน Virtual Machine นอกเหนือจากบริษัทฯ จัดหาให้ ถือเป็นความรับผิดชอบของผู้ใช้บริการเอง

5.6 การติดตั้ง ดัดแปลง โปรแกรมประยุกต์ รวมถึงการดำเนินการใด ๆ ที่ผิดกฎหมาย ถือเป็นความรับผิดชอบของผู้ใช้บริการแต่เพียงผู้เดียว บริษัทฯ จะไม่มีส่วนเกี่ยวข้องกับการกระทำดังกล่าวในทุกกรณี

5.7 ลิขสิทธิ์ของ ซอฟต์แวร์ ระบบสารสนเทศ การพัฒนาโปรแกรม หรือข้อมูลใด ๆ ที่สร้างขึ้นระหว่างการใช้บริการ SAFE Cloud ถือเป็น สิทธิ์ของผู้ใช้บริการ แต่ต้องไม่ละเมิดเงื่อนไขลิขสิทธิ์ระบบปฏิบัติการและโปรแกรมประยุกต์ที่บริษัทฯ จัดเตรียมให้

ภาคผนวก

การบริหารจัดการบัญชีผู้ใช้งานและสิทธิ์การเข้าถึง

ผู้ใช้บริการควรมีแนวทางที่ชัดเจนในการ ลงทะเบียน ยกเลิก และทบทวนบัญชีผู้ใช้งาน โดยในการลงทะเบียนและยกเลิกบัญชีผู้ใช้งาน ควรผ่านกระบวนการ อนุมัติจากหัวหน้าหน่วยงานหรือผู้มีอำนาจ ซึ่งการสร้างบัญชีรายชื่อควรสร้างให้เหมาะสมและให้สิทธิน้อยที่สุดที่เพียงพอต่อการใช้งานที่ร้องขอ และควรแบ่งแยกหน้าที่และความรับผิดชอบ (Segregation of duties) ของผู้ที่เกี่ยวข้องในระบบงานต่าง ๆ เพื่อป้องกันไม่ให้ผู้ใดสามารถเข้าถึงระบบงานทั้งหมด

การกำหนดสิทธิ์ระดับสูง (Admin/Root Privileges)

หากต้องให้สิทธิ Admin หรือ Root ควรมีเครื่องมือทางเทคนิคเพื่อตรวจสอบการทำงาน และการส่งบัญชีรายชื่อและรหัสผ่านควรส่งคนละช่องทาง เช่น ถ้าส่งผ่าน Email แล้วรหัสควรส่งทาง SMS เป็นต้น หากเป็นการส่งทางอิเล็กทรอกนิกส์ควรมีการเข้ารหัสข้อมูลและหากเป็นสิทธิ Admin หรือ Root ควรมีการพิจารณาให้ใช้วิธีการส่งที่ปลอดภัยสูง เช่น การใช้ One-Time Password (OTP), Multi-Factor Authentication (MFA), หรือ Secure Vault สำหรับจัดเก็บรหัสผ่าน เป็นต้น

การจัดการรหัสผ่าน (Password Management)

1. ควรมีการระบุและพิสูจน์ตัวตนของผู้ใช้งานทุกครั้งก่อนเข้าใช้บริการ
2. เก็บรักษาบัญชีผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ให้เป็นความลับ รวมไปถึงไม่เก็บบันทึกรหัสผ่านลงในกระดาษ ไฟล์ข้อมูล ยกเว้นว่ามีขั้นตอนหรือวิธีการเก็บรักษาที่พิสูจน์ได้ว่าปลอดภัยจริง
3. รหัสผ่านควรมีความยาว ไม่น้อยกว่า 8 อักขระ และประกอบด้วย ตัวพิมพ์ใหญ่ (Uppercase), ตัวพิมพ์เล็ก (Lowercase), ตัวเลข (Numbers) และ อักขระพิเศษ (Special Characters) ผสมกัน เพื่อเพิ่มความยากต่อการคาดเดาและลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ (ห้ามซ้ำกับ Username)
4. หลีกเลี่ยงการตั้งรหัสผ่านที่คาดเดาได้ง่าย เช่น ชื่อ-นามสกุล, วันเดือนปีเกิด, เลขบัตรประชาชน หรือคำศัพท์สามัญทั่วไป เป็นต้น เพื่อป้องกันความเสี่ยงจากการถูกคาดเดาหรือโจมตีแบบ Brute Force
5. ควรกำหนดให้อายุรหัสผ่าน (Password Expiration) หมดอายุในระยะเวลาที่เหมาะสม เช่น ทุก 90 วัน เป็นต้น เพื่อป้องกันความเสี่ยงจากการที่รหัสผ่านอาจถูกขโมยหรือรั่วไหล

การจัดการกุญแจเข้ารหัส (Key Management)

หากผู้ใช้บริการมีการเข้ารหัสข้อมูลที่มีความอ่อนไหว (Sensitive Data) หรือข้อมูลระดับชั้นความลับ (Confidential) ควรใช้มาตรการบริหารจัดการกุญแจ (Key) ตั้งแต่ขั้นตอน การสร้างและแจกจ่ายกุญแจ (Key Generation & Distribution), การสำรองกุญแจ (Key Backup), การกู้คืนกุญแจ (Key Recovery) และการเพิกถอนกุญแจ (Key Revoking) พร้อมทั้งมีการจัดเก็บกุญแจในที่ปลอดภัย เช่น Hardware Security Module (HSM) หรือ Key Management System (KMS) เป็นต้น

ผู้ใช้บริการสามารถเลือกใช้การเข้ารหัสข้อมูลแบบ Symmetric Encryption (ใช้กุญแจเดียวกันในการเข้าและถอดรหัส) Asymmetric Encryption (ใช้กุญแจ Public/Private Key ในการเข้ารหัสและถอดรหัส) ทั้งนี้ ควรเลือกใช้ให้สอดคล้องกับนโยบายและมาตรฐานภายในองค์กร เพื่อให้มั่นใจว่าข้อมูลได้รับการปกป้องอย่างเหมาะสม