**Streamdis Webcasting**
***Privacy Statement*** ***– Update 03/2020 – V20200301001***

**Digital Security**
At Streamdis, we take the security of your digital experiences seriously. From our in-depth integration of security into our internal software development processes, we strive to be proactive and nimble. What's more, our collaboration with partners, researchers, and other industry organizations helps us understand the latest security best practices and trends to continually integrate best of breed security practices into the products and services we offer.
This white paper describes the defense-in-depth approach and security procedures implemented by Streamdis to bolster the security of your Streamdis Webcasting Hosted experience and associated data.

**About Streamdis Webcasting**
Streamdis Webcasting is a secure web Streaming platform that offers immersive online webcasting experiences for large-scale webinars. Powering end-to-end, mission-critical web Streaming solutions on virtually any device, Streamdis Webcasting enables organizations to fundamentally improve productivity through collaboration. Streamdis Webcasting is available as Streamdis Webcasting Hosted Multi-tenant, which uses a combination of Streamdis and co-located infrastructure in a shared cloud deployment. On-premise deployment of Streamdis Webcasting is also available upon request.

**Streamdis Webcasting Solution Components**
Streamdis Webcasting includes two components, the Streamdis Webcasting application suite and the Streamdis Webcasting Server. All deployment options require both components however, the location of the Streamdis Webcasting Server changes based on the chosen deployment option (hosted, managed service, or on-premise).

**Streamdis Webcasting Application Suite**
Streamdis Webcasting is composed of several web-based software solutions:
Streamdis Webcasting Webcasting—Create, manage, and conduct online webcasts with polling, live PowerPoint viewing and annotation, webcams, on-demand video, moderated Q&A, and more.

**Streamdis Webcasting Server**
Streamdis Webcasting Server is a platform server that delivers enterprise-class scalability with support for clustered environments and provides the reliability and redundancy to seamlessly support thousands of concurrent users.
You can extend with non-Streamdis systems through a comprehensive set of APIs.

**Web Server**
The web server contains and executes all the business logic necessary for delivering content to users.

**Application Server**
The Streamdis Webcasting Server application server manages users, groups, on-demand content, and client sessions, among other tasks. Some of the application server's specific duties include access control, security, compliance, quotas, and licensing, as well as auditing and management functions, such as clustering, failover, and replication. It also transcodes media.

**Streaming Communication Server**
Streamdis Webcasting Server includes an embedded instance of Streamdis Media Server that acts as the webcasting server. This component handles all the real-time streaming of audio and video, synchronization of data and delivery of rich media content. Streamdis Media Server also plays a vital role in reducing server load and latency by caching frequently accessed streams and shared data.
Streamdis Media Server uses the HTTP streaming Protocol but can also be configured to use Secure Sockets Layer (SSL) for increased data security.

**Database**
The Streamdis Webcasting Server database persistently stores transactional and application metadata.
Streamdis Webcasting Server uses the full version of Microsoft SQL Server. Standard cluster and hot-swap configurations for a Microsoft SQL Server are supported for scalability and failover.

**Analytics**
Streamdis Webcasting provides a range of out-of-the-box reports as well as custom reports that can be configured by customers.
These analytics reports track viewing of webcasts, responses to registration questions, attendance, participation in polls, Q&A,and file download activity during webcasts.

**Media Transcoding**
Streamdis Webcasting Server provides a number of file conversion utilities to automatically convert popular video formats into high-quality files to display in the Player.

**Streamdis Webcasting Data Flow**
Streamdis Webcasting uses the HTTP, HTTPS, Smooth Streaming protocols.

**Data Encryption**
As information flows between Streamdis Webcasting client applications and Streamdis Webcasting Server, industry standard data encryption methods safeguard the confidential information contained within the traffic.

**Streamdis Webcasting Security Architecture**

Administrator features
Customers control users, content, access, and features through the administration controls of Streamdis Webcasting. Customers retain ownership of their content and data. The compliance and control setting sare account-wide settings that broadly consist of the following:
• Control access to webcasts —Administrators and hosts can completely disable guest access so that guests can no longer request entry. Hosts can also automatically deny access to specific usersand groups

An administrator or limited administrator can also customize the permissions list for a file or folder.

These permissions include:
• Manage—Users or groups with Manage permission for a folder or file can view, delete, move, andedit the file or folder. They can also, view reports for files in that folder, set permissions for the file or folder, and create new folders. However, they cannot publish to that folder.
• Denied—Users or groups with a Denied permission setting for a folder or file cannot view, publish, or manage this folder or file.
• Publish—Users or groups with a Publish permission setting for a folder or presentation can publish, update, and view presentations, as well as view reports for files in that folder.

**Streamdis Webcasting User Authentication**
Streamdis Webcasting uses standard access control lists with password policy options and Transport
Layer Security (TLS) encryption to secure access, content, and data
Streamdis Webcasting allows administrators to provision user accounts in several ways:
1. Using the Streamdis Webcasting Authentication module
2. Using the webservice API
3. For Streamdis Webcasting Managed Services, using LDAP/AD synchronization
Authentication takes place on the login screen of the Streamdis Webcasting client or through the webserviceAPI.

**Streamdis Webcasting Hosted Multi-Tenant Data Centers**
Streamdis understands the importance of securing data collection, data content serving, and reporting activities over the Streamdis Webcasting network, composed of Streamdis-managed infrastructure.
To this end, the network architecture for this Streamdis-hosted implementation leverages industry best practices for security design, including segmentation of development and production environments, DMZ segments, hardened bastion hosts, and unique authentication.
Streamdis Webcasting is hosted on Streamdis servers around the world in a shared cloud (multi-tenant) deployment
Streamdis generally hosts the customer's deployment in a data center located in the customer's corresponding region.

**Streamdis Webcasting Managed Services Data Centers**
Streamdis relies upon certified cloud infrastructure providers to operate, manage, and control the components from the hypervisor virtualization layer down to the physical security of the facilities in which Streamdis Webcasting Managed Services operates. These providers also operate the cloud infrastructure used by Streamdis to provision a variety of basic computing resources, including processing and storage. This infrastructure includes facilities, network, and hardware, as well as operational software (e.g., host OS, virtualization software, etc.) that supports the provisioning and use of these resources.
Streamdis requires these providers to adhere to industry-standard practices as well as a varietyof security compliance standards.
Streamdis certified cloud service providers monitor electrical, mechanical, and life support systems and equipment, and environmental states to help with the immediate identification of service issues. In order to maintain the continued operability of equipment, Streamdis cloud providers are required to perform ongoing preventative maintenance.

**Data Center Security**
Streamdis takes the security at all its data centers – whether Streamdis owned or leased – very seriously andmaintains standards for security best practices as well as security compliance requirements.

**Data Protection, Monitoring, and Availability**
Segregating Client Data Streamdis Webcasting relies on application permissions to isolate one customer from another. The only access to these servers and databases is via secure access using the Streamdis Webcasting application. All other access to the application and data servers is made only by authorized Streamdis personnel and is conducted via encrypted channels over secure management. Streamdis also separates its corporate testing environments from its production environments to avoid use of customer data in testing environments.

**Logging**
In order to protect against unauthorized access and modification, Streamdis captures network logs, OS-related logs, and intrusion detections. Sufficient storage capacity for logs is identified, periodicallyreviewed, and, as needed, expanded to help ensure that log storage is not exceeded. Systems generating logs are hardened and access to logs and logging software is restricted to authorized Streamdis Security Team personnel.

**Secure Network Architecture**
Streamdis requires all certified cloud infrastructure providers to employ network devices, including firewall and other boundary devices, to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rulesets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to manage and enforce the flow of traffic. Patch Management

In order to automate patch distribution for Streamdis Webcasting components, Streamdis uses internal patch and
package repositories as well as industry-standard patch and configuration management. Depending on
the role of the host and the criticality of pending patches, Streamdis distributes patches to hosts at
deployment and on a regular patch schedule. If required, Streamdis releases and deploys emergency patch
releases on short notice.
Streamdis cloud infrastructure providers maintain responsibility for patching systems that support the
delivery of IaaS services, such as the hypervisor and networking services.

**Non-Routable, Private Addressing**
All Streamdis servers containing customer data, whether in Streamdis-owned data centers or at a certified cloud infrastructure provider, are configured with non-routable IP addresses. These private addresses, combined with firewalls and NAT, help prevent an individual server on the network frombeing directly addressed from the Internet, greatly reducing the potential vectors of attack.

**Network Monitoring**
Monitoring tools help detect unusual or unauthorized activities and conditions at ingress and egress communication points. In the data centers, Streamdis ensures its infrastructure providers offer protection against traditional network security issues, including:
• Distributed Denial of Service (DDoS) attacks
• Man-in-the-Middle (MITM) attacks
• IP Spoofing
• Port Scanning
• Packet sniffing by other tenants
The Streamdis Network Operations Center (NOC) receives notifications from the various monitoring systems and will immediately attempt to fix an issue or escalate the issue to the appropriate Streamdis personnel.

**Backup Power**
Multiple power feeds from independent power distribution units help to ensure continuous power delivery, 24 hours a day, seven days a week, at all facilities hosting Streamdis Webcasting services. Streamdis also requires automatic transition from primary to backup power and that this transition occurs without service interruption. Each data center facility must provide redundancy at every level, including generators and diesel fuel contracts. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Additionally, each facility must conduct regular testing of its generators under load to ensure availability of equipment.

**Disaster Recovery**
In the event that an Streamdis-owned or leased data center is unavailable due to a problem at the facility,

a local situation, or a regional disaster, both Streamdis and its cloud infrastructure providers follow industry best practices to ensure an effective and accurate recovery.

**Risk & Vulnerability Management**

Penetration Testing

Streamdis approves and engages with leading third-party security firms to perform penetration testing that can uncover potential security vulnerabilities and improve the overall security of Streamdis products and services. Upon receipt of the report provided by the third party, Streamdis documents these vulnerabilities, evaluates their severity, considers their priority, and then creates a mitigation strategy or remediation Plan.

**Incident Response and Notification**

New vulnerabilities and threats evolve each day and Streamdis strives to respond to mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists Streamdis also subscribes to the latest security alert lists issued by major security vendors.

**Customer Data Confidentiality**

Streamdis treats customer data as confidential. Streamdis does not collect, use or share the information collected on behalf of a customer except as may be allowed in a contract with that customer.

**Conclusion**

The proactive approach to security and stringent procedures described in this paper help protect the security of the Streamdis Webcasting solution and your confidential data. At Streamdis, we take the security of your digital experiences very seriously and we continuously monitor the evolving threat landscape to stay ahead of malicious activities and help ensure the protection of our customers' data.

Information in this document is subject to change without notice. For more information on Streamdis solutions and controls, please contact your Streamdis sales representative.

Streamdis
Bitterveldstraat 1
3200 Aarschot
Belgium
www.streamdis.eu

www.streamdis.eu
Streamdis and the Streamdis logo are either registered trademarks or trademarks of Streamdis in Europe and/or other countries. All other trademarks are the property of their respective owners.
© 03/2020 Streamdis. All rights reserved.