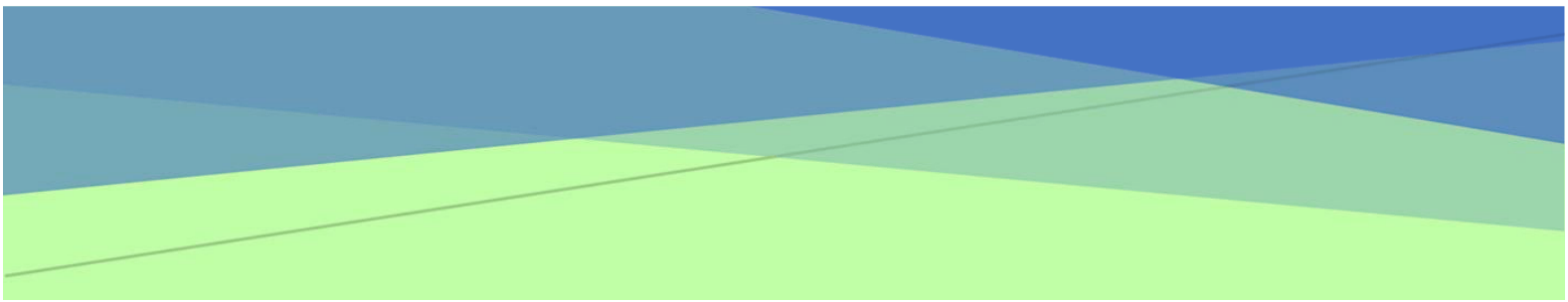

# VIRIMA SAAS POLICIES

# Table of Contents

## Disclaimer

Information in this document is subject to change without prior notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express permission of Virima Inc (“Virima”).

Virima may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give external parties any license to these patents, trademarks, copyrights, or other intellectual property rights except as expressly provided in any written license agreement from Virima.

All other brand and product names are trademarks or registered trademarks of their respective holders.

# I. About This Document

This document is intended to provide subscribers of the Virima software as a service ("Virima SaaS" also "subscription services") with policies regarding:

- Technical Support
- System Maintenance & Updates
- System Availability
- Business Continuity & Disaster Recovery
- Security & Data Protection

# II. Technical Support

Every Virima SaaS subscription includes standard technical support which is available to named system administrators via email and phone during normal business hours (Monday through Friday 8 AM to 5 PM eastern) with a two-hour response assurance. Support channels are monitored all other times for priority requests for which best efforts will be made to respond in a timely fashion. Arrangements to receive support outside of the normal business hours can be made with prior notice.

**Email ID**: support@virima.com

**Phone**: 404.969.4180 ext. 2

In addition to the included standard technical support, Virima also offers a premium support plan for 24x7 response assurance. The optional premium support subscription plan provides customers access to technical support outside of normal business hours per Table 1 below.

Table 1: After Hours Premium Support Plan

| Issue Classification | Definition | Response Time |
|---|---|---|
| P1 | System down or service significantly impacted | 2 hours |
| P2 | Service is impaired but overall system remains operational | 6 hours |
| P3 | Request for information or minor bug reporting | 24 hours |

# III. System Maintenance & Updates

This section describes the included Virima release and upgrade cycles to the subscription services, customer notices, timing, as well as other pertinent information so customers understand and appreciate the nature and pace of these efforts.

**Product Releases**

New features and functionality are enabled by updates and upgrades applied by Virima in accordance with this policy providing our customers the maximum value of the subscription services while minimizing down time. One impact of new releases and upgrades in a SaaS environment is that older versions are not supported and will no longer be available. To ensure customers obtain the maximum value of the offering, customers should ensure they notify Virima of any custom configurations they have implemented for usability and effectiveness prior to any major releases. There are three release types as listed in Table 2.

Table 2: Release Types

| Release Type | Scope | Frequency | Notification |
|---|---|---|---|
| Major | New major functionality, architectural changes, Schema updates | Quarterly<br>3:00 AM (eastern) on third Saturday of March, June, September, and December | One month before |
| Minor | Under a Continuous Integration and Continuous Deployment model, minor patches are released as they become available | Monthly | Once the patch is applied and available for use |
| Hot-fix | Bug fixes and any other patches needed for stability | As required | Target of 48 hours before |

**Release Plan**
A "major" version of the subscription services is released every quarter. These upgrades are designed to provide significant new features and functionality as well as address software bugs.

Along with regular quarterly releases, there may also be "minor" releases between quarterly major releases to push bug fixes and other important updates. In most cases the deployment is done in during the time when customer activity is low, to avoid any disruption to the customers. Virima's approach to release cycles and management for the subscription services is designed to provide stability, quality and predictability coupled with the flexibility to quickly resolve problems and deliver new features or service enhancements to the application.

**Customer Notification**
In the event any Release will materially change either the administrator or user experience, Virima will use reasonable efforts to provide its current Customers a non-production site to observe and/or test the new release prior to such release moving into production. Virima generally provides such a non-production site for a period of thirty (30) days for Customers to ascertain what, if any, impact there may be on its user groups. Additionally, if the nature of the changes requires the Customer to work with Virima on any customization for any of the newly introduced elements, a reasonable period of time to complete such work will be agreed upon between Virima and Customer and access to the non-production site will accordingly be extended during any such period. Virima provides its Customers with advance notice of the upcoming Major and Minor Releases with a reference to the applicable release notes as well as the location of the non-production site noted above.
In the event of a Hot Fix Release, Virima will attempt to provide its Customers at least 48 hours advance notice and will administer such releases in a manner designed to reduce disruption to end users.

# IV. System Availability

Virima SaaS is hosted in Amazon Web Services and follows closely the AWS SLA standards. Best efforts are made to ensure the service available with a monthly uptime percentage of 99.99%.

- Robust architecture (compute & platform)
- Redundancy (load balancing/multi-path/failover)
- Strong code dev processes

- Responsiveness and scalability

# V. Data Back-up & Disaster Recovery

**Data Back-up Process**

The SaaS application's back-end database is configured in a Master/Slave setup, therefore there is a backup copy of the active database at any time. Along with that, Virima has a policy of backing up physical data per the schedule listed in Table 3. The process of the data backup is as follows:

- Back-up of existing customer back-end database is performed regularly using standard back-up procedures
- The backed-up database is compressed and stored according to the customer filter in Amazon Simple Storage Service ("S3") bucket with full redundancy enabled
- Back-ups are kept for 60 days before being permanently deleted

Table 3: Back-up Schedule

| Backup Type | Frequency |
|---|---|
| **Daily** | Every 24 hours |
| **Weekly** | Every Saturday (midnight eastern time) |
| **Monthly** | The last day of the month |

**Restore From Back-up**

In the case of data loss or corruption, Virima will restore from the latest back-up containing valid data. Customers may request Virima to perform a restore from back-up in the event of data loss or corruption resulting from user error however customers are reminded to follow proper data entry procedures to ensure the integrity of all their data.

**Data Deletion and Retention**

Virima will not delete data contained in an active subscription. Back-ups are maintained for 60 days before being overwritten. Virima does not archive data back-ups. Upon termination of a customer's subscription, access to the tenant will be terminated and all active and backed-up data will be permanently deleted within 60 days.

**Disaster Recovery**

As Virima SaaS is hosted in Amazon Web Services, recovering in case of a disaster is a clear-cut process. All the backed-up data is stored in AWS Simple Storage Service ("S3") buckets. Amazon S3 provides a highly durable storage infrastructure designed for mission critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities within a region, designed to provide a durability of 99.999999999% (11 "9s"). So, it is highly unlikely that data loss will happen in case of disaster. Virima also uses high availability architected to span multiple availability zones to guarantee all the nodes do not fail at the same time. Virima follows a Recovery Time Objective (RTO) of 1 hour after AWS recovery and Recovery Point Objective (RPO) of 1 hour in case of complete site failure.

# VI. Security & Data Protection

**Physical safeguards (AWS facilities & certs)**
Virima SaaS is built on top of a robust application platform hosted on Amazon Web Services (AWS) cloud. AWS delivers a scalable cloud computing platform with high availability and dependability. AWS physical and operational security processes are well defined and designed to meet any compliance requirements. Along with AWS security, Virima has its own application security measures to protect data in transit and data at rest.

**AWS Shared Security Model**
Any application hosted in AWS falls under Amazon's shared security model broken into four parts:

- Physical Security
- Network Security
- Platform Security
- People & Procedures

Under the shared security model, AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

**Updates & Patching**
Virima assumes responsibility for, and management of, the operating system hosting the Virima SaaS running within the AWS compute environment. This includes regularly patching the underlying Linux operating system so that it remains current to within 30 days of release. Virima also maintains the underlying and associated application software that the Virima SaaS platform is built on. Since updating the underlying applications requires substantially more effort than OS patching, Virima targets quarterly updates and in some instances, given the nature of the update, may chose not to apply the latest available patch, particularly if it does not address significant security flaws or provide any meaningful improvements to the Virima SaaS platform. Virima also owns the configuration of the AWS-provided security group firewall which does not require frequent modification.

**Policies for Employees**
All software development and customer support are provided by Virima employees within Virima facilities under direct supervision of Virima managers. Virima follows standard business practices when onboarding, directing, and off-boarding employees. High level practices are listed below:

- New employees receive criminal background and reference checks prior to hire
- Access to development systems and individual client data is restricted based on job duties
- Logs are frequently monitored to detect unauthorized access or suspicious activity
- Upon employee separation all access is immediately revoked and tasks are reassigned to ensure minimal disruption to the business

**Technology Safeguards**
Virima has built various safeguards into the platform to help protect data from unauthorized access. Of course, product features designed to improve security are only effective if also properly implemented. As always, the customer is responsible for instituting, enacting and enforcing safe policies and procedures on behalf of their staff.

**Authentication**
Authentication is performed via the Virima SaaS login portal requiring user email and password which are encrypted. Customers have the option of enabling two factor authentication using Active Directory or LDAP. Customers can also setup Single Sign On using SAML and connect to their existing accounts such as Office365, AzureAD, Okta, etc.

**Data field privacy**
Data field privacy allows for asset/CI field data to be encrypted and stored so only permissioned users/roles have access.

**Role-based access**
Virima SaaS includes several predefined roles with set permissions based on common ITAM and ITSM practitioners. System administrators are able to modify existing permissions or create new roles and permission following the standard RACI matrix:

- Responsible
- Accountable
- Consulted
- Informed

**Audit controls**
The system maintains a complete history of all changes made to every ITSM and asset/CI record in the database. Any changes made to an ITSM record or asset/CI is automatically tracked and stored indefinitely. The change history cannot be modified or deleted by the users. Examples of tracked changes include:

- Record added/deleted
- Record updated
- Time stamp of change
- Who made the change

**Rule based escalations and notifications**
Depending on the criticality of the data or the process, automatic escalations and notifications can be setup to alert the stakeholders whenever certain updates occur to specific record data.

**Encryption**
Data is encrypted both at rest and in transit. The device credentials required to complete discovery scans are always stored locally and encrypted within the Discovery Application(s). They are never sent or stored in the cloud and because they are immediately encrypted they are never accessible to anyone. Even during initial configuration of the system, credentials should not be shared with Virima employees. We would never ask for that information when troubleshooting either. Scan data collected by the Discovery Application is also encrypted and transmitted that way to the cloud-based Discovery Server.

Customers may also enable encryption of ITSM records and device configuration data before getting stored into the database.

**Segregation Of Client Data**
Virima SaaS runs in a multi-tenant environment. This means that although clients access a singular software environment, all the data is securely partitioned and tied to individual client instances. This means client data is never stored together or accessible/viewable by users of other instances.

## VII. Personally Identifiable Information Privacy

Virima does not use personally identifiable information ("PII") to market additional Virima services or products nor does Virima sell or exchange customer PII data with any third party for such purposes. Virima may use customer PII, specifically system administrators' email addresses, to advise of product enhancements, system maintenance schedules, product release notes, system status messages or other information intended to enhance customers' experience with the Virima subscription services.

Virima does not offer any privacy protections for PII data customers choose to share with third parties via Virima Application Programming Interfaces ("API's") or any other voluntary integration/data exchange method.

## VIII. Closing

Virima takes system availability and security very seriously and will continue to evaluate and, when needed, modify the aforementioned policies and procedures. We strive to provide a robust, secure, and highly usable SaaS platform that our customers can trust and rely on every day.