IQ3 ENTERPRISE SOFTWARE PLATFORM SECURITY PAPER

TABLE OF CONTENTS

INTRODUCTION

This document details how Revcord security and privacy practices are applied to the
IQ3 Enterprise Software Platform (IQ3) and to provide security assurances to our customers.

IQ3 PRODUCT DESCRIPTION

IQ3 consists of 3 main categories specializing 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, and Investigations using an Android or iOS application. Stream Events Live from the App, Record with Bookmarks and Notes, and Automatically Upload to the Cloud-based Revcord Multi-tenant IQ3 MMS when complete. Manage all of your Interviews, Investigations, and Incidents in one location. Watch them Live or Search later 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 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

IQ3 MMS OPTIONS

- Installed in Customer Site as a Local Server
- Deployed as a Dedicated Instance in Revcord's Data Center
- Configured as a Tenancy in Revcord's Multi-Tenant IQ3 MMS

IQ3 MMS LOCAL SERVER HARDWARE REQUIREMENTS

- Minimum 8GB Ram
- Minimum Quad-Core Processor
- Minimum Windows 10 or Windows Server OS – 2019 or later and 64-bit system

MOBILE DEVICE HARDWARE REQUIREMENTS (IQ3 APP USER)

- Minimum 5GB Ram
- Android 11 or higher or IOS 15
- 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 USERS, 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 run 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
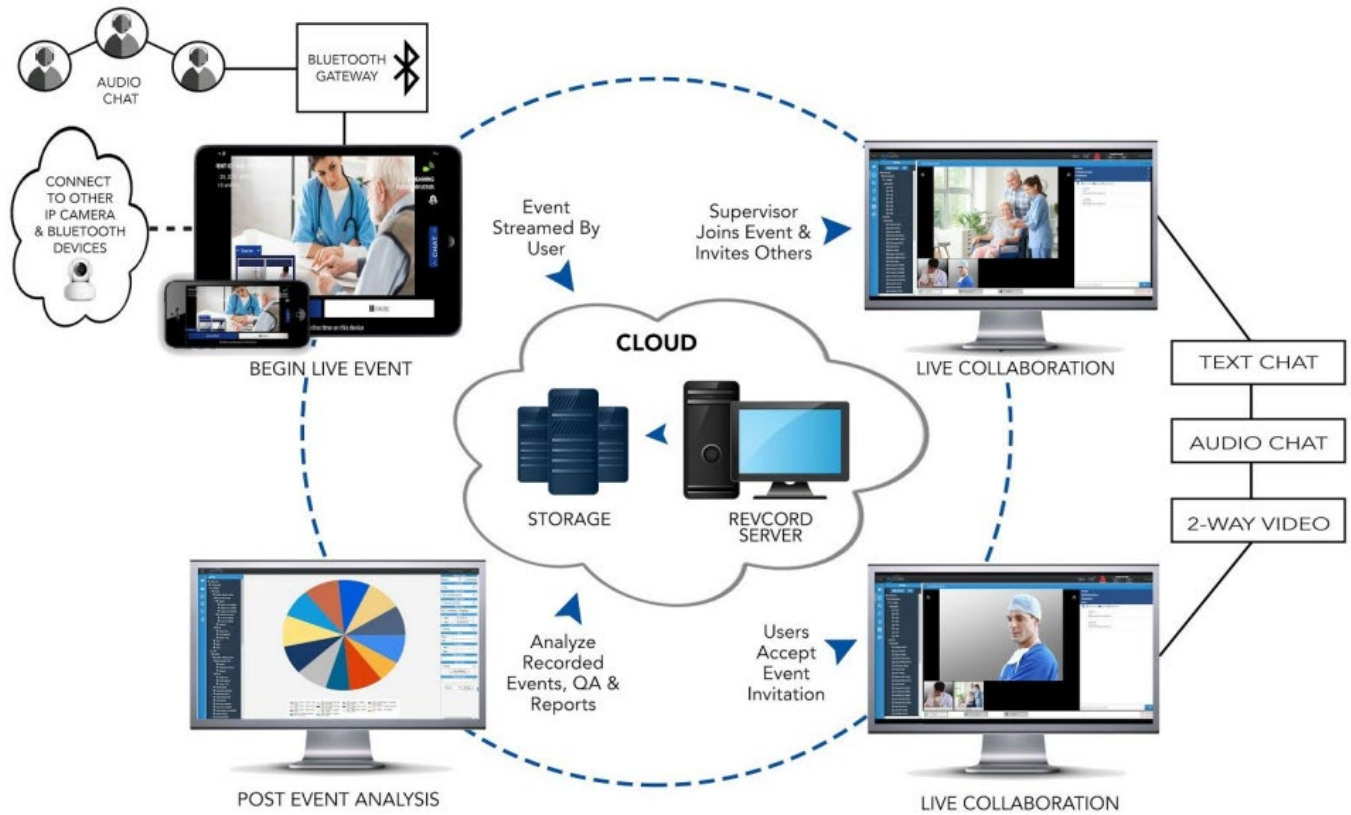
SECURE SERVERS

Oracle Cloud Infrastructure for Government Regions provide a highly secure, enterprise-scale cloud ecosystem that is isolated from commercial customers and built to support regulatory compliant mission-critical public sector workloads.

Oracle Cloud Infrastructure (OCI) mitigates the risk of security threats for cloud workloads. With simple, prescriptive, and integrated security capabilities built into the OCI platform.

- Secure Access
- Certificates Management
- Security Posture Management
- Database Security
- User Access and Entitlements

- Network Firewalls
- Encryption Key Management
- Threat Intelligence
- Vulnerability Management
- Web Application Protection

DISA — DoD DISA IL5, 4, 2

FedRAMP — FedRAMP–High

FIPS VALIDATED 140-2 — FIPS 140-2 for cryptographic modules

VPAT 508 Compliant — VPAT section 508 standards for accessibility

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, SaaS 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.