Kent Record Management Inc.
STORE | SCAN | SHRED

SERVICE LEVEL AND ACCEPTABLE USE AGREEMENT

1. Service Level Terms Introduction

This document details specific responsibilities for both Kent Record Management, Inc. ("KRM") and the Client to ensure that Vaulted Online Backup and Recovery Service (V-OBRS®), Vaulted Electronic Record Management System ("V-ERMS®"), and Cloud Server and/or Cloud Hosted Server aka "Vaulted Hosted Virtual Server Solution" or "V-HVSS", or any billable system that stores Client data or images at KRM to the client are properly commissioned. This document defines what will happen in the event a problem occurs. Although our systems are a managed service, KRM will be responsible for the availability of the service components, the day-to-day operation of the system will in part, depend on certain key processes and related equipment which are wholly under the Client's control. **Client services may be suspended or terminated for violation of the service level or acceptable use agreement provisions in accordance with the service agreement or terms and conditions agreement with KRM.**

2. KRM Responsibilities and Obligations

Installation and Configuration – An authorized KRM representative will deliver the specified products and services to the Client site on a pre-arranged installation date(s) agreed upon by the two parties. All defined products and services will be installed, commissioned, and tested to ensure that the software is operational. KRM does not guarantee compatibility between the operating system and applications.

Training – KRM will provide training for the designated Client representative via a remote session or in-person training.

Data Backup and Restoration – KRM agrees to backup data stored at their primary data center to a remote data center and has procedures in place to restore data.

Service Upgrades and Maintenance – KRM will be responsible for the provision, management, and installation of all product and service releases and engineering changes (hardware, software, or firmware) that it deems necessary to maintain and/or upgrade the product and services unless the system is hosted by a third-party. **KRM will accept no responsibility for storing Client's encryption keys. Loss of the encryption keys by the Client will prevent recovery of encrypted data.**

Network – KRM guarantees that our data center network will be available 99.9% of the time in any given monthly billing period, excluding scheduled maintenance.

Data Center Infrastructure – KRM guarantees that data center HVAC and power will be functioning 99.9% of the time in any given monthly billing period, excluding scheduled maintenance. Infrastructure downtime exists when server downtime occurs because of power or heat problems.

Migration – If KRM systems migration is required because of cloud server host degradation, KRM will notify the Client at least 24 hours in advance of beginning the migration, unless KRM determines in our reasonable judgment, that KRM must begin the migration sooner to protect Client data.

3. Client Responsibilities and Obligations

Installation and Configuration – The Client will be responsible for providing authorized and free access to a KRM representative to deliver the product and services to the Client site on a pre-arranged installation date(s). The Client will be responsible for providing the necessary power, physical and system permissions, network connection, and environment to support the systems. The Client will make available a designated and appropriately qualified representative to work with a KRM representative during the installation of the product and services, as defined in the contract. The designated Client representative will confirm that the functionality of the service has been demonstrated to his/her satisfaction. The Client is responsible for meeting all system (software and hardware) requirements. The Client will be responsible for providing authorized and free access to a KRM representative to deliver the product and services to the Client via the web, VPN, or direct network connection if access over the web is not available. Additional bandwidth or software charges may apply due to network connection type. **The Client is solely responsible for storing their encryption keys in a secure location. Loss of the encryption keys by the Client will prevent recovery of data.**

Data Backup and Restoration – KRM strongly recommends the Client backup their data outside of the KRM systems in the event of a disaster.

Service Upgrades and Maintenance – The Client will accept installation and service releases and engineering changes (hardware, software, or firmware) deemed necessary by KRM to maintain and/or upgrade the System. The Client is responsible for installing and managing software updates to server operating system software and applications supported by the server operating system unless the Client requests KRM to do so for a fee. KRM is not responsible for compatibility issues as a result of a third-party upgrade or patch.

4. Support and Escalation Procedure

Priority 3&2 (Low & Medium) – This is a general inquiry or problem that has no operational impact (*i.e.* loss of data or access) on the Client systems(s). Call and email logging from 8am-5pm EST, weekdays to support@kentrecords.com or 616-459-6681. Time to Fix: Before the end of next business day or to timescale agreed with Client. If the problem requires onsite technical support, this date and time will be scheduled with the Client.

Priority 1 (High) – This is when the Client or KRM has identified a possible error or fault with the installed KRM Service that is impacting multiple Client(s) or causing a severe impact on system operations. Call and email logging 24hrs/day x 7 days/week x 365 days/year to support@kentrecords.com or 616-459-6681. Time to Fix: Problem determination will start immediately, and recovery plan will be proposed to the Client depending on the exact nature, location, and scale of the problem. If the problem requires onsite technical support, this will be scheduled with the Client. General labor rates will apply if issues are not caused by KRM service failure.

Some calls require further investigation and even internal escalation by technical specialists. Although KRM will aim to resolve an open call to the shortest possible time frame, in some cases resolution depends on the availability or diagnostic information from the Client. In these cases, KRM will monitor events at every stage throughout the diagnostic process and keep the Client informed of all developments. In these cases, the appropriate KRM staff will call the assigned Client Service Representative to arrange the necessary remedial action. Any investigative work carried out by KRM personnel on a fault that is not found to be the responsibility of KRM will incur charges per the rate schedule of the party's agreement. Should travel and accommodation be involved, this will also be charged to the Client and may require written authorization before any work being performed.

5. Performance Level Guarantee – If KRM fails to meet guarantees stated above, the Client will be eligible for credit. Credits will be calculated as a percentage of the fees for the servers adversely affected by the failure for the current monthly billing period during which the failure occurred (to be applied at the end of the billing cycle), as five percent (5%) of the fees for each 30 minutes of network downtime, up to, and not to exceed, 100% of the current month's fees.

6. Abuse – Client may not use KRM's network or services in its sole judgment to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including but not limited to: unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network; monitoring data or traffic on any network or system without the express authorization of the owner of the system or network; interference with service to any user of the KRM or other network including, without limitation, mail spamming, flooding, deliberate attempts to overload a system and broadcast attacks; use of an Internet account or computer without the owner's authorization; Collecting or using email addresses, screen names or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting); collecting or using information without the consent of the owner of the information; use of any false, misleading, or deceptive TCP-IP packet header information in an email or a newsgroup posting; Use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user; Use of the service for distribution of advertisement delivery software unless: (i) the user affirmatively consents to the download and installation of such software based on a clear and conspicuous notice of the nature of the software, and (ii) the software is easily removable by use of standard tools for such purpose included on major operating systems (such as Microsoft's "add/remove" tool); or, any conduct that is likely to result in retaliation against the KRM network or website, or KRM's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS), or any other type of external attack.

7. Bulk Email – Client may not use a KRM's Mail Service (such as KRM's Microsoft Exchange®) to send bulk, mass, or SPAM mail. Please see the applicable Product Terms and Conditions for those services. Client may use the dedicated hosted system to send bulk mail, subject to the restrictions in this Agreement. Client must comply with the CAN-SPAM Act of 2003 and other laws and regulations applicable to bulk or commercial email. In addition, the Client bulk and commercial email must meet the following requirements Client intended recipients have given their consent to receive email from Client via some affirmative means, such as an opt-in procedure; client procedures for seeking consent include reasonable means to ensure that the person giving consent is the owner of the email address for which consent is given; client retain evidence of each recipient's consent in a form that can be promptly produced on request, and the Client honor recipient's and KRM requests to produce consent evidence within 72 hours of receipt of the request; client have procedures in place that allow a recipient to revoke their consent, such as a link in the body of the email, or instructions to reply with the word "Remove" in the subject line, the Client honor revocations of consent within 48 hours, and the Client notifies recipients that the revocation of their consent will be implemented in 48 hours; client must post an email address for complaints (such as abuse@yourdoman.com) in a conspicuous place on any website associated with the email, the Client must register that address at abuse.net, and the Client must promptly respond to messages sent to that address; client must have a Privacy Policy posted for each domain associated with the mailing; client have the means to track anonymous complaints; client may not obscure the source of the Client email in any manner, such as omitting, forging, or misrepresenting message headers or return addresses. The Client email must include the recipients email address in the body of the message or the "TO" line of the email; client subject line of the email must clearly describe the subject matter contained in the email, and the message must include valid contact information; and client must not attempt to send any message to an email address if 3 consecutive delivery rejections have occurred and the time between the third rejection and the first rejection is longer than fifteen days. These policies apply to messages sent using the KRM services, or to messages sent from any network by the Client or any person on the Clients behalf that directly or indirectly refer the recipient to a site or an email address hosted via the KRM service. Also, the Client may not use a third party email service that does not practice similar procedures for all its Clients. These requirements apply to distribution lists prepared by third parties to the same extent as if the list were created by the Client. KRM may test and otherwise monitor the Clients compliance with its requirements. **KRM may block the transmission of email that violates these provisions.** KRM may, at its discretion, require certain Clients to seek advance approval for bulk and commercial email, which approval will not be granted unless the Client can demonstrate that all of the requirements stated above will be met.

8. Unsolicited Communications – Client may not use the service to send an email or any other communications to a person who has indicated that they do not wish to receive it. If the communication is bulk mail, then the Client will not be in violation of this section if the Client complies with the 48-hour removal requirement described above.

9. Vulnerability Testing – Client may not attempt to probe, scan, penetrate or test the vulnerability of a KRM system or network, or to breach KRM's security or authentication measures, whether by passive or intrusive techniques, without KRM's express written consent.

10. Newsgroup, Chat Forums, Other Networks – Client must comply with the rules and conventions for postings to any bulletin board, chat group or another forum in which the Client participate, such as IRC and USENET groups including their rules for content and commercial postings. These groups usually prohibit the posting of off-topic, commercial messages or mass postings to multiple forums. The Client must comply with the rules of any other network they access or participate in using the KRM services.

11. Offensive Content – Client may not publish, transmit or store on or via KRM's network and equipment any content or links to any content that KRM in its sole judgment constitutes, depicts, fosters, promotes or relates in any manner to child pornography, bestiality, or non-consensual sex acts; is excessively violent, incites violence, threatens violence, or contains harassing content or hate speech; is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes; is defamatory or violates a person's privacy; creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement; improperly exposes trade secrets or other confidential or proprietary information of another person; is intended to assist others in defeating technical copyright protections; infringes on another person's copyright, trade or service mark, patent, or other property right; promotes illegal drugs, violates export control laws, relates to illegal gambling, or illegal arms trafficking; is otherwise illegal or solicits conduct that is illegal under laws applicable to the Client or to KRM; is otherwise malicious, fraudulent, or may result in retaliation against KRM by offended viewers or recipients, or is intended to harass or threaten; or, conflicts with the spirit and intent of the Agreement with KRM. Content "published or transmitted" via KRM's network or equipment includes Web content, email, bulletin board postings, chat, tweets, and any other type of posting or transmission that relies on the Internet.

12. Live Events – Client may not use the KRM services to stream live sex acts of any kind, even if the content would otherwise comply with this Agreement. KRM may prohibit the Client from streaming other live events where there is a special risk, in KRM's sole discretion, that the event may violate the Offensive Content section above.

13. Copyrighted Material – Client may not use KRM's network or services to download, publish, distribute, store or otherwise copy or use in any manner any text, music, software, art, image, or other work protected by copyright law unless, Client has been expressly authorized by the owner of the copyright for the work to copy the work in that manner, or Client is otherwise permitted by established copyright law to copy the work in that manner.

14. Shared Systems – Client may not use any shared system provided by KRM in a way that unnecessarily interferes with the normal operation of the shared system, or that consumes a disproportionate share of the resources of the system. For example, KRM may prohibit the automated or scripted use of KRM's. Mail Services if it has a negative impact on the mail system, or KRM may require the Client to repair coding abnormalities in the Cloud-hosted code if it unnecessarily conflicts with other Cloud Clients' use of the Cloud. The Client agrees that KRM may quarantine or delete any data stored on a shared system if the data is infected with a virus, or is otherwise corrupted, and has the potential to infect or corrupt the system or other Clients' data that is stored on the same system.

15. Miscellaneous – Client must have valid and current information on file with the Client domain name registrar for any domain hosted on the KRM network. Client may only use IP addresses assigned to the Client by KRM in connection with the KRM services. Client agree that if the KRM IP numbers assigned to the Client account are listed on an abuse database like Spamhaus, the Client will be in violation of this Agreement, and KRM, in its sole discretion, may take reasonable action to protect its IP numbers, including suspension and/or termination of the service, regardless of whether the IP numbers were listed as a result of the Client actions. It is KRM's policy to terminate in appropriate circumstances the services of Clients who are repeat infringers.

16. Limitations – The Client is not entitled to a credit if Client is in breach of the services agreement with KRM (including Client payment obligations to us) until the Client has cured the breach. The Client is not entitled to a credit if downtime would not have occurred due to the Client breach of the agreement with KRM or Client misuse, according to the Agreement, of servers or KRM systems. To receive a credit, the Client must contact a KRM account representative within thirty (30) days following the end of the downtime. Client must show that functionality of the servers was adversely affected in some way as a result of the downtime to be eligible for the credit. This Service Level Guaranty is the **sole and exclusive** remedy for server unavailability. **Notwithstanding anything in this Service Level Guaranty to the contrary, the maximum total credit for the monthly billing period, including all guaranties, shall not exceed 100% of Client fee for that billing period. Credits that would be available but for this limitation will not be carried forward to future billing periods.** This Service Level Guaranty is part of the Agreement with KRM, along with KRM schedules such as terms of service, acceptable use policy and others related to Systems, and are subject to the terms and conditions stated in those documents.