SAFE SYSTEMS CO.
شركة راية الأمان لتقنية المعلومات

SAFE ERP Standard Support and Service Level Agreement (SLA)

سياسة دعم واتفاقية مستوى الخدمة لنظام SAFE ERP

Version: 1.0

Effective Date: 01/08/2026

Provider: SAFE SYSTEMS CO.

1. Overview & Scope

This SLA defines the support services, targets, and operational commitments for SAFE ERP under applicable License Models (Subscription or Perpetual) and Hosting Arrangements (Customer-Hosted or SAFE SYSTEMS-Managed), as designated in the governing Commercial Agreement.

1.1 In-Scope Services

Subject to an active support entitlement, SAFE SYSTEMS provides remote support for:

- Incident investigation, software defect correction, and standard system troubleshooting.
- Guidance on standard system configuration and operation.
- Provision of software updates, patches, and maintenance releases.
- Integration support for explicitly contracted third-party systems.

2. Support Channels & Operating Hours

- Standard Support Hours: Sunday – Thursday, 9:30 AM – 5:00 PM (Egypt Time), excluding official Egyptian public holidays.
- Approved Support Channels: SAFE SYSTEMS Support Portal, official support email, WhatsApp, or any agreed communication channels. Requests must include full details (company, branch, environment, user, financial year, module and/or page names, issue description, error logs/screenshots, and impacted business functions).
- Emergency Support: Available 24/7 strictly for Priority 1 (Critical) issues affecting customers with an active Premium Support agreement.

3. Incident Severity, Target Response Times & Service Commitments

The SLA Service Clock begins upon receipt of a complete support request via an approved channel. Target resolution may include permanent fixes, temporary workarounds, or configuration adjustments.

1. النطاق والنظرة العامة

تحدد هذه الاتفاقية خدمات الدعم الفني، والمستهدفات، والالتزامات التشغيلية لنظام SAFE ERP بموجب نماذج الترخيص المطبقة (اشتراك أو ترخيص دائم) وترتيبات الاستضافة (مستضيفة لدى العميل أو مدارة من قبل راية الأمان)، وفقاً لما هو محدد في الاتفاقية التجارية الحاكمة.

1.1 الخدمات المشمولة بالنطاق

شريطة وجود استحقاق دعم ساري، تقدم شركة راية الأمان خدمات الدعم الفني عن بُعد لكل من:

- التحقيق في الحوادث، وتصحيح عيوب البرمجيات، وإصلاح الأعطال القياسية للنظام.
- تقديم الإرشادات حول الإعدادات والتشغيل القياسي للنظام.
- توفير التحديثات البرمجية، والترقيعات Security Patches، والإصدارات الصيانة.
- تقديم دعم الربط والتكامل للأنظمة الخارجية المتعاقد عليها صراحة.

2. قنوات الدعم وساعات العمل

- ساعات الدعم القياسية: من الأحد إلى الخميس، من الساعة 9:30 صباحاً حتى 5:00 مساءً (بتوقيت جمهورية مصر العربية)، باستثناء العطلات الرسمية.
- قنوات الدعم المعتمدة: بوابة الدعم الفني لشركة راية الأمان، أو البريد الإلكتروني الرسمي للدعم، أو تطبيق WhatsApp أو قنوات الاتصال المتفق عليها. يجب أن تتضمن الطلبات تفاصيل كاملة (اسم الشركة، الفرع، البيئة، المستخدم، السنة المالية، أسماء الشاشات/الوحدات، وصف المشكلة، سجلات الأخطاء/لقطات الشاشة، الوظائف التجارية المتأثرة).
- الدعم الطارئ: متاح على مدار الساعة (7/24) حظرياً لأعطال الأولوية الأولى (P1 - الحرج) للعملاء المسجلين في اتفاقية "الدعم المتميز" (Premium Support) السارية.

3. درجة خطورة الحادثة، وأزمنة الاستجابة المستهدفة، والالتزامات

يبدأ احتساب زمني ساعة الخدمة (SLA Clock) فور استلام طلب دعم مكتمل عبر قناة معتمدة. قد يشمل الحل المستهدف إصلاحات برمجية دائمة، أو حلولاً مؤقتة (Workarounds)، أو تعديلات في الإعدادات.

Priority	Classification	Business Impact	Target Initial Response
P1	**Critical**	Complete outage or severe operational failure with no workaround.	Within 1 Hour
P2	**High**	Core function materially impaired; operations significantly impacted.	Within 2 Business Hours
P3	**Medium**	Non-critical feature impaired; business continues via workaround.	Within 4 Business Hours
P4	**Low**	Minor usability issues, general inquiries, or feature requests.	Within 1 Business Day

الأولوية	التصنيف	الأثر التجاري	زمن الاستجابة الأولية المستهدف
P1	**حرج (Critical)**	انقطاع كامل للنظام أو توقف تشغيلي حاد دون وجود حل مؤقت.	خلال 1 ساعة واحدة
P2	**عالي (High)**	تضرر جوهري لوظيفة رئيسية؛ تأثر العمليات بشكل كبير.	خلال ساعتي عمل (2)
P3	**متوسط (Medium)**	تضرر ميزة غير حرجية؛ استمرار العمل عبر حل مؤقت.	خلال 4 ساعات عمل
P4	**منخفض (Low)**	مشكلات استخدام بسيطة، استفسارات عامة، أو طلبات مميزات جديدة.	خلال يوم عمل واحد (1)

3.1 P1 Resolution Delay & SLA Clock Extension

If SAFE SYSTEMS fails to meet the Target Workaround / Restoration timeframe for a Priority 1 (P1) Incident, the applicable resolution SLA window shall automatically be extended by one (1) full business day for everyone (1) business hour of unexcused delay past the target restoration timeframe.

3.1 تأخير حل المشكلات الحرجية (P1) وتمديد مهلة SLA

في حال فشل شركة راية الأمان في تلبية الإطار الزمني المستهدف للحل المؤقت/الاستعادة لحوادث الأولوية الأولى (P1)، يتم تمديد المهلة الزمنية المسموح بها لاتفاقية مستوى الخدمة بواقع يوم عمل كامل (1) مقابل كل ساعة عمل تأخير واحدة (1) تزيد عن الإطار الزمني المستهدف للاستعادة.

3.2 Mandatory Workaround & Automatic De-escalation (P2 & P3 Incidents)

If SAFE SYSTEMS is unable to deliver a permanent code fix for a P2 (High) or P3 (Medium) incident within the designated Target Resolution period:

- Mandatory Workaround: SAFE SYSTEMS must deliver and deploy an operational workaround, temporary workflow, or system reconfiguration within that target period to mitigate business impact.
- Automatic De-escalation: Once a viable workaround is successfully provided by SAFE SYSTEMS, the ticket severity shall automatically scale down to the next lower priority level:
    - A P2 (High) ticket with an active workaround scale down to P3 (Medium).

3.2 الحلول المؤقتة الإلزامية وخفض التصنيف التلقائي (حوادث P2 و P3)

في حال تعذر على شركة راية الأمان تقديم إصلاح برلمجي دائم لحادثة من الأولوية الثانية (P2) أو الثالثة (P3) خلال فترة الحل المستهدفة:

- الحل المؤقت الإلزامي: تلتزم شركة راية الأمان بنشر وتوفير حل تشغيلي مؤقت، أو مسار عمل بديل، أو إعادة ضبط للنظام خلال الفترة المستهدفة لتخفيف الأثر التجاري.
- التخفيض التلقائي لدرجة الخطورة: بمجرد تقديم حل مؤقت فعال من قبل راية الأمان، يتم تخفيض درجة خطورة التذكرة تلقائياً إلى المستوى الأدنى التالي:
    - تذكرة P2 (عالية) مع وجود حل بديل فعال يتم خفضها إلى P3 (متوسطة).

- A P3 (Medium) ticket with an active workaround scale down to P4 (Low).

- Final Resolution: Permanent code patches for de-escalated tickets shall be incorporated into standard future release packages without violating the primary SLA target.

3.3 Service Credit Remedies & Monthly Cap (P1 Incidents)

Where SAFE SYSTEMS fails to provide either a permanent resolution or a viable workaround for a P1 incident within the target window (including permitted extensions under Section 3.1):

- Credit Calculation: The Customer shall be eligible to request a Service Credit equal to 5% of the monthly hosting/support fee for each full 4-hour period of unexcused delay beyond the target window.
- Monthly Cap: The total cumulative value of Service Credits issued to a Customer in any single calendar month shall not exceed 15% of the total monthly hosting/support fee paid for that month.
- Sole Remedy: Service Credits represent the Customer's sole and exclusive financial remedy for SLA response or resolution delays under this agreement.

4. SLA Clock Suspensions & Dependencies

The SLA Service Clock pauses ("Pending Customer Action") when SAFE SYSTEMS is awaiting:

- Customer information, approvals, access permissions, or credentials.
- Availability of customer technical personnel or infrastructure restoration.
- External third-party dependencies outside SAFE SYSTEMS's reasonable control.

Periods of suspension are excluded from performance calculations

5. Hosting Conditions & System Responsibilities

5.1 General Customer Responsibilities

The Customer shall maintain active license and support entitlements, designate authorized technical contacts, and ensure end-users follow standard SAFE ERP operating procedures.

5.2 Customer-Hosted Environments

Where SAFE ERP is deployed on infrastructure owned, rented, or managed by the Customer, the Customer retains sole and exclusive responsibility for:

- تذكرة P3 (متوسطة) مع وجود حل بديل فعال يتم خفضها إلى P4 (منخفضة).

- الحل النهائي: يتم إدراج الترقيعات البرمجية الدائمة للتذاكر المخفضة ضمن حزم الإصدارات التحديثية المستقبليّة دون الإخلال بالمستهدف الرئيسي للاتفاقية.

3.3 أرصدة تعويض الخدمة والحد الأقصى الشهري (حوادث P1)

في الحالات التي تفشل فيها شركة راية الأمان في تقديم حل دائم أو حل مؤقت فعال لحادثة من الأولوية (P1) خلال النافذة المستهدفة (شاملة التمديدات المسموح بها بموجب البند 3.1):

- احتساب الرصيد: يحق للعميل المطالبة برصيد خدمة (Service Credit) يعادل 5% من قيمة رسوم الاستضافة/الدعم الشهرية عن كل 4 ساعات تأخير غير مبررة تتجاوز النافذة المستهدفة.

- الحد الأقصى الشهري: لا يجوز أن يتجاوز الإجمالي التراكمي لأرصدة الخدمة الصادرة للعميل في أي شهر تقويمي واحد نسبة 15% من إجمالي قيمة رسوم الاستضافة/الدعم الشهرية المدفوعة عن ذلك الشهر.

- التعويض الحصري: تمثل أرصدة الخدمة التعويض المالي الوحيد والحصري للعميل عن تأخيرات الاستجابة أو الحل بموجب هذه الاتفاقية.

4. تعليق احتساب مهلة SLA والاعتماديات

يتوقف احتساب زمني الخدمة مؤقتاً (تحت حالة "بانتظار إجراء العميل") عندما تكون راية الأمان بانتظار:

- الحصول على معلومات، موافقات، صلاحيات وصول، أو بيانات اعتماد من العميل.
- جاهزية الكوادر الفنية للعميل أو استعادة البنية التحتية الخاصة به.
- اعتماديات خارجية من أطراف ثالثة تقع خارج نطاق السيطرة المعقولة لشركة راية الأمان.

وتُستثنى فترات التعليق هذه من حسابات قياس الأداء.

5. شروط الاستضافة ومسؤوليات النظام

5.1 المسؤوليات العامة للعميل

يلتزم العميل بالحفاظ على استحقاقات الترخيص والدعم سارية المفعول، وتعيين جهات اتصال فنية مخولة، وضمان اتباع المستخدمين النهائيين لإجراءات التشغيل القياسية لنظام SAFE ERP.

5.2 البيئات المستضيفة لدى العميل (Customer-Hosted)

عند تثبيت نظام SAFE ERP على بنية تحتية مملوكة للعميل أو مستأجرة أو مدارة من قبله، يتحمل العميل المسئولية الفردية والحصرية عن:

- Cybersecurity & Threat Protection: Implementing and maintaining comprehensive protection against viruses, malware, ransomware, unauthorized access, cyberattacks, and hacking attempts.
- الأمن السيبراني والحماية من التهديدات: تطبيق وحفظ حماية شاملة ضد الفيروسات، البرمجيات الخبيثة، برامج الفدية، الوصول غير المصرح به، والهجمات السيبرانية.
- Backups & Data Integrity: Establishing, maintaining, and regularly testing full database, application, and system backups.
- النسخ الاحتياطي وسلامة البيانات: إنشاء وصيانة واختبار النسخ الاحتياطية الكاملة لقواعد البيانات والتطبيقات والنظام بشكل دوري.
- Licensing & System Updates: Maintaining valid licenses and applying necessary updates or security patches for underlying operating systems, database platforms, third-party software, network hardware, and security tools.
- التراخيص وتحديثات النظام: الحفاظ على تراخيص سارية وتطبيق التحديثات أو الترقيعات الأمنية اللازمة لأنظمة التشغيل، قواعد البيانات، البرامج الخارجية، ومعدات الشبكة.
- Remote Access Provision: Maintaining secure, reliable remote access (VPN, Remote Desktop, credentials) for SAFE SYSTEMS during support hours. SAFE SYSTEMS is not responsible for support delays resulting from restricted access, network downtime, or customer infrastructure failure.
- توفير الوصول عن بُعد: توفير وصول آمن ومستقر عن بُعد (VPN RDP /) لفريق راية الأمان أثناء ساعات الدعم. لا تتحمل راية الأمان أي مسؤولية عن تأخير الدعم الناتج عن قيود الوصول أو أعطال شبكة العميل.

5.3 SAFE SYSTEMS-Managed Hosting & Service Level Commitments

5.3 الاستضافة المدارة من قبل راية الأمان والتزامات الخدمة

Where SAFE SYSTEMS provides or manages the hosting environment, the following conditions apply:

عندما تقوم شركة راية الأمان بتوفير أو إدارة بيئة الاستضافة، تطبق الشروط التالية:

A. Service Availability Commitment (99% Target)

أ. التزام توافر الخدمة (مستهدف 99%)

SAFE SYSTEMS targets a 99% uptime availability for the hosted SAFE ERP application during each calendar month. This commitment applies strictly to core application accessibility

تستهدف راية الأمان نسبة جاهزية وتوافر تبلغ 99% لبيئة نظام SAFE ERP المستضيفة خلال كل شهر تقويمي. يقتصر هذا الالتزام حصرياً على إمكانية الوصول للتطبيق الرئيسي.

The 99% availability target excludes downtime resulting from:

ويُستثنى من حساب نسبة الـ 99% التوقف الناتج عن:

- Emergency security patches or Force Majeure events (as defined in Section 6.3).
- الترقيعات الأمنية الطارئة أو أحداث القوة القاهرة (وفق تعريف البند 6.3).
- Scheduled maintenance exceeding thirty (30) minutes, provided such maintenance is performed during designated off-peak hours and announced to the Customer at least seventy-two (72) hours in advance.
- أعمال الصيانة المجدولة التي تتجاوز ثلاثين (30) دقيقة، بشرط أن تتم خلال أوقات غير الذروة المعلنة، وإخطار العميل بها قبل 72 ساعة على الأقل.

Downtime occurring under any of the above conditions shall not be computed against the 99% monthly service availability target.

ولا تُحسب فترات التوقف التي تقع تحت أي من الظروف أعلاه ضمن نسبة الجاهزية الشهرية المستهدفة.

B. Scope of Customer Access

ب. نطاق وصول العميل

The Customer and its authorized end-users are granted operational access exclusively to the SAFE ERP software application user interface.

يُمنح العميل ومستخدموه المخولون حق الوصول التشغيلي حصرياً واقتصاراً على واجهة المستخدم لنظام SAFE ERP.

C. Server & Infrastructure Restrictions

ج. قيود الخوادم والبنية التحتية

Neither the Customer nor any third party acting on the Customer's behalf shall have any right to access, inspect, log into, or demand administrative rights for underlying servers, virtual machines, database engines, or physical data center devices.

لا يحق للعميل أو أي طرف ثالث يعمل نيابة عنه الوصول، أو التفتيش، أو تسجيل الدخول، أو المطالبة بصلاحيات مسؤولي النظام (Root/Admin) على الخوادم، أو الأجهزة الافتراضية، أو قواعد البيانات، أو الأجهزة الفعالة بمراكز البيانات.

D. Operational Confidentiality & System Secrecy

To protect the cybersecurity, operational integrity, and trade secrets of SAFE SYSTEMS's hosting environment, the Customer has no right to request, inspect, or demand direct access to detailed information regarding:

- Server specifications, cloud architecture, hardware configurations, or physical device locations.
- Internal backup strategies, schedules, automated routines, backup files, or storage destinations.
- Security protocols, firewall parameters, intrusion detection systems, anti-virus protections, or monitoring tools.

E. Reporting & Audit Assurances

For Customers utilizing SAFE SYSTEMS-Managed Hosting, the provision of customized or periodic reports regarding hosting environment health, automated backup attestations, patch compliance, or security posture details is not included under standard support.

Such reporting deliverables are contingent upon the Customer maintaining an active Premium Support Agreement and executing a mutually agreed Special Reporting & Security Addendum. Said addendum shall govern the exact scope, frequency, delivery schedules, non-disclosure conditions, and administrative fees associated with such security and infrastructure reporting. In all cases, direct root, administrative, or infrastructure-level access remains strictly prohibited.

6. Exclusions & Limitations

6.1 Exclusions

Unless covered by a separate Professional Services agreement, support excludes:

- Custom software development, new reports/ dashboards, or major custom enhancements.
- Data entry, manual data cleansing, bulk migration, or user training.
- On-site support, hardware repairs, or support for non-SAFE SYSTEMS software/networks.
- Issues caused by misuse, unauthorized modifications, or failure to follow documented procedures.

6.2 Service Limitations

SAFE SYSTEMS shall not be liable for indirect, consequential, or business loss damages arising from service interruptions, delays, or system downtime to the fullest extent permitted by law.

6.3 Force Majeure & Infrastructure Reinstatement

SAFE SYSTEMS shall not be liable for any failure, delay, or interruption in performance or service availability resulting

د. السرية التشغيلية وسرية النظام

لحماية الأمن السيبراني، والسلامة التشغيلية، والأسرار التجارية لبيئة الاستضافة الخاصة بشركة راية الأمان، لا يحق للعميل طلب أو فحص أو المطالبة بالوصول المباشر إلى المعلومات التفصيلية المتعلقة بما يلي:

- مواصفات الخوادم، أو البنية السحابية، أو تكوينات الأجهزة، أو مواقع الأجهزة الفعلية.
- استراتيجيات النسخ الاحتياطي الداخلية، أو الجداول الزمنية، أو الإجراءات الآلية، أو ملفات النسخ الاحتياطي، أو وجهات التخزين.
- بروتوكولات الأمان، أو معلمات جدران الحماية، أو أنظمة اكتشاف التسلل، أو وسائل الحماية من الفيروسات، أو أدوات المراقبة.

هـ. التقارير والضمانات الرقابية

إن تقديم تقارير مخصصة أو دورية حول صحة بيئة الاستضافة، أو شهادات النسخ الاحتياطي، أو الامتثال للترقيعات البرمجية لا يدخل ضمن خدمات الدعم القياسية.

وتخضع عمليات تقديم هذه التقارير لاحتفاظ العميل باتفاقية دعم متميزة سارية، وإبرام ملحق خاص بالتقارير والأمن يتم الاتفاق عليه بشكل متبادل. ويحدد هذا الملحق النطاق الدقيق، وتكرار التقارير، وجداول التسليم، وشروط عدم الإفصاح، والرسوم الإدارية المرتبطة بتقديم تقارير الأمن والبنية التحتية هذه. وفي جميع الحالات، يظل الوصول المباشر على مستوى الجذر، أو مستوى الإدارة، أو مستوى البنية التحتية محظورًا بشكل صارم.

6. الاستثناءات والقيود

6.1 الاستثناءات

ما لم تُغطَّ باتفاقية خدمات مهنية مستقلة، يستثنى من الدعم:

- تطوير برمجيات مخصصة، أو تقارير/لوحات معلومات جديدة، أو تحسينات مخصصة جوهرية.
- إدخال البيانات، أو تنظيف البيانات يدويًا، أو الترحيل الجماعي للبيانات، أو تدريب المستخدمين.
- الدعم في الموقع، أو إصلاحات الأجهزة، أو دعم البرمجيات/الشبكات غير التابعة لـ راية الأمان.
- المشكلات الناتجة عن سوء الاستخدام، أو التعديلات غير المصرح بها، أو عدم الالتزام بالإجراءات الموثقة.

6.2 حدود المسؤولية

لا تكون شركة راية الأمان مسؤولة عن أي أضرار غير مباشرة، أو تبعية، أو خسائر تجارية ناتجة عن انقطاع الخدمة أو التأخير إلى الحد الأقصى الذي يتيحه القانون المطبق.

6.3 القوة القاهرة وإعادة استعادة البنية التحتية

لا تتحمل راية الأمان أي مسؤولية عن أي فشل أو تأخير أو انقطاع في الأداء أو إتاحة الخدمة ناتج عن أفعال أو أحداث أو ظروف خارجة عن سيطرتها المعقولة. ويشمل ذلك، على سبيل المثال لا الحصر:

from acts, events, or circumstances beyond its reasonable control. These include, but are not limited to:

- Acts of God & Nature: Earthquakes, floods, severe weather, natural disasters, or other catastrophic acts of nature.
- War & Civil Unrest: War, hostilities, acts of terrorism, armed conflict, riots, civil commotions, military actions, or national/regional emergencies.
- Infrastructure & Data Center Failures: Regional telecommunication outages, major internet backbone disruptions, widespread power grid failures, malicious cyberattacks, or third-party cloud data center disasters.
- Governmental Actions & Labor Disputes: Strikes, lockouts, trade embargoes, regulatory restrictions, sanctions, or mandatory legal bans.

During the occurrence of a Force Majeure event:

1. All affected SAFE SYSTEMS SLA response targets, resolution timelines, and hosting availability commitments shall be temporarily suspended without penalty.
2. SAFE SYSTEMS shall use commercially reasonable efforts to mitigate downtime, preserve data integrity under SAFE SYSTEMS-Managed Hosting, and resume normal operational service levels as soon as technical conditions allow.
3. Customer Infrastructure & Reinstatement Costs: In Customer-Hosted Environments (or where infrastructure damage occurs on customer-controlled environments), the Customer remains solely responsible for repairing, replacing, or restoring its hardware, operating systems, network, security layers, and underlying server infrastructure. Any technical assistance requested from SAFE SYSTEMS to rebuild, reinstall, reconfigure, or restore the SAFE ERP environment, databases, or application instances following a Force Majeure event or infrastructure compromise shall be treated as an out-of-scope service and billed to the Customer at SAFE SYSTEMS's standard Professional Services rates.

- القوة القاهرة والكوارث الطبيعية: الزلازل، أو الفيضانات، أو الأحوال الجوية القاسية، أو الكوارث الطبيعية، أو غيرها من الكوارث الطبيعية الجسيمة.
- الحروب والاضطرابات المدنية: الحرب، أو الأعمال العدائية، أو أعمال الإرهاب، أو النزاعات المسلحة، أو أعمال الشغب، أو الاضطرابات المدنية، أو العمليات العسكرية، أو حالات الطوارئ الوطنية/الإقليمية.
- أعطال البنية التحتية ومراكز البيانات: انقطاع خدمات الاتصالات على مستوى المناطق، أو الاضطرابات الرئيسية في البنية التحتية لشبكة الإنترنت، أو حالات انقطاع واسعة النطاق لشبكة الكهرباء، أو الهجمات السيبرانية الخبيثة، أو الكوارث التي تصيب مراكز البيانات السحابية التابعة لأطراف ثالثة.
- الإجراءات الحكومية والنزاعات العمالية: الإضرابات، أو إغلاق المنشآت من جانب أصحاب العمل، أو الحظر التجاري، أو القيود التنظيمية، أو العقوبات، أو الحظر القانوني الإلزامي.

أثناء وقوع حدث من أحداث القوة القاهرة:

1. يتم تعليق جميع أهداف الاستجابة الخاصة باتفاقية مستوى الخدمة (SLA) لدى راية الأمان، والجداول الزمنية للحل، والتزامات إتاحة الاستضافة المتأثرة مؤقتًا دون أي غرامات.
2. تبذل راية الأمان جهودًا معقولة تجاريًا للحد من فترة التوقف، والحفاظ على سلامة البيانات ضمن بيئات الاستضافة المُدارة بواسطة راية الأمان، واستئناف مستويات الخدمة التشغيلية العادية بمجرد أن تسمح الظروف الفنية بذلك.
3. البنية التحتية للعميل وتكاليف إعادة الخدمة: في بيئات الاستضافة لدى العميل (أو في الحالات التي يحدث فيها تلف للبنية التحتية في البيئات الخاضعة لسيطرة العميل)، يظل العميل مسؤولًا بشكل كامل عن إصلاح أو استبدال أو استعادة أجهزته، وأنظمة التشغيل، والشبكات، وطبقات الأمان، والبنية التحتية الأساسية للخوادم. وأي مساعدة فنية يطلبها العميل من راية الأمان لإعادة بناء أو إعادة تثبيت أو إعادة تهيئة أو استعادة بيئة SAFE ERP، أو قواعد البيانات، أو نسخ التطبيقات بعد وقوع حدث من أحداث القوة القاهرة أو حدوث اختراق للبنية التحتية، تُعامل كخدمة خارج نطاق الدعم، ويتم احتساب تكلفتها على العميل وفقًا لأسعار خدمات راية الأمان الاحترافية القياسية.

7. Data Retention & Fee Adjustments

7.1 Data Retention (SAFE SYSTEMS-Managed Hosting)

Upon termination or non-renewal of SAFE SYSTEMS-Managed Hosting, SAFE SYSTEMS will retain customer data for two (2) calendar months ("Data Retention Period"). The Customer must export or request migration assistance (subject to professional service fees) within this window. Following this period, SAFE SYSTEMS will permanently destroy all hosted data and backups.

7.2 Service Suspension for Non-Payment

7. حفظ البيانات وتعديل الرسوم

7.1 الاحتفاظ بالبيانات (الاستضافة المدارة من راية الأمان)

عند إنهاء الخدمة أو عدم تجديد استضافة راية الأمان، تحتفظ الشركة ببيانات العميل لمدة شهرين تقويميين (2) ("فترة الاحتفاظ بالبيانات"). ويجب على العميل تصدير بياناته أو طلب مساعدة النقل (مقابل رسوم خدمات مهنية) خلال هذه النافذة، وبعدها تلتزم راية الأمان بتدمير جميع البيانات والنسخ الاحتياطية بشكل دائم.

7.2 تعليق الخدمة لعدم السداد

If undisputed invoices remain unpaid for more than fifteen (15) calendar days past their due date, SAFE SYSTEMS reserves the right to suspend support, maintenance, hosting, and SLA clock obligations until all outstanding fees are settled.

في حال عدم سداد الفواتير غير المتنازع عليها لمدة تتجاوز خمسة عشر (15) يوماً تقويمياً من تاريخ استحقاقها، تحتفظ راية الأمان بالحق في تعليق خدمات الدعم والصيانة والاستضافة التزاماً والتوقف عن احتساب مهام SLA لحين تسوية المبالغ.

7.3 Fee Adjustments & SLA Changes

7.3 تعديل الرسوم وتغيير الشروط

SAFE SYSTEMS reserves the right to adjust recurring fees at renewal to reflect market, operational, or infrastructure cost changes upon advance notice. SLA terms apply per active service term and may be updated prior to the start of a renewal period.

تحتفظ راية الأمان بالحق في تعديل الرسوم الدورية عند التجديد لمراعاة المتغيرات التشغيلية أو السوقية شريطة الإخطار المسبق.

8. Order of Precedence

8. أولوية التطبيق والتفسير

In case of conflict between contractual documents, the following order applies:

في حالة وجود أي تعارض بين وثائق التعاقد، يطبق الترتيب التالي لأولوية الترجيح:

1. Signed Master Commercial Contract / Service Agreement.
2. Applicable Order Form / Signed Commercial Quotation
3. Hosting Service Schedule
4. This SLA Document
5. Technical Specifications / Supporting Attachments

1. العقد التجاري الرئيسي الموقع / اتفاقية الخدمة.
2. نموذج الطلب المعتمد / العرض التجاري الموقع.
3. جدول خدمات الاستضافة.
4. وثيقة اتفاقية مستوى الخدمة هذه (SLA).
5. المواصفات الفنية / المرفقات الدعامة.

9. Applicability and Customer Acceptance

9. السريان وقبول العميل

This SLA is a standard SAFE ERP Support and Service Level Policy issued by Business Systems Engineering ("SAFE SYSTEMS") and applies to all Customers receiving SAFE ERP software, support, maintenance, subscription, hosting, or related services, subject to the applicable Commercial Agreement, Order Form, Commercial Quotation, Subscription Agreement, License Agreement, or Service Agreement.

تُعد اتفاقية مستوى الخدمة (SLA) هذه سياسة قياسية للدعم ومستوى الخدمة لنظام SAFE ERP، صادرة عن شركة راية الأمان ("راية الأمان")، وتنطبق على جميع العملاء الذين يتلقون برامج SAFE ERP أو خدمات الدعم أو الصيانة أو الاشتراك أو الاستضافة أو الخدمات ذات الصلة، وذلك وفقًا للاتفاقية التجارية أو نموذج الطلب أو عرض الأسعار التجاري أو اتفاقية الاشتراك أو اتفاقية الترخيص أو اتفاقية الخدمة المعمول بها.

The applicable version of this SLA shall be incorporated by reference into the Customer's relevant commercial or contractual documents.

ويتم إدراج النسخة المعمول بها من اتفاقية مستوى الخدمة (SLA) بالإحالة ضمن المستندات التجارية أو التعاقدية ذات الصلة بالعميل.

The Customer shall be deemed to have accepted this SLA upon the earliest occurrence of any of the following:

يُعد العميل قابلاً وموافقاً على هذه الاتفاقية فور تحقق أي من الحالات التالية أيهما أسبق:

- Signing or accepting a Commercial Agreement, Order Form, Commercial Quotation, Subscription Agreement, License Agreement, Service Agreement, or renewal document that refers to this SLA.
- Providing electronic acceptance through a SAFE SYSTEMS-approved system, portal, or electronic acceptance process.
- Activating, accessing, using, or continuing to use SAFE ERP or any related SAFE SYSTEMS support, maintenance, subscription, hosting, or managed service after being provided with, or given access to, this SLA.
- Paying an invoice, subscription fee, support fee, maintenance fee, hosting fee, or renewal fee that

- توقيع أو قبول عقد تجاري، نموذج طلب، أو عرض أسعار يشير إلى هذه الاتفاقية.
- تقديم قبول إلكتروني عبر البوابة أو الأنظمة المعتمدة لـ راية الأمان.
- تفعيل، أو استخدام، أو الاستمرار في استخدام نظام SAFE ERP أو خدمات الدعم والاستضافة بعد تسلم أو إتاحة الوصول لهذه الوثيقة.
- سداد أي فاتورة اشتراك، أو دعم، أو صيانة، أو استضافة تنص صراحة على خضوع الخدمات لهذه الاتفاقية.

expressly states that the applicable services are subject to this SLA.

SAFE SYSTEMS shall maintain reasonable records of Customer acceptance, including, where applicable, the Customer identity, accepted SLA version, acceptance date, acceptance method, and relevant contractual, electronic, or service records.

The Customer acknowledges that it has had a reasonable opportunity to review the applicable SLA before acceptance or continued use of the relevant services.

This SLA may be updated by SAFE SYSTEMS in accordance with Section 7.3. The updated SLA shall apply from the effective date stated in the updated version or from the commencement of the next applicable service or renewal period, subject to the terms of the relevant agreement and applicable law.

تحتفظ راية الأمان بسجلات معقولة لقبول العميل، بما في ذلك، عند الاقتضاء، هوية العميل، وإصدار اتفاقية مستوى الخدمة (SLA) المقبول، وتاريخ القبول، وطريقة القبول، والسجلات التعاقدية أو الإلكترونية أو المتعلقة بالخدمة ذات الصلة.

يقر العميل بأنه أتيحت له فرصة معقولة لمراجعة اتفاقية مستوى الخدمة (SLA) المعمول بها قبل القبول أو الاستمرار في استخدام الخدمات ذات الصلة.

يجوز لـ راية الأمان تحديث اتفاقية مستوى الخدمة (SLA) وفقًا للبند 7.3. وتسري اتفاقية مستوى الخدمة (SLA) المحدثة اعتبارًا من تاريخ السريان المحدد في النسخة المحدثة أو اعتبارًا من بدء فترة الخدمة أو التجديد التالية المعمول بها، وذلك مع مراعاة شروط الاتفاقية ذات الصلة والقانون المعمول به.