REVCORD
Revolutionizing Multimedia Recording

# IQ3 Security Paper

MMS Version 12.1
Revision: 6.2023

REVCORD
MULTI-MEDIA LOGGING SYSTEMS
1250 WOOD BRANCH PARK DR #490
HOUSTON, TEXAS 77079
WWW.REVCORD.COM
281-404-7040

## TABLE OF CONTENTS

# INTRODUCTION

The purpose of this document is to detail how Revcord security and privacy practices are applied to the IQ3 platform features and to provide security assurances to our customers.

# IQ3 PRODUCT DESCRIPTION

Revcord IQ3 consists of 3 main divisions that specialize in data collection, information storage, and interaction analytics resolutions that quickly transform data into actionable intelligence, allowing operational optimization, enhanced performance, and cost reductions.

IQ3 facilitates inspections, interviews, investigations, and incidents using an Android or iOS application. Stream events live to the Revcord Logger, record with bookmarks and notes, and automatically upload to the Revcord Multi-tenant Cloud Server when complete. Manage all of your interviews, investigations, and incidents in one location. Watch them live or later search on date, time, case ID, interviewer/investigator, interviewee, bookmarks, bookmark notes, GPS location, and device ID. In addition, perform QA evaluations and run reports on any of the Search indices.

# KEY FEATURES OF IQ3

- Live Streaming
- Two-way audio/video conference for all participants
- Simple Operation
- Accurate Documentation
- Reports with 40+ Indices
- Allows for Live Collaboration
- Secure File Lockers for all Related Documentation
- Customized Inspection Process Markers
- QA/QC – Analysis and Evaluation
- Manage all Inspections in One Location
- Search for any Inspection for up to 5 years

# SPECIFICATIONS

## MMS Logger Hardware Requirements

- Minimum 8GB Ram
- Minimum Quad-Core Processor
- Minimum Windows 10 or Windows Server OS – 2016 or later and 64-bit system

## Mobile Device Hardware Requirements (IQ3 App User)

- Minimum 5GB Ram
- Android 11 or higher OS
- 5G Connectivity for streaming video (List of Tested 5G Tablets)

# NETWORK PORTS AND SERVICES

## MMS Logger

| Port | Protocol | Service Name | Description of Service | Encrypted | Open/Closed |
|---|---|---|---|---|---|
| 443 | TCP | MMS | Inbound port | Yes | Open |
| 8431 | TCP | Websocket Server | Inbound port | Yes | Open |

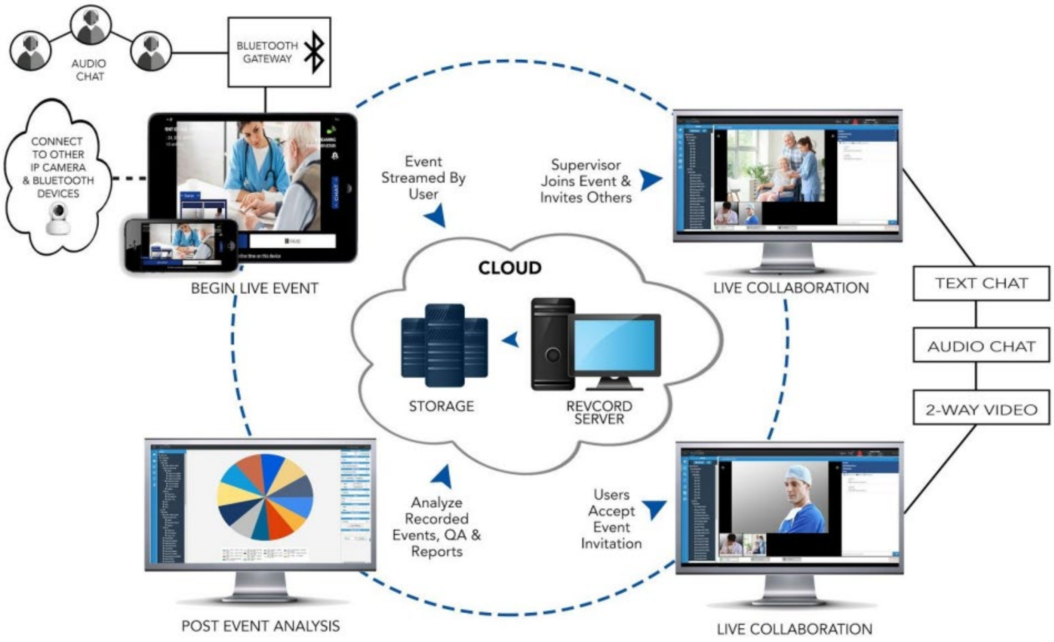
## FOR IQ3 APP USER, IQ3 PARTICIPANTS AND MMS LOGGER

| Port | Protocol | Service Name | Description of Service | Encrypted | Destination |
|---|---|---|---|---|---|
| 443 | TCP | MMS Server | Outbound port | Yes | MMS Logger |
| 8431 | TCP | Websocket Server | Outbound port | Yes | MMS Logger |
| 1935, 8086, 8087, 9443 | TCP | Streaming Server | Outbound port | No | *.revcord.com |
| 443 | TCP | Twilio Services | Outbound port | Yes | *.twilio.com |
| 10000-20000 | UDP | Twilio Services | Outbound port | Yes | *.twilio.com |

## SECURITY OF TRANSMISSION AND STORAGE

- Revcord Streaming and Conferencing servers use only outbound ports.  There is no inbound traffic into the network.
- All communications are initiated from the local server.
- Windows and/or third-party firewall configurations are limited to ports 443 and 8431 for inbound traffic only. Both of these runs IIS (Web Server) and WebSocket Server.
- All network traffic adheres to the TLS 1.2 standard using Secure Web Socket (WSS) as the protocol.  Like HTTPS, WSS (WebSockets over SSL/TLS) is encrypted, protecting against man-in-the-middle attacks.

## NETWORK ARCHITECTURE AND DATA FLOW DIAGRAM



## SECURE SERVERS

Revcord servers are located at a Tier-4 data center. This ensures that in the unlikely event of a disaster at your facility, software can be back online in a matter of minutes. Tier-4 meets the CJIS definition of a physically secure location.

A Tier-4 data center is an enterprise-class data center tier with redundant and dual-powered servers, storage, network links, and power cooling equipment. It is the most advanced type of data center certification, which typically serves enterprise corporations and provide the following:

- 99.99% uptime per year (Tier 4 uptime).
- 2N+ 1 fully redundant infrastructure.
- 96-hour power outage protection.
- >26.3 minutes of annual downtime.

## DATA CENTER PHYSICAL SECURITY

- Facility access is controlled with card control and auditable logs. The facility has alarms and monitoring for fire and unauthorized access as well as camera systems.
- Access to the facility is logged.
- Access is restricted to Site Personnel and Datacenter Remote Hands staff. Equipment is secured within a locked cage restricted to authorized personnel and Datacenter Remote Hands.
- Background checks are performed for all personnel with access to Hosting Infrastructure.
- Media (hard drives) are secured at offsite locations in a SOCII facility within a locked cage, and the facility maintains access controls based on biometrics and card-based access.
- The offsite location is a SOCII facility within a locked cage, and the facility maintains access controls based on biometrics and card-based access. The backed-up data would be images of the Virtual Machines, which would be "turned up" in the remote location so architecture would be identical to the production location.

# DATA CENTER NETWORK SECURITY

- The public-facing web servers and application servers are on a separate layer 2 segments from the database servers, with strict firewall policies and logging monitoring cross-segment traffic.
- The supplier's Endpoint Devices are virtually separated into a "virtual datacenter" with its own VXLAN overlay segments and a virtual firewall. There exists no routability to the hosting infrastructure.
- Firewall logs are routinely monitored as well as set up for Email alerts to IT Director. The logs are monitored every hour for anomalies.

- There are host-based and network-based intrusion prevention systems and intrusion detection systems (IPS/IDS) installed on the Hosting Infrastructure
- IPS/IDS logs in the Hosting Infrastructure are monitored for anomalies on a 24 hour/365-day basis.
- IPS/IDS logs for the Hosting Infrastructure are retained for a period of one year.
- Network device logs for the Hosting Infrastructure are analyzed daily for anomalies.
-

# DATA CENTER HOSTING INFRASTRUCTURE SECURITY

- Each server in the Hosting Infrastructure is protected by ESET Cyber Protect Cloud - Server Security with Dynamic Threat Defense.
- Data Center performs quarterly vulnerability scans on the Hosting Infrastructure.
- Data Center employs a third party to perform annual penetration testing on the Hosting Infrastructure.
- The Multi-Tenant system is virtually and logically separated from all other customers' equipment and data.

# DISCLAIMER

The information contained in this document is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify, or supersede the terms and conditions of any written agreement between such customer and Revcord or Revcord subsidiaries or affiliates (collectively, "Revcord"), including but not limited to our Warranty statement, our LaaS agreement, our Terms and Condition of sale, and our RevShield Service Level Agreement. Revcord does not make any promises or guarantees to the customer that any of the methods or suggestions described in this document will protect, restore or resolve any customer system issues.